جامعة الجزائر1

كلية الحقوق

تنظم ملتقى دولي عن بعد موسوم بـ:

القانون الجنائي في ظل التطور التكنولوجي-
إشكالات ومعالجات-

5 و6 أكتوبر 2022

برنامج فعاليات الملتقى الدولي

اليوم الأول: الأربعاء 5 أكتوبر 2022

الجلسة الافتتاحية:9:00 الى 10:00

آيات بينات من الذكر الحكيم

النشيد الوطني الجزائري

كلمة الأستاذ الدكتور لعلاوي عيسى / عميد كلية الحقوق

كلمة الدكتورة خطاب كريمة رئيس الملتقى الدولي/ رئيس اللجنة العلمية

كلمة الدكتورة التجاني زليخة / رئيس اللجنة التنظيمية

مداخلة افتتاحية الأستاذة الدكتورة علا كريمة/ كلية الحقوق جامعة الجزائر 1

الجلسة العلمية الأولى

برئاسة أ.د. علا كريمة/ كلية الحقوق جامعة الجزائر 1

10:00 -12:00 بتوقيت الجزائر

رابط الجلسة: meet.google.com/ofc-infs-erf

10 دقائق لكل متدخل و20 دقيقة للنقاش في آخر الجلسة

التوقيت	الاسم و اللقب	عنوان المداخلة	مؤسسة الانتماء/ البلد
10:10-10:00	د. خطاب كريمة	القانون والتكنولوجيا -علاقة تأثير وتأثر-	أستاذة محاضرة أ كلية الحقوق جامعة الجزائر 1/الجزائر
10:20-10:10	د. عياد فوزية	دور التكنولوجيا الحديثة في ارتفاع نسبة الجريمة	أستاذة محاضرة أ كلية الحقوق جامعة الجزائر 1/الجزائر
10:30-10:20	د. التجاني زليخة	انعكاسات التطور التكنولوجي على الظاهرة الإجرامية	أستاذة محاضرة أ كلية الحقوق جامعة الجزائر 1/الجزائر
	د. الداوي نجاة		أستاذة محاضرة أ كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح ورقلة/ الجزائر
10:40-10:30	د. بن موسى وردة	تطور أساليب ارتكاب الجريمة في ظل التطور التكنولوجي	أستاذة محاضرة أ كلية الحقوق والعلوم السياسية جامعة البليدة2/الجزائر
10:50-10:40	د. بوعزيز فريد	التطور التكنولوجي والظاهرة الإجرامية في ظل جائحة كورونا كوفيد19	دكتوراه قانون جامعة أحمد بن بلة وهران/ الجزائر
11:00-10:50	د. حساين عومرية	أثر التكنولوجيا في استفحال الجريمة المعلوماتية وسبل مكافحتها في ظل التشريع الجزائري	أستاذة محاضرة أ المركز الجامعي شريف بوشوشة أفلو/ الجزائر
11:10-11:00	د. بوزيدة عادل	الالتزام الجزائي بالحيطة في ظل التطور التكنولوجي	أستاذ محاضر أ كلية الحقوق جامعة الجزائر 1/ الجزائر
11:20-11:10	د. علي غريبي	نحو صياغة قانونية جنائية جديدة في ظل التطور التكنولوجي	أستاذ محاضر ب المركز الوطني للبحث في العلوم الإسلامية والحضارة الأغواط/ الجزائر

الورشة العلمية الأولى

برئاسة د.مالك نسيمة / كلية الحقوق جامعة الجزائر 1

10:00 -11:30 بتوقيت الجزائر

رابط الورشة: meet.google.com/fnk-vrho-zzy

10 دقائق لكل متدخل و20 دقيقة للنقاش فى آخر الجلسة

التوقيت	الاسم و اللقب	عنوان المداخلة	مؤسسة الانتماء/ البلد
10:10-10:00	د, . سوماتي شريفة	متطلبات التحول الرقمي لتحقيق مجتمع المعرفة	أستاذة محاضرة أ كلية الحقوق جامعة الجيلالي بونعامة خميس مليانة/ الجزائر
10:20-10:10	د. رحامنية سعيدة	تأثير التطور التكنولوجي على زيادة الجريمة	أستاذة محاضرة ب جامعة الشهيد عباس لغرور خنشلة/ الجزائر
10:30-10:20	د. رحماني حسيبة	مسألة تفوق انتشار الإجرام الخطير عن سبل الوقاية والمكافحة في ظل التطور التكنولوجي	أستاذة محاضرة أ كلية الحقوق والعلوم السياسية جامعة أكلي محند أولحاج البويرة/ الجزائر
10:40-10:30	د. حبيب فاطمة	التطور التكنولوجي آلية لارتكاب الجرائم المستحدثة	أستاذة محاضر ب كلية الحقوق جامعة الجزائر 1/ الجزائر
10:50-10:40	د. قمار خديجة	التطور التكنولوجي والجريمة الالكترونية – سرعة التأثير وصعوبة التحدي-	أستاذة محاضرة أ كلية الحقوق جامعة الجيلالي بونعامة خميس مليانة/ الجزائر
11:00-10:50	د. فغول عربية	موقف بعض التشريعات العقابية من جرائم تكنولوجيا المعلومات	أستاذة محاضرة أ كلية الحقوق والعلوم السياسية جامعة البليدة2/ الجزائر
11:10-11:00	د. مامي هاجر	المواجهة التشريعية للجرائم المتأثرة بالتطور التكنولوجي المتعلقة بالمصارف -جريمة تبييض الأموال نموذجا-	مفتشة بوزارة المالية / الجزائر
	د. كودري فاطمة الزهراء		أستاذة محاضرة ب جامعة خروبة/ الجزائر

الجلسة العلمية الثانية

برئاسة أ.د. عمارة عبد الحميد/ كلية الحقوق جامعة لجزائر 1

12:30 -14:30 بتوقيت الجزائر

رابط الجلسة: meet.google.com/ofc-infs-erf

10 دقائق لكل متدخل و20 دقيقة للنقاش فى آخر الجلسة

التوقيت	الاسم و اللقب	عنوان المداخلة	مؤسسة الانتماء/ البلد
12:40-12:30	د. محمد جبريل إبراهيم حسن	المواجهة التشريعية للجرائم الالكترونية دراسة تحليلية مقارنة	كلية الحقوق جامعة القاهرة/ مصر
12:50-12:40	د. خدير وليد توفيق	المخدر الرقمي وإشكالية التجريم	أستاذ مؤقت كلية الحقوق والعلوم السياسية جامعة أبو بكر بلقايد تلمسان/ الجزائر
13:00-12:50	د. صابرين يوسف عبد الله	المواجهة التشريعية لجريمة الابتزاز الالكتروني	كلية القانون جامعة البيان بغداد/ العراق
	د. أوج عماد صبري		كلية القانون جامعة البيان بغداد/ العراق
13:10-13:00	د. لبيض بوبكر	المواجهة التشريعية لجرائم العملات الرقمية	أستاذ مؤقت جامعة عمار ثليجي الأغواط/ الجزائر
	د. بوداوي كريم	والمشفرة في نظر السياسة الجنائية	أستاذ مؤقت جامعة عمار ثليجي الأغواط/ الجزائر
13:20-13:10	ط. بن عربية شفاء	التعليق على كيفية تجريم المشرع للجرائم المتصلة بتكنولوجيا الإعلام والاتصال	طالبة دكتوراه كلية الحقوق جامعة الجزائر 1/ الجزائر
13:30-13:20	د. مالك نسيمة	تأثير تكنولوجيات الإعلام والاتصال على حق المؤلف	أستاذة محاضرة أ كلية الحقوق جامعة الجزائر 1/ الجزائر
13:40-13:30	د. أمال بيدي	حدود التقنيات الحديثة في مجال تنفيذ العقوبة الجنائية	أستاذة محاضرة أ كلية الحقوق جامعة زيان عاشور الجلفة/ الجزائر
	د. علي عثماني	بين الرؤية الفقهية والأنظمة الجنائية	أستاذ محاضر أ المركز الجامعي أفلو الأغواط/ الجزائر
13:50-13:40	د. تحانوت نادية	دور التكنولوجية الحديثة في مواجهة مخاطر تطبيق العقوبات السالبة للحرية قصيرة المدة -نظام الوضع تحت المراقبة الالكترونية نموذجا-	أستاذة محاضرة أ كلية الحقوق جامعة الجزائر 1/ الجزائر

الورشة العلمية الثانية

برئاسة د, بن موسى وردة / **أستاذة محاضرة أ كلية الحقوق والعلوم السياسية جامعة البليدة2/الجزائر**

14:40 – 13:00 بتوقيت الجزائر

رابط الورشة:meet.google.com/fnk-vrho-zzy

10 دقائق لكل متدخل و20 دقيقة للنقاش فى آخر الجلسة

التوقيت	الاسم واللقب	عنوان المداخلة	مؤسسة الانتماء/ البلد
13:10-13:00	د. قزوت لامياء	حماية المنتوجات الرقمية من الجرائم الالكترونية	أستاذة مؤقتة كلية الحقوق جامعة الجزائر1/ الجزائر
13:20-13:10	د. بلغيث سمية	مقتضيات تجريم التمييز وخطاب الكراهية عبر الوسائط الالكترونية على ضوء قانون 20/ 05 -تجريم وقائي أم علاجي-	أستاذة محاضرة ب جامعة العربي بن مهيدي أم البواقي/ الجزائر
13:30-13:20	د. كمال حطاب	الحماية الجزائية للمعطيات ذات الطابع الشخصي على ضوء القانون 18/ 07	أستاذ محاضر ب كلية الحقوق والعلوم السياسية 19 مارس 1962 جامعة جيلالي اليابس سيدي بلعباس/ الجزائر
13:40-13:30	ط.د.بعجي عبد النور	THE CRIMINALIZATION OF CYBERTERRORISM	طالب دكتوراه كلية الحقوق جامعة الجزائر1/ الجزائر
13:50-13:40	د. بكوش محمد أمين	دور التطور التكنولوجي في أنسنة الأنظمة العقابية -السوار الالكتروني نموذجا-	أستاذ محاضر ب كلية الحقوق والعلوم السياسية جامعة ابن خلدون تيارت/ الجزائر
14:00-13:50	د. لشهب نادية	انتهاك الخصوصية المعلوماتية للمستخدم عبر المنصات التعليمية الافتراضية ما بين الحماية التقنية والمسؤولية الجنائية	أستاذة مؤقتة كلية الحقوق جامعة الجزائر1/ الجزائر
14:10-14:00	د. بن جدو أمال	السوار الالكتروني كآلية لتنفيذ العقوبة السالبة للحرية قصيرة المدة	دكتوراه قانون كلية الحقوق جامعة الجزائر1/ الجزائر
	ط. د. ابراهيمي رابح		طالب دكتوراه كلية الحقوق جامعة الجزائر1/ الجزائر
14:20-14:10	ط. د. بلفار شوقي	انعكاسات التطور التكنولوجي على تنفيذ الأحكام الجنائية	أستاذ مشارك كلية الحقوق والعلوم السياسية جامعة 08 ماي 1945 قالمة/ الجزائر
	ط. د. بوكتاب خال		أستاذ مشارك كلية الحقوق والعلوم السياسية جامعة باجي مختار عنابة/ الجزائر

اليوم الثاني: الخميس 6 أكتوبر 2022

الجلسة العلمية الثالثة

برئاسة أ.د.خالف عقيلة/ كلية الحقوق جامعة الجزائر 1

00: 10- 30: 11 بتوقيت الجزائر

رابط الجلسة: meet.google.com/ofc-infs-erf

10 دقائق لكل متدخل و20 دقيقة للنقاش فى آخر الجلسة

التوقيت	الاسم واللقب	عنوان المداخلة	مؤسسة الانتماء/ البلد
10:10-10:00	د. غناي زكية	تقنية السوار الالكتروني بين مقاصد العقوبة السالبة للحرية والإصلاح الجنائي	أستاذة محاضرة أ كلية الحقوق جامعة بومرداس/ الجزائر
	أ.د. جمال زيد الكيلاني		عميد كلية الشريعة جامعة النجاح نابلس/ فلسطين
10:20-10:10	د. يحي عبد الحميد	التصوير الضوئي كوسيلة لتسجيل معاينة مسرح الجريمة	أستاذ محاضر أ كلية الحقوق والعلوم السياسية جامعة مستغانم/ الجزائر
10:30-10:20	د. تومي يحي	استخدام تقنية المحادثة المرئية عن بعد في سماع الشهود في مرحلتي التحقيق القضائي والمحاكمة	أستاذ محاضر أ كلية الحقوق والعلوم السياسية جامعة يحي فارس المدية/ الجزائر
	ط.د.مهاد قانة		طالبة دكتوراه كلية الحقوق والعلوم السياسية جامعة يحي فارس المدية/الجزائر
10:40-10:30	د. فرحاتي صبرينة	مخاطر استعمال الدليل العلمي على السلامة العقلية للشخص في ظل التطور العلمي والتكنولوجي	أستاذة محاضرة أ كلية الحقوق جامعة الجزائر 1/ الجزائر
10:50-10:40	د. عباسي محمد الحبيب	استخدام التكنولوجيا الحديثة آلية إستراتيجية في تفعيل التعاون الدولي في مجال مكافحة الإجرام	أستاذ محاضر أ كلية الحقوق والعلوم السياسية جامعة طاهري محمد بشار/ الجزائر
	ط.د. قادري نور الهدى	الأشعة غير المرئية ودورها في الإثبات الجنائي	طالبة دكتوراه كلية الحقوق والعلوم السياسية جامعة سيدي بلعباس جيلالي اليابس/ الجزائر

الورشة العلمية الثالثة

برئاسة د. بوقادوم صليحة يحياوي/ كلية الحقوق جامعة الجزائر 1

10:00 -11:30 بتوقيت الجزائر

رابط الورشة: meet.google.com/fnk-vrho-zzy

10 دقائق لكل متدخل و20 دقيقة للنقاش فى آخر الجلسة

التوقيت	الاسم واللقب	عنوان المداخلة	مؤسسة الانتماء/ البلد
10:10-10:00	د. حيمي سيدي محمد	إشكالات استخدام المراقبة الالكترونية في إجراءات التحري والإثبات الجنائيين	أستاذ محاضر أ كلية الحقوق والعلوم السياسية جامعة أبو بكر بلقايد تلمسان/ الجزائر
10:20-10:10	د. درعي العربي	خصوصية إجراءات الضبط القضائي في جرائم التمييز وخطاب الكراهية	أستاذ محاضر أ كلية الحقوق والعلوم السياسية جامعة عبد الحميد بن باديس مستغانم/ الجزائر
10:30-10:20	د. بوعقبة نعيمة	استخدام البيانات الشخصية في التحقيق الالكتروني بين أولوية مكافحة الجرائم وضمان الحق في الخصوصية	أستاذة محاضرة أ جامعة الشاذلي بن جديد الطارف/ الجزائر
10:40-10:30	د. صيدي عبد الرحمان	أثر التطور التكنولوجي في الإعلام والاتصال على حق المشتبه فيه في المساواة في الأسلحة	أستاذ محاضر أ كلية الحقوق جامعة الجزائر 1/ الجزائر
10:50-10:40	.د. دريهمي عبد الحكيم	تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية	طالب دكتوراه كلية الحقوق جامعة الجزائر 1/ الجزائر
11:00-10:50	د. نهاري نصيرة	وسائل المراقبة الالكترونية في الإثبات الجنائي	أستاذة محاضرة أ كلية الحقوق والعلوم السياسية جامعة وهران2 محمد بن أحمد/ الجزائر
	د.هداية بوعزة		أستاذة محاضرة أ كلية الحقوق والعلوم السياسية جامعة وهران 2 محمد بن أحمد/الجزائر
11:10-11:00	د. مبروك حورية	استخدام التكنولوجية في مرحلة البحث والتحري (مرحلة الاستدلال)	أستاذة محاضرة أ كلية الحقوق جامعة الجزائر 1/ الجزائر

الجلسة العلمية الرابعة

برئاسة أ.د.درياد مليكة/ كلية الحقوق جامعة الجزائر 1

13:00 -14:30 بتوقيت الجزائر

رابط الجلسة: meet.google.com/ofc-infs-erf

10 دقائق لكل متدخل و20 دقيقة للنقاش فى آخر الجلسة

التوقيت	الاسم واللقب	عنوان المداخلة	مؤسسة الانتماء/ البلد
13:10-13:00	د. عيشاوي أمال	التفتيش الالكتروني كإجراء للتحقيق في ظل التطور التكنولوجي	أستاذة محاضرة أ كلية الحقوق والعلوم السياسية جامعة البليدة2/الجزائر
13:20-13:10	ط.د. زروقي أم كلثوم	استخدام تقنية المحادثة المرئية عن بعد كآلية لتطوير مرفق القضاء	طالبة دكتوراه كلية الحقوق جامعة يحي فارس المدية/ الجزائر
13:30-13:20	د. بلعشي مريم	التقاضي الالكتروني وضمانات المحاكمة العادلة	أستاذة محاضرة ب كلية الحقوق جامعة الجزائر1/ الجزائر
13:40-13:30	ط.د. جديدي ضياء الدين رمضان	الطب الشرعي الرقمي كآلية مستحدثة في الإثبات الجنائي	طالب دكتوراه معهد الحقوق والعلوم الاقتصادية المركز الجامعي أحمد عبد الرزاق حمودة سي الحواس بريكة/ الجزائر
	ط. د. دراجي شهرزاد		طالب دكتوراه معهد الحقوق والعلوم الاقتصادية المركز الجامعي أحمد عبد الرزاق حمودة سي الحواس بريكة/ الجزائر
13:50-13:40	ط.د. بن سالم وداد	مشروعية الوسائل التقنية الحديثة في الإثبات الجنائي	طالبة دكتوراه كلية الحقوق جامعة محمد لمين دباغين سطيف2 الهضاب/ الجزائر
14:00-13:50	د. بن بوعبد الله نورة	تداعيات الإثبات الجنائي بوسائل التقنية العلمية الحديثة على حقوق الإنسان	أستاذة محاضرة أ كلية الحقوق جامعة الحاج لخضر باتنة 1/ الجزائر
	ط.د. ديب أكرم		طالب دكتوراه كلية الحقوق جامعة الحاج الحاج لخضر باتنة 1/ الجزائر

الورشة العلمية الرابعة

برئاسة د. مبروك حورية/ كلية الحقوق جامعة الجزائر 1

13:00 -14:40 بتوقيت الجزائر

رابط الورشة: meet.google.com/fnk-vrho-zzy

10 دقائق لكل متدخل و20 دقيقة للنقاش فى آخر الجلسة

التوقيت	الاسم واللقب	عنوان المداخلة	مؤسسة الانتماء/ البلد
13:10-13:00	د. بوقادوم - يحياوي صليحة-	تكنولوجيا الإعلام والاتصال كمحرك لعصرنة العدالة الجنائية	أستاذة محاضرة أ كلية الحقوق جامعة الحزائر 1/ الجزائر
13:20-13:10	د. بطيحي نسمة	الدليل الرقمي ودوره في إثبات الجرائم الالكترونية	أستاذة محاضرة ب كلية الحقوق والعلوم السياسية جامعة سطيف2/ الجزائر
13:30-13:20	د.عميروش هنية	أثر الدليل العلمي على اقتناع القاضي الجزائي	أستاذة محاضرة أ كلية الحقوق والعلوم السياسية جامعة بجاية / الجزائر
13:40-13:30	د. بن لخضر محمد	الإثبات في الجريمة الالكترونية	أستاذ محاضر أ معهد الحقوق والعلوم السياسية المركز الجامعي نور البشير البيض/ الجزائر
13:50-13:40	د.عابد سميرة	حجية الدليل الالكتروني في الإثبات الجنائي	أستاذة محاضرة أ كلية الحقوق جامعة باجي مختار عنابة / الجزائر
14:00-13:50	د. ديدوني بلقاسم	التطور التكنولوجي وأثره على الإثبات الجنائي	أستاذ محاضر أ جامعة عمار ثليجي الأغواط/ الجزائر
	د. محبوبي محمد		أستاذ محاضر أ جامعة عمار ثليجي الأغواط/ الجزائر
14:10-14:00	ط.د. غزلاوي فاطمة الزهراء	دور الأدلة الرقمية في الإثبات الجنائي كآلية لمجابهة الجريمة الالكترونية	طالبة دكتوراه جامعة الدكتور مولاي الطاهر سعيدة/ الجزائر
	ط.د. بن عائشة زكرياء		طالب دكتوراه جامعة الدكتور مولاي الطاهرة سعيدة/ الجزائر
14:20-14:10	د. الحاسي مريم	الدليل الرقمي بين ضرورة الإثبات الجنائي وحماية الحق في الخصوصية	أستاذة محاضرة ب معهد الحقوق والعلوم السياسية مغنية/ الجزائر

الجلسة الـختـامية

- قراءة التوصيات/ الدكتورة تحانوت نادية

كلية الحقوق جامعة الجزائر 1/

رئيس لجنة التوصيات

-كلمة الدكتورة خطاب كريمة

رئيس الملتقى الدولي

-كلمة الأستاذ الدكتور لعلاوي عيسى

- عميد كلية الحقوق جامعة الجزائر 1

جامعة الجزائر 1بن يوسف بن خدة

كلية الحقوق

تنظم

الملتقى الدولي الافتراضي الموسوم بـــ:

" القانون الجنائي في ظل التطورالتكنولوجي

- إشكالات ومعالجات -

يومي 5 و 6 أكتوبر 2022

الهيئة المشرفة على الملتقى الدولي:

البروفيسور مختاري فارس/ رئيس جامعة الجزائر1

البروفيسور لعلاوي عيسى/ عميد كلية الحقوق

الدكتورة خطاب كريمة/ رئيس الملتقى

الدكتورة خطاب كريمة/ رئيس اللجنة العلمية

الدكتورة التجاني زليخة/ رئيس اللجنة التنظيمية

المشرفة العامة على التظاهرات العلمية بالكلية/ السيدة دلمي مونة

ديباجة الملتقى

أفرزت التطورات التي لحقت بمختلف مناحي الحياة العديد من المفاهيم الجديدة منها: مجتمع المعرفة، الثورة المعلوماتية، الثورة التكنولوجية، التعليم الرقمي وغيرها من القيم التي تعبّر عن التقدم التقني والتكنولوجي، وكان من نتاج هذا التطور التأثير على الظاهرة الإجرامية، باعتبار الجريمة ثمرة لتضافر عوامل مختلفة، تتغير بتغير الزمان والمكان ويساعد على تحقيقها الوسائل التكنولوجيا الحديثة.

وهو ما استتبع بالضرورة التأثير على القانون الجنائي الذي يعد أداة الدولة لمواجهة الجريمة، سواء على مستوى قواعد التجريم والعقاب، أو قواعد قانون الإجراءات الجزائية، وترتب على ذلك الرغبة الملحة في تطوير البنية التشريعية ذات الصلة بمكافحة الجريمة، لتتوافق مع تطورات وقدرات مرتكبيها ووسائل ارتكابها، وكذلك مجالات الملاحقة الجنائية وهو ما ترتب عليه إدخال وسائل جديدة لم تكن موجودة من قبل، واعتماد سبل مستحدثة للإثبات كالأدلة العلمية وتطوير أدوات جديدة في إدارة الجلسات وإصدار الأحكام....الخ، أي ظهرت ملامح تأثير التطور التكنولوجي على القانون الجنائي بشقيه الموضوعي والإجرائي، فشمل قواعد وأحكام التجريم والعقاب وكذا قواعد الإجراءات السابقة على الدعوى العمومية (إجراءات الاستدلال) وإجراءات الدعوى العمومية ذاتها (إجراءات التحقيق والمحاكمة) وكذلك المبادئ المتعلقة بالتنفيذ العقابي .

ومما لا شك فيه أنه يجب تحقيق تكامل تشريعي داخل المجتمع، لذلك سنحاول من خلال هذا الملتقى تحديد الوسائل التي عن طريقها يتحقق التكامل بين التشريع الجنائي الموضوعي والإجرائي، فيما يتعلق بالتجريم والعقاب، وكذا الإثبات وإجراءات المتابعة القضائية وتنفيذ الاحكام القضائية، وهو بذلك قد يزيل بعض الصعوبات التي تكتنف قواعد القانون الجنائي نتيجة ما أفرزته الثورة المعلوماتية، والتي ما زالت في جانبيها الموضوعي والإجرائي تحتاج إلى مزيد من التحليل والتأصيل.

إشكالية الملتقى

يمكن تحديد الإشكالية التي تثيرها الدراسة على النحو التالي: انطلاقا من فكرة أن القانون الجنائي هو وسيلة السياسة الجنائية في تحقيق أهدافها داخل المجتمع، فما هي انعكاسات تفعيل آليات التطور التكنولوجي على القانون الجنائي وعلى منظومة العدالة الجنائية؟

وعلى ضوء ما طرحناه من إشكالية، نحاول من خلال هذا الملتقى العلمي أن نناقش القضايا المتعدّدة التي تثيرها التكنولوجيا الحديثة وتطبيقاتها في القانون الجنائي، للوصول إلى إجابات منطقية والخروج بتوصيات واضحة قائمة على أسس علمية، تخدم المجتمع وتعزّز من قيمة البحث العلمي.

وعليه يفتح هذا الملتقى العلمي الدولي الافتراضي المجال أمام الأساتذة والباحثين وكل المهتمين لإثراء الموضوع والمساهمة فيه وعرض التجارب وتقديم الحلول.

أهمية الملتقى

تنبع أهمية هذه الدراسة من أهمية الموضوع ذاته، إذ يتناول فكرة اكتساح التطور التكنولوجي بعض المجالات ذات الصلة بالمجال القانوني والقضائي بصفة عامة ومنظومة العدالة الجنائية بصفة خاصة .

وتزداد أهمية الدراسة في أنها تشير إلى مجالات جديدة يمكن الاستعانة فيها بتقنيات التكنولوجيا الحديثة، لا سيما مع ما أكدته تجربة العالم في تعامله مع جائحة كورونا وما خلفته من نتائج، كان أبرزها ضرورة العمل على إيجاد حلول غير تقليدية لأزمة العدالة بصفة عامة، والعدالة الجنائية خاصة.

وعليه فإن التخلي عن هذه الوسائل الحديثة والمهمة يفقد الجهاز الأمني والقضائي واحدا من أهم الوسائل اللازمة لمكافحة الجرائم والكشف عن غموضها.

أهداف الملتقى

1) إبراز دور التكنولوجيا الحديثة في علاج القضايا المعاصرة، من خلال سهولة التواصل بين العلماء والباحثين والتقريب بين الأفكار من مختلف الدول،
2) رصد عملية التطور التكنولوجي وتحليل النصوص القانونية المنظمة لها وربطها بواقعها العملي،
3) بيان تأثير التطور التكنولوجي على البنية القانونية والقضائية في مجال العدالة الجنائية،
4) خلق بيئة حاضنة للباحثين من مختلف الأقطار ليسمعوا ويناقشوا الجديد من الأفكار،
5) الاستفادة من التكنولوجيا الحديثة في المسائل المستجدة في القضايا الجزائية، وكذلك التقريب بين المذاهب الفقهية والاستفادة منها.

محاورالملتقى

المحور الأول: التطور التكنولوجي والظاهرة الإجرامية

1/ التطور التكنولوجي كمُتطلب لتحقيق مجتمع المعرفة

2/ العلاقة بين الظاهرة الإجرامية والتطور التكنولوجي

المحور الثاني: أثر استخدام التكنولوجيا الحديثة على أحكام التجريم

1/ لمواجهة التشريعية للجرائم المتأثرة بالتطور التكنولوجي

2/ المواجهة التشريعية للجرائم المستحدثة بالتطور التكنولوجي

المحور الثالث: دور التكنولوجية الحديثة في تطوير آلية تطبيق العقوبات

1/ إدخال التكنولوجيا الحديثة من أجل تطوير وإصلاح السجون

2/ التطور التكنولوجي عامل تطور في تطبيق العقوبات السالبة للحرية

المحور الرابع: استخدام التقنيات الحديثة في مجال العدالة الجنائية

1/ التطور التكنولوجي عامل تطور لإجراءات التحري والتحقيق في الجرائم

2/ التطور التكنولوجي عامل تطور لإجراءات المحاكمة

المحور الخامس: تأثير الوسائل العلمية الحديثة على الإثبات الجنائي

1/ التطور التكنولوجي عامل تطور أدلة الإثبات الجنائي

2/ تحديات استعمال الدليل العلمي بالنسبة لحقوق الانسان

أعضاء اللحنة العلمية

الاسم واللقب	جامعة الانتماء
البروفيسور عبد الله أوهايبية	جامعة الجزائر 1 كلية الحقوق
البروفيسور خالف عقيلة	جامعة الجزائر 1 كلية الحقوق
البروفيسور زيدومة درياس	جامعة الجزائر1 كلية الحقوق
البروفيسور خوري عمر	جامعة الجزائر 1 كلية الحقوق
البروفيسور علاكريمة	جامعة الجزائر 1 كلية الحقوق
البروفيسور درياد مليكة	جامعة الجزائر 1 كلية الحقوق
البروفيسور عمارة عبد الحميد	جامعة الجزائر 1 كلية الحقوق
البروفيسور بهلول مليكة	جامعة الجزائر 1 كلية الحقوق
البروفيسور شمامة خير الدين	جامعة باتنة
د. لوني فريدة	جامعة أكلي محند أولحاج البويرة
د. فغول عربية	جامعة البليدة2
د. مبروك حورية	جامعة الجزائر 1 كلية الحقوق
د. بوقادوم صليحة	جامعة الجزائر 1 كلية الحقوق
د. ميثاق بيات الضيفي	جامعة العراق
د. بلعشي مريم	جامعة الجزائر 1 كلية الحقوق
د. قجالي مراد	جامعة الجزائر 1 كلية الحقوق
د. مالك نسيمة	جامعة الجزائر1 كلية الحقوق
د. نبيلة القشطي	جامعة القاهرة
د. دريسي جمال	جامعة الجزائر 1 كلية الحقوق
د. خوجة حسينة	جامعة الجزائر 1 كلية الحقوق
د. سديرة نجوى	جامعة الجزائر 1 كلية الحقوق
د. ماروك أحمد	جامعة الجزائر 1 كلية الحقوق
د. محمد راشد مصطفى شداد	جامعة حلوان
د. لوني نصيرة	جامعة أكلي محند أولحاج البويرة
د. بن موسى وردة	جامعة البليدة2
د. سوماتي شريفة	جامعة خميس مليانة
د. رامز مهدي محمود عاشور	جامعة غزة
د. ايمان أبو المحاسن	جامعة ليدز البريطانية
د. ربيع معزوز	المركز الجامعي علي كافي تندوف
د. مسلم خديجة	جامعة الجزائر 1 كلية الحقوق
د. وابري فريد	جامعة الجزائر 1 كلية الحقوق
د. خفيفجمال	جامعة الجزائر 1 كلية الحقوق
د. بدري فيصل	جامعة الجزائر 1 كلية الحقوق
د. عثماني على	المركز الجامعي آفلو الأغواط
د. الداوي نجاة	جامعة قاصدي مرباح ورقلة
د. بن يعقوب حنان	جامعة الجزائر 1 كلية الحقوق
د. عياد فوزية	جامعة الجزائر 1 كلية الحقوق
د. كروش نعيمة	جامعة الجزائر 1 كلية الحقوق
د. بوروبة سامية	جامعة الجزائر 1 كلية الحقوق
د. بوزيدة عادل	جامعة الجزائر 1 كلية الحقوق
د. فرحاتي صبرينة	جامعة الجزائر 1 كلية الحقوق
د. بباح ابراهيم	جامعة الجزائر 1 كلية الحقوق
د. تحانوت نادية	جامعة الجزائر 1 كلية الحقوق
د. كلاثمر أسماء	جامعة الجزائر 1 كلية الحقوق
د. طاشت وردية	جامعة الجزائر 1 كلية الحقوق
د. طلبي ليلى	جامعة الجزائر 1 كلية الحقوق
د. حبيب فطيمة	جامعة الجزائر 1 كلية الحقوق
د. فاضل خديجة	جامعة الجزائر 1 كلية الحقوق
د. عبد الرزاق اسمهان	جامعة الجزائر 1 كلية الحقوق
د, ريش محمد	جامعة الجزائر 1 كلية الحقوق

أعضاء اللجنة التنظيمية

د. بولعراس الطيب، د. صحراوي عبدالرزاق، د. لشهب نادية ، ط.د. مبرك عزالدين، ط.د.بوقرة علاء الدين، ط.د.عنان كريمة ، ط.د.معيزي علال، ط. د. بن عربية شفاء

شروط المشاركة

1/يكتب البحث طبقا للأصول العلمية المتعارف عليها

2/يشترط في البحث أن يكون أصليا وحديثا ويتسم بالجدية في ظل منهجية محكّمة وتوثيق متكامل للمراجع والمصادر، ولم يتم نشره من قبل بأي صورة من صور النشر العلمي، أو مأخوذ من أطروحة أو بحث علمي

3/يكتب البحث باللغة العربية وفقا لخط simplifiedArabicحجم 14 والهوامش حجم 12،وباللغة الأجنبية بخط Times new roman حجم 12 والهوامش حجم 10

4/أن يشتمل البحث على بيانات الباحث (الكلية،الجامعة،البريدالالكتروني) وملخص بلغة البحث يحتوي على الكلمات المفتاحية

5/تخضع البحوث للتحكيم العلمي لهيئة الملتقى،ويتم الرد على المقبول منهافقط

6/ترفض البحوث التي لا يتماشى مضمونها مع أحد محاور الملتقى

7/يرسل الملخص قبل تاريخ**17جويلية 2022**

8/ يتم الرد على المداخلات المقبولة قبل تاريخ**27جويلية 2022**

9/ ترسل المداخلةكاملة قبل تاريخ**20 أوت 2022**على البريدالالكتروني لرئيسة الملتقى : karimakhettab726@gmail.com

القانون والتكنولوجيا

-علاقة تأثير وتأثر-

إعداد/ الدكتورة خطاب كريمة

أستاذة محاضرة أ كلية الحقوق جامعة الجزائر 1

Karimakhettab726@gmail.com

0560018779

الملخص

لم تعد قاعدة "القانون وليد بيئته" الفاعل المؤثر الوحيد في إنشاء القاعدة القانونية وتحيينها وملاءمتها، بل ظهرت فواعل أخرى أصبحت تلعب دور المحرك في بلورة النصوص القانونية، وعلى رأسها المد التكنولوجي الذي يتميز بالعدد الغزير للمعلومات والمصطلحات العلمية والتقنية، غير أن سرعة التكنولوجيا تفوق بأشواط سرعة القانون، مما يترتب عنه فراغ تشريعي، لذا تأتي هذه الورقة البحثية قصد إيجاد وضع جديد لقوانيننا ولقابليتها لاستيعاب التقنيات التكنولوجية الحديثة دون مخاطر.

الكلمات المفتاحية: القانون، التكنولوجيا، السرعة، الاستقرار، العلاقة

مقدمة

من المعلوم أن سن القانون وتطبيقه واستيعابه يتطلب مرور فترة طويلة من الزمن حفاظا على المراكز القانونية واستقرارها، لكن سرعة الوتيرة الناتجة عن التطور التكنولوجي طرح إشكالية عدم تماشي القوانين وسرعة الفكر التكنولوجي الزائد في التطور، الأمر الذي يعرض كل قانون جديد للتجاوز والنقد، ربما حتى للتعديل أو الإلغاء حسب درجة دقة التفاصيل والجزيئات التي لم يستطع الإلمام بها.

وعليه توحي هذه التناقضات بضرورة إيجاد انسجام وضوابط تحكم العلاقة بين القانون والتكنولوجيا، خاصة بعد أن أظهر الواقع العملي ظهور عديد الآثار التكنولوجية من دون تأطير قانوني.

تتمثل أهمية هذه الدراسة في تقديم قراءة نقدية للقانون، لتحديد الدور الذي يجب أن يلعبه ليواكب إفرازات التكنولوجيا، من خلال فهم وتحليل العلاقة المتبادلة بين "القانون" و "التكنولوجيا"، في محاولة منا لإحداث تجاوب منسجم بين الفكر القانوني والتطورات المعاصرة للتكنولوجيا التي تحتاج إلى تأطيرها قانونيا مراعاة للمصلحة العامة وحقوق الإنسان.

وعليه تسعى هذه الدراسة إلى تحقيق الأهداف التالية:

1/ محاولة الوصول إلى إطار معرفي مناسب يمكن من خلاله تحليل طبيعة العلاقة المتبادلة بين كل من القانون والتكنولوجيا.

2/ السعي إلى الكشف عن الأسباب التي تجعل القانون يفقد السيطرة عن التكنولوجيا.

3/ إيجاد الحلول التي من شأنها أن تمكن القانون من التصدي لتجاوزات التكنولوجيا ومخاطرها قصد احتوائها أو على الأقل التخفيف من حدتها.

إذن تكمن الإشكالية التي يمكن إثارتها في هذا المجال في ما يلي : **كيف تتحقق المعادلة بين القانون والتكنولوجيا بما يحقق قدرة القانون على استيعاب التكنولوجيا وتأطيرها والحد من مخاطرها دون أن يؤدي ذلك إلى عرقلة التطور التكنولوجي؟** إجابة على هذه الإشكالية نقسم موضوع دراستنا إلى محورين رئيسيين، نعالج في المحور الأول فكرة القانون والتكنولوجيا في علاقة تكامل، ثم نخصص المحور الثاني من الدراسة لفكرة تحايل التكنولوجيا على القانون.

المحور الأول: القانون والتكنولوجيا في علاقة تكامل

شاع التفكير لحقبة طويلة من الزمن بأن التكنولوجيا محايدة لا تأثير لها على القانون، وبأن العلاقة العكسية صحيحة، لكن الموضوعية تقتضي الاعتراف بالأثر المتبادل بين الحقلين:

أولا: قوقنة التكنولوجيا

أفرزت التطبيقات التكنولوجيا الحديثة ظهور مجالات جديدة، يجد القانون فيها إمكانيات للتأثير بشكل أو آخر بتأطير آثار التكنولوجيا على مختلف نواحي الحياة الاجتماعية والاقتصادية والسياسية وحتى الثقافية حماية للحقوق والحريات، ومن أهم مظاهر تدخل القانون في التكنولوجيا:

1/تطوير قواعد الإثبات:

إن تطور وسائل الاتصال الحديثة واكتساحها كل مجالات الحياة وكل الأماكن (الإدارة، التعليم، المنزل، المؤسسة....)، بما جعلنا نتحدث عن العقود الإلكترونية خاصة منها التجارية، أجبر المشرع على التدخل لتطوير قواعد الإثبات، حتى تتماشى مع متطلبات مجتمع المعلومات، والاعتراف بالوثيقة الإلكترونية أو اللامادية، وضبط قواعدها كوسيلة من وسائل الإثبات[1] وخاصة إضفاء الحجية عليها، بما يزرع الثقة فيها لدى مستعمليها.

2/ حماية قانونية مستحدثة

إن التداخل المتشعب للتكنولوجيا في كافة مناحي الحياة، أبرز حاجتها الملحة بالاستنجاد بالقانون بغية تبني حقوقا جديدة، أفرزتها التطورات التكنولوجية، فبرزت إلى جانب الحماية الكلاسيكية لسرية المراسلات، وحرمة المسكن مثلا حقوق جديدة، من قبيل الحق في الصورة، الحق في حماية المعطيات ذات الطابع الشخصي، الحق في الملكية الفكرية[2].

---

[1] م. بوطريكي، الثورة المعلوماتية وانعكاساتها على القانون، ملاحظات حول قانون رقم 05/53 المتعلق بالتبادل الالكتروني للمعطيات القانونية، مداخلة قدمت في اليوم الدراسي الذي نظمته الكلية المتعددة التخصصات بالناضور، يوم 28 مايو 2009، حول موضوع "الثورة المعلوماتية وانعكاساتها على القانون" متوفر على الرابط: تم الاطلاع بتاريخ 2022/07/11 http://bdroit.blogspot.com/2010/05/blog-post_1889.html

[2] Voir : Nina Le Bonniec, La cour européenne des droits de Lhomme face aux nouvelles technologies de l'information et de communication numérique, RDLF,N°05, 2018, p22.

3/ تجريم بعض الأفعال الناتجة عن التكنولوجية

أظهرت التكنولوجيا حاجتها للقانون لتجريم عدة أفعال متصلة بالاستخدام الإجرامي لوسائل الاتصال، وإساءة استخدام وسائط المعلومات والاتصال الحديثة التي تعتمد على الآليات التكنولوجية المتقدمة، والتي أصبحت تشكل تهديدا حقيقيا للإنسانية[1]، لذا سارع المشرعون في مختلف دول العالم بإدخال هذه السلوكات في خانة التجريم الذي يستلزم إنزال العقاب، رغم أن هناك صعوبة في حصرها وتحديد كل صورها والأوضاع التي تنفذ فيها والنتائج الجرمية التي تترتب عنها، مما يصعب مسألة وضع قواعد قانونية تتسم بالثبوت لمعالجتها.

ثانيا: حاجة القانون للتكنولوجيا

كان على القانون أن يرفع التحديات المتزايدة الناتجة عن التطورات التكنولوجية، بتقديم أجوبة مناسبة نسبيا وفي الوقت الملائم لكل الإشكالات الناجمة عن هذا التطور، وهكذا فتحت التكنولوجيا ميادين جديدة للبحث والمناقشة القانونية تظهر من خلال:

1/ظهور فروع قانونية تقنية

إذا كانت الثورة التكنولوجية قد استطاعت أن تغير في طبيعة العلاقات التي تحكم الحياة الإنسانية، فلا بد إذا من منظومة قوانين جديدة أو مستحدثة أو مطورة تحكم أو تواكب هذا التغير الحاصل[2].

فقد كان من نتائج هذا التفكير بروز فروع جديدة للقانون تتجاوز عتبة التقسيم التقليدي للقانون – عام وخاص – إلى عتبة التقسيم التقني للقانون كقانون التهيئة والتعمير، قانون الصحة، النقل، قانون المرور، قانون حماية المستهلك، قانون المنافسة، قانون التأمين، قانون البيئة، قانون الملكية الفكرية[3]، قانون المعاملات الإلكترونية أو التجارة الالكترونية، قانون حماية المعطيات الخاصة، بمعنى صاحب كل تطور مهم للعلوم والتكنولوجيا ظهور فرع قانوني جديد، بهدف تنظيم استعمالاتها والحد من آثارها السلبية.

وعليه فإن التكنولوجيا فتحت ميادين جديدة للبحث والمناقشة القانونية، أفرزت فروع قانونية جديدة عززت ثراء القانون.

---

[1] هدى حامد قشقوش، جرائم الحاسب الآلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992 ص 24 وما بعدها.

[2] Marie Charlotte Roques-Bonnet, Le droit peut-il ignorer la révolution numérique, Editions MICHALON, 2010,p11

[3] الجيلالي عجة، مدخل للعلوم القانونية، الجزء الأول، نظرية القانون، برتي، الجزائر، 2009، ص، 181.

2/ ظهور مفاهيم تكنوقانونية

إن وسائل الاتصال الحديثة ومظاهر التطور التكنولوجي تقود بلا شك إلى إحداث تغيير وتطور في المفاهيم القانونية، ولكن هذا التغير يجب التعامل معه من خلال الاعتقاد بأن هناك جزء ثابت في الموضوع وهو محل القاعدة القانونية، ومبرر وجودها وهو الإنسان، وجانب متغير يرتبط بتطور آليات تفعيلها، فأصبحت القاعدة القانونية تخاطب الوضعيات القانونية التي يتواجد فيها الأشخاص[1] وجعلها تكتسي صبغة تقنية نتيجة التطورات التكنولوجية.

أصبح الآن موضوع القانون تلك الأنشطة والأوضاع والعلاقات والعمليات والظواهر في العالم الافتراضي، حيث ظهر ما يسمى بالعقد الالكتروني، التوقيع الالكتروني، والحكومة الافتراضية وغيرهم كثيرون.

3/أتمتة[2] العمل القانوني

استفاد رجال القانون من تقنيات الترقيم والأتمتة الناجمة عن ثورة التكنولوجية، خاصة المعلوماتية في عملية أرشفة وتخزين واسترجاع البيانات القانونية، سواء بشكلها الخام أو بعد استعمالها وتحويرها، فصار ما يعرف بالبنوك التي تخزن المعلومات القانونية، الأنظمة الخبيرة أو المساعدة على اتخاذ القرارات القانونية، الموسوعة الالكترونية القانونية، برامج تعليم القانون بواسطة الكمبيوتر[3].

ولم يتوقف الأمر عند هذا الحد بل امتدت الأتمتة لتشمل العمل القضائي، حيث ساهمت كثيرا في تبسيط الإجراءات القضائية وتسريعها، وحتى فض المنازعات من خلال المحاكم الالكترونية والتحكيم الالكتروني، مما أكسب العمل القضائي في ظلال الأتمتة بعدا جديدا، فالأتمتة ليست هدفا بحد ذاتها بل هي وسيلة دافعة للعمل القضائي.[4]

---

[1] محمد حسين الفيلي، "القانون واستخدام تكنولوجيا الاتصالات في أعمال الإدارة الحكومية والتعاملات الالكترونية"، ورقة مقدمة في المؤتمر الوطني للتشريعات الالكترونية، يومي 9 و10 يونيو 2013، كلية الحقوق جامعة الكويت.

[2] يعد مصطلح أتمتة من المصطلحات الحديثة المرتبطة بالثورة التقنية، ويقصد بعملية الأتمتة الاستغناء على وجود العامل البشري في العملية التي تتم عليها النشاطات التي كانت تعتمد على العنصر البشري، وهو استعمال الحاسبات والماكنات والأجهزة الآلية وذلك لتقليل حجم العمل الذي يقوم به الناس وبسرعة أكبر، للمزيد أنظر:حازم الببلاوي، "الأوتوميشن و الاقتصاد"، مجلة عالم الفكر، المجلد الثاني، العدد الرابع، الإسكندرية، مصر، ص 70.

[3] تكنولوجيا المعلومات والقانون، المركز الاستشاري الدولي، متوفر على الموقع www.iccgaza.com تاريخ التصفح 2022/07/11.

[4] Florence G'sell L'automatisation des décisions de la justice jusqu'ou?, Les métiers du droit au défi du numérique, Les annales des mines, N°03, Septembre 2018, p 22

4/حاجة القانون للخبرة

إن القواعد القانونية الحالية قد لا تكون كافية أو حتى مناسبة لتأطير هذا الواقع التكنولوجي الجديد، وتبعا لذلك كان لا بد على القانون أن يبدي مرونة في التأقلم مع هذا الواقع، باللجوء إلى الخبراء وإشراكهم في وضعه، تطبيقه، وحتى تفسيره.

كما أفرزت التكنولوجيا تخصصات واضحة في نطاق المهن القضائية، والعمل الفقهي والتدريس الجامعي، ودفعت القانونيين والمهتمين الآخرين إلى التعاون الطبيعي مع المختصين الجدد، الذي صار لهم نوع من النفوذ لا يسهل إغفاله، بحيث صارت قدرة القانون على التأقلم مع التطورات التكنولوجية تتسم بحيوية واضحة، والأمثلة في ذلك كثيرة جدا، لذا كان من الضروري مثلا المناداة لإنشاء ضبطية أو جهاز أو هيئة خاصة للتحري والتحقيق في الإجرام الالكتروني، لا تعتمد على القوة البدنية والتدريب لقوات الأمن، بقدر ما تعتمد على المهارة الفنية والتقنية في مجال تكنولوجيا المعلوماتية، وذلك كمرحلة أولى، في انتظار إنشاء قضاء مختص يفصل في هذه الجرائم.[1]

[1] راجع المادة 14 من اتفاقية بودابيست للإجرام المعلوماتي المؤرخة في 23 نوفمبر 2001.

المحور الثاني: تحايل التكنولوجيا على القانون

تتميز التكنولوجيا بقدرة حقيقية على التحايل على القانون، ذلك أن القانون يسعى للحفاظ على خاصيته العملية تحقيقا لوظيفته الضبطية، بحماية الحقوق والحريات والقيم الإنسانية في المجتمع، في حين أن التكنولوجيا مجردة من كل هذه الصفات، فهي مادية في تصورها وتطبيقاتها، وهو ما يجعلها متناثرة يصعب على القانون إحكام القبضة عليها.

لذا سنحاول من خلال هذا المحور تسليط الضوء على مظاهر تحايل التكنولوجيا على القانون، ممثلة في أهم جرائم التطور التكنولوجي من جهة ثم التطرق لأهم التحديات التي لا تزال تعترض القانون لاحتواء التكنولوجيا.

أولا/ جرائم التطور التكنولوجي

في ظل هذا الزخم التكنولوجي المتطور، كان من الطبيعي أن يجد المجرمون في المجتمع ميدانا خصبا لتطوير أفعالهم الإجرامية، سواء باستعمال وسائل جديدة ومتطورة في ارتكاب جرائم تقليدية، أو بإتيان جرائم جديدة كليا لم تكن معروفة من قبل، وهو ما أصبح يندرج اليوم ضمن الإجرام العلمي والذي من أبرز مظاهره الجريمة الالكترونية والحروب الالكترونية.

1/الجريمة الالكترونية

عندما نتحدث عن الجريمة الالكترونية أو الافتراضية فإننا نقصد السلوك الجرمي الجديد الذي صاحب الزخم التكنولوجي الرقمي، وبات يعرفه الفضاء المعلوماتي المفتوح وبالتالي صار ظاهرا للعيان وجود سلوك جرمي مرتبط أساسا بالشبكة العنكبوتية، حيث غزارة المعلومات وتدفق المعطيات الخاصة والعامة أضحى في متناول الجميع.

أصبح مسرح الجريمة الإلكترونية هو الفضاء الرقمي، وهو مسرح للأذكياء، لأن الوقائع غير مادية لا وجود لها، كما أن مرتكبي هذه الجرائم يمكنهم ارتكابها دون تفاعل مادي، سواء مع الضحايا أو المجرمين

المشاركين، فلا يشترط التواجد في مكان واحد أو دولة واحدة بين الجناة والضحايا، وأداة الجريمة تكون هي الحاسوب المرتبط بالشبكة العالمية، وعليه فإننا بصدد الحديث عن الجريمة العابرة للحدود[1].

في هذا السياق أشارت شركة "كاسبيرسكي لاب" للأمن الإلكتروني (kaspersky lab) في أفريل 2018، من أنه قد تمت سرقة مليار دولار من الكثير من البنوك حول العالم خلال عامين فقط عبر عمليات سطو إلكتروني على حسابات هذه البنوك، وفي تقرير الشركة نفسها في فبراير 2018 حول الهجمات الإلكترونية التي تعرض لها القطاع المالي في العالم عام 2017، جاء أن نسبة الاحتيال المالي عبر الإنترنت ارتفعت في 2017 من 47,5% إلى 54% من مجموع حالات الكشف عن الاحتيال عبر الإنترنت[2].

2/الحرب التكنولوجية

توجه الاهتمام بقوة في الآونة الأخيرة نحو حرب التكنولوجيا الحديثة، باعتبارها أداة أساسية في آليات حرب الجيل الرابع، ويطلق عليها "**الحرب عن بعد**"، وهي تطور طبيعي في مفهوم الحروب، نقلها التطور التكنولوجي إلى جيل جديد يعتمد على التحكم والسيطرة عن بعد، دون عناء نقل الجيوش والأسلحة وهي تصنف ضمن الحروب الباردة، تم تعريفها بأنها "حرب ذكية أقوى من أي هجوم بري أو جوي، وأكثر ذكاء وأقل تكلفة، فهي لا تحتاج إلى معدات حربية ولا جنود، لكنها تحتاج إلى قدرات علمية عالية[3]".

هذه الحرب التكنولوجية قد تأخذ صورة حرب إلكترونية، وهي صراع ميدانه شبكة الإنترنت، وينطوي على هجمات ذات دوافع سياسية على المعلومات ونظمها، من خلال اختراق الأنظمة الإلكترونية للعدو أو تدميرها أو إرسال فيروسات مدمرة إلى الأنظمة الالكترونية، حيث يمكنها تعطيل مواقع الويب الرسمية، والشبكات وتعديل الخدمات الأساسية، أو سرقة وتعديل البيانات السرية، وتخريب الأنظمة المالية، وبذلك يمكن السيطرة على نظام الدول إلكترونيا، مثال ذلك فيروس « ستوكسنت » الذي ضرب البرنامج النووي الإيراني في عام 2010 وسبب مشكلة كبيرة له، حتى أن خبيرا ألمانيا في مجال الحاسوب، هو رالف لانجر، قال حينها، إن هذا الفيروس قد أعاد البرنامج النووي الإيراني سنتين إلى الوراء.

---

[1] السيد عوض، التطور التكنولوجي والجريمة، أعمال المؤتمر السنوي الرابع والثلاثون (قضايا السكان والتنمية) 19-22 ديسمبر 2004م، جامعة جنوب الوادي، المركز الديموغرافي بالقاهرة، ص22.

[2] وفقا لتصريح "يوجين كاسبرسكي" المدير التنفيذي لشركة "كاسبرسكي لاب" متوفر على الرابط: https://me.kaspersky.com/about/team تاريخ التصفح 2019/07/11.

[3] عرفها الدكتور بول روزنفياغ، أستاذ القانون في جامعة جورج واشنطن، نقلا عن الحروب الإلكترونية....معارك العالم الافتراضي تنتقل إلى الميدان لندن – الخليج أونلاين 24-03-2018 متوفر على الموقع https://alkhaleejonline.net تاريخ الاطلاع 2020/08/17.

وقد تأخذ هذه الحرب التكنولوجية صورة ثانية، تتمثل في تطوير الاستراتيجيات والأسلحة الذكية، والتي جعلت الدول تتسابق في تطويرها أو تحصيلها، كأسلحة الدفع فوق الصوتي (وهي أسلحة تفوق سرعتها سرعة الصوت بخمس مرات)، والأسلحة الموجودة في الفضاء التي ستكون قادرة على استهداف أي مكان في العالم بشكل شبه فوري، وأسلحة أخرى ستكون قادرة على مهاجمة نطاقات اعتبرت محرمة فيما مضى، مثل الفضاء وشبكات الإمداد. وأسلحة ذكية تمكنت من تحديد الهدف والقضاء عليه في بضع دقائق، كما حدث في أوكرانيا عام 2014، عندما قلصت روسيا الوقت الذي استغرقته طائراتها بدون طيار في الكشف عن أماكن القوات الأوكرانية ومسحها عن وجه الخارطة.

ثانيا: القانون في مواجهة تحديات التكنولوجيا

إن غاية القانون في علاقته بالتكنولوجيا هو تأمينها أو ما يعرف بالأمن التكنولوجي، الذي لن يتأت إلا بتصدي القانون لمجموعة من التحديات التي لا تزال خارج السيطرة، والتي سنحاول التطرق لأهمها فيما يلي:

1/ تحد عالمية التكنولوجيا

بداية، يلاحظ أن القانون كان يسري تقليديا في المجال الوطني الخاضع للسيادة الوطنية، غير أن التكنولوجيا ساهمت في تغيير الوضع ، لأنها لا تخضع للحدود السياسية بين الدول[1] فهي تقفز على حواجز الزمان والمكان والجنسيات والديانات واختلاف اللغات وتنوع القوميات، ولا تخضع لحرس الحدود. وبالموازاة صار القانون الدولي يفرض نفسه على القانون الوطني، مجسدا تقلص السيادة الوطنية على التكنولوجيا.

أظهرت الجرائم العابرة للحدود تحديات لا يزال القانون عاجزا على احتواءها بالقواعد العقابية التقليدية، من قبيل الاختصاص القضائي بهذه الجرائم والقانون واجب التطبيق وإجراءات المتابعة القضائية.

وأمام ما توفره تكنولوجيا المعلومات والاتصالات من فرص هائلة للمجتمع الدولي تتزايد أهميتها باستمرار، "وبالنظر إلى أن سوء استخدامها ينطوي على مخاطر تهدد السلم والأمن الدوليين، أنشأت الجمعية العامة للأمم المتحدة في عام 2013 فريق خبراء حكوميين لبحث "التطورات في ميدان

[1] عبد الرحيم رجواني، عصر المعلومات، جموح تكنولوجيا المعلومات في ظل العولمة، سلسلة المعرفة للجميع، رقم 9، سبتمبر 1999، مطبعة النجاح، الدار البيضاء، ص 44.

المعلومات والاتصالات السلكية واللاسلكية في سياق الأمن الدولي"، خاصة وإن مصلحة جميع الدول العمل على تشجيع استخدام تكنولوجيا المعلومات والاتصالات في الأغراض السلمية، ومنع نشوب النزاعات الناجمة عن سوء استخدامه"[1]، وتقدم فريق الخبراء المشار إليه بعدد من التوصيات عام 2015 كي تنظر الدول في وضع معايير وقواعد ومبادئ لضبط السلوك المسؤول قصد تعزيز إيجاد بيئة آمنة ومستقرة في مجال تكنولوجيا المعلومات والاتصالات على المستوى الدولي.

2/ تحد لا إنسانية التكنولوجيا

تفتقر التكنولوجيات في تطبيقها إلى الروح الاجتماعية والبعد الإنساني، فهي تجعل من العالم المادي ركيزة أساسية لها، وتسعى إلى جعل القوانين متعلقة بأشياء مادية أكثر من إنسانية، فالتكنولوجيا تتميز بقيمتها الاقتصادية، المواكبة لاستعمالاتها التي ترجح الربح على إنسانية الإنسان، بل يمكن القول أنها تعامل الإنسان نفسه والعلاقات المجتمعية كشيء قابل للصنع والتعديل، من خلال مصطلحات المستهلكين والمستفيدين والمستعملين[2]، بل إن التكنولوجيا الحديثة أنشأت ما يسمى بالذكاء الصناعي، الذي ابتكر أجهزة وآلات تسير نفسها بنفسها، متجاهلة البعد الإنساني كليا، لذا يتعين على القانون أن يضع هذا البعد في صلب اهتماماته لتقرير الاستعمال الأنسب للتكنولوجيا[3].

3/تحد المسؤولية القانونية

أمام التقدم التكنولوجي الهائل وولوج عالم الذكاء الاصطناعي الذي مس كل جوانب الحياة، طرحت إشكالية مستقبل المسؤولية التقليدية في مواجهة المسؤولية عن الذكاء الصناعي، وهذا ما يدفعنا إلى التساؤل عما إذا كانت القواعد الحالية لنظام المسؤولية كافية، أم أن الوضع يقتضي إدراج قواعد جديدة قادرة على توضيح المسؤولية القانونية لمختلف الفاعلين (المصنع، المشغل، المالك، المستخدم.....إلخ) ، ولنضرب مثلا على ذلك تطبيقا للمسؤولية القانونية في المجال الطبي، وهو مجال خطير ودقيق سمحت فيه منظومة الذكاء الاصطناعي بإدخال الروبوت مثلا في مجال تشخيص الأمراض، وإجراء التحاليل الطبية، وحتى إجراء العمليات الجراحية، التي لا يمكن للقدرات البشرية انجازها بنفس المستوى من الدقة والسرعة، والتي قد تكون سببا في حدوث خطأ وضرر يستوجب إثارة المسؤولية القانونية، فهنا تتنازع

---

[1] محمد بن عبد العزيز الخليفي، إساءة استخدام تكنولوجيا المعلومات والاتصالات من منظور القانون الدولي، صحيفة الشرق، قطر النسخة الالكترونية الصادرة بتاريخ 10 أكتوبر 2019.

[2] أنظر: ماجد أحمد الزاملي تأثير التكنولوجيا على الاقتصاد العالمي والقانون، الحوار المتمدن، بتاريخ 2022/07/08

[3] Olivier Dyens, La condition inhumaine: Essai sur l’effroi technologique, Flammarion, 2018, p63.

المسؤولية عدة أطراف أو أشخاص، من الطبيب إلى تقني المختبر إلى المشرف التقني على الروبوت، إذ لا يتصور تحميل الروبوت تلك المسؤولية القانونية، ومن يتحمل المسؤولية الأخلاقية والأدبية والقانونية الناجمة عن تصرفات هذه الروبوتات التي تتزايد في كل مكان[1]، هل ينبغي أن تتحملها الشركات المصنعة أم المبرمجون أم المستخدمون؟

وفي معرض المحاولات القانونية للإجابة عن تلك التساؤلات، يسهل القول بأن المسؤولية القانونية تقع على عاتق الجهة المصنعة في منظومات الذكاء الصناعي المستقلة ذاتيا بالكامل، أي عندما يتعلق الأمر بالروبوتات التي تسير نفسها بنفسها وفق برمجيات معينة، دون الحاجة إلى العنصر البشري، لأنه لا يعقل تحميل الآلات المسؤولية القانونية[2].

4/ تحد افتقار القانون للمهارات التكنولوجية

هناك الكثير من الدول التي لم تطور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مسايرة التقدم في الجرائم الإلكترونية وأساليبها، وهذا لا يتوقف عند التشريعات فحسب، وإنما يشمل الشرطة والتحقيق والقضاء، وكيفية التعامل مع الأدلة الرقمية على المستوى الوطني كما هو الحال على المستوى الدولي، فقد استطاعت الجريمة الالكترونية أن تستفحل في المجتمعات نتيجة غياب التشريعات الجزائية وضعف الممارسات الشرطية والقضائية في المحاكمة والتحقيق فيها، وغالبا ما نجد في دول كثيرة ضعف التقنيات المتوافرة وكذلك الخبراء القادرون على متابعة ورصد وملاحقة الجريمة الإلكترونية، داخل المجتمع والعابرة منها للحدود الوطنية.

5/ تحد الملكية الفكرية

تعتبر قضية حماية الملكية الفكرية من أهم التحديات التي يواجهها القانون وهو يحاول استيعاب أثار التكنولوجيا، وذلك بهدف حماية الحقوق القانونية الناجمة عن النشاط الفكري في عصر الرقمنة، وفي هذا الإطار يصعب على القانون إحكام السيطرة على عمليات القرصنة والتزوير والنسخ اللامشروع، وهي

---

[1] سالم علي محمد المطروشي، المسؤولية القانونية لمنظومة الذكاء الاصطناعي، جريدة الخليج النسخة الالكترونية، بتاريخ 09 /07/ 2018 متاح على الرابط: http://www.alkhaleej.ae/alkhaleej/page/2f372996-b853c0d5e5d1-a9ff-4d1d-32e7 تاريخ الاطلاع 15/ 08/ 2022.

[2] همام القوصي، إشكالية الشخص المسؤول عن تشغيل الروبوت (تأثير نظرية "النائب الإنساني" على جدوى القانون في المستقبل) دراسة تحليلية استشرافية في قواعد القانون المدني الأوروبي الخاص بالروبوتات، مجلة جيل الأبحاث القانونية المعمقة، العدد 25، ماي 2018، ص 77.

أفعال تكبد اقتصاديات الدول النامية والمتقدمة على حد سواء خسائر مالية ضخمة[1]، خاصة وأن تتبع آثار هذه الجرائم في العالم الافتراضي صعب، ان لم نقل مستحيلا في الكثير من الأحيان.

خاتمة

حاولنا من خلال هذه الورقة البحثية تحقيق المعادلة بين القانون كوسيلة من وسائل الضبط الاجتماعي، غايته حماية الحقوق والحريات بما يحقق الأمن والاستقرار في المجتمع، وبين التكنولوجيا كأداة تحقق الرقي والرفاهية في مختلف جوانب الحياة دون مخاطر ولا أضرار، وهذا في محاولة للتقريب وتحقيق الانسجام بينهما.

اتضح لنا جليا أن العلاقة بين القانون والتكنولوجيا هي علاقة تأثير وتأثر، فالتكنولوجيا أظهرت حاجتها للقانون لتأطير مفرزاتها للحد من مخاطرها وأضرارها، وانعكس ذلك جليا في إثراء القانون بظهور فروع قانونية جديدة عرفت بالقوانين التقنية لما تحمله من مصطلحات ومفاهيم صاحبت التطور التكنولوجي، كما جرم القانون عديد الأفعال التي يوظف فيها المجرمون وسائط تكنولوجيا المعلومات والاتصالات لغايات غير مشروعة.

من جهة ثانية، برزت حاجة القانون للتكنولوجيا التي فرضت نفسها على كل العلوم بما فيها القانون، الذي وجد نفسه أميا أمام تطبيقاتها ومصطلحاتها، الأمر الذي حتم عليه اللجوء للخبرة في الكثير من الأحيان لفك ألغازها، كما تمت أتمتة العمل القانوني بفضل التكنولوجيا، ما سهل وسرع الإجراءات القضائية، وساهم في فض عديد المنازعات.

إلا أن العلاقة بين التكنولوجيا والقانون لم تقتصر على مجرد استفادة كل منهما من الآخر، بل أن السرعة الفائقة التي تتطور بها التكنولوجيا الحديثة جعلتها تفلت في الكثير من الأحيان من إحكام قبضة القانون عليها، واتضح ذلك جليا بتنامي الفعل الإجرامي المعتمد على الوسائط التكنولوجية، الذي تعدى حدود الجريمة الالكترونية ليدخل العالم في حروب تكنولوجية لا تحمد عقباها.

لذا يتعين على القانون رفع التحديات المحدقة بفعل التطورات التكنولوجية، بتقديم الأجوبة التشريعية والتنظيمية، والاجتهادات القضائية والنظريات الفقهية المناسبة، من خلال اقتراح ما يلي:

---

[1] أنظر: نادية ابراهيم أحمد علي، تكنولوجيا المعلومات وقانون الملكية الفكرية – دراسة وصفية تطبيقية على برامج الحاسوب والوسائط المتعددة – مجلة جامعة الناصر، العدد الثامن، ديسمبر 2017، السودان. ص 251.

-تطويع منظومة القوانين التقليدية في معالجة المشاكل المستجدة ما دام ذلك ممكنا أو متاحا، لذا يتعين على رجال القانون أن يبذلوا ما بوسعهم وغاية جهدهم لاستحداث قوانين جديدة وطبعا الإبقاء على جاهزيتها لمواجهة ما يمكن أن ينشأ من تطورات لحل المشكلات الناشئة على هذا النوع من الظواهر التكنولوجية بما يجعلها أكثر نفعا وأقل سلبية.

-حتى يبقى القانون عمليا وفعالا يجب أن يعتمد مبدأ الواقعية التكنولوجية كعامل للتنويع والتطوير في شكله ومضمونه، لذا يتعين على التنظيم التشريعي التركيز على سلامة وتأمين وسائط تكنولوجيا المعلومات والاتصالات من خلال تفعيل التدابير التنفيذية، وتزويد الجهاز التشريعي بهيئة علمية مساندة في وضع التشريعات للمستجدات العلمية والتكنولوجية، بما يجعل رجل القانون قيمة مضافة في عالم التكنولوجيا وليس أداة لعرقلة تطورها.

-أمام عالمية التكنولوجيا لا بد من تعزيز التعاون الدولي في وضع وتطبيق التدابير التي تضمن زيادة الاستقرار والأمن في استخدام تكنولوجيا المعلومات والاتصالات، وأن تمنع الممارسات المعترف بضررها في هذا المجال كاستعمال تكنولوجيا المعلومات والاتصالات لأغراض إرهابية وإجرامية.

الملتقى الدولي الافتراضي الموسوم بـ "القانون الجنائي في ظل التطور التكنولوجي . إشكالات ومعالجات ".

المحور المشارك به: المحور الأول " التطور التطنولوجي والظاهرة الاجرامية"

عنوان المداخلة: التطوّر التكنولوجي والظاهرة الإجرامية في ظلّ جائحة كورونا كوفيد – 19.

د. بوعزيز فريد، جامعة أحمد بن بلة1، وهران. أستاذ رئيسي بالتعليم الثانوي.

البريد الالكتروني: islamaymen2018@gmail.com

رقم الهاتف: 0667.69.09.26

الملخص

أمام التطوّر التكنولوجي الذي غزا مختلف مجالات حياتنا، استغلّه البعض في تحقيق جرائم بأساليب وتراكيب غير تلك المستعملة في الجرائم التقليدية المعروفة، لتبرز بذلك أنواع جديدة من الجرائم كالجريمة الالكترونية؛ ذلك أنّ التزوير، السرقة والاحتيال ...جرائم أصبحت تتّم عبر أجهزة ووسائل الكترونية. وبالمقابل من هذا رُصِدت تقنيات دقيقة ووسائل ذكية كأجهزة رقابة إلكترونية، تحليل الحمض النووي وبصمات الأصابع... لمواجهة الجريمة في ثوبها الجديد. وفي خِضّم هذا التطوّر وانتشار فيروس كورونا في الآونة الأخيرة، رُفِعت تقارير مُسَجِّلَة انعكاسات ذلك على مستوى الظاهرة الإجرامية.

تهدف هذه الورقة البحثية إلى إبراز تداعيات التطوّر التكنولوجي على الظاهرة الإجرامية في ظل انتشار جائحة كورونا وما تبعها من جملة الإجراءات وحزمة النصوص القانونية والتنظيمية التي اتخذتها الجزائر تحديدا لتطويق الفيروس والحد من الظاهرة الإجرامية، من خلال المنهج الوصفي التحليلي الذي يناسب الموضوع.

الكلمات المفتاحية: الظاهرة الإجرامية، التطور التكنولوجي، فيروس كورونا كوفيد–19، الجريمة الالكترونية.

Title: Technological development and the criminal phenomenon in light of the COVID-19 pandemic.

Abstract

In the face of the technological development that has invaded various areas of our lives, some have exploited it to investigate crimes using methods and structures other than those used in the well-known traditional crimes, thus emerging new types of crimes such as electronic crime ;due to forgery, theft and fraud ... are crimes that are carried out through electronic devices and means. On the other hand, accurate techniques and smart means such as electronic control devices, DNA analysis and fingerprints were monitored to face crime in its new dress. In the midst of this development and the recent spread of the Corona virus, reports have been raised of repercussions. This is at the level of the criminal phenomenon.

This research paper aims to highlight the repercussions of technological development on the criminal phenomenon in light of the spread of the Corona pandemic and the subsequent procedures and a package of legal and regulatory texts taken by Algeria specifically to surround the virus and reduce the criminal phenomenon, through the descriptive analytical approach that fits the topic.

Keywords: criminal phenomenon, technological development, corona virus COVID-19, cybercrime.

المقدّمة

يُوصَف عصرنا اليوم بعصر التقنية والتكنولوجيا، حيث تتسابق في كلّ يوم الاكتشافات والابتكارات بالظُهور؛ ويُعدّ قطاع الاتصالات أكثرها تطوّرا، حيث أصبحت الاتصالات بين الأفراد والبلدان أيْسر بِكَبْسة زِرٍ، بفضل شبكة الانترنت وانتشار الكمبيوتر وخطوط الاتصال المختلفة، وأضحى معها الحصول على المعلومات سَهْلا وبسرعة ومن غير تكلفة، مُوَفِّرة لِمُستخدِمِيها أموالا وجهدا، مُلْغية المسافات الجغرافية، فهي وسائل لا تعترف بالحدود ولا تحجزها المسافات.

لا يُنكر أحد أنّ تكنولوجيا المعلومات أحْدَثت تغييرات أساسية في العالم على شتّى المجالات، وأصبحت وسائلها ضرورية في حياتنا؛ في معاملتنا المصرفية، في تسوّقنا، في الإدارات والمؤسّسات، في علاقة الدّول بعضها ببعض وكذا علاقة الدولة بالأفراد... ، ذلك أنّ تنوّع خدماتها وسهولة الاتصال بها أوْجَد لها مكانا على اختلاف البلدان والأجناس والفئات العُمرية. لكن على الرّغم من التطوّر الهائل في مجال الحاسوب وشبكة الانترنت وايجابيات الوسائل الالكترونية والأهمية التي أصبحت تكتسيها، إلاّ أنّ هناك جانب آخر مُظلم، يتجلّى في الاستخدام غير المشروع لها؛ والذي أدى إلى ميلاد نوع جديد من الجرائم، تحت مُسمّى الجرائم الالكترونية أو جرائم المعلوماتية، التي وَظَّفَ فيها المجرمون وسائل الاتصال الحديثة لخدمة نشاطاتهم الإجرامية، للتنوّع معها أساليب وأدوات ارتكابها ويزداد خطرها، فباتت بذلك مصدرا يُهدّد أمن الدّول واقتصادها، وانتهاك حرمة الحياة الخاصة للأفراد واختراق النظام والآداب العامة.

أمام التخوّفات الوطنية والعالمية من الجريمة الالكترونية والجهود المبذولة لمواجهتها، ظهر تهديد صحّي آخر مع نهاية عام 2019م من خلال انتشار فيروس كورونا كوفيد-19 بداية من مدينة وُوهان الصينية الذي تسبب في أزمة عالمية، صنّفته منظمة الصّحة العالمية أنّه جائحة، إذْ هُدِّمَت معه النُظُم التي تقوم عليها الدّول، واخْتَفت معالم الحياة الطبيعية؛ وبالمقابل انتعش معه كلّ ما هو إلكتروني أو رقمي جرّاء التدابير التي أُتُّخذت لمكافحة انتشار هذا الوباء.

تهدف هذه الورقة البحثية إلى بلورة تداعيات التطوّر التكنولوجي على الظاهرة الإجرامية في ظلّ انتشار جائحة كورونا كوفيد-19 من خلال أبرز مظاهره ممثلّة في الجريمة الالكترونية، وبيان موقف المشرّع الجزائري منها وواقعها في هذا الظرف الصحّي المُقْلق، ضمن جُملة الإجراءات وحُزمة النصوص القانونية والتنظيمية التي اتخذتها الجزائر تحديدا لتطويق الفيروس، باعتماد المنهج الوصفي والاستقرائي والتحليلي الذي يناسب الموضوع.

بناء على ما سبق برز الإشكال الرئيس الآتي: ما هي انعكاسات التطوّر التكنولوجي على ظاهرة الإجرام في ظلّ انتشار فيروس كورونا كوفيد-19؟.

إجابة على الإشكال الرئيس تطلّب الأمر بسط تساؤلات ثانوية أخرى: هل أسْهم التطوّر التكنولوجي في تنامي الظاهرة الإجرامية أو قلّل منها؟ ما علاقة الجريمة الإلكترونية بالتطوّر التكنولوجي في ظلّ انتشار فيروس كورونا كوفيد-19؟ ما موقف المشرّع الجزائري من ظاهرة الإجرام الالكتروني؟ ما هي عوامل

انتشارها؟ هل ثمّة مجالات استهدفتها الجريمة الالكترونية زمن جائحة كورونا كوفيد-19؟ وما هي الآليات التي اتّخذتها الجزائر لمواجهة فيروس كورونا كوفيد-19؟.

منهج الدّراسة

اقتضت التساؤلات المطروحة اعتماد منهج مركّب بين المنهج الوصفي والاستقرائي والتحليلي، بجمع معلومات ومعطيات عن ظاهرة الإجرام الالكتروني تحديدا كونها من تجليآت التطوّر التكنولوجي وبيان واقعها في خضّم انتشار فيروس كورونا كوفيد- 19، تحت مظلّة أبرز النصوص القانونية التي جاء بها المشرّع الجزائري لمواجهة الجريمة الالكترونية، وكذا المراسيم التنفيذية التي اتّخذتها السلطات الجزائرية لمكافحة انتشار جائحة كورونا كوفيد-19.

إجابة على الإشكال الرئيس والتساؤلات المطروحة، تمّ تقسيم الدّراسة إلى النقاط التالية:

أولا . معنى التطوّر التكنولوجي وموقف المشرّع الجزائري من الجريمة الالكترونية

ثانيا . تصنيفات الجريمة الالكترونية وأهمّ المجالات التي استهدفتها في ظل جائحة كورونا كوفيد-19

ثالثا . عوامل انتشار الجريمة الالكترونية زمن تفشي فيروس كورونا كوفيد-19 وأبرز التدابير التي اتخذتها الجزائر لمكافحته.

رابعا . التطوّر التكنولوجي بين خدمة الظاهرة الإجرامية ومكافحتها فترة انتشار فيروس كورونا كوفيد -19

أولا . معنى التطوّر التكنولوجي وموقف المشرّع الجزائري من الجريمة الالكترونية

تُعدّ تكنولوجيا المعلومات والاتصالات من مظاهر التطوّر التكنولوجي الذي نعيشه وثمرة الجهود العلمية التي توصّل إليها الإنسان، وقد سخّرت الدّول إمكانيات مادية وبشرية للاستثمار الأحسن لها، لكن هذا المتغيّر التكنولوجي سلاح ذو حدين، فمن جهة حَسَّنَ من نوعية حياة الإنسان، ومن جهة أخرى كان تربة خِصْبة لبعض الأنشطة السلبية كالجرائم الالكترونية أو المعلوماتية.

إنّ هذا التطوّر الحاصل ومفرازاته، مسّ المجتمع الجزائري كغيره من المجتمعات، وجعله يَعْرِف أنواعا من الجرائم المستحدثة كالجريمة الالكترونية؛ نحاول في هذه الجزئية أن نبيّن معنى التطوّر التكنولوجي في هذا المجال، لِنعقبه بموقف المشرّع الجزائري من الجريمة الالكترونية باعتبارها من مخرجات هذا التطوّر وأهمّ مظاهره غير المشروعة.

1 . معنى التطوّر التكنولوجي

التطوّر التكنولوجي مصطلح رام الكثير إلى إعطاء مفهوم له، لتطفو بذلك جملة من التعاريف أهمّها تعريف خالد القضاة حيث قال: " التطوّر التكنولوجي هو عبارة عن " استمرارية التقدّم والنماء على أساس من توظيف كلّ المعارف في عملية التنمية الشاملة وابتكار وتطوير الوسائل اللازمة لتسخير تلك المعارف في عملية التنمية"[1] ، وعبّر عنه آخرون بأنّه مجموعة الاختراعات أو الطرق التكنولوجية أو الخدمات أو النماذج

[1] . خالد القضاة، التقنيات الحديثة وانعكاساتها الاقتصادية والاجتماعية والنفسية والبيئية، ط1، دار اليازوري العلمية، عمان، 1997م، ص 57.

الجديدة التي تستخدم في الإنتاج، ويترتّب عليها تطوّر في كمية المنتج أو درجة جودته"[2] وقيل: أنّه انتقال الإنسان من مرحلة إلى مرحلة أخرى متباينة، كالانتقال من العصر الحجري إلى العصر النحاسي مثلا، أو الانتقال من عصر النسخ اليدوي في طباعة الكتب إلى عصر المطبعة الآلية، فابتكار الأدوات التي تمكّن بني الإنسان من التعامل مع البيئة المحيطة ومتطلباتها بشكل أفضل. والتعديلات والتحسينات الطارئة على أداء هذه الأدوات، وكذا الحال الابتكار الجديد لهذه الأدوات والذي من شأنه سدّ فجوات في حياة الإنسان العملية، أو العمل على تحسين أو تجويد أو تسريع من أداء الإنسان في نيل أغراضه، كلّ ذلك يدخل تحت مسمّى التطوّر التكنولوجي.[3]

والحقيقة أنّ التطور التكنولوجي يمُرّ بمراحل ويتم بشكل تدريجي عبر مختلف الأزمنة، بدليل التغيّرات العميقة التي طرأت على حياة الإنسان خصوصا، ويُعدّ اليوم التطوّر التكنولوجي مَعْلما على الحضارة الحديثة الذي يتمكّن الإنسان معه من التكيّف مع بيئته ومحيطه وإدخال تحسينات وتعديلات على حياته من خلال الاختراعات والاكتشافات....

ويمكن القول في الجملة أنّ لكلّ عصر أدواته واختراعاته، وكلّ مرحلة من التطوّر ترتكز على معارف وتجارب سابقة لِتبنيّ وتأتيّ بالجديد، وهذا على مختلف المجالات. وإنّ المقصود هَهُنا من التطوّر التكنولوجي هو التزايد التدريجي في الاختراعات المادّية المتمثّلة في الآلات كالسيارات والطائرات والحاسبات الآلية وشبكة المعلومات الدولية....وكذا الاختراعات غير المادّية المتمثّلة في مهارات استخدام تلك الآلات والمَعْرِفة بفُنُونها التي قد يكون لها تأثير مباشر أو غير مباشر على الجريمة.[4] على أنّ مجال هذا التزايد التدريجي في الاختراعات المادية أو غير المادية والذي يتماشى مع موضوع بحثنا هو الذي يكون في إطار ارتكاب الجريمة، ولعلّ من أجلّ وأبرز المظاهر السلبية للتطوّر التكنولوجي اليوم في مجال ظاهرة الإجرام هو الجريمة الالكترونية.

2. موقف المشرّع الجزائري من الجريمة الالكترونية

نتيجة التطوّر الهائل في عالم التكنولوجيا، خصوصا مجال المعلوماتية ووسائل الاتصال وما تتيحه شبكة الانترنيت، برزت مشاكل قانونية، ذلك أنّه ظهرت جرائم جديدة وجب علاجها ومواجهتها ولا يتأتّى ذلك إلا من خلال نصوص قانونية، فالقاضي لا يُجرّم أفعالاً أو يُسلّط عقوبات إلاّ بنص. واسْتِتْبابا للأمن وتوفير الحماية وسدّ الفراغ القانوني من هذا الجانب، حاول المشرّع الجزائري استحداث آليات قانونية من شأنها الحدّ

---

[2] . هاني رزق، خالص جبلي، الإيمان والتقدم العلمي، ط1، دار الفكر المعاصر، بيروت، دار الفكر، دمشق، 2000م، ص 315.

[3] . ليزا سعيد، التقدم التكنولوجي: هل جعلت التكنولوجيا حياتنا أيسر أم أسعد؟ ، https://www.ts3a.com/?p=30551 ، يوم 2022/07/29م.

[4] . السيد عوض، التطوّر التكنولوجي والجريمة، أعمال المؤتمر السنوي الرابع والثلاثون، قضايا السكان والتنمية، 19 . 22ديسمبر 2004م، المركز الديموجرافي بالقاهرة، http://swideg-geography.blogspot.com/2018/03/blog-post_38.html#.YvaI21xBzIU 2022/07/29م.

من مثل هكذا جرائم والوقاية منها من خلال الأمر رقم 04 .15[5]، والقانون 09. 04[6]،والقانون رقم 08 . 01[7] والقانون رقم 18 .05[8] ...فضلا عن القواعد أو النصوص العامة التي تَحْظُر الإضرار والتعدّي على الغير.

وبالرجوع للمادة 2 من القانون 09 . 04 السالف الذكر نجد أنّ المشرّع الجزائري اختار اسم الجرائم المتّصلة بتكنولوجيات الإعلام والاتصال مُعرِّفا إيّاها بقوله: " يقصد في مفهوم هذا القانون بما يأتي: الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".

وهذا التعريف الذي أورده المشرّع الجزائري تعريف مرن يشمل عدد من الجرائم، فيكفي أن ترتكب الجريمة عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية، ليرسم لنا المشرّع الجزائري صور الجرائم المتعلّقة بتكنولوجيات الإعلام والاتصال من خلال المواد 394 مكرر إلى غاية 394 مكرر 8 الواردة في القانون 04 . 15 والقانون 16 . 02[9] والتي يُمكن بيانها بشيء من التفصيل الموجز فيما يأتي:

- الدخول أو البقاء داخل منظومة معلوماتية عن طريق الغش.
- حذف أو تغيير لمعطيات المنظمة.
- إدخال بطريق الغش معطيات في نظم المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.
- كلّ من يقوم عن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها.
- إنشاء أو تكوين جماعة أشرار.

وتجدر الإشارة إلى أنّ وعي المشرّع الجزائري واستشعاره لخطورة هذا النوع المستحدث من الجرائم، جعله يقوم بتعديل عام 2006م في قانون العقوبات بموجب القانون 06 .23 الذي تمّ من خلاله تشديد العقوبة على الأفعال أو الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات، ليستحدث عام 2016م نصا جديدا يتعلّق

---

[5] . القانون رقم 04-15 المؤرّخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدّل والمتمّم للأمر رقم 66-156 المتضمّن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم71.

[6] . القانون رقم 09-04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمّن القواعد الخاصّة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 47.

[7] . القانون رقم 08- 01 المؤرخ في 15 محرم عام 1429هـ، الموافق لـ 23 يناير سنة 2008م، يتمم القانون 83 . 11 المؤرخ في 2 يوليو 1983م، والمتعلق بالتأمينات، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 4.

[8] . القانون 18- 05 المؤرخ في 24 شعبان عام 1439هـ الموافق 10 مايو سنة 2018م، يتعلق بالتجارة الالكترونية، الجريدة الرسمية للجمهورية الجزائرية عدد رقم28.

[9] . القانون 16- 02 المؤرخ في 14 رمضان 1437هـ الموافق لـ19 يونيو 2016م يتمم الأمر رقم 156.66 المؤرخ في 8 يونيو 1966م والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 37.

بالمادة 87 مكرر 12والتي نصت على جريمة جديدة تمثّلت في جناية تجنيد الأشخاص لصالح إرهابي أو منظومة إرهابية باستخدام وسائل تكنولوجيا الإعلام والاتصال.

أمّا على مستوى قانون الإجراءات الجزائية للجرائم المتعلّقة بتكنولوجيات الإعلام والاتصال فإنّ متابعتها تتمّ بنفس الإجراءات التي تُتّبع بها الجرائم التقليدية، لكن جديد المشرع الجزائري هو تمديده الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية من خلال المادة 37 من القانون 17 .07.[10] وكذلك ما نصت عليه المادة 45 في فقرتها الأخيرة من قانون الإجراءات الجزائية 06. 22[11] التي اعتبرت أنّ التفتيش الذي يكون على مستوى المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة. كما نصت المادة 51 فقرة 6 من القانون 06 . 22 السالف الذكر على التوقيف للنّظر في جريمة المساس بأنظمة المعالجة، وكذا اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في المادة 65 مكرر 5 إلى 10 مكرر من نفس المادة[12]. أمّا بالنسبة لباقي الإجراءات من تحقيق ومحاكمة فإنّها تطبق نفس إجراءات الجريمة التقليدية.[13]

مع التنويه هنا أنّه تعدّدت تعريفات هذا النوع من الجرائم ــ ولا نرى من المناسب بَسْطهاــ كما تعدّدت تسمياتها للدّلالة على حقيقة المسمّى، نظرا لتقارب المفاهيم وتداخلها كما في الغش المعلوماتي أو الإجرام الالكتروني، والانحراف الذي يقع بواسطة الحاسب الآلي أو الإنترنت...، فهل الجريمة الالكترونية تحوي الجريمة المعلوماتية أو العكس؟ [14] والذي نراه أنّ مصطلح الجريمة الالكترونية هو الأصوب، ذلك أنّها أدق وأوسع تشمل أي وسيلة إلكترونية فضلا عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات على الحاسوب أو بواسطتها كما أشار إليها المشرّع الجزائري، في حين أنّ الجريمة المعلوماتية تقتصر على الجرائم الماسة بالانترنيت أو الحاسوب أو بواسطتهما فقط.

---

[10] . القانون 17-07 المؤرخ في 28 جمادى الثانية1438هـ الموافق لـ27 مارس 2017م،يعدل ويتمم الأمر رقم 66. 155 المؤرخ في 8 يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية العدد رقم 20.

[11] . القانون 06- 22 المؤرخ في 29 ذي القعدة 1427هـ الموافق لـ20 ديسمبر 2006ميعدل ويتمم الأمر رقم 66 . 155 المؤرخ في في 8يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية،العدد رقم 84.

[12] . الفصل الرابع بعنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور " من الباب الثاني للكتاب الأول من القانون 06 – 22 المعدل والمتمم للأمر رقم 66 . 155 المؤرخ في في 8يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 84، ص 8.

[13] . فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، أعمال المؤتمر الدولي الرابع عشر، طرابلس 24/24مارس2017م، ص 131.

[14] -نميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر، طرابلس 24/24مارس2017م، ص98.

بِيدَ أنّ أجود التعريفات وأوْفاها للجريمة الالكترونية هو ما ذكرته حبيباتني بثينة بأنّها: " كل سلوك غير مشروع تكون تقنية المعلومات وسيلة لارتكاب الجريمة، أو تكون موضوعا لها"[15] وهو تعريف ينسجم مع ما جاء به المشرّع الجزائري.

ثانيا . تصنيفات الجريمة الالكترونية وأهمّ المجالات التي استهدفتها في ظلّ جائحة كورونا كوفيد-19

اختلف الفقه الجنائي والقانون حول تقسيم الجرائم الالكترونية، باختلاف الزاوية التي يُنْظَر منها، فعلى سبيل المثال قد تكون الزاوية من مَنْظُور أنّ النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها، كما قد يكون النظام المعلوماتي هو موضوع أو محل الجريمة الالكترونية، إذ يطول المقام لذكرها ولا نرى ضرورة ذلك، حيث أنه كلّما ظهرت وسيلة جديدة برزت معها جريمة أو أسلوب جديد، فهي متغيرة ومتجّددة. لكن الملاحظ وعلى اختلاف تصنيفات الجريمة الالكترونية أنّها استهدفت جوانب وقطاعات بصفة خاصّة منذ ظهور فيروس كورونا كوفيد-19[16]، نحاول أن نتعرّف على أهمّها بعد أن نستعرض أبرز تصنيفات الجريمة الالكترونية.

1 . تصنيفات الجريمة الالكترونية

سبق القول أنّ تصنيف الجريمة الالكترونية يعود إلى اعتبارات، نذكر منها:

أولا . الجرائم الواقعة بواسطة النظام المعلوماتي: يشتمل هذا التصنيف على أهمّ الجرائم التي تتّصل بالمعلوماتية. والحاسب الآلي في هذه المجموعة وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، يهدف الجاني عادة من وراء ارتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعة، فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته أو برامجه أو نظمه كوسيلة لتنفيذ الجريمة، ومنه لا يكون النظام المعلوماتي هو محل الحماية الجنائية[17] وتقّسم الجرائم بموجب هذا الاعتبار إلى:

أ. الجرائم الواقعة على الأشخاص: تعّددت مظاهر الجرائم الواقعة على الأشخاص، وتعتبر نشر الإباحية والجنس خصوصا عند الأطفال من أهمّها، حيث يتعرّض الأطفال للاستغلال الجنسي على الانترنت بأشكال متعدّدة انطلاقا من الصوّر إلى التسجيلات المرئية للجرائم الجنسية العنيفة، حيث تستمر معاناتهم إلى ما بعد

---

[15] . حبيباتني بثينة، الطبيعة الخاصة للجريمة المعلوماتية، مجلة دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، المجلد12، العدد3، 2020م، ص 609.

[16] - فيروسات كورونا هي مجموعة من الفيروسات التي يمكن أن تصيب الإنسان والحيوان على حدّ سواء، مُسَبِّبة اعتلالات متنوعة، قد تكون خفيفة كنزلات البرد، أو شديدة مثل الالتهاب الرئوي، كمرض سارس (المتلازمة النفسية الحادة الوخيمة) الذي انتشر مابين 2002م و2003م، أو متلازمة الشرق الأوسط التنفسية mers التي ظهرت في 2012م. أمّا كوفيد .19 هو مرض مُعْد، يُسَبِّبه فيروس كورونا، وكمصطلح فهو يتكون من عدّة أجزاء، يحمل كلّ جزء معنى، حيث أنّ: "كو" هو اختصار كورونا، و "في" اختصار لفيروس، و" د" اختصار للداء أو المرض، ورقم 19يشير إلى العام الذي أُعلن فيه عن تفشي هذا المرض الجديد، الذي كان في نهاية ديسمبر 2019م، بداية من مدينة ووهان الصينية. ويطلق البعض عليه تسمية المتلازمة التنفسية الحادة الوخيمة كورونا 2، أو سارز كوف2.

[17] . سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010م،2011م

ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنت[18]، كما أنّ جريمة التهديد والمضايقة والملاحقة خاصة عن طريق البريد الالكتروني أو وسائل الحوارات الآنية عبر شبكة الانترنت كالفايسبوك أو الواتساب ...عرفت انتشارا واسعا، بالإضافة إلى جرائم التغرير والاستدراج وانتحال الشخصية التي أطلق عليها البعض جريمة الألفية الجديدة(سواء انتحال شخصية الفرد، أو انتحال شخصية المواقع) [19] ونفس الأمر يقال عن جرائم السب والقذف الأكثر شيوعا لتلطيخ سمعة الغير والمساس بشرفهم وكرامتهم من خلال غرف الدردشة، أو مقاطع فيديو أو تطبيقات التيك توك ...، الأدهى أنّه يتم تداولها ونشرها عبر المواقع حتّى وإن كانت مغلوطة أو غير صحيحة.

ب . الجرائم الواقعة على الأموال: ويدخل في التقسيم جرائم معتبرة خصوصا مع التطوّر التكنولوجي الحاصل، حيث أخذت وسائل الدفع الالكتروني كالبطاقات الذهبية أو البنكية حيزا من جرائم القرصنة والسرقة والاحتيال والتحويل الالكتروني من حساب بطاقة عميل إلى حساب أو رصيد آخر؛ باعتبارها نقودا إلكترونية، من خلال إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريق غير المشروع عبر قنوات شبكة الانترنت. [20]

ومن أهمّ الجرائم الالكترونية على الأموال، جريمة القمار وغسيل الأموال عبر الانترنت من خلال الكازينوهات الافتراضية وأندية الأقمار الرقمية، إذ أنّها تمنح الراغب ممارستها الخصوصية وخفاء الشخصية، بالإضافة إلى جريمة المخدرات عبر الانترنت والتي لم تعد المواقع تروّج لها أو تُشَوّق النشء لاستخدامها فقط، بل إلى كيفية زراعتها وصناعتها بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة.[21]

ج . الجرائم الواقعة على أمن الدول

استغلّت الكثير من الجماعات المتطرّفة الطبعة الاتصالية للإنترنت من أجل بث معتقداتها وأفكارها، ليصل بها الأمر إلى ممارسات تهدّد أمن الدولة، ممثلة في الإرهاب الالكتروني والجريمة المنظّمة، فقد أتاحت الانترنت لكثير من الدول ممارسة التجسّس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية والاقتصادية ...، كما أعطت الانترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما سهل وجرّ إلى نزاعات وفوضى.[22] لتظهر العلاقة جليا بين الإرهاب والجريمة الالكترونية من خلال تجنيد وتجييش أعضاء جدد في التنظيم أو حشد الهمم بواسطة استخدام مختلف وسائل التواصل الالكتروني، كما

---

[18] . نميدلي رحيمة، خصوصية الجريم الإلكترونية في القانون الجزائري والقوانين المقارنة، المرجع السابق، ص102.

[19] . صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2013م، ص 50، 51.

[20] . خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2010م، ص 67.

[21] . صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2013م، ص 46، 49.

[22] . بوضياف إسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 3، العدد3، 2018م، ص 358.

يتم تبني الدعاية والعمليات الإرهابية من خلال مختلف وسائط التواصل الالكترونية[23] كما أنّ أعضاء الجريمة المنظمة استفادوا من وسائل الاتصال والتكنولوجيا التي لم تعد تعترف بالحدود الجغرافية في تخطيط وتمرير وتوجيه المخططات وتنفيذ العمليات الإجرامية بيسر وسهولة[24].

ثانيا . الجرائم الواقعة على النظام المعلوماتي: وهذا الصّنف من الجرائم يمسّ النظام المعلوماتي، حيث تكون المكونات المادية له، أو المعلومات المدرجة به هدفا يتوصّل إليه، نوضّحها بشيء من الإيجاز كما يلي:

أ . الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

يُقصد بالمكوّنات المادية للنظام المعلوماتي بالأجهزة والمعدّات الملحقة به والتي تستخدم في تشغيله، كالأسطوانات والشرائط والكابلات. ونتيجة للطبيعة المادية لهذه المعدّات تكون الجرائم الواقعة عليها تقليدية كأن تكون محل للسرقة وخيانة الأمانة أو الإتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل، ممّا يترتّب عليها خسائر كبيرة، ولقد حدث هذا النوع من الجرائم في فرنسا، وأدى إلى إتلاف معدّات مؤسّسة كبيرة ومتخصّصة في بيع الأنظمة وتوثيق المعلومات الحسابية، وقُدّرت الخسائر ب5 ملايين فرنك فرنسي.[25]

ب –الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

تُعتبر المعلومة المعالجة آليا ذات أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي، لما لها من قيمة اقتصادية، وتتّم الجرائم عليها من خلال التلاعب فيها بصفة مباشرة أو غير مباشرة أو عن طريق إتلافها أو استبدالها أو محوها، وهذا ما يسمّى بالغش أو التزوير المعلوماتي، فقد قام شخص وهو موظّف بوزارة المالية باستخدام طريقة تدعى BLUFF، حيث قام بإدخال فواتير وهمية لا حصر لها وتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي قام بإنشائها.[26]

ج . الجرائم الواقعة على البرامج الالكترونية[27]: هي جرائم تتطلّب مهارة فنية عالية في مجال البرمجة وتقع على البرامج التطبيقية أو برامج التشغيل.

. الجرائم المعلوماتية الواقعة على البرامج التطبيقية: يحدّد فيها الجاني البرنامج أولا، ثمّ يقوم بالتلاعب فيه لتحقيق أكبر استفادة مالية، وهذا من خلال قيامه بتعديل البرنامج أو التلاعب في البرامج. أما تعديل البرنامج فعادة ما يكون هدفه الرئيس اختلاس النقود، مثاله قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل البرنامج عن طريق إضافة دولار واحد على كل حساب يزيد عن عشر دولارات ،ثم قيامه بقيد هذه المصاريف الزائدة في حساب خاص به يتحصل على إثره على مئات الدولارات خلال كل شهر. أما التلاعب في البرنامج فإنّه يأخذ عدّة أشكال وصور فقد يتم عن طريق ما يُسمّى بالقنبلة المنطقية المتمثلة في برنامج

---

[23] . رحموني محمد، خصائص الجريمة الالكترونية ومجالاتها، مجلة الحقيقة، المجلد 16، العدد3، 2018م، ص448.

[24] . سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر العربي، الإسكندرية، 2007م، ص83.

[25] - بوضياف إسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، المرجع السابق، ص 359.

[26] - نميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المرجع السابق، ص104.

[27] . خلدون عيشة، محاضرات الجريمة المعلوماتية، موجهة لسنة أولى ماستر تخصّص القانون الجنائي والعلوم الجنائية، ص14.

أو جزء من برنامج ينفذ في كل لحظة أو كل فترة زمنية منتظمة يوضع في شبكة معلوماتية بغرض تسهيل عمل غير مشروع، أو عن طريق قيام أحد المبرمجين بزرع برنامج فرعي غير مسموح به في البرنامج الأصلي ممّا يسهّل له عملية الدخول الغير مشروع في العناصر الضرورية لأيّ نظام معلوماتي مع ملاحظة صعوبة اكتشافه بسبب صغره ودقّته.

. الجرائم المعلوماتية الواقعة على برامج التشغيل: برامج التشغيل هي البرامج المسؤولة عن عمل النظام المعلوماتي حيث تقوم بتنظيم وضبط ترتيب تعليماته الخاصة، جريمته تتّم بتزويد البرنامج بتعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسهل الحصول على معلومات النظام وتتّم بالمصيدة بإعداد المبرمج لبرنامج به عيوب وأخطاء عمدا للدخول إليه بسهولة، فهي ممرات خيالية وفواصل وتفرعات في البرنامج تمكّنه من تنفيذ التعديلات الضرورية تمكنه من الدخول للنظام المعلوماتي والوصول إلى معلومات الذاكرة، أو تتم بتصميم برنامج وهمي وذلك بقيام المبرمج بوضع برنامج يصعب اكتشافه مخصص لارتكاب الجريمة ومراقبة تنفيذها.

ثالثا . تصنيف اتفاقية بودابست

لعلّ أهم تصنيف هو الذي جاءت به الاتفاقية الأوربية لمكافحة الجريمة الالكترونية وهي اتفاقية بودابست، والذي يتضمّن أربع مجموعات:

المجموعة الأولى: الجرائم التي تستهدف سرية وسلامة وتوفر المعطيات والنظم، وتشمل:

- الدخول غير قانوني (غير المصرح به).
- الاعتراض غير القانوني.
- تدمير المعطيات.
- اعتراض النظم.
- إساءة استخدام الأجهزة. [28]

المجموعة الثانية: الجرائم المرتبطة بالكمبيوتر، أي الجرائم التي يلعب فيها الكمبيوتر أو الحاسوب الآلي دور الوسيلة كجرائم الاحتيال والتزوير الالكتروني.

المجموعة الثالثة: الجرائم المرتبطة بالمحتوى، حيث يلعب فيها الكمبيوتر دور البيئة الإجرامية، وتتعلّق الجرائم بالأفعال اللاأخلاقية وجرائم القمار وغسيل الأموال والمخدرات.[29]

المجموعة الرابعة: وهي الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة – قرصنة البرمجيات.[30]

---

[28] . يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – أبو ظبي 10-12 /2/2002م،
http://almuhamatresalah.blogspot.com/2014/03/blog-post_2785.html يوم 2022/07/30م

[29] . نميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المرجع السابق، ص 105.

[30] . يونس عرب، جرائم الكمبيوتر والانترنت، المرجع السابق.

2. أهمّ المجالات التي استهدفتها الجريمة الالكترونية في ظلّ جائحة كورونا

سَجَّلت الجريمة الالكترونية في السنوات الأخيرة ارتفاعا ملحوظا، لتتبلور أكثر خلال الأزمة الصّحّية العالمية فيما يعرف بجائحة كورونا، ويبدو أنّ هناك أنشطة ومجالات كانت مُستهدَفَة أكثر من غيرها خلال هذه الفترة الوبائية، يمكن أن نبيّنها فيما يلي:

المجال الصّحي: يعتبر القطاع الصّحي من أكثر القطاعات تضرّرا من الجريمة الالكترونية، ففي ضوء الطلب المتزايد على منتجات الحماية الشخصية والنظافة الصحية، استغل المجرمون هذا الظرف لجني الأرباح وتحقيق الكسب المادي عن طريق بيع منتجات مقلّدة أو لا تستوفي المعايير المطلوبة مثل الكمامات الجراحية ومضادات الفيروس والفيتامينات، وحتّى أدوية وهمية لعلاج فيروس كورونا، وأحيانا أخرى سرقتها، لتزدهر مبيعات المنتجات الصحية المزيّفة والمعقّمات المزوّرة عبر المواقع الالكترونية والاشهارات على مختلف شبكات الاتصال والتواصل. كما في حالة إحدى الشركات الأوروبية التي طلبت مواد حماية، من بينها أقنعة ومعقّمات ومطهّرات من شركة في سنغافورة مقابل 6.6 ملايين يورو، لكنّ البضاعة لم تصل، ذلك أنّ هناك عصابات قامت باختراق أنظمة الشركة واستولت على المبيعات. وفي عملية مشتركة للشرطة الأوروبية، بالتعاون مع 90 دولة، أسفرت عن مصادرة 34 ألف كمامة مزيفة على مستوى العالم، فضلاً عن العثور على 4.4 ملايين عقار مقلدا، بعدما جرى اكتشاف 37 عصابة واعتقال 121 شخصاً، كما جرى تحديد أكثر من 2000 موقع إلكتروني يعرض مواد معقّمة غير فعّالة ضد الفيروس، وجرت مصادرة 4 ملايين وحدة دواء وأجهزة تنفس وهمية ضمن عمليات للشرطة الأوروبية.[31] كما استهدف مجرمو المعلوماتية ولصوص الحظر أنظمة المؤسّسات الصحية واختراقها ظنّا منهم أنّ هذه المؤسّسات ستضطر إلى دفع المال أو الفدية لاستعادة أنظمتها. فقد تعرّض مستشفى في جمهورية التشيك لهجوم إلكتروني، وفقاً لـ"يوروبول"، ما اضطر المستشفى لوقف نظام تكنولوجيا المعلومات لديه، ما أجّل المعاملات الطبية.[32]

المجال المالي: يعدّ هذا المجال هو الآخر ممّن استهدفه مجرمو ومخترقو المعلوماتية، من خلال عمليات السرقة التي تتم عبر ماكينات الصرف الآلي والبنوك باعتماد نسخ البيانات واستخدامها لنهب وسحب أموال الضحية، أو إنشاء مواقع في صفحات الانترنت مماثلة للمؤسّسات المصرفية أو البنكية، ومطالبة العميل إدخال بياناته، ومن ثَمّ سرقتها. أو من خلال رسائل البريد الالكتروني، فكثيرا ما تأتي رسائل من مصادر مجهولة بخصوص طلب المساهمة في تحويل الأموال من الخارج مع الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد الالكتروني بفوزه بإحدى الجوائز وتطالب بموافاة الجهة برقم حسابه المصرفي.[33] خصوصا أنّ الجزائر وغيرها من الدول شجّعت في فترة انتشار فيروس كورونا على استعمال البطاقات البنكية أو الذهبية... تفاديا للاحتكاك بين المواطنين، وهذا ما استغله قراصنة المعلوماتية. فقد كشفت تقارير

---

[31] . ازدهار سوق المنتجات الطبية والوقائية المزيفة في زمن كورونا، https://www.alaraby.co.uk/ 2022/07/30م.

[32]. ازدهار سوق المنتجات الطبية والوقائية المزيفة في زمن كورونا، https://www.alaraby.co.uk/2022/07/30م.

[33] . محمود شرقي، صلاح الدين جبار، تأثير تطور تكنولوجية المعلوماتية على تنامي الجريمة، https://www.asjp.cerist.dz/en/downArticle/354/8/1/62499 2022/07/30م.

مختصّة بأمن المعلومات أنّ مخترقون استهدفوا أشخاصا ومؤسّسات من خلال روابط مشبوهة للحصول على بيانات الدخول إلى الحسابات المالية، وأنشؤوا أكثر من 100 ألف نطاق جديد لمواقع إلكترونية عن كوفيد19، في محاولة خداع الأفراد كي يسجلوا بياناتهم.[34] وفي تقرير آخر تعرّضت شبكة "بولي نت وورك" العاملة كمنصة لتداول العملات الافتراضية المشفرة، إلى اختراق من جانب مجهولين، تمكنوا خلاله من سرقة عملات بقيمة 600 مليون دولار.

وذكرت الشبكة في سلسلة تغريدات عبر صفحتها على "تويتر" أنّ السرقة جَرْت بعد قيام مجهولين باختراق أنظمتها الأمنية، داعية عملاءها لتجنّب أية مراسلات تتضمّن رموزا مشفرة.[35]

المجال الترفيهي للألعاب الالكترونية: أجبر الوباء الناس على البقاء في منازلهم ممّا جعلهم يلجؤون إلى العالم الافتراضي بعيدا عن الأزمة الصحية العالمية، من خلال الألعاب الالكترونية خاصّة، التي توسّع استعمالها خلال أزمة الوباء العالمي إلى حدّ الإدمان، وتعتبر فئة الأطفال أكثر الضحايا من هذه الناحية.

ولطالما استغل المحتالون المتخفيّون بفيروس كورونا الوضع، ومثال ذلك استغلالهم الألعاب الأونلاين وأصبحت هدفا ثمينا لهم، نظرا لأنّها تتضمّن عُملات ومشتريات داخل الألعاب إلى جانب العُملات الحقيقية الموجودة في المحافظ.

بالإضافة إلى خطر الألعاب الالكترونية من جهة إدمانها وفَقْد المال، هناك مخاطر أخرى، في مقدّمتها احتواء هذه الألعاب على برامج ضارة، ففي بعض الأحيان يحتاج المستخدّم إلى تنزيل مكوّن برمجي إضافي من أجل تشغيل لعبة معيّنة، وقد يتم إعادة توجيهه بعد ذلك إلى مواقع أخرى حيث يُمْكن للبرامج الضارة فيها إلحاق الأذى بأمان جهاز المستخدم وخصوصيته. أيضًا قد تكون الفيروسات مضمَّنة في ملفات اللعبة التي قد يسمح المستخدم بتنزيلها على النظام دون أن يدري أثناء التثبيت. كما أنّ من مخاطر الألعاب الأونلاين انتهاك الخصوصية عن طريق جمع البيانات من الألعاب وغيرها من المصادر، فقد يتمكّن المتسلّلون من الوصول إلى حسابات أخرى لك، مثل حساباتك على مواقع التواصل الاجتماعي، أو إنشاء حسابات جديدة باسمك، بل وحتى إنشاء هويات رقمية كاملة باسمك[36]! والأخطر في الألعاب الالكترونية أنّ بعضها تدفع بالانتحار، وخير مثال لعبة الحوت الأزرق وهي تطبيق يُحمّل على أجهزة الهواتف الذكية وتتكوّن من 50 مهمة، تستهدف المراهقين بين 12 و16 عاماً، وبعد أن يقوم المراهق بالتسجيل لخوض التحدي، يُطلب منه نقش الرمز التالي "F57" أو رسم الحوت الأزرق على الذراع بأداة حادة، ومن ثَمَ إرسال صورة للمسؤول للتأكّد من أنّ الشخص قد دخل في اللعبة فعلاً، بعد ذلك يُعطى الشخص أمراً بالاستيقاظ في وقت مبكر

---

[34]. دبي للمستقبل، توجهات عالمية لتعزيز الأمن الرقمي وتبني الذكاء الاصطناعي لحماية القطاعات https://pressn.net/article/8564830?news 2022/07/30م.

[35] . منصة عملات مشفرة تتعرّض للاختراق وسرقة 600 مليون دولار، https://www.alaraby.co.uk/economy 2022/07/29م.

[36] . عمليات النصب المتعلقة بالألعاب الأونلاين في ظل انتشار فيروس كورونا: سبل لحمايتك وعائلتك، https://me.kaspersky.com/resource-center/threats/coronavirus-gaming-scams 2022/08/02م.

جداً، عند 4:20 فجراً مثلاً، ليصل إليه مقطع فيديو مصحوب بموسيقى غريبة تضعه في حالة نفسية كئيبة. وتستمر المهمات إلى أن يصل اليوم الخمسون، الذي يُطلب فيه منه الانتحار إما بالقفز من النافذة أو الطعن بسكين[37] ونتيجة للأرواح التي حصدها هذا التطبيق في العالم والجزائر خصوصا، أطلقت الجزائر حملة توعوية في المدارس والمساجد وعبر وسائل الإعلام من خطورة لعبة الحوت الأزرق، لتقرّر في الأخير حجب هذه اللعبة من المواقع الالكترونية. والأكيد لولا الحملات التحسيسية وقرار الحجب لهذه اللعبة ومثيلاتها قبل جائحة كورونا لكانت الكارثة.

. مجال الدردشة والاجتماعات والمؤتمرات عبر المنصّات الرقمية: تعرّضت هي الأخرى المحادثات الالكترونية إلى الاختراق وظهرت فيها ثغرات أمنية استغلها لصوص الحظر، تمّ تحذير الملايين من مستخدمي «Microsoft Teams» من هجوم جديد يمنح المتسللين سيطرة كاملة على أجهزة الكمبيوتر الخاصة بهم، حيث لجأ الكثيرون إلى هذا التطبيق لعقد الاجتماعات من خلال الإنترنت، منذ اندلاع وباء فيروس كورونا، وتضمّ المنصة الآن أكثر من 270 مليون مستخدم نشط شهريًا، يستهدف المتسلّلون الاجتماعات عبر الإنترنت بالبرامج الضارة، ووفقًا لفريق الأمان فيAvanan، بدأ المتسلّلون مهاجمة مستخدمي «Microsoft Teams» عبر ملفات exe الضارة المُضَمّنة في سلاسل المحادثات. وبمجرد التنزيل، يبدأ المتسلّلون في مهاجمة أجهزة الكمبيوتر وتثبيت البرامج الضارة التي تمنحهم وصولاً كاملاً إلى الجهاز وكلّ ما يتم تخزينه عليه.[38] وفي نفس السياق فقد اكتشف أحد الباحثين عيبين جديدين في تطبيق مؤتمرات الفيديو Zoom يسمحان للهاكرز باختراق كاميرا الويب للمستخدمين وميكروفونهم، ووفقا لما ذكرته صحيفة "ديلى ميل" البريطانية، سمحت هذه الثغرات التي تم تحديدها سابقًا للهاكرز بسرقة كلمات مرور Windowsوأيضًا اختراق أمان آخر للأمن على أجهزة Mac من خلال السماح لهم بالاستفادة من كاميرا الويب والميكروفون للمستخدمين. وكشف التقرير حاليا عيوب جديدة في تطبيق مؤتمرات الفيديوZoom، تَعْرضُ الصوت ومقاطع الفيديو. كما أنّ هناك خطأ ثانٍ تمّ تحديده بواسطة واردل، والذي يتضمّن أيضًا الوصول المادي إلى الجهاز، الذي يضرّ بتدفّق الصوت والفيديو فيZoom حيث يعمل الهاكرز من خلال إدخال شفرة ضارة فيZoom، وبالتالي يتمكّنوا من خداع الخدمة لتسليم كاميرا الويب والوصول إلى الميكروفون لمستخدم آخر.[39] كما حذّر مكتب التحقيقات الفدرالية الأميركي المواطنين من الاختراق الذي يحدث عبر تطبيق الاجتماعات "زوم" الشهير، وذلك بعد أنْ تمَّ اختراق فصلين دراسيين على الشبكة أثناء استخدام مكالمات الفيديو. وقالت وسائل إعلام أميركية إنّ "زوم" شهد زيادة هائلة في عدد المستخدمين منذ

---

[37]. هديل كرنيب ما هي لعبة الحوت الأزرق التي "تدفع بالأطفال إلى الانتحار"؟
https://www.annahar.com/arabic/article/713833 2022/08/02م.

[38] . كلود عمر، لمستخدمي» ..Microsoft Teams هاكرز» يتبعون حيلة لاختراق الهواتف عن طريق التطبيق،
https://lite.almasryalyoum.com/technolight/259934 2022/08/02م.

39 . اكتشاف ثغرات جديدة بـ Zoom تتيح للمتسللين اختراق الكاميرا والميكروفون
https://www.youm7.com/story/2020/4/3 2022/08/02م.

أنْ أجبر وباء كورونا عددا كبيرا من الأشخاص على البقاء في منازلهم، واللجوء إلى اجتماعات الفيديو للعمل أو الدراسة أو التفاعلات الاجتماعية.[40]

ثالثا . عوامل انتشار الجريمة الالكترونية زمن تفشي فيروس كورونا كوفيد-19 وأبرز التدابير التي اتّخذتها الجزائر لمكافحته

هناك عوامل مختلفة ومتداخلة أسْهمت في تنامي الجريمة الالكترونية، ولعلّ الوضع الوبائي وما صاحبه من إجراءات كان له نصيب كبير في تفاقمها، نبيّن في هذه النقطة من الدّراسة بعض التدابير التي اتّخذتها السلطات التشريعية لمكافحة انتشار فيروس كورونا كوفيد-19، لنعرّج بعدها على عوامل انتشار هذه الجريمة في ظلّ هذه التدابير وتداعيات الفيروس.

1- أبرز التدابير التي اتّخذتها الجزائر لمواجهة انتشار فيروس كورونا كوفيد-19

انتشر فيروس كورونا كوفيد-19 بالجزائر وانتقل إلى مواطنيها، حيث تمّ الإعلان عن أول حالة في 25 فيفري 2020م لرعية إيطالي كان يعمل بحقل نفط في حاسي مسعود، لتتوالى فيما بعد الإصابات بهذا الفيروس، ما جعل رئيس الجمهورية يأمر على جناح السرعة بغلق المعاهد والمؤسّسات التعليمية وروضات الأطفال. وبعد أن تجاوز عدد المصابين 27 خلال الفترة 16، 17 مارس 2020م، تمّ تعليق كافة الرحلات الجوية نحو أوروبا، كما أمر وزير الشؤون الدينية والأوقاف بغلق المساجد ومنع صلاة الجمعة عبر كافة التراب الوطني... وفي ظلّ تزايد عدد الإصابات وعدم وجود لقاح أو دواء لهذا الفيروس، تمّ إصدار مجموعة من التدابير الصحية لتطويق هذا الفيروس وكبح انتشاره، ويأتي في مقدّمتها المرسوم التنفيذي رقم 69/20[41] والمرسوم 70/20[42] والمرسوم رقم 127/20[43] ومن أبرز ما جاء فيها:

. غلق محلات بيع المشروبات، ومؤسّسات وفضاءات الترفيه والتسلية والعرض والمطاعم باستثناء تلك التي تضمن خدمة التوصيل إلى المنازل.

. تقليص عدد الموظفين وتعليق النقل الجماعي وغلق المقاهي ومنع التجمعات.

---

[40] . المؤسس يعترف بالتقصير.. القراصنة يقصفون تطبيق "زوم" وشركات كبرى تمنع العمل به، https://www.aljazeera.net/news/scienceandtechnology/2020/4/2 2022/08/02م.

[41] . المرسوم التنفيذي رقم 69/20، المؤرخ في26 رجب 1441هـ، الموافق لـ21 مارس 2020م المتعلق بتدابير الوقاية من انتشار وباء فيروس كورونا كوفيد19 ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد15.

[42] . المرسوم التنفيذي رقم 70/20 المؤرخ في 29رجب 1441 هـ، الموافق 24 مارس 2020 م، الذي يحدّد تدابير تكميلية للوقاية من انتشار وباء فيروس كورونا كوفيد 19 –ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 16.

[43] . مرسوم تنفيذي رقم 127/20 مؤرخ في 27 رمضان 1441هـ، الموافق لـ20 ماي 2020م، يعدّل ويتمم المرسوم التنفيذي رقم 70/20 الذي يحدد التدابير التكميلية للوقاية من انتشار وباء فيروس كورونا كوفيد19 ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 30.

. الحجر المنزلي، والذي يكون كليا أو جزئيا[44] ولفترات محدّدة، حسب الوضعية الوبائية للولاية أو البلدية المعنية.

. احترام التباعد الأمني بين شخصين في الأماكن العامة والعمل بمتر واحد على الأقل.

. ارتداء القناع الواقي.

. منح تراخيص لتنقل الأشخاص خارج أوقات الحجر على سبيل الاستثناء من قبل لجان مختصة.

. تعريض الغير للخطر بنقل عدوى فيروس كورونا كوفيد19 يعاقب عليه القانون. وقد أحال المرسومين التنفيذيين 70/20 والمرسوم 127/20 السالفين الذكر، إلى تطبيق الجزاءات على المخالفين إلى أحكام قانون العقوبات بموجب المادة 8 من القانون 06/20 المعدل والمتمم لقانون العقوبات[45] بموجب المادة 290مكرر، والتي نصت " يعاقب بالحبس من ستة(6) أشهر إلى سنتين(2) وبغرامة من 60.000دج إلى 200.000دج كل من يعرض حياة الغير أو سلامته الجسدية مباشرة للخطر بانتهاكه المتعمد والبيّن لواجب من واجبات الاحتياط أو السلامة التي يفرضها القانون أو التنظيم. تكون العقوبة الحبس من ثلاث(3) سنوات إلى خمس(5) سنوات والغرامة من 300.000دج إلى 500.000دج، إذا ارتكبت الأفعال المذكورة أعلاه خلال فترات الحجر الصحي أو خلال وقوع كارثة طبيعية أو بيولوجية أو تكنولوجية أو غيرها من الكوارث. يعاقب الشخص المعنوي الذي يرتكب الجريمة المنصوص عليها فيهذه المادة وفقا للأحكام المنصوص عليها في هذا القانون." والملاحظ من هذه المادة أن العقوبات الجزائية المقرّرة لجريمة تعريض الغير للخطر تتفاوت بين الشخص الطبيعي والمعنوي، كما أنّها تتفاوت فيما إذا كانت الظروف عادية أو إستثنائية.

2 ـ عوامل انتشار الجريمة الالكترونية زمن جائحة كورونا كوفيد-19

بالرجوع للأسباب التي شجعت أو كانت من وراء تنامي الظاهرة الإجرامية الالكترونية تحديدا نجدها متعدّدة فمنها ما هو اجتماعي ومنه ما هو اقتصادي، أمني ، نفسي... فضلا التدابير المتّخذة لمكافحة انتشار فيروس كورونا كوفيد -19 سواء على المستوى الوطني أو الدولي، يمكن أن نبيّنها إجمالا فيما يأتي:

- قضاء الكثير من الأفراد أوقاتهم في الحاسوب والهاتف نتيجة الحجر الصحي، ما أدى بوقوع عدد منهم في الاحتيال الالكتروني والانسياق وراء الاشهارات الالكترونية الكاذبة والتضليلية.
- الإقبال المنقطع النظير على أسواق التجارة الالكترونية والاعتماد على التسوق الالكتروني وخدمة التوصيل المنزلي، خصوصا بعد تشجيع الدول لها باعتبارها آلية آمنة من حيث انتشار فيروس كورونا

---

[44] . المادة 04 من المرسوم التنفيذي70/20" يتمثل الحجر المنزلي الكلي في إلزام الأشخاص بعدم مغادرة منازلهم أو آماكن إقامتهم خلال الفترة المعنية ماعدا في الحالات المنصوص عليها في هذا المرسوم. و/أو الفترات الزمنية المقررة من طرف السلطات العمومية. ويتمثل الحجر المنزلي الجزئي في إلزام الأشخاص بعدم مغادرة منازلهم أو آماكن إقامتهم خلال الفترة و/أو الفترات الزمنية المقررة من طرف السلطات العمومية.

[45] . قانون رقم 06/20 المؤرخ في 5 رمضان 1441هـ الموافق لـ28 أبريل 2020م يعدل ويتمم الأمر 156/66 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 25.

كوفيد-19، كونها تُجَنّب الاحتكاك المباشر والملامسة... ما أوقع بالكثير كضحايا لجرائم النصب والغش...

- الإفراج عن المحبوسين في السجون، حيث اتجهت بعض الدول إلى الإفراج عن المسجونين بتهم جنائية خطرة تخوّفاً من إصابات في صفوفهم بمرض "كورونا"، وهو ما دفعهم إلى ممارسة الإجرام مرة أخرى. ولعلّ الحالة التركية معبرة في هذا السياق، حيث كشفت بعض وسائل الإعلام التركية، مثل صحف "زمان" و"بيرجون" و"إيفرنسال"، عن الجرائم التي ارتكبها المجرمون المستفيدين من قرار العفو بعد إقرار البرلمان التركي لذلك، رغم التحذيرات التي أطلقها الخبراء من تداعيات الإفراج عن هؤلاء على الأمن الوطني[46].
- قلّة الوعي المعلوماتي والافتقار لثقافة الأمن والحماية الالكترونية.
- زيادة فترة استخدام شبكة الانترنت في ظل انتشار فيروس كورونا، خصوصا أنّ العمل والتعليم والتسوّق ...أصبحت تتم عن بعد، ما زاد معه عدد الاختراقات والهجمات الالكترونية.
- نجم عن القلق والخوف من فيروس كورونا كوفيد 19 الى لجوء الكثير بالبحث عن معلومات عبر شبكة الانترنت لتفادي الإصابة بهذا المرض، غير آبهين أو مدركين للفخاخ الالكترونية، ذلك أنه توجد مواقع بمجرد الدخول إليها يتم اختراق الأجهزة أو سرقة البيانات الشخصية، وهذا ما قام به المجرمين الالكترونيين في هذه الفترة من خلال المواقع والروابط.
- تركيز المؤسّسات العسكرية والأمنية على التدابير المتخذة لمواجهة انتشار كورونا كوفيد 19 ومدى التزام المواطن بها.
- ضُعْف الدخل وشيوع البطالة بسبب تدابير الحجر المنزلي وإجراءات التعليق والغلق التي مست بعض الأنشطة، ما أسفر عن انتشار عمليات النصب والخداع خصوصا عبر مواقع التواصل الاجتماعي.
- حبّ التحدّي واثبات التفوّق في مجال وسائل التقنية ونظام المعلوماتية، حيث أن بعض الأشخاص همهم وهدفهم هو الوقوف أمام شاشات الهاتف أو الحاسوب إثباتا لبراعتهم وقدرتهم على اختراق الأنظمة والمواقع والبرامج وما هو جديد في هذا المجال.
- اللجوء إلى الألعاب الالكترونية خاصّة الأطفال بسبب الحجر المنزلي والعطلة الطويلة التي عرفها قطاع التربية والتعليم تسبب في إدمانهم لهذه الألعاب، ما جعل الكثير من هذه الشريحة تصاب بالجنون والانهيارات العصبية والانتحار، من بينها لعبة "بوبجي" و"فري فاير"[47]
- التحسّن المستمر لشبكة الاتصالات والانترنت والاستعمال الواسع لها، خاصة في فترة تفشي فيروس كورونا كوفيد-19.

---

[46]. كيف أثر منع التجول على جرائم ما بعد "كورونا" في الإقليم؟، https://futureuae.com/m/Mainpage/Item/5571 2022/08/02م.

[47] . آمال عيساوي، ألعاب تصيب الأطفال بالجنون والانهيارات العصبية، https://www.echoroukonline.com/ 2022/07/30م.

- سهولة إخفاء معالم الجريمة الالكترونية وصعوبة الوصول إلى دليل واضح للإدانة أو كشف هوية الفاعل، في ظلّ سرعة محو أدوات الجريمة وتقاعس أو إحجام الكثير عن التبليغ عن الجرائم الالكترونية وقت ارتكابها والتي يرجع أحد أسبابها إلى تداعيات فيروس كورونا وانشغال الناس به.
- الخصائص التي تتميّز بها وسائل الاتصال الحديثة كالهواتف والحواسيب في تحقيق جرائم كثيرة، من سرعة وسهولة وتحرّر جغرافي باعتبارها عابرة للحدود، التي انجر عنها مشكلة الاختصاص القضائي كونها واقعة في فضاء إلكتروني والفاعل خارج الحدود.
- التهديد الأمني فيما يعرف بالإرهاب الالكتروني أو التجسس الالكتروني، والذي يكون عادة لزعزعة استقرار الدول من خلال الإشاعات والأفكار التي تنشر الفوضى.

رابعا . التطوّر التكنولوجي بين خدمة الظاهرة الإجرامية ومكافحتها فترة انتشار فيروس كورونا كوفيد -19

أربك تفشي فيروس كورونا كوفيد-19 العالم، وتغيّرت معه تفاصيل الحياة العادية، فأُغلقت الحدود والمطارات...وأصدرت حزمة من القوانين والمراسيم كتدابير لمواجهته؛ والجريمة ليست استثناء عن هذا التحوّل، فإغلاق الدول للحدود وانعزال الأشخاص في منازلهم بسبب الحجر المنزلي وجد المجرمون صعوبة في كسب المال بالطرق التقليدية في هذا الظرف الوبائي، ما جعلهم يلجؤون إلى سبل أخرى وفّرها لهم بالدرجة الأولى التطوّر التكنولوجي، فقد استعان هؤلاء بوسائل تكنولوجية وتقنيات حديثة لتنفيذ مخططاتهم وجرائمهم، فالهواتف والحواسيب وما توفره شبكة الانترنت أصبحت ملاذا لتنسيق أنشطتهم وتحقيق مآربهم نظرا لما تتميز به من سهولة وسرعة واختصار المسافات ....فعمليات السرقة مثلا أصبحت تتّم عبر أجهزة الكمبيوتر.

في خضّم الأزمة الصحية العالمية التي تسبّبت فيها جائحة كورونا رُفعت تقارير بناء على مؤتمرات عُقِدَت عبر دول العالم تفيد بتراجع الجرائم التقليدية كجرائم السطو على المنازل والسرقة والقتل إلى 50 بالمائة، بينما ازداد الاحتيال الإلكتروني وجرائم الإنترنت، ذلك أنّ الإجراءات الاستثنائية والاحترازية التي قامت بها الدول في أعقاب تفشي كورونا ساهمت في تراجع الجرائم التقليدية، إلاّ أنّ الجريمة المنظمة مثلا استطاعت أن تُبدي قدرًا من التكيف مع هذه المتغيرات واستغلال الأزمة وتوظيفها لتحقيق أهدافها والاستمرار في سلوكها الإجرامي، [48] ليُشكّل التزاوج بين التطوّر التكنولوجي وانتشار فيروس كورونا بيئة خصبة ومناخا ملائما لنشاط عدد من الجرائم، خاصّة الجريمة الالكترونية، والقرصنة والفساد المالي، والجريمة المنظّمة،...تغيّرت معه الجرائم نوعًا وكمًا، ليظهر مجرمو المعلوماتية ومجرمو كورونا مستغلين مشاعر الخوف والقلق التي يثيرها فيروس كوفيد -19.

وفي هذا الصدد حذّرت شركة "تشيك بوينت" الأميركية للأمن السيبراني من وجود أكثر من أربعة آلاف نطاق على الإنترنت متعلقة بفيروس كورونا – أي أنّها تحتوي على كلمات مثل كورونا أو كوفيد- منذ بداية عام 2020. واعتبر تقرير الشركة أنّ 3% من هذه النطاقات ضار، و5% أخرى مشبوهة. وقد لا يبدو 3% رقما

---

[48] . محمد اسماعيل، الجريمة في زمن كورونا .. https://www.youm7.com/story/2021/3/22/5251259 يوم 2022/07/31م.

كبيرا، ولكن وفقًا "لتشيك بوينت" أنّ هذه النطاقات المرتبطة بفيروس كورونا من المرجح أن تكون أكثر ضررا بنسبة 50% من أي نطاق آخر مسجّل خلال الفترة الزمنية نفسها. [49] كما أعلنت المنظمة الدولية للشرطة الجنائية (الانتربول) عن ضبط كمامات مقلّدة ومستحضرات تعقيم لليدين غير مستوفية لمعايير السلامة وأدوية مضادة للفيروسات غير مرخصة، بعدما كشفت حوالي 2000 رابط إعلاني إلكتروني لمنتوجات متعلّقة بفيروس كورونا المستجد. منوّهة عن تنوّع أشكال الاحتيال الالكتروني في ظلّ هذه الأزمة الصحية العالمية، فحسب تقارير للمنظمة الدولية، أنّ بعض المجرمين الالكترونيين يعملون على الاتصال بالضحايا لتوهيمهم أنّهم موظفون في عيادات طبية أو مستشفيات أو بنيات علاجية أخرى، ويزعمون أن أحد أقارب الشخص المتصَل به أصيب بالعدوى بالفيروس ليطالبوه بتسديد تكاليف العلاج الطبي. واستنادا (الانتربول) فقد ظهرت "مواقع التصيد الاحتيالي"، وهي عبارة عن رسائل إلكترونية، يفترض أنها صادرة عن أجهزة وطنية أو هيئات صحية عالمية من أجل خداع الضحايا وحملهم على توفير معلومات شخصية عنهم أو تفاصيل الدفع، أو أيضا فتح ملف مرفق يحتوي على برمجية خبيثة. [50] كما أعلنت "وكالة الشرطة الأوروبية" (يوروبول) أنّ جائحة "كوفيد-19" ساهمت في زيادة الجرائم الإلكترونية في أنحاء أوروبا، وخصوصاً لجهة المواد الإباحية المتعلقة بالأطفال وعمليات الاحتيال عبر الإنترنت. كذلك رصدت الوكالة في ذروة الأزمة الصحية "زيادة كبيرة" في المواد التي تنطوي على استغلال جنسي للأطفال على الإنترنت، وأشارت إلى أنّ نشر مواد من هذا النوع "أصبح أكثر شعبيةً مما كان عليه" بسبب القيود على السفر. وفي بيان عن المفوضة الأوروبية للشؤون الداخلية إيلفا يوهانسن إنّ الجائحة أدت إلى تباطؤ جوانب عدة في الحياة المعتادة للناس، لكنّها للأسف زادت وتيرة النشاط الإجرامي عبر الإنترنت."[51]

بالإضافة إلى ظهور العديد من التطبيقات والمواقع الالكترونية، المتبوعة باشهارات تضليلية وكاذبة عبر مختلف وسائل الاتصال الحديثة، فإنّه تمّ تسجيل اختراقات وهجمات إلكترونية وصناعة للفيروسات ونشرها في ظلّ هذه الجائحة، فحتّى منظمة الصحة العالمية شهدت منذ بدء جائحة كوفيد-19 زيادة هائلة في عدد الهجمات الإلكترونية الموجهة إلى موظفيها، وفي عمليات الانتحال الاحتيالية بالبريد الإلكتروني التي تستهدف الجمهور بشكل عام، ففي خلال أسبوع، أدّى هجوم إلكتروني إلى تسريب نحو 450 من عناوين

---

[49] . كيف ازدادت نسب الجرائم الإلكترونية خلال جائحة كورونا
https://www.aljazeera.net/news/scienceandtechnology/2020/5/6 2022/07/31م.

[50] . عبد الله العلوي، فيروس كورونا يفاقم من حدة الجريمة الالكترونية عبر العالم،
https://mapanticorona.map.ma/ar/node/3704 2022/07/31م.

[51] . جائحة كورونا رفعت من نسبة الجرائم الإلكترونية
https://www.alaraby.co.uk/entertainment_media 2022/07/29م.

البريد الإلكتروني وكلمات المرور التابعة للمنظمة، بالإضافة إلى آلاف العناوين وكلمات المرور الخاصة بأشخاص آخرين يعملون في مجال الاستجابة لفيروس كورونا المستجد.[52]

وفي تقرير صادر عن شركة «مايم كاست» المختصّة في حلول الأمن السيبراني ومجال الذكاء الاصطناعي ، بعنوان «100 يوم من فيروس كورونا» عن ارتفاع عدد الجرائم الإلكترونية بنسبة 33% منذ مطلع العام 2020 حتى نهاية مارس من العام نفسه، مع ازدياد عدد زيارات الروابط غير الآمنة أكثر ممّا كان قبل تفشي الوباء، ولا شك أنّ تصاعد خطر الهجمات الإلكترونية بصورة لافتة خلال النصف الأول من العام 2020م لا يمكن فهمه بمعزل عن التحوّلات التي أحدثها فيروس كورونا المستجد«كوفيد- 19» في المجالات كافّة، والتي دفعت معظم دول العالم إلى الاعتماد على التكنولوجيا في تسيير شئونها، وخاصة فيما يتعلق بالعمل عن بُعد، والتعليم عن بُعد، وتزايد اللجوء إلى الاجتماعات الافتراضية، وإدارة أنشطة سوق التجارة والخدمات الإلكترونية. [53]

صحيح أنّ التطوّر التكنولوجي استغله البعض لأنشطة غير مشروعة، ما ساعد على انتشار بعض الجرائم كالجريمة الالكترونية، خصوصا في جائحة كورونا، لكن هذا لا يلغي ايجابياته التي امتدت على مختلف الميادين. كما أنّ ظهور هذه الجرائم المستحدثة جعلت الباحثين وخبراء التقنية والتكنولوجيا في هذا المجال يبتكرون طُرقًا وآليات من شأنها الكشف عن المجرمين والحدّ من هذه الجرائم. فمن ثمرات جهود الباحثين في عالم الجريمة عموما برنامج التنبؤ بالجريمة الذي يُعرف باسم PredPo الذي يمكّنُه التنبؤ بوقوع جريمة ما بدرجة بالغة الدقة، وقد بدأت قوات الشرطة في الولايات المتحدة باستخدامه، فالبرنامج يحسب تنبؤاته استناداً إلى أوقات وأماكن الجرائم السابقة، ويربطها بمعلومات حول السلوك الإجرامي وأنماطه. كما أنّ هناك تقنية باسمShotSpotter ، تعمل من خلال عشرات الميكروفونات المُثَبّتة حول المدينة لترصد أصوات الأعيرة النارية وتحديد مكانها في محيط 40 إلى 50 قدماً، حيث يرى خبراء الشرطة أنّ للبرنامج أهمية، خاصّة في الأماكن التي يندر وجود شهود عيان فيها. وتستخدم أجهزة الشرطة في مقاطعات من مدينة نيويورك التقنية، حيث تحلل بيانات أصوات الطلقات النارية إضافة إلى أدوات لرسم الخرائط وتحليل البيانات لتحديد هويات سكان المكان، وما إذا كان من بينهم مجرمون أو مفرج عنهم تحت المراقبة. وفي تقرير لمدينة تشارلتون الأمريكية أنّه بفضل أحد التقنيات انخفضت معدلات الجرائم الخطرة بنسبة 31 بالمائة.[54] وفي هذا الصّدد قالت وزارة الداخلية البريطانية إنّ خبراءها يعكفون على محاولة التنبؤ بما سيحدث من تقدّم في أساليب الجريمة في المستقبل بهدف الاستعداد لمواجهتها، كما أكّد وزير العلوم البريطاني أنّ

---

[52] . منظمة الصحة العالمية تعلن عن تزايد الهجمات الإلكترونية بمقدار خمسة أضعاف وتحث على اليقظة https://www.who.int/ar/news/item/30-08-1441 2022/08/02م.

[53] . داليا السيد أحمد، لماذا تصاعد خطر الهجمات الإلكترونية في ظل وباء كورونا؟ http://www.nationshield.ae/index.php/home/details/research يوم2022/07/29م.

[54] . أشرف مرحلي، التكنولوجيا تتحدى الجريمة والخارجين على القانون، https://www.alkhaleej.ae/ يوم 2022/07/28م

هناك أبحاثا علمية تجرى ستوفر في المستقبل وسائل متطوّرة لمكافحة الجريمة، وقال إنّه ينبغي الاستفادة من كل سبل الاستعانة بالتكنولوجيا من أجل خفض معدلات الجريمة وبالتالي تحقيق تقدم نوعي في حياة المجتمعات الحديثة.[55]

حاصل الكلام أنّه يمكن الاستفادة ما لفظته التكنولوجيا من وسائل لمكافحة الجرائم خصوصا منها الالكترونية، من خلال تبادل المعلومات المتعلّقة بالمجرمين إلكترونيا، وتعميم بياناتهم في المطارات الدولية، واستخدام البريد الالكتروني في المراسلات بين الجهات الأمنية، واستخدام كلّ الوسائل التقنية الحديثة كالانترنت، الأقمار الصناعية، أجهزة الكشف عن الأسلحة والمخدرات، واستعمال البصمة الالكترونية والعين الالكترونية وتحاليل الحمض النووي لمعرفة المجرمين.[56] وتتبّع المجرمين ورصد تحركاتهم من خلال السوار الالكتروني أو من خلال استعمالاتهم للهوية البيوميترية...، كما يمكن الاستفادة من القنوات الفضائية وشبكة الانترنت وخطوط الهاتف عبر الرسائل النصية في نشر الوعي للمواطنين وبيان خطورة الجرائم بكافة أشكالها خصوصا فئة الأطفال باعتبارهم أكثر الضحايا.

الخاتمة

أعطى عصر التقنية والتطوّر التكنولوجي بُعدا جديدا للجريمة من حيث أدواتها وأساليبها ...فظهرت الجريمة الالكترونية التي لا تعترف بالحدود الجغرافية، شكلّت هاجسا أمنيا للدّول، وما زاد الأمر صعوبة وتحدّيا هو دخول العالم في أزمة صحية بسبب انتشار فيروس كورونا كوفيد-19، حيث حاول الأشرار والجماعات الإجرامية الاستفادة من هذا الظرف باستغلال وسائل التطوّر التكنولوجي لإنعاش أنشطتهم وتحقيق مآربهم.

بعد التطرّق للتطوّر التكنولوجي وتسليط الضوء على الجريمة الالكترونية ـ باعتبارها أبرز مظاهره ـ في ظلّ جائحة كورونا كوفيد-19، خلصت الدّراسة إلى النتائج والتوصيات التالية:

1 ـ النتائج

- ✓ ينصرف معنى التطوّر التكنولوجي في مجال الجريمة إلى ذلك التزايد التدريجي في الاختراعات المادّية كالحاسبات الآلية وشبكة المعلومات....وكذا الاختراعات غير المادّية كمهارات استخدام تلك الآلات والمَعْرِفة بفُنُونها التي قد يكون لها تأثير مباشر أو غير مباشر على الجريمة.
- ✓ تُعدّ الجريمة الالكترونية من إفرازات التطوّر التكنولوجي وأبْرَزِ مظاهره السلبية في عصرنا اليوم.
- ✓ أسْهم التطوّر التكنولوجي في تراجع الظاهرة الإجرامية التقليدية كالضرب، القتل، السرقة في ظلّ انتشار فيروس كورونا، وبالمقابل عرفت الجريمة الالكترونية نموا وتزايدا ملحوظا فترة تفشي هذا الفيروس.

---

[55] ـ استخدام التكنولوجيا الحديثة لمكافحة الجريمة،
http://news.bbc.co.uk/hi/arabic/news/newsid_690000/690928.stm ، 2022/07/28م.

[56] . أحمد عبد الرحمان المجالي، الظواهر الاجرامية الحديثة والجريمة المنظمة، مجلة العلوم الانسانية، بسكرة، المجلد 13، العدد2 ، 2013م، ص232 ،233.

- ✓ نظّم المشرع الجزائري الجريمة الالكترونية واصطلح عليها بـ الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، محاولا الحدّ من خطورة هذه الجرائم من خلال القانون 09/ 04 بالإضافة إلى تعديلات على قانون العقوبات وقانون الإجراءات الجزائية.
- ✓ للجريمة الالكترونية عوامل مختلفة ومتداخلة، ويعتبر انتشار فيروس كورونا كوفيد-19 والتدابير المتّخذة لمكافحته من أبرز العوامل في تناميها وتزايدها.
- ✓ من المجالات التي استهدفتها الجريمة لالكترونية في فترة جائحة كورونا: المجال الصحي، المالي، مجال الترفيه للألعاب الالكترونية، مجال الدردشة والمؤتمرات والاجتماعات عبر المنصات الرقمية.
- ✓ تعتبر المراسيم التنفيذية 69/20، 70/20، 127/20 من أهم الآليات التي اتّخذتها الجزائر لمكافحة فيروس كورونا كوفيد-19 والتي استغلّها لصوص الحظر ومجرمو المعلوماتية في تنفيذ نشاطاتهم.
- ✓ استحداث المشرّع الجزائري للقسم السابع مكرر في الفصل الثالث من الباب الثاني للكتاب الثالث من قانون العقوبات يعدّ خطوة هامّة وقفزة في مجال التشريع، مواكبا التطوّرات التشريعات.
- ✓ الجرائم المتّصلة بتكنولوجيا الإعلام والاتصال ذات طابع خاص كونها واقعة في عالم افتراضي، عابرة للحدود، يصعب فيها الاختصاص القضائي، واثبات الدليل المادي وتتبّع فاعلها، وفي الوقت نفسه يسهل ارتكابها.
- ✓ تصنّف الجريمة الالكترونية باعتبارات مختلفة، من الصعوبة بمكان حَصْرُها لتجدّد وسائلها وأساليبها.
- ✓ التطوّر الكبير في وسائل التكنولوجيا يحتّم الإسراع في كلّ مرّة إلى وضع آليات قانونية لمكافحة انتشار الجرائم الالكترونية، على المستوى الوطني والدولي.
- ✓ الآليات القانونية لمكافحة الجرائم الالكترونية غير كافية وحدها، فلا بد من الاعتماد على وسائل تقنية لا تقل حداثة عن تلك المستعملة في ارتكابها، كأجهزة الرقابة الإلكترونية وأدلة بصمات الأصابع وقرنيات العيون وتحليل الأحماض النووية... فضلا عن التوعية والتحسيس.

2 ـ التوصيات

- ✓ ضرورة الاهتمام بتعزيز الأمن الإلكتروني، وسد الثغرات التي يمكن أن تشكل تهديداً للبنية الرقمية والمعلوماتية، والاستفادة من شركات التقنية والانترنيت، خصوصا ما يتعلّق بالبرامج والقواعد المتعلّقة بحماية الأجهزة والبيانات.
- ✓ نشر الوعي الرقمي والتحسيس بخطورة الجرائم الالكترونية وعقوبتها، وكيفية تجنّب الوقوع في فخاخ لصوص المعلوماتية.
- ✓ ضرورة التعاون الدولي في مجال التحقيق والمتابعة والإثبات في الجرائم الالكترونية وإبرام الاتفاقيات لتحديد الاختصاص القضائي وكشف هوية الفاعلين ومعاقبتهم.
- ✓ عقد مؤتمرات وندوات بصفة دورية ومستمرة، للاطلاع على تطوّرات الإجرام المعلوماتي ومِنْ ثَمَ معالجتها.

- ✓ العمل على تكوين وتأهيل عناصر الضبطية القضائية ورجال الأمن والتحرّي على كيفية معالجة أو التعامل مع الأدلة الرقمية.
- ✓ توفير وتسخير الوسائل المادية والتقنية الحديثة للحدّ من ظاهرة الإجرام الالكتروني، فالمواجهة تكون بنفس سلاح الإجرام وأكثر.
- ✓ طرح مشكلة الجريمة الالكترونية أمام مختصّين اجتماعيين ونفسانيين ...لمعالجة الأسباب والتقليل من تفشيها.
- ✓ رغم الجهود التشريعية . الوطنية خاصة والدولية عامة . المبذولة لمكافحة الجريمة الالكترونية، إلا أنّها غير كافية بعضها يحتاج إلى تعديل، وبعضها الآخر يحتاج إلى توصيف خاصة الحقوق المتعلقة بالملكية الفكرية والحقوق المجاورة التي يصعب تطبيقها في بيئة رقمية إذا ما بقيت النصوص القديمة.

المراجع

أولا - القوانين والنصوص التنظيمية

1. القانون 06 . 22 المؤرخ في 29 ذي القعدة 1427هـ الموافق لـ20 ديسمبر 2006ميعدل ويتمم الأمر رقم 66 . 155 المؤرخ في في 8يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الريدة الرسمية للجمهورية الجزائرية،العدد رقم 84.
2. القانون 16 . 02 المؤرخ في 14 رمضان 1437هـ الموافق لـ19 يونيو 2016م يتمم الامر رقم 156.66 المؤرخ في 8 يونيو 1966م والمتضمن قانون العقوبات ، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 37.
3. القانون 17 .07 المؤرخ في 28 جمادى الثانية1438هـ الموافق لـ27 مارس 2017م،يعدل ويتمم الأمر رقم 66. 155 المؤرخ في 8 يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية العدد رقم 20.
4. القانون 18 . 05 المؤرخ في 24 شعبان عام 1439هـ الموافق 10 مايو سنة 2018م،يتعلق بالتجارة الالكترونية، الجريدة الرسمية للجمهورية الجزائرية عدد رقم28.
5. القانون رقم 04-15 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم71.
6. القانون رقم 08 . 01 المؤرخ في 15 محرم عام 1429هـ، الموافق لـ 23 يناير سنة 2008م، يتمم القانون 83 . 11 المؤرخ في 2 يوليو 1983م، والمتعلق بالتأمينات، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 4.
7. القانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 47.
8. القانون رقم 06/20 المؤرخ في 5 رمضان 1441هـ الموافق لـ28 أبريل 2020م يعدل ويتمم الأمر 156/66 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 25.
9. المرسوم التنفيذي رقم 69/20، المؤرخ في26 رجب 1441هـ، الموافق لـ21 مارس 2020م المتعلق بتدابير الوقاية من انتشار وباء فيروس كورونا كوفيد19 ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد15.

10.المرسوم التنفيذي رقم 70/20 المؤرخ في 29رجب 1441 هـ، الموافق 24 مارس 2020 م، الذي يحدّد تدابير تكميلية للوقاية من انتشار وباء فيروس كورونا كوفيد 19 –ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 16.

11.مرسوم تنفيذي رقم 127/20 مؤرخ في 27 رمضان 1441هـ، الموافق لـ20 ماي 2020م، يعدّل ويتمم المرسوم التنفيذي رقم 70/20 الذي يحدد التدابير التكميلية للوقاية من انتشار وباء فيروس كورونا كوفيد19 ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 30.

ثانيا- الكتب

1. خالد القضاة، التقنيات الحديثة وانعكاساتها الاقتصادية والاجتماعية والنفسية والبيئية، ط1، دار اليازوري العلمية، عمان، 1997م.
2. خالد بن سعود البشر، تلخيص الظواهر الإجرامية المستحدثة وسبل مواجهتها، 2005م.
3. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2010م.
4. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر العربي، الاسكندرية، 2007م.
5. هاني رزق، خالص جبلي، الإيمان والتقدم العلمي، ط1، دار الفكر المعاصر، بيروت، دار الفكر، دمشق، 2000م.

ثالثا- المجلات العلمية

1. أحمد عبد الرحمان المجالي، الظواهر الاجرامية الحديثة والجريمة المنظمة، مجلة العلوم الانسانية، بسكرة، المجلد 13، العدد2 ، 2013م.
2. بوضياف إسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 3، العدد3، 2018م.
3. حبيباتني بثينة، الطبيعة الخاصة للجريمة المعلوماتية، مجلة دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، المجلد12، العدد3، 2020م.
4. رحموني محمد، خصائص الجريمة الالكترونية ومجالاتها، مجلة الحقيقة، المجلد 16، العدد3، 2018م.

رابعا - المذكرات ورسائل الماجستير والدكتوراه

1. خلدون عيشة، محاضرات الجريمة المعلوماتية، موجهة لسنة أولى ماستر تخصّص القانون الجنائي والعلوم الجنائية. بدون تاريخ.
2. سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010م،2011م.
3. صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2013م.

خامسا - المؤتمرات والملتقيات

1. السيد عوض، التطوّر التكنولوجي والجريمة، أعمال المؤتمر السنوي الرابع والثلاثون، قضايا السكان والتنمية، 19 . 22ديسمبر 2004م، المركز الديموجرافي بالقاهرة.
2. فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، أعمال المؤتمر الدولي الرابع عشر، طرابلس 24/24مارس2017م.
3. نميدلي رحيمة، خصوصية الجريم الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر، طرابلس 24/24مارس2017م.

4. يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – ابو ظبي 10-12 /2/2002م.

سادسا ـ المقالات

1. ازدهار سوق المنتجات الطبية والوقائية المزيفة في زمن كورونا، https://www.alaraby.co.uk/ 2022/07/30م.
2. استخدام التكنولوجيا الحديثة لمكافحة الجريمة، http://news.bbc.co.uk/hi/arabic/news/newsid_690000/690928.stm ، 2022/07/28م.
3. أشرف مرحلي، التكنولوجيا تتحدى الجريمة والخارجين على القانون، https://www.alkhaleej.ae/ يوم 2022/07/28م.
4. اكتشاف ثغرات جديدة بـ Zoom تتيح للمتسللين اختراق الكاميرا والميكروفون https://www.youm7.com/story/2020/4/3 2022/08/02م.
5. آمال عيساوي، ألعاب تصيب الأطفال بالجنون والانهيارات العصبية، https://www.echoroukonline.com/ 2022/07/30م.
6. جائحة كورونا رفعت من نسبة الجرائم الإلكترونية https://www.alaraby.co.uk/entertainment_media 2022/07/29م.
7. داليا السيد أحمد، لماذا تصاعد خطر الهجمات الإلكترونية في ظل وباء كورونا؟ http://www.nationshield.ae/index.php/home/details/research 2022/07/29م.
8. دبي للمستقبل ، توجهات عالمية لتعزيز الأمن الرقمي وتبني الذكاء الاصطناعي لحماية القطاعات https://pressn.net/article/8564830?news 2022/07/30م.
9. عبد الله العلوي، فيروس كورونا يفاقم من حدة الجريمة الالكترونية عبر العالم، https://mapanticorona.map.ma/ar/node/3704 2022/07/31م.
10. عمليات النصب المتعلقة بالألعاب الأونلاين في ظل انتشار فيروس كورونا: سبل لحمايتك وعائلتك، https://me.kaspersky.com/resource-center/threats/coronavirus-gaming-scams 2022/08/02م.
11. كلود عمر، لمستخدمي» ..Microsoft Teams هاكرز» يتبعون حيلة لاختراق الهواتف عن طريق التطبيق، https://lite.almasryalyoum.com/technolight/259934 2022/08/02م.
12. كيف أثر منع التجول على جرائم ما بعد "كورونا" في الإقليم؟، https://futureuae.com/m/Mainpage/Item/5571 2022/08/02م.
13. كيف ازدادت نسب الجرائم الإلكترونية خلال جائحة كورونا ؟ https://www.aljazeera.net/news/scienceandtechnology/2020/5/6 2022/07/31م.
14. ليزا سعيد، التقدم التكنولوجي: هل جعلت التكنولوجيا حياتنا أيسر أم أسعد؟ https://www.ts3a.com/?p=30551 ، يوم 2022/07/29م.
15. محمد اسماعيل، الجريمة في زمن كورونا .. https://www.youm7.com/story/2021/3/22/5251259 يوم 2022/07/31م.
16. محمود شرقي، صلاح الدين جبار، تأثير تطور تكنولوجية المعلوماتية على تنامي الجريمة، https://www.asjp.cerist.dz/en/downArticle/354/8/1/62499 2022/07/30م.

17. منصة عملات مشفرة تتعرض للاختراق وسرقة 600 مليون دولار، https://www.alaraby.co.uk/economy 2022/07/29م.
18. منظمة الصحة العالمية تعلن عن تزايد الهجمات الإلكترونية بمقدار خمسة أضعاف وتحث على اليقظة https://www.who.int/ar/news/item/30-08-1441 2022/08/02م.
19. المؤسس يعترف بالتقصير.. القراصنة يقصفون تطبيق "زوم" وشركات كبرى تمنع العمل به، https://www.aljazeera.net/news/scienceandtechnology/2020/4/2 2022/08/02م.
20. هديل كرنيب ما هي لعبة الحوت الأزرق التي "تدفع بالأطفال إلى الانتحار"؟ https://www.annahar.com/arabic/article/713833 2022/08/02م.

انعكاسات التطور التكنولوجي على الظاهرة الإجرامية

The Implications of technological development on the criminal phenomenon

د/التجاني زليخة ،كلية الحقوق جامعة الجزائر1، tidjanizoulikha71@gmail.com

د/ الداوي نجاة، كلية الحقوق والعلوم السياسية –جامعة قاصدي مرباح ورقلة– ،
dr.nadjetdaoui@gmail.com

الملخص:

تدرس الورقة البحثية التأثيرات التي أفرزتها التكنولوجيا على الجريمة وعلى أسلوب إرتكابها وعلى مميزات المجرم الذي أصبح أكثر ذكاء باعتماده على التكنولوجيا.مع التعرض لمختلف المشكلات التي تترتب عن الجرائم الالكترونية سواء من الناحية الموضوعية أو الإجرائية.

Abstract:

The paper examines the effects of technology on crime, the manner in which it is committed and the characteristics of the criminal, who has become more inte lligent by relying on technology. It also examines the various problems posed b y cybercrime, both substantively and procedurally.

مقدمة :

غيّر التطور التكنولوجي حياة البشر في مختلف المجالات وعاد عليها بالايجاب من خلال تسهيل المعاملات و سرعة انجازها،لكنه أيضا في جانب سلبي ساهم في تطور الجريمة والزيادة في مستوياتها،حيث ظهرت جرائم مستحدثة تختلف عن تلك التقليدية في نواح مختلفة لعل

أبرزها:مميزات القائم بها،وقيامها على استعمال التقنية المتطورة ،وتعقيدها وصعوبة كشفها،وامتداد آثارها على دول عدة ،وتجاوزها بالتالي حدود الدولة الواحدة ،الأمر الذي يصعب تتبعها و القبض على مرتكبيها.

و وصمت الجرائم المرتبطة بالتكنولوجيا بالجرائم الالكترونية أو كما تسمى عندنا بجرائم تكنولوجيا الإعلام والاتصال ،ويشكل تفاقمها اليوم تهديدا صريحا بالأمن الاجتماعي وحقوق الأفراد ،و من خلال ورقتنا البحثية نطرح الإشكالية التالية :

ما هي الجوانب التي أثرت فيها التكنولوجيا على الظاهرة الإجرامية ؟

الإجابة تكون عبر المحاور التالية :

المحور الأول : مفهوم الجرائم المرتبطة بتكنولوجيات الإعلام و الاتصال

المحور الثاني: المجرم الالكتروني

المحور الثالث : المشكلات القانونية التي تثيرها الجرائم المرتبطة بتكنولوجيا الإعلام و الاتصال

المحور الأول : مفهوم الجرائم المرتبطة بتكنولوجيات الإعلام و الاتصال

الجريمة ظاهرة اجتماعية لازمت البشرية منذ الأزل،ومع الزمن وما يعرفه من تطورات أصبح مضمون الجريمة ونطاقها يتغير تبعا لهذه التطورات؛ وفيما يأتي نتعرض لكل من التعريف بالجريمة عموما والجرائم المرتبطة بتكنولوجيات الإعلام والاتصال،ومن ثم نعرج على خصائصها.

أولا –التعريف بالجريمة

تعددت التعريفات التي تناولت الجريمة كل حسب الاتجاه الذي ينظر إليها من خلالها:

1–تعرف الجريمة لغة:

الجريمة مصدر لفعل جرّم بمعنى قطع، فنقول جرمه يجرمه جرما بمعنى قطعه،وشجرة جريمة بمعنى مقطوعة.

كما يأتي مصطلح الجريمة للدلالة على التعدي،والجرم هو الذنب،وجرم بمعنى كسب[1] حيث قال تعالى:" يَا أَيُّهَا الَّذِينَ آمَنُوا كُونُوا قَوَّامِينَ لِلَّهِ شُهَدَاءَ بِالْقِسْطِ وَلَا يَجْرِمَنَّكُمْ شَنَآنُ قَوْمٍ عَلَى أَلَّا تَعْدِلُوا اعْدِلُوا هُوَ أَقْرَبُ لِلتَّقْوَى وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ خَبِيرٌ بِمَا تَعْمَلُونَ [2] .

2-تعريف الجريمة اجتماعيا:

تعرف الجريمة بمدلولها الاجتماعي بأنها "كل فعل أو سلوك آثم أو خاطئ مخالف للآداب والأخلاق أو العدالة في المجتمع جدير بالتجريم و العقاب،ويشمل المدلول الاجتماعي للجريمة ليشمل كل المخالفات مهما كان مصدرها أخلاقيا أو اجتماعيا أو قانونيا" [3]،أو هو كل "كل فعل يتعارض مع الأفكار والمبادئ السائدة في المجتمع" .

3-تعريف الجريمة في الفقه الإسلامي:

للجريمة في الفقه الإسلامي معنيين عام وخاص،المعنى الأول يفيد بأن الجريمة هي معصية الله و رسوله،وهو يشمل ما كان له عقاب في الدنيا وفي الآخيرة، وقد ذكر المفكر الإسلامي الشيخ أبو زهرة بأن الجريمة هي فعل ما نهى الله عنه وعصيان ما أمر الله به.

أما المعنى الخاص فجاء في تعريف الماوردي للجرائم "بأنها محظورات شرعية زجر الله تعالى عنها بحد أو تعزير"،وقيل أيضا "بأنها محظورات شرعية زجر الله تعالى عنها بحد أوتعزير سواء كان الفعل ظاهرا أم باطنا ."[4]

---

[1]) محمد أحمد لريد،نظرية ظروف الجريمة في الفقه الجنائي الإسلامي وقانون العقوبات الجزائري،رسالة دكتوراه،كلية العلوم الإنسانية والحضارة الإسلامية،جامعة وهران،2008-2009، ص 7.

[2]) سورة المائدة الآية 08.

[3])عبد الله أوهايبية،شرح قانون العقوبات –منقح بأحدث التعديلات لغاية الأمر 21-15 المؤرخ 12/28/ 2021 –،طبعة 2022،بيت الأفكار ، الجزائر،ص 61.

[4])https://crimedz.blogspot.com/p/adsbygoogle-window_35.html _ أطلع عليه 07/20/ 2022 ،الساعة 14سا 30 .

4-التعريف القانوني للجريمة :

لا يعرف النص القانوني الجريمة،وإنما يعرف كل جريمة على حده، لكن يرى كتاب القانون أن المدلول القانوني للجريمة يأخذ مفهومين واسع و آخر ضيق،الأول ينصرف لكل مخالفة لأي قاعدة قانونية جزائية أو إدارية أو مدنية ...،أما المفهوم الضيق للجريمة ينحصر في الأفعال التي تمس بأحكام قانون العقوبات و القوانين المكملة له،وبتالي ينحصر مفهوم الجريمة في جناية و جنحة و مخالفة.

وعليه تعرف الجريمة جزائيا بأنها "كل فعل أو امتناع يمكن إسناده لمرتكبه ويقرر له عقوبة جنائية،أو هي سلوك إيجابي أو سلبي يجرمه القانون ويقرر له عقوبة أو تدابير أمن،باعتباره اعتداء على مصالح فردية أو اجتماعية يحميها قانون العقوبات[1].

ثانيا: تعريف الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال

الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال هي من الجرائم المستحدثة وتختلف تسميتها بين الكترونية وسيبرانية .

وقد وضعت عدة تعريفات لهذا النوع من الجرائم أبرزها التعريف الضيق و الموسع للجرائم المرتبطة بتكنولوجيات الإعلام والاتصال،وتعريفات أخرى مختلفة التوجهات .

1-التعريف الضيق، والتعريف الموسع:

بالنسبة للتعريف الأول ذهب مجموعة من الفقهاء إلى تعريف الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال تعريفا من ذلك،الفقيه Merwe الذي يرى بأنها الجرائم التي يتورط في ارتكابها الحاسب الآلي ،ويعرفها Ros blat بأنها كل نشاط غير مشروع موجه لنسخ أو تغيير أوحذف أوالوصول إلى المعلومات المخزنة داخل الحاسب الآلي وإلى تحويل طريقه[2].

أما التعريف الموسع فقد ذهب الفقيه Credo إلى أن جريمة الحاسب تشمل استخدام الحاسب كأداة لارتكاب الجريمة،بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحساب

---

[1]) عبد الله أوهايبية،المرجع السابق،ص ص 64-65.

[2])عبد العال الديربي،محمد صادق إسماعيل،الجرائم الالكترونية ،ط1،المركز القومي للإصدارات القانونية، القاهرة،2012،ص 40.

المجني عليه أو بياناته،كما تمتد لتشمل الاعتداءات المادية؛ كما تعرف بأنها فعل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به التي يحميها قانون العقوبات ويفرض لها عقاب[1].

2- **تعاريف أخرى** :

سيقت تعاريف عديدة الجرائم للمرتبطة بتكنولوجيات الإعلام والاتصال وفق اتجاهات متعددة نذكر منها[2]:

الاتجاه الأول يعرف الجريمة بالاستناد على وسيلة ارتكاب الجريمة بأنها "كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب"، أو هو "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"،وهو ما يوافق ما جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فيينا سنة 2000 عند تعريفها للجريمة الالكترونية بأنها:"أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية،أو داخل نظام حاسوبي،والجريمة تلك تشمل من الناحية المبدئية،جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

الاتجاه الثاني:يعرف الجريمة باشتراط أن يكون الحاسب الآلي هو محلها،وبالتالي الجريمة هي "نشاط غير مشروع موجه لنسخ أو تغيير موجه لنسخ أو تغيير أوحذف أو الوصول إلى المعلومات المخزنة داخل الحاسب" .

الاتجاه الثالث :يعرف الجريمة على أساس صفات شخصية مرتكب الفعل ،وعليه هي "أية جريمة لفاعلها معرفة فنية بالحاسوب تمكنه من ارتكابها، أو أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب".

---

[1]) عبد العال الديربي،محمد صادق إسماعيل،المرجع نفسه،ص 41.

[2]) لمزيد من التفصيل: عبد الله دغش العجمي،المشكلات العملية و القانونية للجرائم الالكترونية –دراسة مقارنة– ،رسالة ماجستير ،جامعة الشرق الأوسط، الأردن 2014، ص ص 12–13.

–رحموني محمد،خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة،العدد 41 ،تصدر عن جامعة أحمد دراية،أدرار، ص ص 435–436 .

ويمكننا أن نلاحظ هذه الاتجاهات فيما جاء في اتفاقية بودابست[1]،فالجريمة الالكترونية هي كافة النشاطات غير القانونية أو غير المشروعة المرتبطة بأجهزة الكمبيوتر وباستخدام الشبكة العنكبوتية،وصنفت هذه الاتفاقية الجرائم المرتكبة إلى عدة فئات منها الجرائم التي ترتكب ضد سلامة المعلومات وخصوصيتها،والجرائم ذات الصلة بالكمبيوتر،والجرائم المتعلقة بمحتوى الكمبيوتر،والجرائم المتعلقة بالعلامات التجارية والملكية الفكرية.

3-التعريف القانوني:

عرف المشرع الجزائري الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة 2-أ من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها [2]، بأنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية[3] أو نظام للاتصالات الالكترونية،...".

بهذا التعريف جمع المشرع الحالات التي تكون فيها نظم المعلوماتية وشبكات الاتصال إما موضوعا للجريمة أو وسيلة أو دعامة لجرائم تقليدية،فإصباغ صفة الجريمة المعلوماتية أوالالكترونية مرتبط بالنظم المعلوماتية وشبكات الاتصال.

ثالثا: خصائص الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال(الجرائم الالكترونية)

ترتبط جرائم تكنولوجيات الإعلام والاتصال بجهاز الحاسوب و شبكة الانترنت،الأمر الذي أضفى على الجريمة مجموعة من الخصائص التي تميزها عن الجرائم التقليدية،نذكر فيما يلي أبرزها :

1-الحاسوب عنصر أساسي في ارتكاب الجريمة:

---

[1])انعقدت الاتفاقية الأوروبية لجرائم الانترنت في بودابست بتاريخ2001/11/23 وتعتبر هي الأساس الأول للتعاون الدولي في مجال المكافحة الدولية للجريمة المنظمة عبر الأنترنت،على موقع : https://rm.coe.int/budapest-convention-in-arabic ،الساعة 15:00،اليوم 2022/07/25.

[2])القانون 09-04 مؤرخ 14شعبان عام 1430الموافق 5غشت سنة 2009 (الجريدة الرسمية عدد 47 مؤرخة 16 غشت سنة 2009).

[3])تنص المادة 2-ب :"منظومة معلوماتية:أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة،يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين، ..."

الحاسوب عنصر مهم في الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال،وهو ميزة تنفرد بها عن غيرها،ولا يمكن للمجرم أن ينفذها إلا من خلاله،والحاسوب إما أن يكون موضوعا للجريمة،أو هدفا للجريمة،أو أداة مساعدة في التخطيط للجريمة و تنفيذها.

2-جريمة عابرة للحدود:

تتميز الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال بكونها غير مقيدة بحدود جغرافية معينة،فالنظام الدولي للمعلومات يحقق فرصة الخروج إلى العالمية والبيئة التي تحصل فيها هذه الجرائم لا تعترف بالحدود[1]،وعليه الجرائم الالكترونية تقع في عمومها بين أكثر من دولة وغالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر،كما قد يكون الضرر المتحصل في بلد ثالث في الوقت نفسه .

3-صعوبة اكتشاف واثبات جرائم تكنولوجيات الإعلام والاتصال

يصعب اكتشاف واثبات جرائم تكنولوجيات الإعلام والاتصال،فهي خفية ومستترة، قد لا يتفطن إليها المجني عليه،فهي في الغالب لا تترك أثرا ماديا ظاهرا يمكن ضبطه،فالوسيلة المستخدمة لارتكاب الجريمة هي نبضة أو ذبذبات إلكترونية ينتهي دورها في أقل من ثانية واحدة مما يجعل هذه الجرائم سريعة التنفيذ،كما يصعب الاحتفاظ الفني بآثارها إن وجدت،وهو الأمر الذي ينعكس على تطبيق الإجراءات الجزائية عليها فيصعب البحث و التحري والتحقيق فيها.

4- جرائم تكنولوجيات الإعلام والاتصال جرائم ناعمة

تتطلب الجرائم التقليدية عادة مجهودا عضلي،لكن الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ،تعتمد على المكنة الذهنية والتفكير العلمي القائم على تقنية الحاسوب.

هذا النوع من الجرائم لا يحتاج فيه المجرم إلى العنف بل تكفيه القدرة على التعامل مع جهاز الحاسوب والخبرة في استخدام شبكة المعلومات الدولية[2].

---

[1])خليل يوسف جندي،المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني(دراسة مقارنة)،مجلة كلية القانون للعلوم القانونية والسياسية،جامعة كركوك ،العراق ،المجلد 7، العدد 31،عام 2018،ص 90.

[2]) خليل يوسف جندي،المرجع السابق، ص 93.

المحور الثاني: المجرم الالكتروني

كان للجريمة الإلكترونية تأثيرها على المجرم الذي يرتكبها،فهو يتميز بمجموعة من الخصائص،كما عمل المختصون في مجال المعلوماتية على تقسيم المجرم الإلكتروني إلى طوائف.

أولا: خصائص المجرم الإلكتروني

يمتلك المجرم الالكتروني سمات خاصة إضافة إلى تلك التي توجد في المجرم التقليدي،يمكننا إجمالها فيما يلي:

1- الذكاء والتخصص:

يتميز المجرم الالكتروني بالذكاء فهو يمتلك المهارة التي تمكنه من تعديل وتطوير الأنظمة الأمنية الالكترونية ،كما له الدراية بآخر ماوصلت إليه التقنية الرقمية بفضل ما اكتسبه من مهارة عن طريق الدراسة المتخصصة أو الخبرة المكتسبة في مجال تكنولوجيا المعلومات،فالمجرم الالكتروني يمهد لارتكاب جرائمه بالتعرف على كافة الظروف المحيطة به لاسيما التقنية منها وهذا ما أكده الباحثون في أوروبا وأمريكا عن دور مستوى الذكاء في نوع الجريمة [1] ،فالمجرم الالكتروني يتخصص في جرائم الحاسوب ويكون من الصعب على المجرم المبتدئ الذي لا يكتسب المهارة في هذا المجال أن يرتكب مثل هذه الجرائم،كما يتمتع المجرم الالكتروني بقدرة تقنية يستغلها في اختراق الشبكات وكشف كلمات المرور أو الشفرات بغية الحصول على البيانات والمعلومات الموجودة في أجهزة الحاسوب.

2)العودة للإجرام وعدم استعمال العنف

يعود المجرم الإلكتروني دائما للجريمة،فهو يوظف مهاراته في كيفية عمل الحواسيب وتخزين البيانات والمعلومات و التحكم في أنظمة الشبكات في الدخول غير المصرح به مرات عدة.

---

[1]) مشتاق طالب وهيب،مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها،مجلة العلوم القانونية و السياسية،المجلد 3،العدد1،2013،ص 351.

كما يعود المجرم الالكتروني إلى الجريمة انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليه،ويبتعد هذا النوع من المجرمين من العنف ويرتكب جريمته باعتماد الحيلة خاصة و أنه لا يتعامل مع ضحاياه بصورة مباشرة بل عن طريق الحاسوب،كما أن هدفه من الجريمة هو الحصول على مكاسب مادية أو بسبب الفضول أو التحدي أو المغامرة و إثبات المهارة في المجال الالكتروني،أو لدوافع أخرى [1].

ثانيا:طوائف المجرم الالكتروني

تظهر الدراسات أن هناك طوائف للمجرم الالكتروني تبعا للتطور السريع الذي تعرفه الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال،وهذه الطوائف لا تعني أن كل مجرم إلكتروني يندرج تحت فئة محددة دون غيرها من الفئات المذكورة بل يمكن للمجرم الواحد أن يكون مزيجا من أكثر من طائفة،هناك من يقسمهم إلى صغار المجرمين (صغار السن) ،والمجرمين البالغين.

صغار مجرمي المعلوماتية هو صغار نوابغ المعلوماتية وهم شباب مفتنون بالمعلوماتية وأنظمتها،ودفعهم فضولهم و حب المغامرة إلى ولوج عالم الإجرام.

واختلفت مواقف القانونيين[2] منهم بين من يرى بأنه من غير المناسب إدراج هؤلاء الشباب ضمن الطوائف الإجرامية لأن لديهم ميل للمغامرة و ليس لهم أهداف إجرامية،بل قد لا يقدرون نتائج أفعالهم.

ورأي ثان يرى بأنها فئة مفيدة ويناصرها،ويرى أنها تقدم خدمة لأمن المعلومات،من خلال كشفهم للثغرات الأمنية في تقنية المعلومات[3].

---

[1]) مشتاق طالب وهيب،المرجع السابق، ص 352.

[2])أنظر مجموع هذه الآراء،نهلا عبد القادر المومني،الجرائم المعلوماتية،ط2،2010،دار الثقافة للنشر والتوزيع،الأردن، ص 82.

[3]) احتفت شركة آبل Appel الأمريكية بالشاب الجزائري م واز عبد القادر الذي كشف إحدى الثغرات الخطيرة في نظامها الأمني ،وأدرجت إسمه مرتين على قائمة الشرف الخاصة بها التي تنشرها في موقعها الإلكتروني،يجدر الذكر أن آبل تنشر هذه القائمة تقديرا و شكرا لأولئك الذين أبلغوا عن مشاكل أمنية محتملة في خوادم الويب الخاصة بالشركة.ينظر موقع :
https://www.aljazeera.net/news/scienceandtechnology/2022/8/21 الإطلاع الساعة 17:00 بتاريخ 2022 /08/22 .

ورأي ثالث يرى أن هذه الطائفة تصنف ضمن مجرمي المعلوماتية،لأن أفعالهم تشكل انتهاكا للأنظمة الالكترونية،ويجب عدم التقليل من خطورتهم لأنها فئة قد تتعدى مرحلة الهواية إلى احتراف الجريمة.

ومن أبرز التصنيفات للمجرم الإلكتروني ذلك الذي ورد في كتاب جرائم الكمبيوتر الصادر سنة 1995 بتصنيفهم إلى: المخترقون، المحترفون ،الحاقدون[1].

1-المخترقون أو المتطفلون:

ينطلقون في ارتكاب جرائمهم من دوافع التحدي وإثبات المقدرة منهم:

- Pranksters:وهم الأشخاص يرتكبون جرائم إلكترونية بالحيلة ضد الآخرين دون قصد إحداث ضرر معين،فهم شباب مفتنون بكل ما هو إلكتروني و بالحاسوب.

- Hackers: أشخاص هدفهم الدخول إلى أنظمة الحاسب الآلي غير المصرح لهم الدخول إليها، وكسر الحواجز الأمنية بهدف اكتساب الخبرة و بدافع الفضول،أو لمجرد إثبات القدرة على الإختراق.

2-المحترفون:

المحترفون هم الأكثر خطورة بين مجرمي الانترنت حيث يهدف البعض منهم إلى تحقيق مكاسب مادية أو لتحقيق أغراض سياسية ،ومنهم:

-Software Crackers:هي طائفة متخصصة بفك شفرات البرامج وليس تخريب الشبكة،إذ يقومون بخرق مقاييس الحماية،ويكون هدفها تحقيق الربح المادي.

-Career criminals:مجموعة من المجرمين يقصدون الحصول على الربح المادي بطريقة غير مشروعة،وغالبا ما تعمل هذه الطائفة في شكل عصابات.

- Extremet advocates:هي مجموعة تقوم بتوظيف معارفها في مجال المعلوماتية لتمرير طروحاتها التي تخدم توجهها السياسي أو الإيديولوجي.

ونشير أن اتصالات الجزائر ضمت الشاب مواز لمركز الدفاع السيبراني التابع لها.

[1]) للتفصيل أكثر: مشتاق طالب وهيب،مرجع سابق، ص ص 353، 354.

- Mercenaries:هم جماعة تستخدمهم مؤسسات أو حكومات أو أفراد لاقتحام برامج ونظم حاسوبية معينة لتدميرها أو سرقة ما فيها أو التعديل فيها مقابل الأموال.

- Malicious hackers:أشخاص هدفهم إلحاق خسائر بالمجني عليهم دون الحاجة للحصول على مكاسب مادية،ويدخل في هذه الطائفة صانعوا الفيروسات،وهدفهم هدم النظم المعلوماتية.

3-الحاقدون:

لا يتوفر لدى الحاقدون أهداف و أغراض الجريمة المتوفرة لدى الطائفتين السابقتين ،فالدافع عندهم هو الانتقام و الثأر لتصرف صاحب العمل أو مؤسسة معهم،ولا يتسم هؤلاء بالمعرفة التقنية الاحترافية كسابقيهم من الطوائف،ليس هناك ضوابط معينة لأعمارهم ،ولا يفاخرون بأنشطتهم.

المحور الثالث:المشكلات القانونية التي تثيرها الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال

إن الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال (الجرائم الإلكترونية) جرائم مستحدثة ومواجهتها لم تكن سهلة فهي تثير في بعض الأحيان (حسب التشريعات) مشكلات قانونية يمكنني أن أستعرض بعضها:

أولا : على صعيد التجريم

أمام تطور الإجرام الالكتروني عمد المشرع الجزائري على سد الفراغ القانوني فيما يتعلق هذا النوع من الجرائم،فنص لأول مرة على تجريم الأفعال الماسة بأنظمة الحاسوب الآلي سنة 2004 بتعديله قانون العقوبات بالقانون 04-15 المؤرخ في 2004/11/10 حيث نص على جرائم المساس بأنظمة المعالجة الآلية للمعطيات في المواد394مكرر إلى 394 مكرر8 ق ع .

كذلك نص عبر نصوص خاصة على أفعال مجرمة ترتبط بالمعاملات الالكترونية من خلال الأمر رقم 03-05 المؤرخ 19يوليو2003 يتعلق بحقوق المؤلف والحقوق المجاورة

[1]،لاسيما فيما يتعلق بحماية المصنفات الرقمية كبرامج الحاسوب وقواعد البيانات مثلا ،والقانون رقم 09-04 المؤرخ 05 غشت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،هذا القانون عرّف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

رغم محاولات التجريم هذه، لكن الأكيد أن المشرع لم يجرم كل الأفعال الواجب تجريمها رغم وجودها في أرض الواقع،ولقد اختار الطريق الأسهل من خلال تعريف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة 2-1 باستعمال عبارة "....أي جريمة أخرى ترتكب أويسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية" ،فهل هذا يعني إسقاط نصوص قانون العقوبات فيما يتعلق أركان كل جريمة على تلك التي ترتكب الكترونيا مثلا نصوص النصب و السرقة و التحريض على الفسق هي نفسها إذا ما كنا أمام النصب الالكتروني و السرقة الالكترونية و التحريض على الفسق الالكتروني،إن اعتماد هذا الأمر آراه مخالفا لمبدأ الشرعية و قصورا في النص التشريعي المكافح للجرائم الالكترونية،حيث نجد على سبيل المثال اتفاقية بودابست[2] تصنف الجرائم الالكترونية إلى 4 طوائف رئيسية:

أ-الجرائم التي تستهدف سلامة وسرية المعطيات والنظم.

ب-الجرائم المرتبطة بالكمبيوتر.

ج-الجرائم المرتبطة بالمحتوى.

د-الجرائم المرتبطة بالأشخاص والأموال.

فهل أحاط المشرع الجزائري من خلال نصوص التجريم بكل الأفعال غير المشروعة المرتكبة إلكترونيا خاصة تلك الموجودة في أرض الواقع و تمس بالمجتمع الجزائري،الإجابة لا.

---

[1])الجريدة الرسمية المؤرخة 23يوليو 2003 عدد 44 ص ص 3-21 .

[2] تم اعتماد الاتفاقية و تقريرها التفسيري من طرف لجنة وزراء أوروبا في دورتها التاسعة بعد المائة (08نوفبر/تشرين الثاني 2001 وفتح باب التوقيع على الاتفاقية في بودابست في 23نوفمبر/تشرين الثاني 2001بمناسبة المؤتمر الدولي حول الجريمة الالكترونية.
والجزائر لم توقع على هذه الاتفاقية.

ثانيا:على صعيد إجراءات المتابعة و الإثبات

نلمس من خلال قانون الإجراءات الجزائية والقانون رقم 09-04 المؤرخ 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،اهتمام المشرع بمتابعة هذه الجريمة والوقاية منها.

فقانون الإجراءات الجزائية اتبع بشأن جرائم تكنولوجيات الإعلام والاتصال نفس الإجراءات المقررة للجرائم التقليدية ماعدا بعض الاختلافات تخص تمديد الاختصاص القضائي، شروط التفتيش، والتوقيف للنظر ،بالإضافة إلى إجراءات البحث والتحري الخاصة (اعتراض المراسلات وتسجيل الأصوات و التقاط الصور ،وإجراء التسرب) [1]،أما القانون 09-04 فقد أقر بدوره مجموعة من الإجراءات الهامة للبحث والتحري عن هذا النوع من الجرائم منها المراقبة الالكترونية ،تفتيش المنظومة المعلوماتية،حجز المعطيات،إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته من مهامها مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات،والنص على التعاون الدولي لمكافحة هذه الجريمة،واختصاص المحاكم الجزائرية بهذا النوع من الجرائم إذا ارتكبها أجنبي وكانت تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني[2].

دون شك أن المشرع قام بقفزة نوعية من خلال النص على مجموعة من الإجراءات لمواجهة جرائم تكنولوجيات الإعلام والاتصال وتعزيز البحث والتحري أو التحقيق والمحاكمة في هذه الجرائم،لكن يجب أن لا يفوتنا أن مسألة الاختصاص القضائي تحتاج إلى توضيح أكثر فماذا عن جرائم التي يرتكبها أجانب ولا تتعلق بالمصالح المذكورة في المادة 15 من القانون 09-04 ،كذلك مسألة ضبط الدليل الرقمي أو اثبات الجريمة الإلكترونية صعبة لسهولة التخلص منه بضغطت زر على لوحة مفاتيح الحاسوب من الجاني،والتفتيش الرقمي قد يتطلب أن يكون خارج حدود الدولة وينطبق الأمر على المعاينة،و هنا تدق مسألة التعاون الدولي الفعال الذي يتطلب استخدام بروتوكولات موحدة لنظم التخزين والحماية المعلوماتية.

---

[1]) المواد 45،44 /7، 51/ 6، 65 مكرر5 ق إج

[2])المواد 4، 5،6،14، 15،16 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها.

ومن المسائل المهمة أيضا افتقاد الجهاز الشبه قضائي والقضائي للمهارات في مجال التقنية المتطورة وسبل التعاون مع غيرها من الأجهزة النظيرة لها خارجيا ،هذا دون التقليل من أهمية ما تقدمه المراكز البحث عن الجرائم كالمعهد الوطني للأدلة الجنائية و علم الإجرام،ومركز البحث و التطوير.

الخاتمة :

أظهرت الدراسة النتائج التالية:

-لا وجود لتعريف جامع أو موحد للجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.

-تأثير التكنولوجيا على خصائص الجريمة التي تتميز بكونها عابرة للحدود ويصعب كشفها وإثباتها.

-تأثير التكنولوجيا على المجرم الذي يتميز بالذكاء و التخصص والابتعاد عن العنف،والرغبة الدائمة في العودة إلى الجريمة.

-تثير الجرائم الالكترونية مشكلات قانونية سواء موضوعية أو إجرائية من خلال :

صعوبة السيطرة على الجريمة الالكترونية وكذلك إثباتها.

التوصيات :

-التعريف الدقيق للجرائم المرتبطة بتكنولوجيات الإعلام و الاتصال.

-وضع نص قانوني واحد يهتم بالجرائم المرتبطة بتكنولوجيات الإعلام والاتصال.

- صعوبة السيطرة على الجريمة الالكترونية وكذلك في إثباتها.

- وضع قواعد جزائية موضوعية تحدد الأفعال التي يمكن اعتبارها اعتداء على الحقوق المعلوماتية أو جريمة بواسطة الحاسوب.

-تحديد النصوص الإجرائية الكفيلة بكشف الجريمة والمجرمين ،من خلال اعتماد إجراءات مستحدثة تعتمد على التكنولوجيا إلى جانب الإجراءات المحددة في قانون الإجراءات الجزائية.

-الرفع من الإمكانات والكفاءات المطلوبة في جهاز القضاء، بأن يكون للقضاة وعي و خبرة بشأن الجريمة الالكترونية.

-تعزيز التعاون الدولي لمكافحة الجريمة الالكترونية.

المراجع:

أولا: نصوص قانونية

1-الاتفاقية الأوروبية لجرائم الانترنت في بودابست بتاريخ 2001/11/23 وتعتبر هي الأساس الأول للتعاون الدولي في مجال المكافحة الدولية للجريمة المنظمة عبر الأنترنت،على موقع : https://rm.coe.int/budapest-convention-in-arabic ،الساعة 15:00،اليوم 2022/07/25.

2-القانون 09-04 مؤرخ 14شعبان عام 1430الموافق 5غشت سنة 2009 (الجريدة الرسمية عدد 47 مؤرخة 16 غشت سنة 2009).

ثانيا: كتب

1-عبد العال الديربي،محمد صادق إسماعيل،الجرائم الالكترونية ،ط 1، 2012،المركز القومي للإصدارات القانونية، القاهرة.

2-عبد الله أوهايبية،شرح قانون العقوبات -منقح بأحدث التعديلات لغاية الأمر 21-15 المؤرخ 12/28/ 2021 -،طبعة 2022،بيت الأفكار ، الجزائر.

3-نهلا عبد القادر المومني،الجرائم المعلوماتية،ط2،2010،دار الثقافة للنشر والتوزيع،الأردن.

ثالثا:مقالات

1-خليل يوسف جندي،المواجهة التشريعية للجريمة المعلوماتية على المستويين الدولي والوطني(دراسة مقارنة)،مجلة كلية القانون للعلوم القانونية والسياسية،جامعة كركوك ،العراق ،المجلد 7، العدد 31،عام 2018.

2- رحموني محمد،خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة،العدد 41 ،تصدر عن جامعة أحمد دراية،أدرار،سنة 2017.

3- مشتاق طالب وهيب،مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها،مجلة العلوم القانونية و السياسية،المجلد 3،العدد1 ، 2013.

رابعا: رسائل ومذكرات

أ-دكتوراه

1-محمد أحمد لريد،نظرية ظروف الجريمة في الفقه الجنائي الإسلامي وقانون العقوبات الجزائري،رسالة دكتوراه،كلية العلوم الإنسانية والحضارة الإسلامية،جامعة وهران،2008-2009.

ب-ماجستير

- عبد الله دغش العجمي،المشكلات العملية والقانونية للجرائم الالكترونية -دراسة مقارنة-،رسالة ماجستير،جامعة الشرق الأوسط، الأردن 2014.

تطور أساليب ارتكاب الجريمة في ظل التطور التكنولوجي

The evolution of methods of committing crime in light of technological development

بن موسى وردة

أستاذة محاضرة أ

كلية الحقوق والعلوم السياسية جامعة البليدة -2-

ward73.b@gmail.com

الملخص

تهدد الجريمة الأفراد والمجتمعات بحيث يتم الاعتداء من خلالها على مصالح محمية قانونا بجزاء جنائي، هذه المصالح المتضاربة ينتج عنها صراعات تدفع إلى ارتكاب جرائم يختلف نوعها بالنظر إلى هذه المصلحة؛ التي تمس إما الأشخاص أو ممتلكاتهم أو كرامتهم وشرفهم وغيرها من المصالح، وتعد هذه الجرائم قديمة قدم المجتمعات، ولكن قد تحدث ظروف ومتغيرات مفاجئة تساهم وتساعد الأفراد على ارتكاب بعض الأفعال بالرغم من أنها لا تحتوي على القسوة والعنف، إنما تعتمد على بعض الأساليب الأكثر خطورة على الأفراد والمجتمعات.

تتميز هذه الجرائم بخصوصية؛ لأنها ظهرت نتيجة تطور التكنولوجية الحديثة وكل ما يتصل بها من تقنيات جديدة، رغم أن المشرع لا يعتد عادة بالوسيلة المستعملة في ارتكاب الجريمة، لكن استعمال وسائل التكنولوجية الحديثة هي التي أضفت عليها هذه الخصوصية، الأمر الذي دفع المشرع إلى التدخل لتجريم هذه الأفعال من أجل حماية مصالح جديرة بالحماية القانونية، هذه المصالح التي تهدد الأمن الاجتماعي أو الاقتصادي أو السياسي باعتبار أن النصوص الموجودة عاجزة على التطبيق، الأمر الذي يدعو دائما المشرع للتدخل وتجريم هذه الأفعال الجديدة، فانتشار واستعمال الوسائل الحديثة يؤدي إلى تزايد الإجرام وتعدد المجرمين.

الكلمات المفتاحية:

التطور التكنولوجي والجريمة، تطور الجريمة، الثورة التكنولوجية، أساليب ارتكاب الجريمة، التقدم التكنولوجي.

Abstract:

The crime threatens individuals and societies so that legally protected interests are attacked with a criminal penalty. These conflicting interests result in conflicts that push the commission of crimes of different types in view of this interest; These crimes are as old as societies, but sudden circumstances and variables may occur that contribute and help individuals to commit some acts, although they do not contain cruelty and violence, but rely on some of the most dangerous methods on the individuals and societies.

These crimes are peculiar; Because it appeared as a result of the development of modern technology and all the new technologies related to it, although the legislator does not usually take into account the means used to commit the crime, but the use of modern technological means is what added to it this privacy, which prompted the legislator to intervene to criminalize these acts in order to protect Interests worthy of legal protection, these interests that threaten social, economic or political security, given that the existing texts are unable to be implemented, which always calls the legislator to intervene and criminalize these new acts, as the spread and use of modern means leads to an increase in crime and a multiplicity of criminals.

Key words:
Technological development and crime, crime development, technological revolution, methods of committing a crime, technological Improvement.

مقدمة

تعد الجريمة ظاهرة اجتماعية؛ تتطور وتتبدل في المجتمع وتتعارض مع القيم الموجودة فيه، وهو الذي يؤدي إلى الإضرار به، فقد تظهر ظروف وعوامل وأسباب تساهم في ارتكاب الجريمة، وبالتالي تتجدد وتتخذ أشكالا تبعا لتجدد الأفكار والحاجات المتطورة للإنسان، الأمر الذي يترتب عنه ظهور أنواع جديدة من الجرائم تختلف عن الجرائم الموجودة أو كما تسمى الجرائم التقليدية، وذلك بسبب طريقة ارتكابها أو الوسيلة المعتمد عليها في ارتكابها أو عن طريق استعمال الحيلة والخداع دون أن تنطوي على العنف.

أثر التقدم في جميع الميادين؛ في الفرد خاصة من جانب سلوكياته، التي أصبحت سلبية يستغل من خلالها هذا التقدم في ابتكار أفعال وأشياء ووسائل جديدة لم تكن موجودة من قبل، فيحاول إثبات كفاءاته من خلال إظهار مهاراته وقدراته على التفوق على الوسائل الحديثة.

ساهمت التكنولوجية الحديثة في تطوير الأدوات الطبية، وساهمت في تطوير وسائل الاتصالات ووسائل المواصلات، ولكن استخدمه المجرمون في الإجرام واستفادوا من التطور التكنولوجي واستحدثوا أساليب جديدة لارتكاب جرائمهم.

نتناول دراسة هذا الموضوع بعد طرح الإشكالية الآتية:

ما هي أهمية التكنولوجيا، وإلى أي مدى ساهمت في تطوير أساليب ارتكاب الجريمة؟

وللإجابة عن هذه الإشكالية نتناول الموضوع من خلال المحورين الآتيين:

المحور الأول: ايجابيات وسلبيات التطور التكنولوجي

المحور الثاني: خصوصية جرائم التكنولوجيا الحديثة

المحور الأول: ايجابيات وسلبيات التطور التكنولوجي

أصبحت التكنولوجيا عنصرا مهما في حياة الإنسان بحيث سهلت له سبل معيشته، لكن بالمقابل استغلها في ارتكاب صور عديدة من الجرائم منها الماسة بالأموال أو الأشخاص أو المعتقدات أو الأسرة أو الشرف والاعتبار وغيرها، نتناول في هذا المحور الأول نقطتين، الأولى تتعلق بأهمية التكنولوجيا أما الثانية فتتعلق بمساهمة التكنولوجيا في تطوير الجريمة.

أولا: أهمية التكنولوجيا

تعرف التكنولوجيا بأنها "الأساليب الفنية التي يستخدمها الإنسان بهدف إشباع حاجاته المختلفة وتحسين حياته"[1]، ولقد اشتهرت عبارة تكنولوجيا في القرن العشرين مع الثورة الصناعية الثانية، وتطورت استخداماتها في جميع الميادين؛ رغم أنها في الأصل تتعلق بالتعليم الفني في الغالب، ولكن امتد استخدام هذا المصطلح إلى جميع الميادين[2]، ويعتبر التطور التكنولوجي سلسلة من المراحل المتغيرة بشكل تدريجي؛ تستفيد كل مرحلة من المرحلة التي سبقتها، وتضاف عليها اختراعات جديدة ومهارات استخدام هذه الآلات والوسائل، إما في مصلحة الأفراد والمجتمعات أو ضد مصلحتهم.

التطور التكنولوجي نظرية تصف التحول الجذري للمجتمع (البشرية في انتقال)، من استعمال الأداة إلى إنشاء الآلة إلى التشغيل الذاتي وهو إزالة عنصر التحكم البشري، ويترتب عن ذلك الاعتماد على الجهد العقلي والعمل الفكري أكثر من الجهد البدني[3].

ولقد تنوعت الحياة بمختلف الأدوات الحديثة التي أصبحت من الضروريات؛ فلا يستطيع الإنسان الاستغناء عنها، أكثر من ذلك ظهرت آلات حلت محل عمل الإنسان، وبالتالي خدمته وتم الاستغناء عنه، وتغيرت معالم الحياة بفعل التطور التكنولوجي؛ باعتبار أن الدول تعمل على إدخال التكنولوجيا في جميع الميادين، فالإنسان يعمل دائما على إيجاد أدوات ووسائل تساعده في قضاء حاجياته المختلفة والمتنوعة، لذا يحاول دائما أن يطورها بما يتماشى مع هذه الاحتياجات، فانتشرت التكنولوجية بسرعة مست جميع المجالات وأصبح لها أهمية بالغة، وتغلغلت في حياة الأفراد وذلك من خلال عنصر التكنولوجية والتقنيات الحديثة.

ويعرف التقدم التكنولوجي بأنه؛ عملية إنسانية بحتة يتم من خلالها ابتكار الأدوات التي يعتمد عليها الإنسان للتعامل مع البيئة التي يعيش فيها بشكل أفضل، مع تحسين أداء هذه الأدوات وكل تحسين أو تجويد أو تسريع من أداء الإنسان في نيل أغراضه[4].

---

[1] عادل عامر، تطور الجريمة في عصر التكنولوجيا، دنيا الوطن تاريخ الشر 2017/09/20، تاريخ الاطلاع 2022/07/21 على الساعة 19:30 ، ص 02.

[2] عبد العزيز موهيب، دور التقدم التكنولوجي في الرفع من جرائم النصب الاليكتروني، مقال نشر في هبة زووم أضيف في 24 مايو 2020 http://hibazoom.com تم الاطلاع عليه بتاريخ 2022/07/28.

[3] من ويكيبيديا الموسوعة الحرة، التطور التكنولوجي، أخر تعديل 2021/11/25، تاريخ الاطلاع 2022/07/29.

[4] هالة فهمي، تعريف التقدم التكنولوجي، https://mufahras.com بتاريخ 2021/07/09، تاريخ الاطلاع 2022/07/29.

وأدى التقدم التكنولوجي إلى رفع التنمية الاقتصادية، الأمر الذي ساهم في التقدم الاقتصادي والاجتماعي، وسهل تبادل العلاقات بين الدول واختصر بذلك المسافات وسمح بفتح الحدود بين الدول رغم اختلاف ثقافاتهم، وأصبح بالتالي مكسبا للمجتمعات وليس حكرا على دولة دون أخرى[1]، وللتقدم التكنولوجي أهمية كبيرة أيضا؛ بحيث أدى إلى رفع التنمية وحقق التقدم في جميع الميادين وقرب بين الدول؛ ومكن من عقد اجتماعات وملتقيات وحل مشاكل دون أن يحتاج ذلك إلى الانتقال أو الانتظار.

لكن رغم هذه الايجابيات إلا أنه نتج بالمقابل؛ الاستعمال السلبي لهذه التقنيات الحديثة وذلك بارتكاب أفعال إجرامية تختلف عن الأفعال التقليدية.

ثانيا: مساهمة التكنولوجيا في تطوير الجريمة

نشأت جرائم جديدة ارتبطت بالتكنولوجية الحديثة، لارتباطها بالأجهزة وكذا جميع التقنيات الحديثة، فالتطور التكنولوجي هو تلك الأدوات والأجهزة التي جعلت حياة الإنسان سهلة، وأثرت على مجالات عديدة منها التعليم، الطب، الصناعة، التجارة، والثقافة، والزراعة، كما تم استخدام هذه التكنولوجية في سبيل النهوض بالاقتصاد وغيرها، لذا تستخدم التكنولوجية الحديثة في الإيجاب وفي السلب، وإن طريقة استخدامها هي التي تحدد خيرها أو شرها، بحيث انتشرت التكنولوجية وتم التلاعب بها بما يخدم الأغراض الشريرة للأفراد[2].

تستعمل عادة وسائل التكنولوجية الحديثة في الجريمة من أجل الحصول على المال أو لأغراض أخرى منها الابتزاز، أو لغرض إرهابي، وهذا بالتحكم في وسائل النقل الجوية والبحرية، أو بإجراء تحويل للأموال من أجل استغلالها في العمليات الإرهابية.

تطورت الأساليب الحديثة في ارتكاب الجريمة بسبب التكنولوجية الحديثة التي أوجدت فرص لأنشطة إجرامية، بحيث تم إساءة استعمال هذه التكنولوجية فظهرت أنواع متعددة من الجرائم التي تمس الأفراد والمجتمعات.

ظهرت جرائم ارتبطت بتطور التقنيات الحديثة تختلف عن الجرائم التقليدية نتج عنها مشاكل أقلقت الأفراد والدول، بحيث برز خبراء يمتازون بالحرفية استغلوا ذلك في ارتكاب جرائم جديدة؛ وذلك باستعمال وسائل مبتكرة وأساليب تؤدي إلى شلل في أكثر الأنظمة الحساسة لأي دولة؛ وهذا دون أن يترك

---

[1] عبد العزيز موهيب، دور التقدم التكنولوجي في الرفع من جرائم النصب الاليكتروني، مرجع سابق.

[2] روبرتو دي بيترو، التكنولوجيا والجريمة: صراع دائم ومستمر، مقال مقدم من إدارة الاتصال بجامعة حمد بن خليفة قطر، https://www.hbku.edu.qa تاريخ النشر 23 أغسطس 2021، تاريخ الاطلاع 2022/07/28.

المجرم وراءه أي أثر ملموس[1]، وتعتبر الجريمة المعلوماتية من أهم وأكثر هذه الجرائم انتشارا، بحيث سهلت شبكة الانترنت للمجرمين في تطوير سبل ارتكاب الجرائم التقليدية، وتصنف هذه الجرائم إلى جرائم ضد الحاسوب والمرتبطة بالحاسوب، التجسس على المؤسسات العسكرية، القرصنة الالكترونية، الإرهاب الالكتروني، جرائم التشهير وجرائم نشر الفيروسات.

نجد عدة عوامل ساهمت وساعدت على ارتكاب هذه الجرائم خاصة تكنولوجية المعلومات والاتصالات التي تحرك هذه الأشكال الجديدة عن طريق هذه الأساليب الحديثة التي تضمنتها فنجد عدة أنواع من الجرائم المستحدثة منها الإرهاب الالكتروني، قرصنة بطاقات الائتمان، وتضاف أسباب وعوامل أخرى مثل العولمة، النزاعات المسلحة، ضعف سيادة القانون، سرعة ظهور أشكال جديدة من التكنولوجية الحديثة، استخدام الفساد لتسهيل ارتكاب الجريمة، بحيث تستمر عمليات العولمة والتطور التكنولوجي في دفع عجلة الابتكار الإجرامي، بالإضافة إلى خلق عوامل وأساليب لارتكاب الجريمة، وتعتبر العوامل الإنسانية أكثر هذه العوامل تأثيرا وأهمية.

قام المجرمون بإدخال طرق وتقنيات لارتكاب الجرائم التقليدية في مجال السرقة والقتل والانتحار وذلك باستعمال أشعة الليزر، وعن طريق أجهزة التحكم من بعد، واعتمد المجرمون بكثرة على الحاسب الآلي وشبكة الانترنت التي سهلت كل ذلك وبذلك تظهر أهمية التكنولوجيا في المساهمة في تسهيل وتطوير الإجرام.

المحور الثاني: خصوصية جرائم التكنولوجيا الحديثة

تتدخل الدول لمواجهة كل ما يستجد من جرائم التي ترتكب باستعمال التقنيات الحديثة؛ وتضع قواعد موضوعية منها وإجرائية نظرا لخصوصيتها، لأن النصوص التقليدية تقف عاجزة عن مواكبة هذا التطور في الإجرام؛ سواء باستعمال هذه التقنيات الحديثة في ارتكاب الجرائم التقليدية أو بارتكاب جرائم جديدة لم تكن معروفة من قبل، نتناول من خلال هذا المحور الخصائص المميزة لجرائم التكنولوجيا الحديثة أولا، ونتناول ثانيا مواكبة القانون الموضوعي والإجرائي لتطور الجريمة.

[1] نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، رسالة ماجستير في القانون العام، كلية الدراسات العليا جامعة النجاح الوطنية في نابلس فلسطين، 2017، ص02-03.

أولا: الخصائص المميزة لجرائم التكنولوجيا الحديثة

أتيحت للجريمة وسائل استثنائية سمح بامتدادها في نطاق غير محدود، وأصبحت ظاهرة عالمية تستغل فيها التقنيات الحديثة، ويكون فيها اعتداء على مصالح أساسية، فظهرت أشكالا جديدة للجريمة بظهور أشكال جديدة للتكنولوجية تسهل وتساهم في ارتكابها، ينطوي استخدامها على العديد من المخاطر التي تؤثر على الإنسان، فتطور الابتكار التكنولوجي بشكل سريع هو الذي يمهد الطريق للاستخدام غير المشروع ويمكن أن تتسلل هذه الجرائم إلى جميع القطاعات[1].

يتم ارتكاب الجرائم التقليدية باستخدام أساليب التكنولوجية الحديثة، وذلك بالاعتماد على شبكة الانترنت باعتبارها بيئة جديدة سهلت للمجرمين ارتكاب جرائمهم؛ ووسعت من نشاطهم الإجرامي، وهو الذي أدى إلى تزايد الإدماج والارتباط بين الدول والمجتمعات بإلغاء الحدود الإقليمية، كل هذه الظروف سهلت ارتكاب أنواع مختلفة من الجرائم[2].

وأصبح الإنسان يعتمد على التكنولوجية الحديثة في كافة المجالات، وفي تطوير أشكال الإجرام وظهور أنواع جديدة وتجاوزت بذلك الحدود الجغرافية للدول[3]، فيقوم المجرمون بانتحال شخصية أخرى؛ سواء كانت شخصية حقيقية أو شخصية وهمية، من أجل إخفاء هويتهم الحقيقية، واستخدام مهاراتهم وذكائهم في استعمال هذه الوسائل الحديثة والمتطورة بدون عناء، الأمر الذي يصعب الكشف عنه وعن أفعاله الإجرامية.

تتميز هذه الجرائم بأنها تعتمد على التقنيات الحديثة وتعتمد على وسائل ذكية يرتكبها مجرمون يتميزون بالذكاء؛ وهو الذي يساهم في إخفاء الأدلة، الأمر الذي يصعب على الأجهزة المختصة الكشف عنهم وعن جرائمهم، وتمتاز هذه الجرائم بطريقة خاصة للتخطيط لها وفي أسلوب تنفيذها وفي الوسائل المستعملة في ذلك، لذا انتشرت واستفحلت بسرعة الأمر الذي يجعلها أشد الجرائم خطورة بالمقارنة مع الجرائم التقليدية، وهو الذي يؤدي إلى عدة أضرار اجتماعية اقتصادية وغيرها[4].

---

[1] روبرتو دي بيترو، التكنولوجيا والجريمة: صراع دائم ومستمر، مرجع سابق، بدون صفحة.

[2] عادل عامر، مرجع سابق، ص 4-5.

[3] محمود شرقي، صلاح الدين جبار، تأثير تطور تكنولوجية المعلوماتية على تنامي الجريمة، مجلة الأدب والعلوم الاجتماعية، مجلد 8، عدد 1، 2015، الجزائر.

[4] زيتوني عائشة، محاضرات الجرائم المستحدثة لطلبة السنة الثانية ماستر تخصص انحراف وجريمة، جامعة باجي مختار كلية الآداب والعلوم الإنسانية قسم علم الاجتماع، 2020- 2021، ص03-04.

إن استخدام التقنيات الحديثة والمتطورة لارتكاب الجريمة، سلوكيات أفرزتها تيارات إنحرافية بسبب التحولات التي شهدتها الحياة المعاصرة، تتميز بالدقة والذكاء وهي خطيرة على الأمن ككل وعلى المجتمع، أكثر من ذلك قد يمتد أثر هذه الجرائم إلى خارج إقليم الدولة الواحدة، وهو ما يصعب ضبط أدلة ارتكابها[1]، ويعتمد هذا النوع من الجرائم على الدقة والإدراك، فلا تحتوي هذه الأفعال على العنف فهي جرائم فنية يسبقها التخطيط والذكاء، ويعتمد هؤلاء على كفاءاتهم ويستغلون ذلك في ارتكاب جرائمهم.

يتطور هذا النوع من الجرائم مع تطور التكنولوجيا؛ وظهور أحدث التقنيات واستغلالها في ارتكاب الجرائم وتعتبر من أخطر الجرائم المستحدثة، بحيث تؤثر على المنظومة القانونية لوجود ثغرات، بالإضافة إلى تأثيرها على كل من الاقتصاد والاستقرار السياسي والاجتماعي للدول.

استغل المجرمون ما توصلت إليه التكنولوجية الحديثة في تطوير جرائمهم واستحداث جرائم جديدة؛ ترتبط بأحدث ما توصلت إليه هذه التكنولوجية، إما أن يعتمدها كوسيلة لارتكاب جرائمه أو تكون هي محل هذه الجرائم، لذا ارتكبت جرائم لم تكن معروفة قبل هذه الثورة المعلوماتية وهي أكثر خطورة من الجرائم التقليدية، لأنها ترتكب أفعالها بكل سهولة وبساطة ثم يتم إخفاء أثارها.

تهدد هذه الجرائم أمن واستقرار المجتمع، الأمر الذي أدى إلى ظهور مهارات وكفاءات جديدة إما في مجال استخدام الطاقة، أو في مجال استخدام الحاسوب وغيرها، لذا استحدثت جرائم استخدمت وسائل وأساليب تكنولوجية حديثة كشف عن تحول في صور وأنماط الجرائم وفي مرتكبيها وفي أساليب ارتكابها؛ إذ تعد هذه الجرائم من الخطورة التي تستدعي التصدي لها باعتبارها جرائم خطيرة تطال كافة الدول وتكمن خطورتها أيضا في أنها جرائم خفية، لا تترك وراءها أدلة مادية تدين مرتكبيها[2].

نتج عن التطور التكنولوجي إلغاء الحدود بين الدول؛ بحيث مكنت وسهلت ارتكاب الجرائم التي يبدأ التحضير لها في دولة وتنفذ في دولة ثانية أو دولة ثالثة وهكذا دون أن يلتقي المجرمون، فهؤلاء يوسعون نشاطاتهم ويتبادلون طرق ارتكابها ويتعاونون فيما بينهم من أجل ارتكاب جرائمهم خفية ودون أن يتركوا أي أثار.

---

[1] زيتوني عائشة، مرجع سابق، ص 08.

[2] السيد عوض، التطور التكنولوجي والجريمة، أعمال المؤتمر السنوي الرابع والثلاثون قضايا السكان والتنمية، 19-22 ديسمبر 2004، المركز الديموغرافي بالقاهرة، https://wsideg-geography.biogspot.com 19 مارس 2018، تاريخ الاطلاع 2022/07/29.

ثانيا: مواكبة القانون الموضوعي والإجرائي لتطور الجريمة

صار القانون الدولي يفرض نفسه على القانون الوطني، بسبب عدم تمكن هذا الأخير من السيطرة على التكنولوجيا، وإن تنظيم استعمالات وأثار التكنولوجيا يساعد على عولمة القانون وهو الذي يقتضي تصور مناهج حديثة لوضعه، أكثر من ذلك سرعة التطور يجعل الخطر موجود ومتطور أيضا الأمر الذي يقتضي التدخل بتعديل وإلغاء القانون، ولقد هيمنت العلوم والتكنولوجية على تشريعات بعض الدول وهذا من أجل حماية الأفراد من الاستعمال المنحرف للعلوم والتقنيات، بحيث يجب الموازنة بين التقدم العلمي والمعرفي وبين الحفاظ على حقوق وحريات الأفراد، فيجب التوفيق بين فكرتين أن التقدم العلمي يعمل على تنمية الإنسانية وفكرة تدهور الإنسانية بسبب التقدم العلمي[1].

إن ظهور هذا النوع الحديث من الجرائم استلزم تدخل الدول بإصدار تشريعات خاصة؛ تتناول بالتجريم والعقاب هذه السلوكيات الجديدة، وما يستلزم ذلك من النص على إجراءات وقواعد خاصة تختلف عن تلك المنصوص عليها بالنسبة للجرائم التقليدية، رغم أن علاقة القانون بالتكنولوجيا معقدة وغامضة، ولكن العالم يحتاج إلى إطار قانوني جوهري يفيد العلم والتكنولوجيا، ومن جهة أخرى تساهم التكنولوجية في ابتكار قانون جديد[2].

بدأت هذه الظاهرة كسلوكيات غير أخلاقية، اعتمدت فيها على كل التقنيات الحديثة ولكن مع استفحالها بدأ الاهتمام بهذه الظواهر الجديدة التي سببت أضرارا مادية ومعنوية فكان لزاما التصدي لها، وذلك بتجريمها والعقاب عليها بالعقوبات المناسبة لها، وأصبح حماية أمن المعلومات والاتصالات والشبكات ومواجهة الجريمة الالكترونية من أولويات العديد من الدول، باعتباره خطر يمس جميع القطاعات وينتج عنها خسائر.

وللتوفيق بين المبادئ التقليدية وتلك المبادئ والقواعد التي يجب أن تتماشى وهذا التطور، يجب على القانون أن يعتمد مبدأ الواقعية التكنولوجية في شكله ومضمونه، بحيث يتم استعمال المفاهيم والمصطلحات الحديثة تمكن القانون من التطور والتأقلم، وهذا حتى لا تتمكن التكنولوجيا من التحايل على

---

[1] محمد الإدريسي العلمي المشيشي، لهث القانون وراء تهافت العلم والتكنولوجي، الرباط 14 فبراير 2013، http://www.ism.ma ، ص 01-08، تاريخ الاطلاع 2022/07/30.

[2] محمد الإدريسي العلمي المشيشي، مرجع سابق، ص22-25.

القانون، ويجب أن يحتوي دائما على الأجوبة المناسبة؛ وهذا بإدخال كل المفردات التقنية المتطورة وكل ما يرتبط بالانعكاسات السياسية والاقتصادية والاجتماعية والثقافية والإيديولوجية والأخلاقية[1].

إن الكشف عن هذه الجرائم من الصعوبة بمكان؛ لأن الدليل يتم محوه بسهولة باعتبارها تختلف عن تلك المعتمد عليها في الجرائم التقليدية؛ لأنها تتعلق بالوسائل الفنية والتقية المستعملة لارتكاب هذا النوع من الجرائم، لذا يمكن الاعتماد على كل دليل يستخلص من أي وسيلة تكنولوجية أو أي تقنية استخدمها الجاني عند القيام بفعله الإجرامي.

ترتكب هذه الجرائم ولا تترك أثرا، الأمر الذي يصعب الكشف عنها، بالإضافة إلى أنه إذا تم اكتشافها فيكون بعد مدة طويلة من ارتكابها، لذا يجب على رجال الضبطية القضائية أن تعتمد على التكنولوجية الحديثة للكشف على هذا النوع من الجرائم، ويجب تدريبهم ومنحهم أدوات ومؤهلات، للوصول إلى البيانات الموجودة في الحاسوب، وتدريبهم على استعمال جميع التقنيات الحديثة من أجل الوصول إلى الأدلة والكشف عن الجريمة والمجرمين.

فكما اعتمد الجناة على هذه التقنيات؛ يجب أن ينص القانون الإجرائي على هذه الوسائل الحديثة للكشف عن هذه الجرائم (فكما استخدم المجرم التكنولوجيا في ارتكاب الجريمة يجب أن تستعمل التكنولوجية للقبض على المجرمين)، سواء من حيث مراقبة هذه الوسائل وكل ما يساعد السلطات المختصة في الكشف عنها والبحث عن الأدلة والنص على الإجراءات الخاصة بالتفتيش وضبط الأشياء، بالإضافة إلى تلك الإجراءات المستحدثة والمنصوص عليها في القوانين الإجرائية؛ التي يمكن الاعتماد عليها عند توافر الشروط الشكلية لذلك.

ازداد دور التكنولوجية الحديثة في النشاط الإجرامي؛ بالإضافة إلى استعمال الطرق التقليدية وهو الذي أدى إلى تعقيدها، الأمر الذي يحول دون كشفها أو الوصول إلى الأدلة بسهولة ولا تتمكن الجهات القضائية من الوصول إليها.

[1] محمد الإدريسي العلمي المشيشي، مرجع سابق، ص 15-17.

الخاتمة

نتج عن التطور العلمي والتكنولوجي تطور الإجرام، فاستغل الفرد التقنية الحديثة التي استعملها بصفة ايجابية وترتب عنها تقدم وازدهار في شتى المجالات، ثم تحول عن هذا المسار وتوجه إلى الاستخدام السلبي لها.

تقتضي التكنولوجية الحديثة معرفة صحيحة في كيفية استخدامها، لأن سوء استخدامها قد يؤدي إلى عواقب وخيمة، لذا يجب احتواء الأوضاع التي قد تؤدي إلى سوء استخدام التكنولوجية في ارتكاب الجريمة، بحيث يستغل المجرم هذه التكنولوجية لتطوير أساليب ووسائل ارتكاب جرائمه، فلقد أساء استخدام هذه الوسائل وأصبحت تسهل ارتكابها الأمر الذي يدفع السلطات المختصة إلى الاعتماد على وسائل وأساليب حديثة للكشف عن الجريمة وإثباتها وذلك بتنظيم هذه الإجراءات في إطار القانون.

أدى التطور الهائل لنظم تقنية المعلومات إلى تطور الجريمة باعتبارها أصبحت عابرة للحدود الوطنية بسبب تطور أساليب ارتكابها وهي مشكلة تمس المجتمع الدولي.

المراجع:

أولا–رسالة ماجستير

–نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، رسالة ماجستير في القانون العام، كلية الدراسات العليا جامعة النجاح الوطنية في نابلس فلسطين، 2017.

ثانيا–المقالات

1–روبرتو دي بيترو، التكنولوجيا والجريمة: صراع دائم ومستمر، مقال مقدم من إدارة الاتصال بجامعة حمد بن خليفة قطر، https://www.hbku.edu.qa تاريخ النشر 23 أغسطس 2021، تاريخ الاطلاع 2022./07/28

2–عادل عامر، تطور الجريمة في عصر التكنولوجيا، دنيا الوطن تاريخ النشر 2017/09/20، تاريخ الاطلاع 2022/07/21 على الساعة 19:30.

3–عبد العزيز موهيب، دور التقدم التكنولوجي في الرفع من جرائم النصب الاليكتروني، مقال نشر في هبة زووم(الرباط) أضيف في 24 مايو 2020 http://hibazoom.com تم الاطلاع عليه بتاريخ 2022/07/28.

4–محمد الإدريسي العلمي المشيشي، لهث القانون وراء تهافت العلم والتكنولوجي، الرباط 14 فبراير 2013، http://www.ism.ma ، ص 01–04، تاريخ الاطلاع 2022/07/30.

5–محمود شرقي، صلاح الدين جبار، تأثير تطور تكنولوجية المعلوماتية على تنامي الجريمة، مجلة الأدب والعلوم الاجتماعية مجلد 8 عدد 1 الجزائر 2015.

6–هالة فهمي، تعريف التقدم التكنولوجي، https://mufahras.com بتاريخ 2021/07/09، تاريخ الاطلاع 2022/07/29.

ثالثا–مراجع أخرى

–السيد عوض، التطور التكنولوجي والجريمة، أعمال المؤتمر السنوي الرابع والثلاثون قضايا السكان والتنمية، 19–22 ديسمبر 2004، المركز الديموغرافي بالقاهرة،
https://wsideg–geography.biogspot.com 19 مارس 2018، تاريخ الاطلاع 2022/07/29.

–زيتوني عائشة، محاضرات الجرائم المستحدثة لطلبة السنة الثانية ماستر تخصص انحراف وجريمة، جامعة باجي مختار كلية الآداب والعلوم الإنسانية قسم علم الاجتماع، 2020– 2021.

–من ويكيبيديا الموسوعة الحرة، التطور التكنولوجي، أخر تعديل 2021/11/25، تاريخ الاطلاع 2022/07/29.

الملتقى الدولي الافتراضي الموسوم بـ "القانون الجنائي في ظل التطور التكنولوجي . إشكالات ومعالجات ".

المحور المشارك به: المحور الأول " التطور التطنولوجي والظاهرة الاجرامية"

عنوان المداخلة: التطوّر التكنولوجي والظاهرة الإجرامية في ظلّ جائحة كورونا كوفيد – 19.

د. بوعزيز فريد، جامعة أحمد بن بلة1، وهران. أستاذ رئيسي بالتعليم الثانوي.

البريد الالكتروني: islamaymen2018@gmail.com

رقم الهاتف: 0667.69.09.26

الملخص

أمام التطوّر التكنولوجي الذي غزا مختلف مجالات حياتنا، استغلّه البعض في تحقيق جرائم بأساليب وتراكيب غير تلك المستعملة في الجرائم التقليدية المعروفة، لتبرز بذلك أنواع جديدة من الجرائم كالجريمة الالكترونية؛ ذلك أنّ التزوير، السرقة والاحتيال ...جرائم أصبحت تتّم عبر أجهزة ووسائل الكترونية. وبالمقابل من هذا رُصِدت تقنيات دقيقة ووسائل ذكية كأجهزة رقابة إلكترونية، تحليل الحمض النووي وبصمات الأصابع... لمواجهة الجريمة في ثوبها الجديد. وفي خِضّم هذا التطوّر وانتشار فيروس كورونا في الآونة الأخيرة، رُفِعت تقارير مُسَجِّلَة انعكاسات ذلك على مستوى الظاهرة الإجرامية.

تهدف هذه الورقة البحثية إلى إبراز تداعيات التطوّر التكنولوجي على الظاهرة الإجرامية في ظل انتشار جائحة كورونا وما تبعها من جملة الإجراءات وحزمة النصوص القانونية والتنظيمية التي اتخذتها الجزائر تحديدا لتطويق الفيروس والحد من الظاهرة الإجرامية، من خلال المنهج الوصفي التحليلي الذي يناسب الموضوع.

الكلمات المفتاحية: الظاهرة الإجرامية، التطور التكنولوجي، فيروس كورونا كوفيد–19، الجريمة الالكترونية.

Title: Technological development and the criminal phenomenon in light of the COVID-19 pandemic.

Abstract

In the face of the technological development that has invaded various areas of our lives, some have exploited it to investigate crimes using methods and structures other than those used in the well-known traditional crimes, thus emerging new types of crimes such as electronic crime ;due to forgery, theft and fraud ... are crimes that are carried out through electronic devices and means. On the other hand, accurate techniques and smart means such as electronic control devices, DNA analysis and fingerprints were monitored to face crime in its new dress. In the midst of this development and the recent spread of the Corona virus, reports have been raised of repercussions. This is at the level of the criminal phenomenon.

This research paper aims to highlight the repercussions of technological development on the criminal phenomenon in light of the spread of the Corona pandemic and the subsequent procedures and a package of legal and regulatory texts taken by Algeria specifically to surround the virus and reduce the criminal phenomenon, through the descriptive analytical approach that fits the topic.

Keywords: criminal phenomenon, technological development, corona virus COVID-19, cybercrime.

المقدّمة

يُوصَف عصرنا اليوم بعصر التقنية والتكنولوجيا، حيث تتسابق في كلّ يوم الاكتشافات والابتكارات بالظُهور؛ ويُعدّ قطاع الاتصالات أكثرها تطوّرا، حيث أصبحت الاتصالات بين الأفراد والبلدان أيْسر بِكَبْسة زِرٍ، بفضل شبكة الانترنت وانتشار الكمبيوتر وخطوط الاتصال المختلفة، وأضحى معها الحصول على المعلومات سَهْلا وبسرعة ومن غير تكلفة، مُوَفِّرة لِمُستخدِمِيها أموالا وجهدا، مُلْغية المسافات الجغرافية، فهي وسائل لا تعترف بالحدود ولا تحجزها المسافات.

لا يُنكر أحد أنّ تكنولوجيا المعلومات أحْدَثت تغييرات أساسية في العالم على شتّى المجالات، وأصبحت وسائلها ضرورية في حياتنا؛ في معاملتنا المصرفية، في تسوّقنا، في الإدارات والمؤسّسات، في علاقة الدّول بعضها ببعض وكذا علاقة الدولة بالأفراد... ، ذلك أنّ تنوّع خدماتها وسهولة الاتصال بها أوْجَد لها مكانا على اختلاف البلدان والأجناس والفئات العُمرية. لكن على الرّغم من التطوّر الهائل في مجال الحاسوب وشبكة الانترنت وايجابيات الوسائل الالكترونية والأهمية التي أصبحت تكتسيها، إلاّ أنّ هناك جانب آخر مُظلم، يتجلّى في الاستخدام غير المشروع لها؛ والذي أدى إلى ميلاد نوع جديد من الجرائم، تحت مُسمّى الجرائم الالكترونية أو جرائم المعلوماتية، التي وَظَّفَ فيها المجرمون وسائل الاتصال الحديثة لخدمة نشاطاتهم الإجرامية، للتنوّع معها أساليب وأدوات ارتكابها ويزداد خطرها، فباتت بذلك مصدرا يُهدّد أمن الدّول واقتصادها، وانتهاك حرمة الحياة الخاصة للأفراد واختراق النظام والآداب العامة.

أمام التخوّفات الوطنية والعالمية من الجريمة الالكترونية والجهود المبذولة لمواجهتها، ظهر تهديد صحّي آخر مع نهاية عام 2019م من خلال انتشار فيروس كورونا كوفيد-19 بداية من مدينة وُوهان الصينية الذي تسبب في أزمة عالمية، صنّفته منظمة الصّحة العالمية أنّه جائحة، إذْ هُدِّمَت معه النُظُم التي تقوم عليها الدّول، واخْتَفت معالم الحياة الطبيعية؛ وبالمقابل انتعش معه كلّ ما هو إلكتروني أو رقمي جرّاء التدابير التي أُتُّخذت لمكافحة انتشار هذا الوباء.

تهدف هذه الورقة البحثية إلى بلورة تداعيات التطوّر التكنولوجي على الظاهرة الإجرامية في ظلّ انتشار جائحة كورونا كوفيد-19 من خلال أبرز مظاهره ممثلّة في الجريمة الالكترونية، وبيان موقف المشرّع الجزائري منها وواقعها في هذا الظرف الصحّي المُقْلق، ضمن جُملة الإجراءات وحُزمة النصوص القانونية والتنظيمية التي اتخذتها الجزائر تحديدا لتطويق الفيروس، باعتماد المنهج الوصفي والاستقرائي والتحليلي الذي يناسب الموضوع.

بناء على ما سبق برز الإشكال الرئيس الآتي: ما هي انعكاسات التطوّر التكنولوجي على ظاهرة الإجرام في ظلّ انتشار فيروس كورونا كوفيد-19؟.

إجابة على الإشكال الرئيس تطلّب الأمر بسط تساؤلات ثانوية أخرى: هل أسْهم التطوّر التكنولوجي في تنامي الظاهرة الإجرامية أو قلّل منها؟ ما علاقة الجريمة الإلكترونية بالتطوّر التكنولوجي في ظلّ انتشار فيروس كورونا كوفيد-19؟ ما موقف المشرّع الجزائري من ظاهرة الإجرام الالكتروني؟ ما هي عوامل

انتشارها؟ هل ثمّة مجالات استهدفتها الجريمة الالكترونية زمن جائحة كورونا كوفيد-19؟ وما هي الآليات التي اتّخذتها الجزائر لمواجهة فيروس كورونا كوفيد-19؟.

منهج الدّراسة

اقتضت التساؤلات المطروحة اعتماد منهج مركّب بين المنهج الوصفي والاستقرائي والتحليلي، بجمع معلومات ومعطيات عن ظاهرة الإجرام الالكتروني تحديدا كونها من تجليآت التطوّر التكنولوجي وبيان واقعها في خضّم انتشار فيروس كورونا كوفيد- 19، تحت مظلّة أبرز النصوص القانونية التي جاء بها المشرّع الجزائري لمواجهة الجريمة الالكترونية، وكذا المراسيم التنفيذية التي اتّخذتها السلطات الجزائرية لمكافحة انتشار جائحة كورونا كوفيد-19.

إجابة على الإشكال الرئيس والتساؤلات المطروحة، تمّ تقسيم الدّراسة إلى النقاط التالية:

أولا . معنى التطوّر التكنولوجي وموقف المشرّع الجزائري من الجريمة الالكترونية

ثانيا . تصنيفات الجريمة الالكترونية وأهمّ المجالات التي استهدفتها في ظل جائحة كورونا كوفيد-19

ثالثا . عوامل انتشار الجريمة الالكترونية زمن تفشي فيروس كورونا كوفيد-19 وأبرز التدابير التي اتخذتها الجزائر لمكافحته.

رابعا . التطوّر التكنولوجي بين خدمة الظاهرة الإجرامية ومكافحتها فترة انتشار فيروس كورونا كوفيد -19

أولا . معنى التطوّر التكنولوجي وموقف المشرّع الجزائري من الجريمة الالكترونية

تُعدّ تكنولوجيا المعلومات والاتصالات من مظاهر التطوّر التكنولوجي الذي نعيشه وثمرة الجهود العلمية التي توصّل إليها الإنسان، وقد سخّرت الدّول إمكانيات مادية وبشرية للاستثمار الأحسن لها، لكن هذا المتغيّر التكنولوجي سلاح ذو حدين، فمن جهة حَسَّنَ من نوعية حياة الإنسان، ومن جهة أخرى كان تربة خِصْبة لبعض الأنشطة السلبية كالجرائم الالكترونية أو المعلوماتية.

إنّ هذا التطوّر الحاصل ومفرازاته، مسّ المجتمع الجزائري كغيره من المجتمعات، وجعله يَعْرِف أنواعا من الجرائم المستحدثة كالجريمة الالكترونية؛ نحاول في هذه الجزئية أن نبيّن معنى التطوّر التكنولوجي في هذا المجال، لِنعقبه بموقف المشرّع الجزائري من الجريمة الالكترونية باعتبارها من مخرجات هذا التطوّر وأهمّ مظاهره غير المشروعة.

1 . معنى التطوّر التكنولوجي

التطوّر التكنولوجي مصطلح رام الكثير إلى إعطاء مفهوم له، لتطفو بذلك جملة من التعاريف أهمّها تعريف خالد القضاة حيث قال: " التطوّر التكنولوجي هو عبارة عن " استمرارية التقدّم والنماء على أساس من توظيف كلّ المعارف في عملية التنمية الشاملة وابتكار وتطوير الوسائل اللازمة لتسخير تلك المعارف في عملية التنمية"[1] ، وعبّر عنه آخرون بأنّه مجموعة الاختراعات أو الطرق التكنولوجية أو الخدمات أو النماذج

[1] . خالد القضاة، التقنيات الحديثة وانعكاساتها الاقتصادية والاجتماعية والنفسية والبيئية، ط1، دار اليازوري العلمية، عمان، 1997م، ص 57.

الجديدة التي تستخدم في الإنتاج، ويترتّب عليها تطوّر في كمية المنتج أو درجة جودته"[2] وقيل: أنّه انتقال الإنسان من مرحلة إلى مرحلة أخرى متباينة، كالانتقال من العصر الحجري إلى العصر النحاسي مثلا، أو الانتقال من عصر النسخ اليدوي في طباعة الكتب إلى عصر المطبعة الآلية، فابتكار الأدوات التي تمكّن بني الإنسان من التعامل مع البيئة المحيطة ومتطلباتها بشكل أفضل. والتعديلات والتحسينات الطارئة على أداء هذه الأدوات، وكذا الحال الابتكار الجديد لهذه الأدوات والذي من شأنه سدّ فجوات في حياة الإنسان العملية، أو العمل على تحسين أو تجويد أو تسريع من أداء الإنسان في نيل أغراضه، كلّ ذلك يدخل تحت مسمّى التطوّر التكنولوجي.[3]

والحقيقة أنّ التطور التكنولوجي يمُرّ بمراحل ويتم بشكل تدريجي عبر مختلف الأزمنة، بدليل التغيّرات العميقة التي طرأت على حياة الإنسان خصوصا، ويُعدّ اليوم التطوّر التكنولوجي مَعْلما على الحضارة الحديثة الذي يتمكّن الإنسان معه من التكيّف مع بيئته ومحيطه وإدخال تحسينات وتعديلات على حياته من خلال الاختراعات والاكتشافات....

ويمكن القول في الجملة أنّ لكلّ عصر أدواته واختراعاته، وكلّ مرحلة من التطوّر ترتكز على معارف وتجارب سابقة لِتبنيّ وتأتيّ بالجديد، وهذا على مختلف المجالات. وإنّ المقصود هَهُنا من التطوّر التكنولوجي هو التزايد التدريجي في الاختراعات المادّية المتمثّلة في الآلات كالسيارات والطائرات والحاسبات الآلية وشبكة المعلومات الدولية....وكذا الاختراعات غير المادّية المتمثّلة في مهارات استخدام تلك الآلات والمَعْرِفة بفُنُونها التي قد يكون لها تأثير مباشر أو غير مباشر على الجريمة.[4] على أنّ مجال هذا التزايد التدريجي في الاختراعات المادية أو غير المادية والذي يتماشى مع موضوع بحثنا هو الذي يكون في إطار ارتكاب الجريمة، ولعلّ من أجلّ وأبرز المظاهر السلبية للتطوّر التكنولوجي اليوم في مجال ظاهرة الإجرام هو الجريمة الالكترونية.

2. موقف المشرّع الجزائري من الجريمة الالكترونية

نتيجة التطوّر الهائل في عالم التكنولوجيا، خصوصا مجال المعلوماتية ووسائل الاتصال وما تتيحه شبكة الانترنيت، برزت مشاكل قانونية، ذلك أنّه ظهرت جرائم جديدة وجب علاجها ومواجهتها ولا يتأتّى ذلك إلا من خلال نصوص قانونية، فالقاضي لا يُجرّم أفعالاً أو يُسلّط عقوبات إلاّ بنص. واسْتِتْبابا للأمن وتوفير الحماية وسدّ الفراغ القانوني من هذا الجانب، حاول المشرّع الجزائري استحداث آليات قانونية من شأنها الحدّ

---

[2] . هاني رزق، خالص جبلي، الإيمان والتقدم العلمي، ط1، دار الفكر المعاصر، بيروت، دار الفكر، دمشق، 2000م، ص 315.

[3] . ليزا سعيد، التقدم التكنولوجي: هل جعلت التكنولوجيا حياتنا أيسر أم أسعد؟ ، https://www.ts3a.com/?p=30551 ، يوم 2022/07/29م.

[4] . السيد عوض، التطوّر التكنولوجي والجريمة، أعمال المؤتمر السنوي الرابع والثلاثون، قضايا السكان والتنمية، 19 . 22ديسمبر 2004م، المركز الديموجرافي بالقاهرة، http://swideg-geography.blogspot.com/2018/03/blog-post_38.html#.YvaI21xBzIU 2022/07/29م.

من مثل هكذا جرائم والوقاية منها من خلال الأمر رقم 04 .15[5]، والقانون 09. 04[6]،والقانون رقم 08 . 01[7] والقانون رقم 18 .05[8] ...فضلا عن القواعد أو النصوص العامة التي تَحْظُر الإضرار والتعدّي على الغير.

وبالرجوع للمادة 2 من القانون 09 . 04 السالف الذكر نجد أنّ المشرّع الجزائري اختار اسم الجرائم المتّصلة بتكنولوجيات الإعلام والاتصال مُعرِّفا إيّاها بقوله: " يقصد في مفهوم هذا القانون بما يأتي: الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".

وهذا التعريف الذي أورده المشرّع الجزائري تعريف مرن يشمل عدد من الجرائم، فيكفي أن ترتكب الجريمة عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية، ليرسم لنا المشرّع الجزائري صور الجرائم المتعلّقة بتكنولوجيات الإعلام والاتصال من خلال المواد 394 مكرر إلى غاية 394 مكرر 8 الواردة في القانون 04 . 15 والقانون 16 . 02[9] والتي يُمكن بيانها بشيء من التفصيل الموجز فيما يأتي:

- الدخول أو البقاء داخل منظومة معلوماتية عن طريق الغش.
- حذف أو تغيير لمعطيات المنظمة.
- إدخال بطريق الغش معطيات في نظم المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.
- كلّ من يقوم عن طريق الغش بتصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها.
- إنشاء أو تكوين جماعة أشرار.

وتجدر الإشارة إلى أنّ وعي المشرّع الجزائري واستشعاره لخطورة هذا النوع المستحدث من الجرائم، جعله يقوم بتعديل عام 2006م في قانون العقوبات بموجب القانون 06 .23 الذي تمّ من خلاله تشديد العقوبة على الأفعال أو الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات، ليستحدث عام 2016م نصا جديدا يتعلّق

---

[5] . القانون رقم 04-15 المؤرّخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدّل والمتمّم للأمر رقم 66-156 المتضمّن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم71.

[6] . القانون رقم 09-04 مؤرّخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمّن القواعد الخاصّة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 47.

[7] . القانون رقم 08- 01 المؤرخ في 15 محرم عام 1429هـ، الموافق لـ 23 يناير سنة 2008م، يتمم القانون 83 . 11 المؤرخ في 2 يوليو 1983م، والمتعلق بالتأمينات، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 4.

[8] . القانون 18- 05 المؤرخ في 24 شعبان عام 1439هـ الموافق 10 مايو سنة 2018م، يتعلق بالتجارة الالكترونية، الجريدة الرسمية للجمهورية الجزائرية عدد رقم28.

[9] . القانون 16- 02 المؤرخ في 14 رمضان 1437هـ الموافق لـ19 يونيو 2016م يتمم الأمر رقم 156.66 المؤرخ في 8 يونيو 1966م والمتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 37.

بالمادة 87 مكرر 12والتي نصت على جريمة جديدة تمثّلت في جناية تجنيد الأشخاص لصالح إرهابي أو منظومة إرهابية باستخدام وسائل تكنولوجيا الإعلام والاتصال.

أمّا على مستوى قانون الإجراءات الجزائية للجرائم المتعلّقة بتكنولوجيات الإعلام والاتصال فإنّ متابعتها تتمّ بنفس الإجراءات التي تُتّبع بها الجرائم التقليدية، لكن جديد المشرع الجزائري هو تمديده الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية من خلال المادة 37 من القانون 17 .07.[10] وكذلك ما نصت عليه المادة 45 في فقرتها الأخيرة من قانون الإجراءات الجزائية 06. 22[11] التي اعتبرت أنّ التفتيش الذي يكون على مستوى المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة. كما نصت المادة 51 فقرة 6 من القانون 06 . 22 السالف الذكر على التوقيف للنّظر في جريمة المساس بأنظمة المعالجة، وكذا اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في المادة 65 مكرر 5 إلى 10 مكرر من نفس المادة[12]. أمّا بالنسبة لباقي الإجراءات من تحقيق ومحاكمة فإنّها تطبق نفس إجراءات الجريمة التقليدية.[13]

مع التنويه هنا أنّه تعدّدت تعريفات هذا النوع من الجرائم ــ ولا نرى من المناسب بَسْطهاــ كما تعدّدت تسمياتها للدّلالة على حقيقة المسمّى، نظرا لتقارب المفاهيم وتداخلها كما في الغش المعلوماتي أو الإجرام الالكتروني، والانحراف الذي يقع بواسطة الحاسب الآلي أو الإنترنت...، فهل الجريمة الالكترونية تحوي الجريمة المعلوماتية أو العكس؟ [14] والذي نراه أنّ مصطلح الجريمة الالكترونية هو الأصوب، ذلك أنّها أدق وأوسع تشمل أي وسيلة إلكترونية فضلا عن جرائم المساس بأنظمة المعالجة الآلية للمعطيات على الحاسوب أو بواسطتها كما أشار إليها المشرّع الجزائري، في حين أنّ الجريمة المعلوماتية تقتصر على الجرائم الماسة بالانترنيت أو الحاسوب أو بواسطتهما فقط.

---

[10] . القانون 17-07 المؤرخ في 28 جمادى الثانية1438هـ الموافق لـ27 مارس 2017م،يعدل ويتمم الأمر رقم 66. 155 المؤرخ في 8 يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية العدد رقم 20.

[11] . القانون 06- 22 المؤرخ في 29 ذي القعدة 1427هـ الموافق لـ20 ديسمبر 2006ميعدل ويتمم الأمر رقم 66 . 155 المؤرخ في في 8يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية،العدد رقم 84.

[12] . الفصل الرابع بعنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور " من الباب الثاني للكتاب الأول من القانون 06 – 22 المعدل والمتمم للأمر رقم 66 . 155 المؤرخ في في 8يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 84، ص 8.

[13] . فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، أعمال المؤتمر الدولي الرابع عشر، طرابلس 24/24مارس2017م، ص 131.

[14] -نميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر، طرابلس 24/24مارس2017م، ص98.

بِيدَ أنّ أجود التعريفات وأوْفاها للجريمة الالكترونية هو ما ذكرته حبيباتني بثينة بأنّها: " كل سلوك غير مشروع تكون تقنية المعلومات وسيلة لارتكاب الجريمة، أو تكون موضوعا لها"[15] وهو تعريف ينسجم مع ما جاء به المشرّع الجزائري.

ثانيا . تصنيفات الجريمة الالكترونية وأهمّ المجالات التي استهدفتها في ظلّ جائحة كورونا كوفيد-19

اختلف الفقه الجنائي والقانون حول تقسيم الجرائم الالكترونية، باختلاف الزاوية التي يُنْظَر منها، فعلى سبيل المثال قد تكون الزاوية من مَنْظُور أنّ النظام المعلوماتي هو أداة الجريمة ووسيلة تنفيذها، كما قد يكون النظام المعلوماتي هو موضوع أو محل الجريمة الالكترونية، إذ يطول المقام لذكرها ولا نرى ضرورة ذلك، حيث أنه كلّما ظهرت وسيلة جديدة برزت معها جريمة أو أسلوب جديد، فهي متغيرة ومتجّددة. لكن الملاحظ وعلى اختلاف تصنيفات الجريمة الالكترونية أنّها استهدفت جوانب وقطاعات بصفة خاصّة منذ ظهور فيروس كورونا كوفيد-19[16]، نحاول أن نتعرّف على أهمّها بعد أن نستعرض أبرز تصنيفات الجريمة الالكترونية.

1 . تصنيفات الجريمة الالكترونية

سبق القول أنّ تصنيف الجريمة الالكترونية يعود إلى اعتبارات، نذكر منها:

أولا . الجرائم الواقعة بواسطة النظام المعلوماتي: يشتمل هذا التصنيف على أهمّ الجرائم التي تتّصل بالمعلوماتية. والحاسب الآلي في هذه المجموعة وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، يهدف الجاني عادة من وراء ارتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعة، فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته أو برامجه أو نظمه كوسيلة لتنفيذ الجريمة، ومنه لا يكون النظام المعلوماتي هو محل الحماية الجنائية[17] وتقّسم الجرائم بموجب هذا الاعتبار إلى:

أ. الجرائم الواقعة على الأشخاص: تعّددت مظاهر الجرائم الواقعة على الأشخاص، وتعتبر نشر الإباحية والجنس خصوصا عند الأطفال من أهمّها، حيث يتعرّض الأطفال للاستغلال الجنسي على الانترنت بأشكال متعدّدة انطلاقا من الصوّر إلى التسجيلات المرئية للجرائم الجنسية العنيفة، حيث تستمر معاناتهم إلى ما بعد

---

[15] . حبيباتني بثينة، الطبيعة الخاصة للجريمة المعلوماتية، مجلة دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، المجلد12، العدد3، 2020م، ص 609.

[16] - فيروسات كورونا هي مجموعة من الفيروسات التي يمكن أن تصيب الإنسان والحيوان على حدّ سواء، مُسَبِّبة اعتلالات متنوعة، قد تكون خفيفة كنزلات البرد، أو شديدة مثل الالتهاب الرئوي، كمرض سارس (المتلازمة النفسية الحادة الوخيمة) الذي انتشر مابين 2002م و2003م، أو متلازمة الشرق الأوسط التنفسية mers التي ظهرت في 2012م. أمّا كوفيد .19 هو مرض مُعْد، يُسَبِّبه فيروس كورونا، وكمصطلح فهو يتكون من عدّة أجزاء، يحمل كلّ جزء معنى، حيث أنّ: "كو" هو اختصار كورونا، و "في" اختصار لفيروس، و" د" اختصار للداء أو المرض، ورقم 19يشير إلى العام الذي أُعلن فيه عن تفشي هذا المرض الجديد، الذي كان في نهاية ديسمبر 2019م، بداية من مدينة ووهان الصينية. ويطلق البعض عليه تسمية المتلازمة التنفسية الحادة الوخيمة كورونا 2، أو سارز كوف2.

[17] . سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010م،2011م

ارتكاب الجريمة بسبب إمكانية تناقل الصور عبر الانترنت[18]، كما أنّ جريمة التهديد والمضايقة والملاحقة خاصة عن طريق البريد الالكتروني أو وسائل الحوارات الآنية عبر شبكة الانترنت كالفايسبوك أو الواتساب ...عرفت انتشارا واسعا، بالإضافة إلى جرائم التغرير والاستدراج وانتحال الشخصية التي أطلق عليها البعض جريمة الألفية الجديدة(سواء انتحال شخصية الفرد، أو انتحال شخصية المواقع) [19] ونفس الأمر يقال عن جرائم السب والقذف الأكثر شيوعا لتلطيخ سمعة الغير والمساس بشرفهم وكرامتهم من خلال غرف الدردشة، أو مقاطع فيديو أو تطبيقات التيك توك ...، الأدهى أنّه يتم تداولها ونشرها عبر المواقع حتّى وإن كانت مغلوطة أو غير صحيحة.

ب . الجرائم الواقعة على الأموال: ويدخل في التقسيم جرائم معتبرة خصوصا مع التطوّر التكنولوجي الحاصل، حيث أخذت وسائل الدفع الالكتروني كالبطاقات الذهبية أو البنكية حيزا من جرائم القرصنة والسرقة والاحتيال والتحويل الالكتروني من حساب بطاقة عميل إلى حساب أو رصيد آخر؛ باعتبارها نقودا إلكترونية، من خلال إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريق غير المشروع عبر قنوات شبكة الانترنت. [20]

ومن أهمّ الجرائم الالكترونية على الأموال، جريمة القمار وغسيل الأموال عبر الانترنت من خلال الكازينوهات الافتراضية وأندية الأقمار الرقمية، إذ أنّها تمنح الراغب ممارستها الخصوصية وخفاء الشخصية، بالإضافة إلى جريمة المخدرات عبر الانترنت والتي لم تعد المواقع تروّج لها أو تُشَوّق النشء لاستخدامها فقط، بل إلى كيفية زراعتها وصناعتها بكافة أصنافها وأنواعها وبأبسط الوسائل المتاحة.[21]

ج . الجرائم الواقعة على أمن الدول

استغلّت الكثير من الجماعات المتطرّفة الطبعة الاتصالية للإنترنت من أجل بث معتقداتها وأفكارها، ليصل بها الأمر إلى ممارسات تهدّد أمن الدولة، ممثلة في الإرهاب الالكتروني والجريمة المنظّمة، فقد أتاحت الانترنت لكثير من الدول ممارسة التجسّس على دول أخرى، وذلك بالاطلاع على مختلف الأسرار العسكرية والاقتصادية ...، كما أعطت الانترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما سهل وجرّ إلى نزاعات وفوضى.[22] لتظهر العلاقة جليا بين الإرهاب والجريمة الالكترونية من خلال تجنيد وتجييش أعضاء جدد في التنظيم أو حشد الهمم بواسطة استخدام مختلف وسائل التواصل الالكتروني، كما

---

[18] . نميدلي رحيمة، خصوصية الجريم الإلكترونية في القانون الجزائري والقوانين المقارنة، المرجع السابق، ص102.

[19] . صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2013م، ص 50، 51.

[20] . خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2010م، ص 67.

[21] . صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2013م، ص 46، 49.

[22] . بوضياف إسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 3، العدد3، 2018م، ص 358.

يتم تبني الدعاية والعمليات الإرهابية من خلال مختلف وسائط التواصل الالكترونية[23] كما أنّ أعضاء الجريمة المنظمة استفادوا من وسائل الاتصال والتكنولوجيا التي لم تعد تعترف بالحدود الجغرافية في تخطيط وتمرير وتوجيه المخططات وتنفيذ العمليات الإجرامية بيسر وسهولة[24].

ثانيا . الجرائم الواقعة على النظام المعلوماتي: وهذا الصّنف من الجرائم يمسّ النظام المعلوماتي، حيث تكون المكونات المادية له، أو المعلومات المدرجة به هدفا يتوصّل إليه، نوضّحها بشيء من الإيجاز كما يلي:

أ . الجرائم الواقعة على المكونات المادية للنظام المعلوماتي

يُقصد بالمكوّنات المادية للنظام المعلوماتي بالأجهزة والمعدّات الملحقة به والتي تستخدم في تشغيله، كالأسطوانات والشرائط والكابلات. ونتيجة للطبيعة المادية لهذه المعدّات تكون الجرائم الواقعة عليها تقليدية كأن تكون محل للسرقة وخيانة الأمانة أو الإتلاف العمدي أو الإحراق أو العبث بمفاتيح التشغيل، ممّا يترتّب عليها خسائر كبيرة، ولقد حدث هذا النوع من الجرائم في فرنسا، وأدى إلى إتلاف معدّات مؤسّسة كبيرة ومتخصّصة في بيع الأنظمة وتوثيق المعلومات الحسابية، وقُدّرت الخسائر ب5 ملايين فرنك فرنسي.[25]

ب –الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي

تُعتبر المعلومة المعالجة آليا ذات أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي، لما لها من قيمة اقتصادية، وتتّم الجرائم عليها من خلال التلاعب فيها بصفة مباشرة أو غير مباشرة أو عن طريق إتلافها أو استبدالها أو محوها، وهذا ما يسمّى بالغش أو التزوير المعلوماتي، فقد قام شخص وهو موظّف بوزارة المالية باستخدام طريقة تدعى BLUFF، حيث قام بإدخال فواتير وهمية لا حصر لها وتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي قام بإنشائها.[26]

ج . الجرائم الواقعة على البرامج الالكترونية[27]: هي جرائم تتطلّب مهارة فنية عالية في مجال البرمجة وتقع على البرامج التطبيقية أو برامج التشغيل.

. الجرائم المعلوماتية الواقعة على البرامج التطبيقية: يحدّد فيها الجاني البرنامج أولا، ثمّ يقوم بالتلاعب فيه لتحقيق أكبر استفادة مالية، وهذا من خلال قيامه بتعديل البرنامج أو التلاعب في البرامج. أما تعديل البرنامج فعادة ما يكون هدفه الرئيس اختلاس النقود، مثاله قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل البرنامج عن طريق إضافة دولار واحد على كل حساب يزيد عن عشر دولارات ،ثم قيامه بقيد هذه المصاريف الزائدة في حساب خاص به يتحصل على إثره على مئات الدولارات خلال كل شهر. أما التلاعب في البرنامج فإنّه يأخذ عدّة أشكال وصور فقد يتم عن طريق ما يُسمّى بالقنبلة المنطقية المتمثلة في برنامج

---

[23] . رحموني محمد، خصائص الجريمة الالكترونية ومجالاتها، مجلة الحقيقة، المجلد 16، العدد3، 2018م، ص448.

[24] . سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر العربي، الإسكندرية، 2007م، ص83.

[25] - بوضياف إسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، المرجع السابق، ص 359.

[26] - نميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المرجع السابق، ص104.

[27] . خلدون عيشة، محاضرات الجريمة المعلوماتية، موجهة لسنة أولى ماستر تخصّص القانون الجنائي والعلوم الجنائية، ص14.

أو جزء من برنامج ينفذ في كل لحظة أو كل فترة زمنية منتظمة يوضع في شبكة معلوماتية بغرض تسهيل عمل غير مشروع، أو عن طريق قيام أحد المبرمجين بزرع برنامج فرعي غير مسموح به في البرنامج الأصلي ممّا يسهّل له عملية الدخول الغير مشروع في العناصر الضرورية لأيّ نظام معلوماتي مع ملاحظة صعوبة اكتشافه بسبب صغره ودقّته.

. الجرائم المعلوماتية الواقعة على برامج التشغيل: برامج التشغيل هي البرامج المسؤولة عن عمل النظام المعلوماتي حيث تقوم بتنظيم وضبط ترتيب تعليماته الخاصة، جريمته تتّم بتزويد البرنامج بتعليمات إضافية يسهل الوصول إليها بواسطة شفرة تسهل الحصول على معلومات النظام وتتّم بالمصيدة بإعداد المبرمج لبرنامج به عيوب وأخطاء عمدا للدخول إليه بسهولة، فهي ممرات خيالية وفواصل وتفرعات في البرنامج تمكّنه من تنفيذ التعديلات الضرورية تمكنه من الدخول للنظام المعلوماتي والوصول إلى معلومات الذاكرة، أو تتم بتصميم برنامج وهمي وذلك بقيام المبرمج بوضع برنامج يصعب اكتشافه مخصص لارتكاب الجريمة ومراقبة تنفيذها.

ثالثا . تصنيف اتفاقية بودابست

لعلّ أهم تصنيف هو الذي جاءت به الاتفاقية الأوربية لمكافحة الجريمة الالكترونية وهي اتفاقية بودابست، والذي يتضمّن أربع مجموعات:

المجموعة الأولى: الجرائم التي تستهدف سرية وسلامة وتوفر المعطيات والنظم، وتشمل:

- الدخول غير قانوني (غير المصرح به).
- الاعتراض غير القانوني.
- تدمير المعطيات.
- اعتراض النظم.
- إساءة استخدام الأجهزة. [28]

المجموعة الثانية: الجرائم المرتبطة بالكمبيوتر، أي الجرائم التي يلعب فيها الكمبيوتر أو الحاسوب الآلي دور الوسيلة كجرائم الاحتيال والتزوير الالكتروني.

المجموعة الثالثة: الجرائم المرتبطة بالمحتوى، حيث يلعب فيها الكمبيوتر دور البيئة الإجرامية، وتتعلّق الجرائم بالأفعال اللاأخلاقية وجرائم القمار وغسيل الأموال والمخدرات.[29]

المجموعة الرابعة: وهي الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة – قرصنة البرمجيات.[30]

---

[28] . يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – أبو ظبي 10-12 /2/2002م،
http://almuhamatresalah.blogspot.com/2014/03/blog-post_2785.html يوم 2022/07/30م

[29] . نميدلي رحيمة، خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة، المرجع السابق، ص 105.

[30] . يونس عرب، جرائم الكمبيوتر والانترنت، المرجع السابق.

2. أهمّ المجالات التي استهدفتها الجريمة الالكترونية في ظلّ جائحة كورونا

سَجَّلت الجريمة الالكترونية في السنوات الأخيرة ارتفاعا ملحوظا، لتتبلور أكثر خلال الأزمة الصّحّية العالمية فيما يعرف بجائحة كورونا، ويبدو أنّ هناك أنشطة ومجالات كانت مُستهدَفَة أكثر من غيرها خلال هذه الفترة الوبائية، يمكن أن نبيّنها فيما يلي:

المجال الصّحي: يعتبر القطاع الصّحي من أكثر القطاعات تضرّرا من الجريمة الالكترونية، ففي ضوء الطلب المتزايد على منتجات الحماية الشخصية والنظافة الصحية، استغل المجرمون هذا الظرف لجني الأرباح وتحقيق الكسب المادي عن طريق بيع منتجات مقلّدة أو لا تستوفي المعايير المطلوبة مثل الكمامات الجراحية ومضادات الفيروس والفيتامينات، وحتّى أدوية وهمية لعلاج فيروس كورونا، وأحيانا أخرى سرقتها، لتزدهر مبيعات المنتجات الصحية المزيّفة والمعقّمات المزوّرة عبر المواقع الالكترونية والاشهارات على مختلف شبكات الاتصال والتواصل. كما في حالة إحدى الشركات الأوروبية التي طلبت مواد حماية، من بينها أقنعة ومعقّمات ومطهّرات من شركة في سنغافورة مقابل 6.6 ملايين يورو، لكنّ البضاعة لم تصل، ذلك أنّ هناك عصابات قامت باختراق أنظمة الشركة واستولت على المبيعات. وفي عملية مشتركة للشرطة الأوروبية، بالتعاون مع 90 دولة، أسفرت عن مصادرة 34 ألف كمامة مزيفة على مستوى العالم، فضلاً عن العثور على 4.4 ملايين عقار مقلدا، بعدما جرى اكتشاف 37 عصابة واعتقال 121 شخصاً، كما جرى تحديد أكثر من 2000 موقع إلكتروني يعرض مواد معقّمة غير فعّالة ضد الفيروس، وجرت مصادرة 4 ملايين وحدة دواء وأجهزة تنفس وهمية ضمن عمليات للشرطة الأوروبية.[31] كما استهدف مجرمو المعلوماتية ولصوص الحظر أنظمة المؤسّسات الصحية واختراقها ظنّا منهم أنّ هذه المؤسّسات ستضطر إلى دفع المال أو الفدية لاستعادة أنظمتها. فقد تعرّض مستشفى في جمهورية التشيك لهجوم إلكتروني، وفقاً لـ"يوروبول"، ما اضطر المستشفى لوقف نظام تكنولوجيا المعلومات لديه، ما أجّل المعاملات الطبية.[32]

المجال المالي: يعدّ هذا المجال هو الآخر ممّن استهدفه مجرمو ومخترقو المعلوماتية، من خلال عمليات السرقة التي تتم عبر ماكينات الصرف الآلي والبنوك باعتماد نسخ البيانات واستخدامها لنهب وسحب أموال الضحية، أو إنشاء مواقع في صفحات الانترنت مماثلة للمؤسّسات المصرفية أو البنكية، ومطالبة العميل إدخال بياناته، ومن ثَمّ سرقتها. أو من خلال رسائل البريد الالكتروني، فكثيرا ما تأتي رسائل من مصادر مجهولة بخصوص طلب المساهمة في تحويل الأموال من الخارج مع الوعد بنسبة من المبلغ، أو تلك التي توهم صاحب البريد الالكتروني بفوزه بإحدى الجوائز وتطالب بموافاة الجهة برقم حسابه المصرفي.[33] خصوصا أنّ الجزائر وغيرها من الدول شجّعت في فترة انتشار فيروس كورونا على استعمال البطاقات البنكية أو الذهبية... تفاديا للاحتكاك بين المواطنين، وهذا ما استغله قراصنة المعلوماتية. فقد كشفت تقارير

---

[31] . ازدهار سوق المنتجات الطبية والوقائية المزيفة في زمن كورونا، https://www.alaraby.co.uk/ 2022/07/30م.

[32]. ازدهار سوق المنتجات الطبية والوقائية المزيفة في زمن كورونا، https://www.alaraby.co.uk/2022/07/30م.

[33] . محمود شرقي، صلاح الدين جبار، تأثير تطور تكنولوجية المعلوماتية على تنامي الجريمة، https://www.asjp.cerist.dz/en/downArticle/354/8/1/62499 2022/07/30م.

مختصّة بأمن المعلومات أنّ مخترقون استهدفوا أشخاصا ومؤسّسات من خلال روابط مشبوهة للحصول على بيانات الدخول إلى الحسابات المالية، وأنشؤوا أكثر من 100 ألف نطاق جديد لمواقع إلكترونية عن كوفيد19، في محاولة خداع الأفراد كي يسجلوا بياناتهم.[34] وفي تقرير آخر تعرّضت شبكة "بولي نت وورك" العاملة كمنصة لتداول العملات الافتراضية المشفرة، إلى اختراق من جانب مجهولين، تمكنوا خلاله من سرقة عملات بقيمة 600 مليون دولار.

وذكرت الشبكة في سلسلة تغريدات عبر صفحتها على "تويتر" أنّ السرقة جَرْت بعد قيام مجهولين باختراق أنظمتها الأمنية، داعية عملاءها لتجنّب أية مراسلات تتضمّن رموزا مشفرة.[35]

المجال الترفيهي للألعاب الالكترونية: أجبر الوباء الناس على البقاء في منازلهم ممّا جعلهم يلجؤون إلى العالم الافتراضي بعيدا عن الأزمة الصحية العالمية، من خلال الألعاب الالكترونية خاصّة، التي توسّع استعمالها خلال أزمة الوباء العالمي إلى حدّ الإدمان، وتعتبر فئة الأطفال أكثر الضحايا من هذه الناحية.

ولطالما استغل المحتالون المتخفيّون بفيروس كورونا الوضع، ومثال ذلك استغلالهم الألعاب الأونلاين وأصبحت هدفا ثمينا لهم، نظرا لأنّها تتضمّن عُملات ومشتريات داخل الألعاب إلى جانب العُملات الحقيقية الموجودة في المحافظ.

بالإضافة إلى خطر الألعاب الالكترونية من جهة إدمانها وفَقْد المال، هناك مخاطر أخرى، في مقدّمتها احتواء هذه الألعاب على برامج ضارة، ففي بعض الأحيان يحتاج المستخدّم إلى تنزيل مكوّن برمجي إضافي من أجل تشغيل لعبة معيّنة، وقد يتم إعادة توجيهه بعد ذلك إلى مواقع أخرى حيث يُمْكن للبرامج الضارة فيها إلحاق الأذى بأمان جهاز المستخدم وخصوصيته. أيضًا قد تكون الفيروسات مضمَّنة في ملفات اللعبة التي قد يسمح المستخدم بتنزيلها على النظام دون أن يدري أثناء التثبيت. كما أنّ من مخاطر الألعاب الأونلاين انتهاك الخصوصية عن طريق جمع البيانات من الألعاب وغيرها من المصادر، فقد يتمكّن المتسلّلون من الوصول إلى حسابات أخرى لك، مثل حساباتك على مواقع التواصل الاجتماعي، أو إنشاء حسابات جديدة باسمك، بل وحتى إنشاء هويات رقمية كاملة باسمك[36]! والأخطر في الألعاب الالكترونية أنّ بعضها تدفع بالانتحار، وخير مثال لعبة الحوت الأزرق وهي تطبيق يُحمّل على أجهزة الهواتف الذكية وتتكوّن من 50 مهمة، تستهدف المراهقين بين 12 و16 عاماً، وبعد أن يقوم المراهق بالتسجيل لخوض التحدي، يُطلب منه نقش الرمز التالي "F57" أو رسم الحوت الأزرق على الذراع بأداة حادة، ومن ثَمَ إرسال صورة للمسؤول للتأكّد من أنّ الشخص قد دخل في اللعبة فعلاً، بعد ذلك يُعطى الشخص أمراً بالاستيقاظ في وقت مبكر

---

[34]. دبي للمستقبل، توجهات عالمية لتعزيز الأمن الرقمي وتبني الذكاء الاصطناعي لحماية القطاعات https://pressn.net/article/8564830?news 2022/07/30م.

[35] . منصة عملات مشفرة تتعرّض للاختراق وسرقة 600 مليون دولار، https://www.alaraby.co.uk/economy 2022/07/29م.

[36] . عمليات النصب المتعلقة بالألعاب الأونلاين في ظل انتشار فيروس كورونا: سبل لحمايتك وعائلتك، https://me.kaspersky.com/resource-center/threats/coronavirus-gaming-scams 2022/08/02م.

جداً، عند 4:20 فجراً مثلاً، ليصل إليه مقطع فيديو مصحوب بموسيقى غريبة تضعه في حالة نفسية كئيبة. وتستمر المهمات إلى أن يصل اليوم الخمسون، الذي يُطلب فيه منه الانتحار إما بالقفز من النافذة أو الطعن بسكين[37] ونتيجة للأرواح التي حصدها هذا التطبيق في العالم والجزائر خصوصا، أطلقت الجزائر حملة توعوية في المدارس والمساجد وعبر وسائل الإعلام من خطورة لعبة الحوت الأزرق، لتقرّر في الأخير حجب هذه اللعبة من المواقع الالكترونية. والأكيد لولا الحملات التحسيسية وقرار الحجب لهذه اللعبة ومثيلاتها قبل جائحة كورونا لكانت الكارثة.

. مجال الدردشة والاجتماعات والمؤتمرات عبر المنصّات الرقمية: تعرّضت هي الأخرى المحادثات الالكترونية إلى الاختراق وظهرت فيها ثغرات أمنية استغلها لصوص الحظر، تمّ تحذير الملايين من مستخدمي «Microsoft Teams» من هجوم جديد يمنح المتسللين سيطرة كاملة على أجهزة الكمبيوتر الخاصة بهم، حيث لجأ الكثيرون إلى هذا التطبيق لعقد الاجتماعات من خلال الإنترنت، منذ اندلاع وباء فيروس كورونا، وتضمّ المنصة الآن أكثر من 270 مليون مستخدم نشط شهريًا، يستهدف المتسلّلون الاجتماعات عبر الإنترنت بالبرامج الضارة، ووفقًا لفريق الأمان فيAvanan، بدأ المتسلّلون مهاجمة مستخدمي «Microsoft Teams» عبر ملفات exe الضارة المُضَمّنة في سلاسل المحادثات. وبمجرد التنزيل، يبدأ المتسلّلون في مهاجمة أجهزة الكمبيوتر وتثبيت البرامج الضارة التي تمنحهم وصولاً كاملاً إلى الجهاز وكلّ ما يتم تخزينه عليه.[38] وفي نفس السياق فقد اكتشف أحد الباحثين عيبين جديدين في تطبيق مؤتمرات الفيديو Zoom يسمحان للهاكرز باختراق كاميرا الويب للمستخدمين وميكروفونهم، ووفقا لما ذكرته صحيفة "ديلى ميل" البريطانية، سمحت هذه الثغرات التي تم تحديدها سابقًا للهاكرز بسرقة كلمات مرور Windowsوأيضًا اختراق أمان آخر للأمن على أجهزة Mac من خلال السماح لهم بالاستفادة من كاميرا الويب والميكروفون للمستخدمين. وكشف التقرير حاليا عيوب جديدة في تطبيق مؤتمرات الفيديوZoom، تَعْرضُ الصوت ومقاطع الفيديو. كما أنّ هناك خطأ ثانٍ تمّ تحديده بواسطة واردل، والذي يتضمّن أيضًا الوصول المادي إلى الجهاز، الذي يضرّ بتدفّق الصوت والفيديو فيZoom حيث يعمل الهاكرز من خلال إدخال شفرة ضارة فيZoom، وبالتالي يتمكّنوا من خداع الخدمة لتسليم كاميرا الويب والوصول إلى الميكروفون لمستخدم آخر.[39] كما حذّر مكتب التحقيقات الفدرالية الأميركي المواطنين من الاختراق الذي يحدث عبر تطبيق الاجتماعات "زوم" الشهير، وذلك بعد أنْ تمَّ اختراق فصلين دراسيين على الشبكة أثناء استخدام مكالمات الفيديو. وقالت وسائل إعلام أميركية إنّ "زوم" شهد زيادة هائلة في عدد المستخدمين منذ

---

[37]. هديل كرنيب ما هي لعبة الحوت الأزرق التي "تدفع بالأطفال إلى الانتحار"؟
https://www.annahar.com/arabic/article/713833 2022/08/02م.

[38] . كلود عمر، لمستخدمي» ..Microsoft Teams هاكرز» يتبعون حيلة لاختراق الهواتف عن طريق التطبيق،
https://lite.almasryalyoum.com/technolight/259934 2022/08/02م.

39 . اكتشاف ثغرات جديدة بـ Zoom تتيح للمتسللين اختراق الكاميرا والميكروفون
https://www.youm7.com/story/2020/4/3 2022/08/02م.

أنْ أجبر وباء كورونا عددا كبيرا من الأشخاص على البقاء في منازلهم، واللجوء إلى اجتماعات الفيديو للعمل أو الدراسة أو التفاعلات الاجتماعية.[40]

ثالثا . عوامل انتشار الجريمة الالكترونية زمن تفشي فيروس كورونا كوفيد-19 وأبرز التدابير التي اتّخذتها الجزائر لمكافحته

هناك عوامل مختلفة ومتداخلة أسْهمت في تنامي الجريمة الالكترونية، ولعلّ الوضع الوبائي وما صاحبه من إجراءات كان له نصيب كبير في تفاقمها، نبيّن في هذه النقطة من الدّراسة بعض التدابير التي اتّخذتها السلطات التشريعية لمكافحة انتشار فيروس كورونا كوفيد-19، لنعرّج بعدها على عوامل انتشار هذه الجريمة في ظلّ هذه التدابير وتداعيات الفيروس.

1- أبرز التدابير التي اتّخذتها الجزائر لمواجهة انتشار فيروس كورونا كوفيد-19

انتشر فيروس كورونا كوفيد-19 بالجزائر وانتقل إلى مواطنيها، حيث تمّ الإعلان عن أول حالة في 25 فيفري 2020م لرعية إيطالي كان يعمل بحقل نفط في حاسي مسعود، لتتوالى فيما بعد الإصابات بهذا الفيروس، ما جعل رئيس الجمهورية يأمر على جناح السرعة بغلق المعاهد والمؤسّسات التعليمية وروضات الأطفال. وبعد أن تجاوز عدد المصابين 27 خلال الفترة 16، 17 مارس 2020م، تمّ تعليق كافة الرحلات الجوية نحو أوروبا، كما أمر وزير الشؤون الدينية والأوقاف بغلق المساجد ومنع صلاة الجمعة عبر كافة التراب الوطني... وفي ظلّ تزايد عدد الإصابات وعدم وجود لقاح أو دواء لهذا الفيروس، تمّ إصدار مجموعة من التدابير الصحية لتطويق هذا الفيروس وكبح انتشاره، ويأتي في مقدّمتها المرسوم التنفيذي رقم 69/20[41] والمرسوم 70/20[42] والمرسوم رقم 127/20[43] ومن أبرز ما جاء فيها:

. غلق محلات بيع المشروبات، ومؤسّسات وفضاءات الترفيه والتسلية والعرض والمطاعم باستثناء تلك التي تضمن خدمة التوصيل إلى المنازل.

. تقليص عدد الموظفين وتعليق النقل الجماعي وغلق المقاهي ومنع التجمعات.

---

[40] . المؤسس يعترف بالتقصير.. القراصنة يقصفون تطبيق "زوم" وشركات كبرى تمنع العمل به، https://www.aljazeera.net/news/scienceandtechnology/2020/4/2 2022/08/02م.

[41] . المرسوم التنفيذي رقم 69/20، المؤرخ في26 رجب 1441هـ، الموافق لـ21 مارس 2020م المتعلق بتدابير الوقاية من انتشار وباء فيروس كورونا كوفيد19 ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد15.

[42] . المرسوم التنفيذي رقم 70/20 المؤرخ في 29رجب 1441 هـ، الموافق 24 مارس 2020 م، الذي يحدّد تدابير تكميلية للوقاية من انتشار وباء فيروس كورونا كوفيد 19 –ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 16.

[43] . مرسوم تنفيذي رقم 127/20 مؤرخ في 27 رمضان 1441هـ، الموافق لـ20 ماي 2020م، يعدّل ويتمم المرسوم التنفيذي رقم 70/20 الذي يحدد التدابير التكميلية للوقاية من انتشار وباء فيروس كورونا كوفيد19 ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 30.

. الحجر المنزلي، والذي يكون كليا أو جزئيا[44] ولفترات محدّدة، حسب الوضعية الوبائية للولاية أو البلدية المعنية.

. احترام التباعد الأمني بين شخصين في الأماكن العامة والعمل بمتر واحد على الأقل.

. ارتداء القناع الواقي.

. منح تراخيص لتنقل الأشخاص خارج أوقات الحجر على سبيل الاستثناء من قبل لجان مختصة.

. تعريض الغير للخطر بنقل عدوى فيروس كورونا كوفيد19 يعاقب عليه القانون. وقد أحال المرسومين التنفيذيين 70/20 والمرسوم 127/20 السالفين الذكر، إلى تطبيق الجزاءات على المخالفين إلى أحكام قانون العقوبات بموجب المادة 8 من القانون 06/20 المعدل والمتمم لقانون العقوبات[45] بموجب المادة 290مكرر، والتي نصت " يعاقب بالحبس من ستة(6) أشهر إلى سنتين(2) وبغرامة من 60.000دج إلى 200.000دج كل من يعرض حياة الغير أو سلامته الجسدية مباشرة للخطر بانتهاكه المتعمد والبيّن لواجب من واجبات الاحتياط أو السلامة التي يفرضها القانون أو التنظيم. تكون العقوبة الحبس من ثلاث(3) سنوات إلى خمس(5) سنوات والغرامة من 300.000دج إلى 500.000دج، إذا ارتكبت الأفعال المذكورة أعلاه خلال فترات الحجر الصحي أو خلال وقوع كارثة طبيعية أو بيولوجية أو تكنولوجية أو غيرها من الكوارث. يعاقب الشخص المعنوي الذي يرتكب الجريمة المنصوص عليها فيهذه المادة وفقا للأحكام المنصوص عليها في هذا القانون." والملاحظ من هذه المادة أن العقوبات الجزائية المقرّرة لجريمة تعريض الغير للخطر تتفاوت بين الشخص الطبيعي والمعنوي، كما أنّها تتفاوت فيما إذا كانت الظروف عادية أو إستثنائية.

2 ـ عوامل انتشار الجريمة الالكترونية زمن جائحة كورونا كوفيد-19

بالرجوع للأسباب التي شجعت أو كانت من وراء تنامي الظاهرة الإجرامية الالكترونية تحديدا نجدها متعدّدة فمنها ما هو اجتماعي ومنه ما هو اقتصادي، أمني ، نفسي... فضلا التدابير المتّخذة لمكافحة انتشار فيروس كورونا كوفيد -19 سواء على المستوى الوطني أو الدولي، يمكن أن نبيّنها إجمالا فيما يأتي:

- قضاء الكثير من الأفراد أوقاتهم في الحاسوب والهاتف نتيجة الحجر الصحي، ما أدى بوقوع عدد منهم في الاحتيال الالكتروني والانسياق وراء الاشهارات الالكترونية الكاذبة والتضليلية.
- الإقبال المنقطع النظير على أسواق التجارة الالكترونية والاعتماد على التسوق الالكتروني وخدمة التوصيل المنزلي، خصوصا بعد تشجيع الدول لها باعتبارها آلية آمنة من حيث انتشار فيروس كورونا

---

[44] . المادة 04 من المرسوم التنفيذي70/20" يتمثل الحجر المنزلي الكلي في إلزام الأشخاص بعدم مغادرة منازلهم أو آماكن إقامتهم خلال الفترة المعنية ماعدا في الحالات المنصوص عليها في هذا المرسوم. و/أو الفترات الزمنية المقررة من طرف السلطات العمومية. ويتمثل الحجر المنزلي الجزئي في إلزام الأشخاص بعدم مغادرة منازلهم أو آماكن إقامتهم خلال الفترة و/أو الفترات الزمنية المقررة من طرف السلطات العمومية.

[45] . قانون رقم 06/20 المؤرخ في 5 رمضان 1441هـ الموافق لـ28 أبريل 2020م يعدل ويتمم الأمر 156/66 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 25.

كوفيد-19، كونها تُجَنّب الاحتكاك المباشر والملامسة... ما أوقع بالكثير كضحايا لجرائم النصب والغش...

- الإفراج عن المحبوسين في السجون، حيث اتجهت بعض الدول إلى الإفراج عن المسجونين بتهم جنائية خطرة تخوّفاً من إصابات في صفوفهم بمرض "كورونا"، وهو ما دفعهم إلى ممارسة الإجرام مرة أخرى. ولعلّ الحالة التركية معبرة في هذا السياق، حيث كشفت بعض وسائل الإعلام التركية، مثل صحف "زمان" و"بيرجون" و"إيفرنسال"، عن الجرائم التي ارتكبها المجرمون المستفيدين من قرار العفو بعد إقرار البرلمان التركي لذلك، رغم التحذيرات التي أطلقها الخبراء من تداعيات الإفراج عن هؤلاء على الأمن الوطني[46].
- قلّة الوعي المعلوماتي والافتقار لثقافة الأمن والحماية الالكترونية.
- زيادة فترة استخدام شبكة الانترنت في ظل انتشار فيروس كورونا، خصوصا أنّ العمل والتعليم والتسوّق ...أصبحت تتم عن بعد، ما زاد معه عدد الاختراقات والهجمات الالكترونية.
- نجم عن القلق والخوف من فيروس كورونا كوفيد 19 الى لجوء الكثير بالبحث عن معلومات عبر شبكة الانترنت لتفادي الإصابة بهذا المرض، غير آبهين أو مدركين للفخاخ الالكترونية، ذلك أنه توجد مواقع بمجرد الدخول إليها يتم اختراق الأجهزة أو سرقة البيانات الشخصية، وهذا ما قام به المجرمين الالكترونيين في هذه الفترة من خلال المواقع والروابط.
- تركيز المؤسّسات العسكرية والأمنية على التدابير المتخذة لمواجهة انتشار كورونا كوفيد 19 ومدى التزام المواطن بها.
- ضُعْف الدخل وشيوع البطالة بسبب تدابير الحجر المنزلي وإجراءات التعليق والغلق التي مست بعض الأنشطة، ما أسفر عن انتشار عمليات النصب والخداع خصوصا عبر مواقع التواصل الاجتماعي.
- حبّ التحدّي واثبات التفوّق في مجال وسائل التقنية ونظام المعلوماتية، حيث أن بعض الأشخاص همهم وهدفهم هو الوقوف أمام شاشات الهاتف أو الحاسوب إثباتا لبراعتهم وقدرتهم على اختراق الأنظمة والمواقع والبرامج وما هو جديد في هذا المجال.
- اللجوء إلى الألعاب الالكترونية خاصّة الأطفال بسبب الحجر المنزلي والعطلة الطويلة التي عرفها قطاع التربية والتعليم تسبب في إدمانهم لهذه الألعاب، ما جعل الكثير من هذه الشريحة تصاب بالجنون والانهيارات العصبية والانتحار، من بينها لعبة "بوبجي" و"فري فاير"[47]
- التحسّن المستمر لشبكة الاتصالات والانترنت والاستعمال الواسع لها، خاصة في فترة تفشي فيروس كورونا كوفيد-19.

---

[46]. كيف أثر منع التجول على جرائم ما بعد "كورونا" في الإقليم؟، https://futureuae.com/m/Mainpage/Item/5571 2022/08/02م.

[47] . آمال عيساوي، ألعاب تصيب الأطفال بالجنون والانهيارات العصبية، https://www.echoroukonline.com/ 2022/07/30م.

- سهولة إخفاء معالم الجريمة الالكترونية وصعوبة الوصول إلى دليل واضح للإدانة أو كشف هوية الفاعل، في ظلّ سرعة محو أدوات الجريمة وتقاعس أو إحجام الكثير عن التبليغ عن الجرائم الالكترونية وقت ارتكابها والتي يرجع أحد أسبابها إلى تداعيات فيروس كورونا وانشغال الناس به.
- الخصائص التي تتميّز بها وسائل الاتصال الحديثة كالهواتف والحواسيب في تحقيق جرائم كثيرة، من سرعة وسهولة وتحرّر جغرافي باعتبارها عابرة للحدود، التي انجر عنها مشكلة الاختصاص القضائي كونها واقعة في فضاء إلكتروني والفاعل خارج الحدود.
- التهديد الأمني فيما يعرف بالإرهاب الالكتروني أو التجسس الالكتروني، والذي يكون عادة لزعزعة استقرار الدول من خلال الإشاعات والأفكار التي تنشر الفوضى.

رابعا . التطوّر التكنولوجي بين خدمة الظاهرة الإجرامية ومكافحتها فترة انتشار فيروس كورونا كوفيد -19

أربك تفشي فيروس كورونا كوفيد-19 العالم، وتغيّرت معه تفاصيل الحياة العادية، فأُغلقت الحدود والمطارات...وأصدرت حزمة من القوانين والمراسيم كتدابير لمواجهته؛ والجريمة ليست استثناء عن هذا التحوّل، فإغلاق الدول للحدود وانعزال الأشخاص في منازلهم بسبب الحجر المنزلي وجد المجرمون صعوبة في كسب المال بالطرق التقليدية في هذا الظرف الوبائي، ما جعلهم يلجؤون إلى سبل أخرى وفّرها لهم بالدرجة الأولى التطوّر التكنولوجي، فقد استعان هؤلاء بوسائل تكنولوجية وتقنيات حديثة لتنفيذ مخططاتهم وجرائمهم، فالهواتف والحواسيب وما توفره شبكة الانترنت أصبحت ملاذا لتنسيق أنشطتهم وتحقيق مآربهم نظرا لما تتميز به من سهولة وسرعة واختصار المسافات ....فعمليات السرقة مثلا أصبحت تتّم عبر أجهزة الكمبيوتر.

في خضّم الأزمة الصحية العالمية التي تسبّبت فيها جائحة كورونا رُفعت تقارير بناء على مؤتمرات عُقِدَت عبر دول العالم تفيد بتراجع الجرائم التقليدية كجرائم السطو على المنازل والسرقة والقتل إلى 50 بالمائة، بينما ازداد الاحتيال الإلكتروني وجرائم الإنترنت، ذلك أنّ الإجراءات الاستثنائية والاحترازية التي قامت بها الدول في أعقاب تفشي كورونا ساهمت في تراجع الجرائم التقليدية، إلاّ أنّ الجريمة المنظمة مثلا استطاعت أن تُبدي قدرًا من التكيف مع هذه المتغيرات واستغلال الأزمة وتوظيفها لتحقيق أهدافها والاستمرار في سلوكها الإجرامي، [48] ليُشكّل التزاوج بين التطوّر التكنولوجي وانتشار فيروس كورونا بيئة خصبة ومناخا ملائما لنشاط عدد من الجرائم، خاصّة الجريمة الالكترونية، والقرصنة والفساد المالي، والجريمة المنظّمة،...تغيّرت معه الجرائم نوعًا وكمًا، ليظهر مجرمو المعلوماتية ومجرمو كورونا مستغلين مشاعر الخوف والقلق التي يثيرها فيروس كوفيد -19.

وفي هذا الصدد حذّرت شركة "تشيك بوينت" الأميركية للأمن السيبراني من وجود أكثر من أربعة آلاف نطاق على الإنترنت متعلقة بفيروس كورونا – أي أنّها تحتوي على كلمات مثل كورونا أو كوفيد- منذ بداية عام 2020. واعتبر تقرير الشركة أنّ 3% من هذه النطاقات ضار، و5% أخرى مشبوهة. وقد لا يبدو 3% رقما

---

[48] . محمد اسماعيل، الجريمة في زمن كورونا .. https://www.youm7.com/story/2021/3/22/5251259 يوم 2022/07/31م.

كبيرا، ولكن وفقًا "لتشيك بوينت" أنّ هذه النطاقات المرتبطة بفيروس كورونا من المرجح أن تكون أكثر ضررا بنسبة 50% من أي نطاق آخر مسجّل خلال الفترة الزمنية نفسها. [49] كما أعلنت المنظمة الدولية للشرطة الجنائية (الانتربول) عن ضبط كمامات مقلّدة ومستحضرات تعقيم لليدين غير مستوفية لمعايير السلامة وأدوية مضادة للفيروسات غير مرخصة، بعدما كشفت حوالي 2000 رابط إعلاني إلكتروني لمنتوجات متعلّقة بفيروس كورونا المستجد. منوّهة عن تنوّع أشكال الاحتيال الالكتروني في ظلّ هذه الأزمة الصحية العالمية، فحسب تقارير للمنظمة الدولية، أنّ بعض المجرمين الالكترونيين يعملون على الاتصال بالضحايا لتوهيمهم أنّهم موظفون في عيادات طبية أو مستشفيات أو بنيات علاجية أخرى، ويزعمون أن أحد أقارب الشخص المتصَل به أصيب بالعدوى بالفيروس ليطالبوه بتسديد تكاليف العلاج الطبي. واستنادا (الانتربول) فقد ظهرت "مواقع التصيد الاحتيالي"، وهي عبارة عن رسائل إلكترونية، يفترض أنها صادرة عن أجهزة وطنية أو هيئات صحية عالمية من أجل خداع الضحايا وحملهم على توفير معلومات شخصية عنهم أو تفاصيل الدفع، أو أيضا فتح ملف مرفق يحتوي على برمجية خبيثة. [50] كما أعلنت "وكالة الشرطة الأوروبية" (يوروبول) أنّ جائحة "كوفيد-19" ساهمت في زيادة الجرائم الإلكترونية في أنحاء أوروبا، وخصوصاً لجهة المواد الإباحية المتعلقة بالأطفال وعمليات الاحتيال عبر الإنترنت. كذلك رصدت الوكالة في ذروة الأزمة الصحية "زيادة كبيرة" في المواد التي تنطوي على استغلال جنسي للأطفال على الإنترنت، وأشارت إلى أنّ نشر مواد من هذا النوع "أصبح أكثر شعبيةً مما كان عليه" بسبب القيود على السفر. وفي بيان عن المفوضة الأوروبية للشؤون الداخلية إيلفا يوهانسن إنّ الجائحة أدت إلى تباطؤ جوانب عدة في الحياة المعتادة للناس، لكنّها للأسف زادت وتيرة النشاط الإجرامي عبر الإنترنت."[51]

بالإضافة إلى ظهور العديد من التطبيقات والمواقع الالكترونية، المتبوعة باشهارات تضليلية وكاذبة عبر مختلف وسائل الاتصال الحديثة، فإنّه تمّ تسجيل اختراقات وهجمات إلكترونية وصناعة للفيروسات ونشرها في ظلّ هذه الجائحة، فحتّى منظمة الصحة العالمية شهدت منذ بدء جائحة كوفيد-19 زيادة هائلة في عدد الهجمات الإلكترونية الموجهة إلى موظفيها، وفي عمليات الانتحال الاحتيالية بالبريد الإلكتروني التي تستهدف الجمهور بشكل عام، ففي خلال أسبوع، أدّى هجوم إلكتروني إلى تسريب نحو 450 من عناوين

---

[49] . كيف ازدادت نسب الجرائم الإلكترونية خلال جائحة كورونا
https://www.aljazeera.net/news/scienceandtechnology/2020/5/6 2022/07/31م.

[50] . عبد الله العلوي، فيروس كورونا يفاقم من حدة الجريمة الالكترونية عبر العالم،
https://mapanticorona.map.ma/ar/node/3704 2022/07/31م.

[51] . جائحة كورونا رفعت من نسبة الجرائم الإلكترونية
https://www.alaraby.co.uk/entertainment_media 2022/07/29م.

البريد الإلكتروني وكلمات المرور التابعة للمنظمة، بالإضافة إلى آلاف العناوين وكلمات المرور الخاصة بأشخاص آخرين يعملون في مجال الاستجابة لفيروس كورونا المستجد.[52]

وفي تقرير صادر عن شركة «مايم كاست» المختصّة في حلول الأمن السيبراني ومجال الذكاء الاصطناعي ، بعنوان «100 يوم من فيروس كورونا» عن ارتفاع عدد الجرائم الإلكترونية بنسبة 33% منذ مطلع العام 2020 حتى نهاية مارس من العام نفسه، مع ازدياد عدد زيارات الروابط غير الآمنة أكثر ممّا كان قبل تفشي الوباء، ولا شك أنّ تصاعد خطر الهجمات الإلكترونية بصورة لافتة خلال النصف الأول من العام 2020م لا يمكن فهمه بمعزل عن التحوّلات التي أحدثها فيروس كورونا المستجد«كوفيد- 19» في المجالات كافّة، والتي دفعت معظم دول العالم إلى الاعتماد على التكنولوجيا في تسيير شئونها، وخاصة فيما يتعلق بالعمل عن بُعد، والتعليم عن بُعد، وتزايد اللجوء إلى الاجتماعات الافتراضية، وإدارة أنشطة سوق التجارة والخدمات الإلكترونية. [53]

صحيح أنّ التطوّر التكنولوجي استغله البعض لأنشطة غير مشروعة، ما ساعد على انتشار بعض الجرائم كالجريمة الالكترونية، خصوصا في جائحة كورونا، لكن هذا لا يلغي ايجابياته التي امتدت على مختلف الميادين. كما أنّ ظهور هذه الجرائم المستحدثة جعلت الباحثين وخبراء التقنية والتكنولوجيا في هذا المجال يبتكرون طُرقًا وآليات من شأنها الكشف عن المجرمين والحدّ من هذه الجرائم. فمن ثمرات جهود الباحثين في عالم الجريمة عموما برنامج التنبؤ بالجريمة الذي يُعرف باسم PredPo الذي يمكّنُه التنبؤ بوقوع جريمة ما بدرجة بالغة الدقة، وقد بدأت قوات الشرطة في الولايات المتحدة باستخدامه، فالبرنامج يحسب تنبؤاته استناداً إلى أوقات وأماكن الجرائم السابقة، ويربطها بمعلومات حول السلوك الإجرامي وأنماطه. كما أنّ هناك تقنية باسمShotSpotter ، تعمل من خلال عشرات الميكروفونات المُثَبّتة حول المدينة لترصد أصوات الأعيرة النارية وتحديد مكانها في محيط 40 إلى 50 قدماً، حيث يرى خبراء الشرطة أنّ للبرنامج أهمية، خاصّة في الأماكن التي يندر وجود شهود عيان فيها. وتستخدم أجهزة الشرطة في مقاطعات من مدينة نيويورك التقنية، حيث تحلل بيانات أصوات الطلقات النارية إضافة إلى أدوات لرسم الخرائط وتحليل البيانات لتحديد هويات سكان المكان، وما إذا كان من بينهم مجرمون أو مفرج عنهم تحت المراقبة. وفي تقرير لمدينة تشارلتون الأمريكية أنّه بفضل أحد التقنيات انخفضت معدلات الجرائم الخطرة بنسبة 31 بالمائة.[54] وفي هذا الصّدد قالت وزارة الداخلية البريطانية إنّ خبراءها يعكفون على محاولة التنبؤ بما سيحدث من تقدّم في أساليب الجريمة في المستقبل بهدف الاستعداد لمواجهتها، كما أكّد وزير العلوم البريطاني أنّ

---

[52] . منظمة الصحة العالمية تعلن عن تزايد الهجمات الإلكترونية بمقدار خمسة أضعاف وتحث على اليقظة https://www.who.int/ar/news/item/30-08-1441 2022/08/02م.

[53] . داليا السيد أحمد، لماذا تصاعد خطر الهجمات الإلكترونية في ظل وباء كورونا؟ http://www.nationshield.ae/index.php/home/details/research يوم2022/07/29م.

[54] . أشرف مرحلي، التكنولوجيا تتحدى الجريمة والخارجين على القانون، https://www.alkhaleej.ae/ يوم 2022/07/28م

هناك أبحاثا علمية تجرى ستوفر في المستقبل وسائل متطوّرة لمكافحة الجريمة، وقال إنّه ينبغي الاستفادة من كل سبل الاستعانة بالتكنولوجيا من أجل خفض معدلات الجريمة وبالتالي تحقيق تقدم نوعي في حياة المجتمعات الحديثة.[55]

حاصل الكلام أنّه يمكن الاستفادة ما لفظته التكنولوجيا من وسائل لمكافحة الجرائم خصوصا منها الالكترونية، من خلال تبادل المعلومات المتعلّقة بالمجرمين إلكترونيا، وتعميم بياناتهم في المطارات الدولية، واستخدام البريد الالكتروني في المراسلات بين الجهات الأمنية، واستخدام كلّ الوسائل التقنية الحديثة كالانترنت، الأقمار الصناعية، أجهزة الكشف عن الأسلحة والمخدرات، واستعمال البصمة الالكترونية والعين الالكترونية وتحاليل الحمض النووي لمعرفة المجرمين.[56] وتتبّع المجرمين ورصد تحركاتهم من خلال السوار الالكتروني أو من خلال استعمالاتهم للهوية البيوميترية...، كما يمكن الاستفادة من القنوات الفضائية وشبكة الانترنت وخطوط الهاتف عبر الرسائل النصية في نشر الوعي للمواطنين وبيان خطورة الجرائم بكافة أشكالها خصوصا فئة الأطفال باعتبارهم أكثر الضحايا.

الخاتمة

أعطى عصر التقنية والتطوّر التكنولوجي بُعدا جديدا للجريمة من حيث أدواتها وأساليبها ...فظهرت الجريمة الالكترونية التي لا تعترف بالحدود الجغرافية، شكلّت هاجسا أمنيا للدّول، وما زاد الأمر صعوبة وتحدّيا هو دخول العالم في أزمة صحية بسبب انتشار فيروس كورونا كوفيد-19، حيث حاول الأشرار والجماعات الإجرامية الاستفادة من هذا الظرف باستغلال وسائل التطوّر التكنولوجي لإنعاش أنشطتهم وتحقيق مآربهم.

بعد التطرّق للتطوّر التكنولوجي وتسليط الضوء على الجريمة الالكترونية ـ باعتبارها أبرز مظاهره ـ في ظلّ جائحة كورونا كوفيد-19، خلصت الدّراسة إلى النتائج والتوصيات التالية:

1 ـ النتائج

- ✓ ينصرف معنى التطوّر التكنولوجي في مجال الجريمة إلى ذلك التزايد التدريجي في الاختراعات المادّية كالحاسبات الآلية وشبكة المعلومات....وكذا الاختراعات غير المادّية كمهارات استخدام تلك الآلات والمَعْرِفة بفُنُونها التي قد يكون لها تأثير مباشر أو غير مباشر على الجريمة.
- ✓ تُعدّ الجريمة الالكترونية من إفرازات التطوّر التكنولوجي وأبْرَزِ مظاهره السلبية في عصرنا اليوم.
- ✓ أسْهم التطوّر التكنولوجي في تراجع الظاهرة الإجرامية التقليدية كالضرب، القتل، السرقة في ظلّ انتشار فيروس كورونا، وبالمقابل عرفت الجريمة الالكترونية نموا وتزايدا ملحوظا فترة تفشي هذا الفيروس.

---

[55] ـ استخدام التكنولوجيا الحديثة لمكافحة الجريمة،
http://news.bbc.co.uk/hi/arabic/news/newsid_690000/690928.stm ، 2022/07/28م.

[56] . أحمد عبد الرحمان المجالي، الظواهر الاجرامية الحديثة والجريمة المنظمة، مجلة العلوم الانسانية، بسكرة، المجلد 13، العدد2 ، 2013م، ص232 ،233.

- ✓ نظّم المشرع الجزائري الجريمة الالكترونية واصطلح عليها بـ الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، محاولا الحدّ من خطورة هذه الجرائم من خلال القانون 09/ 04 بالإضافة إلى تعديلات على قانون العقوبات وقانون الإجراءات الجزائية.
- ✓ للجريمة الالكترونية عوامل مختلفة ومتداخلة، ويعتبر انتشار فيروس كورونا كوفيد-19 والتدابير المتّخذة لمكافحته من أبرز العوامل في تناميها وتزايدها.
- ✓ من المجالات التي استهدفتها الجريمة لالكترونية في فترة جائحة كورونا: المجال الصحي، المالي، مجال الترفيه للألعاب الالكترونية، مجال الدردشة والمؤتمرات والاجتماعات عبر المنصات الرقمية.
- ✓ تعتبر المراسيم التنفيذية 69/20، 70/20، 127/20 من أهم الآليات التي اتّخذتها الجزائر لمكافحة فيروس كورونا كوفيد-19 والتي استغلّها لصوص الحظر ومجرمو المعلوماتية في تنفيذ نشاطاتهم.
- ✓ استحداث المشرّع الجزائري للقسم السابع مكرر في الفصل الثالث من الباب الثاني للكتاب الثالث من قانون العقوبات يعدّ خطوة هامّة وقفزة في مجال التشريع، مواكبا التطوّرات التشريعات.
- ✓ الجرائم المتّصلة بتكنولوجيا الإعلام والاتصال ذات طابع خاص كونها واقعة في عالم افتراضي، عابرة للحدود، يصعب فيها الاختصاص القضائي، واثبات الدليل المادي وتتبّع فاعلها، وفي الوقت نفسه يسهل ارتكابها.
- ✓ تصنّف الجريمة الالكترونية باعتبارات مختلفة، من الصعوبة بمكان حَصْرُها لتجدّد وسائلها وأساليبها.
- ✓ التطوّر الكبير في وسائل التكنولوجيا يحتّم الإسراع في كلّ مرّة إلى وضع آليات قانونية لمكافحة انتشار الجرائم الالكترونية، على المستوى الوطني والدولي.
- ✓ الآليات القانونية لمكافحة الجرائم الالكترونية غير كافية وحدها، فلا بد من الاعتماد على وسائل تقنية لا تقل حداثة عن تلك المستعملة في ارتكابها، كأجهزة الرقابة الإلكترونية وأدلة بصمات الأصابع وقرنيات العيون وتحليل الأحماض النووية... فضلا عن التوعية والتحسيس.

2 ـ التوصيات

- ✓ ضرورة الاهتمام بتعزيز الأمن الإلكتروني، وسد الثغرات التي يمكن أن تشكل تهديداً للبنية الرقمية والمعلوماتية، والاستفادة من شركات التقنية والانترنيت، خصوصا ما يتعلّق بالبرامج والقواعد المتعلّقة بحماية الأجهزة والبيانات.
- ✓ نشر الوعي الرقمي والتحسيس بخطورة الجرائم الالكترونية وعقوبتها، وكيفية تجنّب الوقوع في فخاخ لصوص المعلوماتية.
- ✓ ضرورة التعاون الدولي في مجال التحقيق والمتابعة والإثبات في الجرائم الالكترونية وإبرام الاتفاقيات لتحديد الاختصاص القضائي وكشف هوية الفاعلين ومعاقبتهم.
- ✓ عقد مؤتمرات وندوات بصفة دورية ومستمرة، للاطلاع على تطوّرات الإجرام المعلوماتي ومِنْ ثَمَ معالجتها.

- ✓ العمل على تكوين وتأهيل عناصر الضبطية القضائية ورجال الأمن والتحرّي على كيفية معالجة أو التعامل مع الأدلة الرقمية.
- ✓ توفير وتسخير الوسائل المادية والتقنية الحديثة للحدّ من ظاهرة الإجرام الالكتروني، فالمواجهة تكون بنفس سلاح الإجرام وأكثر.
- ✓ طرح مشكلة الجريمة الالكترونية أمام مختصّين اجتماعيين ونفسانيين ...لمعالجة الأسباب والتقليل من تفشيها.
- ✓ رغم الجهود التشريعية . الوطنية خاصة والدولية عامة . المبذولة لمكافحة الجريمة الالكترونية، إلا أنّها غير كافية بعضها يحتاج إلى تعديل، وبعضها الآخر يحتاج إلى توصيف خاصة الحقوق المتعلقة بالملكية الفكرية والحقوق المجاورة التي يصعب تطبيقها في بيئة رقمية إذا ما بقيت النصوص القديمة.

المراجع

أولا - القوانين والنصوص التنظيمية

1. القانون 06 . 22 المؤرخ في 29 ذي القعدة 1427هـ الموافق لـ20 ديسمبر 2006ميعدل ويتمم الأمر رقم 66 . 155 المؤرخ في في 8يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الريدة الرسمية للجمهورية الجزائرية،العدد رقم 84.
2. القانون 16 . 02 المؤرخ في 14 رمضان 1437هـ الموافق لـ19 يونيو 2016م يتمم الامر رقم 156.66 المؤرخ في 8 يونيو 1966م والمتضمن قانون العقوبات ، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 37.
3. القانون 17 .07 المؤرخ في 28 جمادى الثانية1438هـ الموافق لـ27 مارس 2017م،يعدل ويتمم الأمر رقم 66. 155 المؤرخ في 8 يونيو 1966م والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية العدد رقم 20.
4. القانون 18 . 05 المؤرخ في 24 شعبان عام 1439هـ الموافق 10 مايو سنة 2018م،يتعلق بالتجارة الالكترونية، الجريدة الرسمية للجمهورية الجزائرية عدد رقم28.
5. القانون رقم 04-15 المؤرخ في27 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم71.
6. القانون رقم 08 . 01 المؤرخ في 15 محرم عام 1429هـ، الموافق لـ 23 يناير سنة 2008م، يتمم القانون 83 . 11 المؤرخ في 2 يوليو 1983م، والمتعلق بالتأمينات، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 4.
7. القانون رقم 09-04 مؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، عدد رقم 47.
8. القانون رقم 06/20 المؤرخ في 5 رمضان 1441هـ الموافق لـ28 أبريل 2020م يعدل ويتمم الأمر 156/66 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد 25.
9. المرسوم التنفيذي رقم 69/20، المؤرخ في26 رجب 1441هـ، الموافق لـ21 مارس 2020م المتعلق بتدابير الوقاية من انتشار وباء فيروس كورونا كوفيد19 ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد15.

10.المرسوم التنفيذي رقم 70/20 المؤرخ في 29رجب 1441 هـ، الموافق 24 مارس 2020 م، الذي يحدّد تدابير تكميلية للوقاية من انتشار وباء فيروس كورونا كوفيد 19 –ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 16.

11.مرسوم تنفيذي رقم 127/20 مؤرخ في 27 رمضان 1441هـ، الموافق لـ20 ماي 2020م، يعدّل ويتمم المرسوم التنفيذي رقم 70/20 الذي يحدد التدابير التكميلية للوقاية من انتشار وباء فيروس كورونا كوفيد19 ومكافحته، الجريدة الرسمية للجمهورية الجزائرية، العدد 30.

ثانيا- الكتب

1. خالد القضاة، التقنيات الحديثة وانعكاساتها الاقتصادية والاجتماعية والنفسية والبيئية، ط1، دار اليازوري العلمية، عمان، 1997م.
2. خالد بن سعود البشر، تلخيص الظواهر الإجرامية المستحدثة وسبل مواجهتها، 2005م.
3. خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2010م.
4. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر العربي، الاسكندرية، 2007م.
5. هاني رزق، خالص جبلي، الإيمان والتقدم العلمي، ط1، دار الفكر المعاصر، بيروت، دار الفكر، دمشق، 2000م.

ثالثا- المجلات العلمية

1. أحمد عبد الرحمان المجالي، الظواهر الاجرامية الحديثة والجريمة المنظمة، مجلة العلوم الانسانية، بسكرة، المجلد 13، العدد2 ، 2013م.
2. بوضياف إسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 3، العدد3، 2018م.
3. حبيباتني بثينة، الطبيعة الخاصة للجريمة المعلوماتية، مجلة دراسات وأبحاث المجلة العربية للأبحاث والدراسات في العلوم الإنسانية والاجتماعية، المجلد12، العدد3، 2020م.
4. رحموني محمد، خصائص الجريمة الالكترونية ومجالاتها، مجلة الحقيقة، المجلد 16، العدد3، 2018م.

رابعا - المذكرات ورسائل الماجستير والدكتوراه

1. خلدون عيشة، محاضرات الجريمة المعلوماتية، موجهة لسنة أولى ماستر تخصّص القانون الجنائي والعلوم الجنائية. بدون تاريخ.
2. سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2010م،2011م.
3. صغير يوسف، الجريمة المرتكبة عبر الإنترنت، مذكرة ماجستير في القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2013م.

خامسا - المؤتمرات والملتقيات

1. السيد عوض، التطوّر التكنولوجي والجريمة، أعمال المؤتمر السنوي الرابع والثلاثون، قضايا السكان والتنمية، 19 . 22ديسمبر 2004م، المركز الديموجرافي بالقاهرة.
2. فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، أعمال المؤتمر الدولي الرابع عشر، طرابلس 24/24مارس2017م.
3. نميدلي رحيمة، خصوصية الجريم الإلكترونية في القانون الجزائري والقوانين المقارنة، أعمال المؤتمر الدولي الرابع عشر، طرابلس 24/24مارس2017م.

4. يونس عرب، جرائم الكمبيوتر والانترنت، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – ابو ظبي 10-12 /2/2002م.

سادسا ـ المقالات

1. ازدهار سوق المنتجات الطبية والوقائية المزيفة في زمن كورونا، https://www.alaraby.co.uk/ 2022/07/30م.
2. استخدام التكنولوجيا الحديثة لمكافحة الجريمة، http://news.bbc.co.uk/hi/arabic/news/newsid_690000/690928.stm ، 2022/07/28م.
3. أشرف مرحلي، التكنولوجيا تتحدى الجريمة والخارجين على القانون، https://www.alkhaleej.ae/ يوم 2022/07/28م.
4. اكتشاف ثغرات جديدة بـ Zoom تتيح للمتسللين اختراق الكاميرا والميكروفون https://www.youm7.com/story/2020/4/3 2022/08/02م.
5. آمال عيساوي، ألعاب تصيب الأطفال بالجنون والانهيارات العصبية، https://www.echoroukonline.com/ 2022/07/30م.
6. جائحة كورونا رفعت من نسبة الجرائم الإلكترونية https://www.alaraby.co.uk/entertainment_media 2022/07/29م.
7. داليا السيد أحمد، لماذا تصاعد خطر الهجمات الإلكترونية في ظل وباء كورونا؟ http://www.nationshield.ae/index.php/home/details/research 2022/07/29م.
8. دبي للمستقبل ، توجهات عالمية لتعزيز الأمن الرقمي وتبني الذكاء الاصطناعي لحماية القطاعات https://pressn.net/article/8564830?news 2022/07/30م.
9. عبد الله العلوي، فيروس كورونا يفاقم من حدة الجريمة الالكترونية عبر العالم، https://mapanticorona.map.ma/ar/node/3704 2022/07/31م.
10. عمليات النصب المتعلقة بالألعاب الأونلاين في ظل انتشار فيروس كورونا: سبل لحمايتك وعائلتك، https://me.kaspersky.com/resource-center/threats/coronavirus-gaming-scams 2022/08/02م.
11. كلود عمر، لمستخدمي» ..Microsoft Teams هاكرز» يتبعون حيلة لاختراق الهواتف عن طريق التطبيق، https://lite.almasryalyoum.com/technolight/259934 2022/08/02م.
12. كيف أثر منع التجول على جرائم ما بعد "كورونا" في الإقليم؟، https://futureuae.com/m/Mainpage/Item/5571 2022/08/02م.
13. كيف ازدادت نسب الجرائم الإلكترونية خلال جائحة كورونا ؟ https://www.aljazeera.net/news/scienceandtechnology/2020/5/6 2022/07/31م.
14. ليزا سعيد، التقدم التكنولوجي: هل جعلت التكنولوجيا حياتنا أيسر أم أسعد؟ https://www.ts3a.com/?p=30551 ، يوم 2022/07/29م.
15. محمد اسماعيل، الجريمة في زمن كورونا .. https://www.youm7.com/story/2021/3/22/5251259 يوم 2022/07/31م.
16. محمود شرقي، صلاح الدين جبار، تأثير تطور تكنولوجية المعلوماتية على تنامي الجريمة، https://www.asjp.cerist.dz/en/downArticle/354/8/1/62499 2022/07/30م.

17. منصة عملات مشفرة تتعرض للاختراق وسرقة 600 مليون دولار، https://www.alaraby.co.uk/economy 2022/07/29م.
18. منظمة الصحة العالمية تعلن عن تزايد الهجمات الإلكترونية بمقدار خمسة أضعاف وتحث على اليقظة https://www.who.int/ar/news/item/30-08-1441 2022/08/02م.
19. المؤسس يعترف بالتقصير.. القراصنة يقصفون تطبيق "زوم" وشركات كبرى تمنع العمل به، https://www.aljazeera.net/news/scienceandtechnology/2020/4/2 2022/08/02م.
20. هديل كرنيب ما هي لعبة الحوت الأزرق التي "تدفع بالأطفال إلى الانتحار"؟ https://www.annahar.com/arabic/article/713833 2022/08/02م.

وزارة التعليم العالي والبحث العلمي

جامعة الجزائر 1 بن يوسف بن خدة

كلية الحقوق

الملتقى الدولي الافتراضي حول :

القانون الجنائي في ظل التطور التكنولوجي

- اشكالات ومعالجات -

الرتبة العلمية: استاذة محاضرة قسم - أ -

مؤسسة الانتماء: المركز الجامعي شريف بوشوشة - افلو -

البريد الالكتروني: o.hassaine@cu-aflou.edu.dz

محور المداخلة: المحور الثاني (اثر استخدام التكنولوجيا على احكام التجريم)

عنوان المداخلة : اثر التكنولوجيا في استفحال الجريمة المعلوماتية وسبل مكافحتها في ظل التشريع الجزائري

اثر التكنولوجيا في استفحال الجريمة المعلوماتية وسبل مكافحتها في ظل التشريع الجزائري

The impact of technology on the exacerbation of information crime and ways to combat it under the Algerian legislation

الملخص:

ان التطور التكنولوجي الهائل والثورة التكنولوجية قد ادت الى ظهور مجموعه من الافعال والتصرفات الإجرامية التي مست بالحياة الخاصة للأفراد والمت بأضرار كبيرة خاصة ما يتعلق ببرامج الحواسيب و بأنظمتها المعلوماتية، الامر الذي اصبح يستدعي ضرورة وضع اليات

قانونيه تحارب مثل هذه الجرائم المعلوماتية كونها ترتبط بالوسائل الإلكترونية واهمها الحاسوب وما يحمله من خصائص ومعلومات حول الحياه الشخصية للفرد.

و الجزائر مثلها مثل جميع الدول اصبحت تعاني من استفحال الجرائم الإلكترونية بكل انواعها في المجتمع، والتي بدأت تهدد امن وسلامه المجتمعات وذلك نظرا لخطورتها، خاصه وانها تعد من بين الجرائم العابرة للحدود، وفي سبيل ذلك حاول المشرع من خلال اصداره ترسانة من القوانين والنصوص في اطار حمايه والحد او على الاقل التقليل من ارتكاب مثل هذه الجرائم الإلكترونية .

الكلمات المفتاحية: التكنولوجيا، الجريمة، المعلوماتية، الانترنت، التشريع الجزائري.

Abstract:

The tremendous technological development and the technological revolution has led to the emergence of a group of criminal acts and behaviors that affected the private lives of individuals and caused great damage, especially with regard to computer programs and their information systems, which has become a necessity to develop legal mechanisms to combat such information crimes as they are linked to electronic means and the most important of them. The computer and its characteristics and information about the personal life of the individual.

And Algeria, like all countries, has become suffering from the spread of electronic crimes of all kinds in society, which began to threaten the security and safety of societies, due to its seriousness, especially as it is considered among the cross-border crimes, and for that the legislator tried through issuing an arsenal of laws and texts within the framework of Protect and limit or at least reduce the commission of such cyber crime

Key words: Technology, crime, informatics, the Internet, Algerian legislation.

مقدمة:

ان تطور المجتمعات مع مرور الوقت، ادى الى تطور الاجرام ذلك انه وليد بالتبعية لذلك التطور فمع تطور التقنية يتطور الإجرام و يزداد خطورة و تعقيدا، يقف وراء ذلك التقدم العلمي خاصة في مجال الاتصالات شبكة اتصال العالمية او الانترنت، وهي شبكة اتصالات عالمية تسمح بتبادل المعلومات بين شبكات أصغر تتصل من خلالها الحواسيب حول العالم تعمل وفق أنظمة محددة ويعرف بالبروتوكول الموحد وهو بروتوكول إنترنت .

كان استخدام الانترنت في بداية الأمر مقتصرا على المجال العسكري ثم تطور إلى المجال البحث العلمي و مع الوقت أصبح يعتمد عليها في مختلف الحياة و ارتفع عدد مشتركيها و كان من بين هؤلاء من له نوايا إجرامية استخدم تلك الوسائل لتنفيذ ذلك الإجرام ،حيث اصبحت وسيلة حديثة لتنفيذ نوع جديد من الإجرام الخفي، و البعيد عن أعين الرقابة الأمنية

الامر الذي ادى الى ضرورة التفكير في وسائل قانونية و تقنية للحماية و الردع من هذا النوع من الإجرام حيث تصدى له المجتمع في البداية بمختلف القوانين التقليدية التي تعالج الإجرام العادي وذلك حتى لا يفلت الجاني من العقاب ثم بدأ التفكير في إيجاد حلول قانونية تناسب هذا النوع من الإجرام باعتبار ان الجريمة المرتكبة عبر الانترنت تتميز بالسرعة و التطور و الخفاء و تتطلب أساليب خاصة للتحري و التحقيق ، فكان لابد من مسايرتها عن طريق إجراءات و قوانين خاصة لهذا النوع من الإجرام و هو بالفعل ما تم حيث بدأت عديد من المؤتمرات في انعقاد لإثراء البحوث القانونية بمشاركة فقهاء القانون و علماء الاجتماع في وضع تصورات و خطط لمواجهة هذا النوع من الجريمة.[1]

ومن خلال ما تقدم نطرح الاشكال الاتي: **ما مدى نجاعة وفعالية الترسانة القانونية التي وضعها المشرع الجزائري في سبيل مكافحة الجريمة المعلوماتية للحد من استفحالها او على الاقل للتقليل من وقوعها خاصة امام الواقع الذي يفرضه التطور التكنولوجي والقرصنة المعلوماتية؟**

وللإجابة عن هذه الإشكالية قسمت هذه الورقة البحثية الى محورين: تناولت في المحور الاول: الجريمة المعلوماتية وكل ما يتعلق بمفهومها خصائصها الى غير ذلك.

اما المحور الثاني فقد خصصته لدراسة اثر التكنولوجيا في انتشار هذه الجريمة وكذا سبل واليات مكافحتها ودائما وفق التشريع الجزائري.

المبحث الأول: مفهوم الجريمة المعلوماتية

خلقت التقنية الحديثة خصوصا نوعا جديدا من الإجرام لم يكن معهودا سابقا مجاله هو عالم الانترنت, لذلك ظهرت مصطلحات جديدة للدلالة على هذا النوع من الإجرام منها جرائم المعلوماتية. و جرائم الحاسوب وتتميز هذه الجرائم بمفاهيم خاصة و مصطلحات محددة .

المطلب الأول :تعريف الجريمة المعلوماتية

واكب ظهور الأنترنت بداية الإجرام المعلوماتي بصفة عامة و الإجرام الخاص بعالم الأنترنت بصفة خاصة و الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم[2].

الفرع الأول : التعريف الفقهي

يرى بعض الفقه انه عند تعريف هذه الجرائم يجب الاستناد الى موضوع الجريمة او الى انماط السلوك محل التجريم فيعرفها« Rosenballt » انها نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه او هي أي نمط من انماط الجرائم المعروف في قانون العقوبات طالما كان مرتبط بتقنية المعلومات.

---

[1] بذلت جهودا لا يستهان بها، مؤكدة على وجوب تعزيز العمل المشترك بين أعضاء منظمة الامم المتحدة من أجل التعاون على الحد من انتشار الجريمة المعلوماتية، و هذا من خلال مؤتمراتها لمنع الجريمة و معاملة المجرمين بدءا بالمؤتمر السابع عام 1985إلى غاية المؤتمر الثاني عشر عام 2010 .إضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات و ذلك تحت إشراف الأمم المتحدة عام 1994، الذي نتج عنه عدة توصيات و قرارات ذات صلة بالجرائم المعلوماتية، و قد تضمنت شقين اثنين واحد موضوعي يتناول الأفعال التي تقع تحت طائلة الإجرام المعلوماتي، و ثاني إجرائي يتضمن الإجراءات الواجب إتباعها لتطبيق القواعد الموضوعية .كما كان للمنظمة العالمية للملكية الفكرية دور بارز في هذا المجال، و ذلك من خلال خلقها لنصوص قانونية خاصة بحماية برامج الحاسب الآلي و هذا من خلال المادة 04 و 05 من اتفاقية تريبس.

[2] DEBRAY Stéphane, Internet face aux substances illicites : complice de la cybercriminalité ou outil de prévention ?, DESS média électronique & Internet, Université de Paris 8, 2002-2003, p 08.

في حين ترى الدكتورة هدى قشقوش أنها : " كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات"، في الوقت الذي اوجد مكتب المحاسبة العامة للولايات المتحدة الأمريكية « GOA » تعريف لهذه الجرائم بانها » أو إساءة استخدام المخرجات إضافة إلى أفعال أخرى تشكل جرائم اكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر[3] لكن جرائم الانترنت هي امتداد لما عرف بجرائم الحاسوب والمقصود بجرائم الحاسوب: " كل عمل إجرامي يرتكب باستخدام الحاسوب كأداة أساسية، ودور الحاسوب في تلك الجرائم قد يكون هدفا للجريمة أو أداة لها. "

وهناك تعريفات فقهية انطلقت من وسيلة ارتكاب الجريمة، من بينها تعريف الاستاذ: جون فورستر، والأستاذ(Eslied ball) الذي جاء فيه انها: "كل فعل اجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الامريكية انها: "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا "، وقد لاقت هذه التعريفات انتقادات كون تعريف الجريمة يجب ان ينصب على السلوك المكون لها و ليس فقط على الوسيلة التي تم بها فيقول الاستاذ:R _ FandeRson انه "ليس لمجرد ان الحاسب قد استخدم في جريمة ان نعتبرها من الجرائم المعلوماتية[4] ".

وامام الانتقادات التي وجهت للتعريفات الفقهية القاصرة على معيار واحد بدأت تظهر تعريفات جمعت بين أكثر من معيار، مثل التعريف الذي جاء به الأستاذ John corrol :وتبناه الأستاذ GION GREEN والذي جاء فيه انها: (أي عمل ليست له في القانون أو أعراف قطاع الأعمال جزاء ، يضر بالأشخاص والأموال أو يوجه ضد أو يستخدم التقنية المتقدمة العالية لنظم المعلومات).

الفرع الثاني: التعريف القانوني

القانون المصري النموذجي في مادته الأولى عرف جرائم المعلوماتية أنها» كل فعل يتم ارتكابه عبر أي وسيط الكتروني ويقصد في تطبيق أحكام هذا القانون بالكلمات والعبارات الآتية في حين لم يعرف تعديل قانون العقوبات الجزائري بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 جرائم الانترنت، بل اكتفى بالعقاب على بعض الأفعال، تحت عنوان » الجرائم الماسة بنظام المعالجة الآلية للمعطيات.

اما المشرع السعودي من خلال نظام مكافحة جرائم المعلوماتية قد وضع تعريفا لها بأنها :" كل فعل يرتكب متضمنا استخدام الحاسب الآلي والشبكة المعلوماتية بالمخالفة لأحكام هذا النظام ".[5]

المطلب الثاني: خصائص الجريمة المعلوماتية

من بين أهم خصائصها عابرة للحدود، سريعة التنفيذ وصعوبة الإثبات، كما انها جرائم ناعمة.

---

[3] بعد تطور أشكال الجريمة مع استخدام الحاسب الآلي والانترنت واستهدافها لكافة المصالح و الحقوق ، أصبحت الجرائم الإلكترونية تقع على الأشخاص و الأموال والمعلومات وخلق البرامج الضارة وإرسالها و إدخال معلومات خاطئة إلي نظام الحاسب الآلي والاحتيال و التلاعب في البطاقات المالية وسرقة المعلومات .

[4] الاتفاقية الدولية للإجرام المعلوماتي قدمت تعريف للنظام المعلوماتي في مادتها الثانية على النحو التالي:

Système informatique désigne tout dispositif isolé ou ensemble de dispositifs interconnecté ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement ou tonatisé de données

[5] عبد الفتاح بيومي حجازي/جرائم الكمبيوتر والأنترنت في التشريعات العربية"دراسة مقارنة مع التطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية ،ط1 ،دار .النهضة العربية، الإسكندرية، 2009 ،ص:17 .

الفرع الأول: عابرة للدول

فقدت الحدود الجغرافية كل اثر لها في الفضاء الشبكي او الآلي ، فهو لا يعترف بالحدود الجغرافية حيث يتم تبادل البيانات في شكل حزم الكترونية توجه إلى عنوان افتراضي ليس له صلة بالمكان الجغرافي ، فهو فضاء ذو طبيعة لا مركزية و يمكن إجمال أهم خصائصه في عدم التبعية لأي سلطة حاكمة .فالفضاء الآلي: نظام الكتروني معقد لأنه عبارة عن شبكة اتصال لا متناهية غير مجسدة و غير مرئية متاحة لأي شخص حول العالم وغير تابعة لأي سلطة حاكمة فالسلوك المرتكب فيها يتجاوز الأماكن بمعناه التقليدي له وجود حقيقي وواقعي لكنه غير محدد المكان لكنه حقيقة واقعا .

فالشبكة عالمية النشاط والخدمات لا تخضع لأي قوة مهيمنة إلا في بدايتها حيث كان تمويل هذه الشبكة حكوميا يعتمد على المؤسسة العسكرية الأمريكية، أما ألان فقد أصبح التمويل يأتي من القطاع الخاص حيث الشركات الإقليمية ذات الغرض التجاري التي تبحث عن كافة السبل للاستفادة من خدماتها بمقابل مالي[6].

والجريمة المرتكبة عبر شبكة الانترنت جريمة تعبر الحدود والقارات، وهو ما يدرجها ضمن موضوعات القانون الجنائي الدولي، الذي يقابل القانون الدولي الخاص في القانون المدني، وهو ذلك الفرع من القانون الذي يحدد ضوابط مجالات التعاون الدولي في مجال مكافحة الجريمة بالتزام الدول الموقعة على الاتفاقيات بالعمل بمقتضاها في مكافحة الجريمة .وقد ازدادت أهمية القانون الجنائي الدولي بعدما تطورت الجريمة المنظمة في وقت تقلص فيه المفهوم التقليدي للسيادة، حيث اتسع نظام المعاهدات الدولية لمكافحة الجرائم العابرة للحدود فالجانب الدولي للجريمة المعلوماتية لا يعد عنصرا من عناصرها كما هو الحال في الجريمة الدولية بل يعد هو نطاقها المكاني.

الفرع الثاني: سرعة التنفيذ و صعوبة الإثبات

ضحايا جرائم الانترنت لا يلاحظون أنهم ضحية فعل إجرامي لان هذا النوع من الإجرام يمتاز الخفاء والتستر ,فأثناء وجود مستعمل الانترنت في الشبكة يكون واقع تحت رحمة مجرم في الطرف الأخر من الخط، لان المجرم المعلوماتي يمتاز بالذكاء والحنكة اللتان تجعلان منه مثل الشبح، فمثلا عند إرسال فيروسات مدمرة أو سرقة البيانات الخاصة بالأموال أو إتلافها والتجسس وسرقة المعلومات وغيرها من الجرائم[7] .

فضحية جريمة الانترنت في أكثر صورها خفية لا يلاحظها أو لا يدري حتى بوقوعها. ذلك نظرا لأن المجرمون الإلكترونيون يتبادلون الخبرات و التجارب مع بعضهم البعض في العالم الافتراضي في منتديات خاصة تسمى منتديات القراصنة أو الهاكرز، لذلك تعتبر جريمة الانترنت أكثر تطورا من التشريعات التي تتصدى لها.[8]

الفرع الثالث: جرائم ناعمة

ترتكب الجرائم التقليدية باستخدام العنف سواء اللفظي أو العضلي مثل جريمة السرقة فهي تمتاز بالعنف العضلي مثل الكسر أو التعدي بالضرب على الضحية.

لكن الجرائم المرتكبة بتقنية الانترنت تمتاز بانها جريمة يمكن ان نطلق عليها الجرائم الصامتة او الناعمة أي تخلو من كل أشكال العنف المادي أو مظاهر العنف مثل الجروح أو الرضوض أو استخدام المعدات الخاصة مثل الأسلحة وهذا ما يجعل منها جريمة خالية من كل

---

[6] خالد ممدوح إبراهيم / أمن الجريمة الإلكترونية ، دار الجامعية ، الإسكندرية ، الإسكندرية ، 2008 ، ص 82.

[7] محمد عبيد الكعبي/الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت ،دار النهضة العربية ،لقاهرة، ص 32.

[8] هشام محمد فريد /الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، ط1 ، 1994،ص82.

اشكال العنف المادي .فسلاح المجرم في جريمة الانترنت لا يعدو ان يكون جهاز معلوماتي متصل بالشبكة الدولية مع وجود مجرم ذو كفاءة عالية في التعامل مع العالم الرقمي ومعرفة معمقة بتقنيات الكمبيوتر ومن امثلة الجرائم الهادئة جريمة التجسس أو سرقة البيانات الخاصة ببطاقات الائتمان.

المبحث الثاني: اثر التكنولوجيا على انتشار الجريمة المعلوماتية

وفي هذا الاطار سنحاول تحديد كل من اركان الجريمة الالكترونية، وكذا اساليب البحث والتحري للكشف عنها.

المطلب الاول: اركان الجريمة المعلوماتية

حتى تقوم الجريمة يجب ان تتوافر ثلاث الأركان وهي الركن المادي، الركن المعنوي ثم الركن الشرعي.

الفرع الاول: الركن المادي

يتمثل الركن المادي في أشكال الاعتداء على نظم المعالجة الآلية للمعطيات و التي هي:

- الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على نظام المعالجة الآلية للمعطيات.
- الاعتداءات العمدية على سلامة المعطيات الموجودة داخل النظام.

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتوجات النظام:

الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات نصت عليه المادة 394 مكرر قانون العقوبات[9]، وكما نصت على ذلك المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي.

الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.[10]

أ- فعل الدخول: لا يقصد بالدخول هنا الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، و في نفس الاتجاه إلى جهاز الحاسب الآلي و إنما يجب أن ينظر إليه كظاهرة معنوية، تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكة التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات.

ب- فعل البقاء Le maintien

قد يتخذ النشاط الإجرامي الذي يتكون منه الركن المادي في الجريمة محل الدراسة صورة البقاء داخل النظام، و يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له

---

[9] تنص المادة 394 مكرر من القانون04-15 المؤرخ في رمضان 1425الموافق ل:10نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات "يعاقب بالحبس من ثلاثة أشهر إلى سنة و بغرامة من 50.000 إلى 200.000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 300.000 دج".

[10] رشيد خلوفي/قانون العقوبات، كليك للنشر،المحمدية،الجزائر،2017،ص:142.

الحق في السيطرة على هذا النظام وقد يتحقق البقاء المعاقب عليه داخل النظام مستقلا عن الدخول على النظام، وقد يجتمعان. [11]

ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا. ومن أمثلة ذلك: إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ أو السهو، إذ كان يجب في هذه الحالة على المتدخل أن يقطع وجوده وينسحب فورًا، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع إذا توافر لها الركن المعنوي. ويكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والاطلاع فقط ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، والتي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه.[12]

ويكفي لتوفر هذا الظرف وجود علاقة سببية بين الدخول غير المشروع أو البقاء غير المشروع و تلك النتيجة الضارة، و لا يشترط أن تكون تلك النتيجة الضارة مقصودة، لأن تطلب مثل هذا الشرط يكون غير معقول ، حيث أن المشرع نص على تجريم الاعتداء المقصود على النظام عن طريق محو أو تعديل المعطيات التي يحتويها باعتباره جريمة مستقلة. كما لا يشترط أن تكون تلك النتيجة مقصودة.

وعمومًا التلاعب في المعطيات الموجودة داخل النظام يتخذ إحدى الأشكال التالية:

- **الإدخال L'intrusion:** يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية، أم كان يوجد عليها معطيات من قبل، ويتحقق هذا الفعل في الغرض الذي يستخدم فيه الحامل الشرعي لبطاقات السحب الممغنطة، هاته الأخيرة ليسحب بمقتضاها النقود من أجهزة السحب الآلي وذلك حين يستخدم رقمه الخاص والسري للدخول لكي يسحب مبلغا من النقود أكثر من المبلغ الموجود في حسابه، وكذلك الحامل الشرعي لبطاقة الائتمان و التي يسدد عن طريقها مبلغ أكثر من المبلغ المحدد له وبصفة عامة يتحقق فعل الإدخال في كل حالة يتم فيها الاستخدام التعسفي لبطاقات السحب أو الائتمان سواء من صاحبها الشرعي أم من غيره في حالات السرقة أو الفقد أو التزوير، كما يتحقق فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب« فيروس...الخ» يضيف معطيات جديدة.[13]

- **المحو L'effacement**: يقصد بفعل المحو إزالة جزء من المعطيات المسجلة على دعامة والموجودة داخل النظام أو تحطيم تلك الدعامة، أو نقل و تخزين جزء من المعطيات إلى المنطقة الخاصة بالذاكرة.

- **التعديل Modification:** يقصد بفعل التعديل تغيير المعطيات الموجودة داخل نظام واستبدالها بمعطيات أخرى، ويتحقق فعل المحو والتعديل عن طريق برامج غريبة بتلاعب في المعطيات سواء بمحوها كليا أو جزئيا أو بتعديلها وذلك باستخدام القنبلة المعلوماتية الخاصة بالمعطيات وبرنامج الممحاة Gomme d'effacement أو برنامج الفيروسات بصفة عامة، وهذه الأفعال المتمثلة في الإدخال والمحو والتعديل وردت على سبيل الحصر فلا يقع تحت طائلة

---

[11] علي عبد الله القهوجي/الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999 ص 17.

[12] معتوق عبد اللطيف / الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ،مذكرة (مكملة لنيل شهادة الماجستير وعلوم الجنائية، 2012 2011 ، ص:88 .

[13] معتوق عبد اللطيف/ الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مرجع سابق،2011 /2012، ص: 90

التجريم أي فعل آخر غيرها حتى ولو تضمن الاعتداء على المعطيات الموجودة داخل نظام المعالجة الآلية.[14].

الفرع الثاني: الركن المعنوي

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط ماديات الجريمة وشخصية الجاني[15]،كما الركن المعنوي في مختلف الاعتداءات الماسة بالأنظمة المعلوماتية تتخذ صورة القصد الجنائي إضافة إلى نية الغش.

أولا: الدخول و البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات: يلزم لتوافر الركن المعنوي أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء و أن يعلم الجاني بأنه ليس له الحق في الدخول إلى النظام والبقاء فيه، وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو في البقاء أو في نطاق هذا الحق، كأن يجهل بوجود حظر للدخول أو البقاء، أو كان يعتقد خطأ أنه مسموح له بالدخول، فإذا توافر القصد الجنائي بعنصريه العلم و الإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى ولو كان الباعث هو الفضول أو إثبات القدرة على المهارة و الانتصار على النظام بالنسبة لنية الغش تبدو من خلال الغش الذي يتم به الدخول من خرق الجهاز الرقابي الذي يحمي النظام، بالنسبة للبقاء فيستنتج من العمليات التي تمت داخل النظام.

ثانيا: الاعتداءات على سير نظام المعالجة الآلية للمعطيات: إن هذه الجريمة جريمة عمدية، إذ أن من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يشكل ظرفا مشددا لجريمة الدخول والبقاء الغير مشروع داخل النظام وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة.

ثالثا: الاعتداءات العمدية على المعطيات: جريمة الاعتداء العمدي على المعطيات جريمة عمدية يتخذ فيها الركن المعنوي صورة القصد الجنائي بعنصريه العلم والإرادة، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل كما يجب أن يعلم الجاني بان نشاطه الجرمي يترتب عليه التلاعب في المعطيات، ويعلم أيضا أن ليس له الحق في القيام بذلك وانه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته.

كما يشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش ، لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه.

الفرع الثالث: الركن الشرعي

طبقا لقانون العقوبات وبناءا على المواد 211 و 131 من الاتفاقية الدولية للأجرام المعلوماتي فان العقوبات المقررة للإجرام المعلوماتي يجب ان تكون رادعة و تتضمن عقوبات سالبة للحرية و التي تتمثل في العقوبات الأصلية تكميلية على الشخص الطبيعي و الشخص المعنوي.

اولا: العقوبات المطبقة على الشخص الطبيعي:

أ/ العقوبات الأصلية: عقوبة الحبس تتراوح من شهرين إلى ثلاث سنوات، حسب الفعل المرتكب والغرامة تتراوح قيمتها خمسين الف دينار جزائري إل مئة الف دينار جزائري، حسب الفعل المرتكب: الدخول والبقاء بالغش (الجريمة البسيطة)، الدخول والبقاء بالغش (الجريمة المشددة)

---

[14] سفيان سوير/ جرائم معلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، سنة 2010-2011، ص: 86.

[15] خالد ممدوح إبراهيم/ فن التحقيق الجنائي في الجرائم الالكترونية ، دار الفكر ،الإسكندرية ،2009 ، ط1 ، ص:53.

وتضاعف العقوبة إذا ترتب عن هذه الأفعال حذف او تغيير لمعطيات المنظومة، الإعتداء العمدي للمعطيات.[16]

ب/ العقوبات التكميلية: الصادرة تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية مع مراعاة حقوق الغير حسن النية، واغلاق المواقع والأمر يتعلق بالمواقع، التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية، وإغلاق المحل أو مكان الاستغلال اذا كانت الجريمة قد ارتكبت بعلم مالكها.[17]

عقوبة الشروع: جاءت به المادة 11 من الإتفاقية الدولية للإجرام المعلوماتي و اعتمده المشرع الجزائري بالنسبة للجرائم الماسة بالأنظمة المعلوماتية بحيث توسع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، اذ اصبح الشروع معاقب عليه بنفس العقوبة المقررة الجنحة ذاتها.[18]

الظروف المشددة: نص القانون على ظرف تشدد به العقوبة جريمة الدخول و البقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندا ينتج عن الدخول او البقاء اما حذف او تغيير المعطيات التي يحتويها النظام واما تخريب النظام اشتغال النظام، تضاعف العقوبة اذا استهدفت الدفاع الوطني او الهيئات او المؤسسات العامة.[19]

ثانيا: العقوبات المطبقة على الشخص المعنوي: يسأل الشخص المعنوي عن هاته الجرائم سواءا بصفته فاعلا اصليا او شريكا كما يسأل عن الجريمة التامة او الشروع فيها ،كل ذلك بشرط ان تكون الجريمة قد ارتكبت لحساب شخص معنوي بواسطة احد اعضائه او ممثليه وبتالي العقوبة الشخص المعنوي تتمثل في الغرامة في خمس مرات الى لحد الاقصى المقررة للشخص الطبيعي.[20]

عقوبات الاتفاق الجنائي: تبنى المشرع الجزائري بغرض تحضير لجرائم الماسة بالأنظمة المعلوماتية وعقوبة الاشتراك بالاتفاق تكون نفس العقوبة التي تم التحضير لها فاذا تعددت الجرائم تكون العقوبة هي العقوبة الجريمة الاشد .[21]

المطلب الثاني: الأساليب الخاصة بالبحث و التحري في الجريمة المعلوماتية

---

(16) انظر المواد 394 مكرر 1 و 2.

(17) انظر المادة394 مكرر6 من القانون04-15 المؤرخ في رمضان 1425الموافق ل:10نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات " مع الاحتفاظ بحقوق الغير حسن النية بحكم مصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا للجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على إغلاق المحل او المكان الاستغلال اذا كانت الجريمة قد ارتكبت بعلم مالكها .

(18) انظر المادة 394مكرر7 من القانون04-15 المؤرخ في رمضان 1425الموافق ل:10نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات "يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها.

(19) انظر المادة 394 مكرر3 من القانون04-15 المؤرخ في رمضان 1425الموافق ل:10نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات 'تضاعف العقوبة المنصوص عليها في هذا القسم اذا العقوبة اذا استهدفت الدفاع الوطني او الهيئات او المؤسسات"

(20) انظر المادة 394 مكرر من القانون04-15 المؤرخ في رمضان 1425الموافق ل:10نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات 4 " يعاقب الشخص المعنوي الذي يرتكب احد هاته الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الاقصى المقرر للشخص الطبيعي" .

(21) انظر المادة 394 مكرر 5 من القانون04-15 المؤرخ في رمضان 1425الموافق ل:10نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات "كل من شارك في مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

للمكافحة هذه الجريمة يحب اعتماد على طرق و أليات تختلف عن تلك المعهودة سابقا و من بين أهم الوسائل والأليات التفتيش، المعاينة و الخبرة .

الفرع الأول التفتيش: هو إجراء من إجراءات التحقيق يقوم به موظف مختص وفق قانون الإجراءات الجزائية يهدف التفتيش إلى جمع الأدلة من مكان وقوع الجريمة .

أما في الجرائم المتعلقة بشبكة الانترنت نجد أن الدخول غير المشروع إلى الأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة عما قد يتصل بجريمة وقعت، إجراء يفيد في كشف الحقيقة عنها وعن مرتكبها، وتقتضيه مصلحة وظروف التحقيق في الجرائم المعلوماتية ،اما طبيعة التكنولوجيا الرقمية قد عقَّدت من التحدي أمام أعمال التفتيش والضبط ، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماماً عن الموقع المادي للتفتيش وإن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية الجاري تفتيشها، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر.

وعند القيام بالتحقيق في الجريمة يتم ذلك بالاعتماد على مجموعة وسائل في هذا المجال هي:

اولا: الوسائل المادية: وهي الأدوات الفنية التي غالباً ما تستخدم في بنية نظم المعلومات والتي يمكن باستخدامها تنفيذ إجراءات وأساليب التحقيق المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها ومن أهمها:

أ. **عناوينIP ، والبريد الإلكتروني، وبرامج المحادثة**: عنوان الإنترنت هو المسئول عن تراسل حزم البيانات عبر شبكة الإنترنت وتوجيهها إلى أهدافها، وهو يوجد بكل جهاز مرتبط بالإنترنت، وفي حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية، ويمكن لمزود خدمة الإنترنت أن يراقب المشترك، كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضاً إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك.[22]

ب. **البروكسي :PROXY** يعمل البروكسي كوسيط بين الشبكة ومستخدميها بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة . Cache Memory وتقوم فكرة البروكسي على تلقى مزود البروكسي طلباً من المستخدم للبحث عن صفحة ما ضمن ذاكرة Cache المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل، فيقوم بإعادة إرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أم إنه لم يتم تنزيلها من قبل فيتم إرسال الطلب إلي الشبكة العالمية، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين IP ومن أهم مزايا مزود البروكسي أن ذاكرة Cache المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت عليها مما يجعل دوره قوى في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة.[23]

ج. **برامج التتبع**: تقوم هذه البرامج بالتعرف على محاولات الاختراق التي تتم ،وتقدم بيان شامل بها إلى المستخدم الذي تم اختراق جهازه، ويحتوى هذا البيان على اسم الحدث وتاريخ حدوثه

---

(22) خالد ممدوح ابراهيم / فن التحقيق الجنائي في الجرائم الالكترونية ، دار الفكر الجامعي،الإسكندرية،ط2009،1،ص :30.

(23) بلال بن جامع / المشكلات الأخلاقية و القانونية المثارة حول شبكة الانترنيت ، ماجستير في علم المكتبات تخصص إعلام علمي و تقني، جامعة منتوري، قسنطينة، 2006 ، ص :163.

وعنوان IP التي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الإنترنت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الإنترنت ومعلومات أخرى.[24]

د. **نظام كشف الاختراق Intrusion Detection System:** ويرمز له اختصاراً بالأحرف IDSوهذه الفئة من البرامج تتولي مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثاً عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب أو الشبكة ،[25] وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عده ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة .

هـ. **نظام جرة العسل Honey Pot:** وهو نظام حاسوبي مصمم خصيصاً لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أية بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعاً خاطئاً بسهولة الاعتداء على هذا النظام بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز آخر في الشبكة، في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء، وتحليلها.

و. **أدوات فحص ومراقبة الشبكات**: هذه الأدوات تستخدم في فحص بروتوكول TCP/IP وذلك لمعرفة ما قد يصيب الشبكة من مشاكل، ومعرفة العمليات التي تتعرض لها، ومن هذه الأدوات:

أداة :ARP ووظيفتها تحديد مكان الحاسب الآلي فيزيائياً على الشبكة.

برنامج :Visual Route 5.2a وهو عبارة عن برنامج يلتقط أي عملية فحص عملت ضد الشبكة، فيقوم بتقديم أجوبة تبين المعلومات التي حدث فيها مسح، والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان IP أو اسم الجهة يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

أداة :TRACER تقوم هذه الأداة برسم مسار بين جهازين تظهر فيه كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها والوقت والفترات التي قضاها، وهي تسمح برؤية المسار الذي اتخذه IP من مضيف إلى آخر، وتستخدم هذه الأداة الخيار Time To Live TTLالتي تكون ضمن IP لكي تستقبل من كل موجه رسالة وبذلك يكون هو العدد الحقيقي للوثبات، ويتم بذلك تحديد وبشكل دقيق المسار التي تسلكه الرزمة، وهذه الأداة تستخدم في الأساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها، إذ أنه يبين الشبكة وتخطيطها والجدران النارية المستخدمة ونظام الترشيح ونقاط الضعف، ولكن يمكن أيضاً من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها.

أداة :NET STAT هي أداة لفحص حالة الاتصال الحالي للبرتوكولTCP/IP ، ولها عدد من المهام من أهمها عرض جميع الاتصالات الحالية، ومنافذ التنصت، وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لجدول التوجيه[26].

ثانيا: الوسائل الإجرائية

ويقصد بها الإجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها ومنها:

(24) خالد عياد الحلبي/ إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، دار الثقافة، الأردن، ط 2011،ص:206.
(25) خالد عياد الحلبي/ إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت ،المرجع السابق،ص:208.
(26) خالد عياد الحلبي/ إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت المرجع السابق،ص:211.

أ / **اقتفاء الأثر**: من أخطر ما يخشاه مجرم نظم المعلومات تقصي أثره أثناء ارتكابه للجريمة، فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح أولاها نصيحة هي قم بمسح آثارك Cover Your Tracks ، فلو لم يقم المخترق بمسح آثاره فمؤكد أنه سوف يتم القبض عليه حتى وإن كانت عملية الاختراق قد تمت بشكل سليم، ويمكن تقصي الأثر بطرق عدة سواء عن طريق بريد إلكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق.(27)

ب/ الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته: ينبغي على المحقق وهو بصدد التحقيق في إحدى جرائم الانترنت أن يطلع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، وعليه الاطلاع على عمليات النظام المعلوماتي كقاعدة البيانات وإدارتها وخطة تأمينها ومعرفة مواد النظام والمستفيدين والملفات والإجراءات وتصنيف الموارد العامة، ومدى مزامنة الأجهزة، ومدى تخصيص وقت معين في اليوم يسمح باستخدام كلمات المرور، توزيع الصلاحيات للمستفيدين، إجراءات أمن العاملين، أسلوب النسخ الاحتياطي، والاستعانة ببرامج الحماية.

ج/ **الاستعانة بالذكاء الصناعي**: أثبتت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها، فيمكن الاستعانة به في حصر الحقائق والاحتمالات والأسباب والفرضيات و استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسب الآلي، وفق برامج صممت خصيصا لهذا الغرض.(28)

الفرع الثاني: مفهوم المعاينة

المعاينة من المراحل الأولى للاستدلال حول ملابسات الجريمة نظرا لي ما توفره من أدلة جول الإثبات و تزداد أهميتها في النوع من الإجرام لأن م السهولة محو أثار الجريمة، و هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها كذلك جميع الأشياء الأخرى ،التي تفيد في كشف الحقيقة، واتخاذ ما يلزم من إجراءات كضبط بعض الأشياء.(29)

يجوز الالتجاء إلى المعاينة في كافة الجرائم، وهي إجراء هادف غايته كشف وصيانة العناصر المادية التي تتعلق بالجريمة، وتفيد في التحقيق الجاري بشأنها، فإذا انعدمت بالنسبة للتحقيق جدواها وفائدتها لم تكن ثمة مجال أو مقتضى لإجرائها، ولا تجدي في كشف الحقيقة بشأنه المعاينة، مثل جريمة التزوير المعنوي وجريمة القذف والسب التي تقع بالقول في غير العلانية وغيرها.

- **مسرح الجريمة المرتكبة عبر الإنترنت:**

ينبغي عند الشروع في جمع الأدلة من مسرح جريمة الحاسوب والإنترنت، التعامل معه على أنه مسرحين.

- **مسرح تقليدي** :ويقع خارج بيئة الحاسوب، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى المسرح أية جريمة تقليدية قد يترك فيها الجاني آثار عدة، كالبصمات وغيرها، وربما تركك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه.
- **مسرح سيبراني** :ويقع داخل بيئة الحاسوب، ويتكون من البيانات الرقمية التي تتواجد وتنقل داخل بيئة الحاسوب وشبكاته، في ذاكرته وفي الأقراص الصلبة الموجودة بداخله، والتعامل

---

(27) نفس المرجع،ص:213.

(28) خالد عياد الحلبي/ إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت المرجع السابق، ص ص :213-214.

(29) محمد حماد مرهج الهيتي/ جرائم الحاسوب، دار المناهج، عمان، ط 2006 ، 1، ص: 255.

مع الأدلة الموجودة في هذا المسرح يجب أن لا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع.[30]

أهمية المعاينة في الجريمة المرتكبة عبر الإنترنت:

تكمن أهمية وجدارة المعاينة عقب وقوع جريمة من الجرائم التقليدية في أنها تتبوأ مكانة الصدارة على ما عداها من الإجراءات الاستقصائية الأخرى، بحكم مركز المحورية لدورها في تصور كيفية وقوع الجريمة، وظروف وملابسات ارتكابها وتوفير الأدلة المادية من المادة التي تجمع عن طريقها وتمحيص وتقييم الأدلة الأخرى والتنسيق بينها في ضوء المعلومات التي منها، بما يكفل في ذات الوقت التخطيط السليم لعمليات البحث، والتحقيق الجنائي وتطويرها.[31]

حتى يكون للمعاينة في الجرائم المتعلقة بشبكة الإنترنت فائدة في كشف الحقيقة عنها وعن مرتكبيها مراعاة عدة قواعد وإرشادات فنية أبرزها ما يلي[32]:

1-تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

2-العناية بملاحظة الطريقة التي تم بها إعداد النظام.

3-ملاحظة واثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.

4-عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

5-التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها، ويرفع عليها البصمات ذات الصلة بالجريمة.

6-التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

7-قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوفر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات.

يتم التوثيق مسرح الجريمة ووصفه بكامل محتوياته بشكل جيد مع توثيق كل دليل على حدة بما فيها الأدلة الرقمية، بحيث يتم توضيح مكان الضبط والهيئة التي كان عليها ومن قام برفعه وتحريزه وكيف ومتى تم ذلك، بل إن البعض يرى أن التوثيق يجب أن يشمل كافة المصادر المتاحة على الشبكة التي ترتبط بها الأجهزة محل التحقيق ولعل أبرز الأماكن التي يحتمل وجود الأدلة الجنائية المتعلقة بجرائم الإنترنت فيها ما يلي:

-الورق :على الرغم من وجود أجهزة الحاسب الآلي قلل من حجم الأوراق الملفات التقليدية المستخدمة حيث يتم حفظ المعلومات والبيانات على أجهزة الحاسب الآلي، نجد الكثيرين ممن يقوموا بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستند أو الرسالة أو الرسومات، وبالتالي فهي تعتبر من الأدلة التي ينبغي الاهتمام بها في البحث عن الحقيقة.

-جهاز الحاسب الآلي وملحقاته :وجود جهاز الحاسب الآلي هام جدا للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو جريمة حاسوبية، وانها مرتبطة بالمكان أو الشخص الحائز على

---

[30] محمد بن نصير محمد السرحاني/ مهارت التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت- دارسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، تخصص، القيادة الأمنية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الشرطية، الرياض،2004 ،ص:77.

[31] عبد الفتاح بيومي حجازي/ مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى،2006 ، ص:101.

(32) محمد ابو العلا عقيدة/"التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية ، .http://arblawinfo.com اطلع عليه بتاريخ 2019/04/14 على الساعة 16:45.

الجهاز، ولأجهزة الحاسب الآلي أشكال وأحكام وألوان مختلفة وخبير لحاسب الآلي وحده الذي يستطيع أن يتعرف على الحاسب الآلي ومواصفاته بسرعة فائقة.[33]

- **البرمجيات** :إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص أو ليس واسع الانتشار، فإن أخذ الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.
- **وسائط التخزين المتحركة** :كالأقراص المدمجة" أقراص الليزر "والأقراص المرنة والأشرطة المغناطيسية وغيرها، وتعد هذه الوسائط جزء من الجريمة المرتكبة عبر الإنترنت متى كانت محتوياتها عنصر من عناصر الجريمة.
- **المراشد:** الخاصة بالمكونات المادية والمنطقية للحاسب الآلي والتي تفيد في معرفة التفاصيل الدقيقة لكيفية عملها.
- **المودم** :وهو الوسيلة التي تمكن أجهزة الحاسب الآلي من الاتصال ببعضها البعض عبر خطوط الهاتف، وفي الوقت الحالي تطور المودم ليكون جهاز إرسال واستقبال فاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها.[34]

الفرع الثالث: الخبرة

الخبرة هي الوسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات، فهي في الحقيقة ليست دليلا مستقلا عن القولي أو الدليل المادي، إنما هي تقييم فني لهذا الدليل والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة، الشهادة والتفتيش.

ويقصد بها مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرها إلى معرفة فنية أو دراية علمية لا تتوافر لديه.

يطلق لفظ الخبير على كل شخص توافرت لديه معرفة عملية وفنية لتخصصه في مادة معينة وتستعين به السلطة القضائية وجهات التحقيق في تقدير المسائل الفنية استكمالا لنقص معلومات القاضي في هذه النواحي، ومساعدة له في اكتشاف الحقيقة لهذا الغرض يجب أن يتوفر لديه القدرة على تطبيق تلك القواعد النظرية على الحالات الواقعية ولا يتحقق ذلك إلا بالممارسة العملية.[35]

أ / مجالات الخبرة بالنسبة للجرائم المعلوماتية:

تتنوع العمليات الإلكترونية بتنوع المجالات التي تستخدم شبكة الإنترنت، فنجد أمثلة لها في الأعمال المصرفية، الإدارة الإلكترونية، والتجارة الإلكترونية، ولذلك فإنه يتصور تنوع الجرائم التي تقع على هذه العمليات وفقا لنوع العمليات الإلكترونية المستخدمة في ارتكابها. تقتضي عمليات البحث الجنائي والتحقيق في جرائم الإنترنت الاستعانة بخبرات عديدة ومتنوعة، فإن اختيار خبير في نوعية الإجرام في مجال الإنترنت الذي تندرج الواقعة المرتكبة في اختصاصه يغدو أمرا بالغ الأهمية، ويمكن الاسترشاد في عملية الاختيار هذه بتصنيف لهذا الإجرام، يرتكز على نوعية الأساليب المستخدمة في الارتكاب إلى ما يلي[36]:

- تزوير المستندات المدخلة في أنظمة الحاسبات الآلية أو الناتجة بعد المعالجة.
- التلاعب في البيانات.
- التلاعب في البرامج الأساسية أو برامج التطبيقات.
- الغش أثناء نقل وبث البيانات

---

(33) محمد الأمين البشري/ مؤتمر القانون و الكمبيوتر والإنترنت، جامعة ،" التحقيق في جرائم الحاسب الآلي "،جامعة الإمارات العربية المتحدة، كلية الشريعة و القانون،1-3مايو2000،المجلد الثالث،ص:1058.

(34) حسين بن سعيد الغافري/ " التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الإنترنت " http://www.eastlaws.com اطلع عليه بتاريخ 22-04-2019 على الساعة 13:23.

(35) محمد فاروق عبد الحميد كامل/ القواعد الفنية الشرطية للتحقيق والبحث الجنائي، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 1999 ، ص:286.

(36) هشام محمد فريد رستم/"الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة للتدريب التخصصي " 1-3 ماي 2000 ،جامعة الإمارات- بحوث مؤتمر القانون والكمبيوتر والإنترنت، العربية المتحدة، كلية الشريعة والقانون، المجلد الثاني، الطبعة الثالثة2004 ، ص:407 .

ب /الشروط المتطلبة في الخبرة في مجال الجرائم المرتكبة عبر الإنترنت:

تقتضي فاعلية الخبرة ضرورة الجمع بين التعمق في كل من الدراسة العلمية والنظرية والممارسة العملية للتخصص العلمي والنظري، وكذا متابعة مستمرة للتطورات التي تلحق بفروع التخصص، غير أن ذلك ليس شرطا لازما في بعض الأحيان فقد يقتصر الخبير على مجرد الخبرة العملية في فرع التخصص دون أن يكون هناك رصيد من الدراسة العلمية والنظرية وهو الأمر الذي نلاحظه في مجالات الخبرة في الفروع المهنية المختلفة، منها مجال الحاسب الآلي، حيث يتعين في خبراء الحاسب الآلي المنتدبين للتحقيق أن تتوافر لديهم القدرة الفنية والإمكانات العلمية في المسألة موضوع الخبرة، ولا يكفي في ذلك حصول الخبير على شهادة علمية، بل يجب مراعاة الخبرة العملية لأنها هي التي تحقق الكفاءة الفنية، ولذلك لا وجود لخبير لديه معرفة متعمقة في سائر أنواع الحاسبات وبرمجياتها وشبكاتها، أو لديه القدرة على التعامل مع كل أنواع الجريمة المرتكبة عبر الإنترنت.[37]

الخاتمة:

وختاما لما تقدم ذكره ارتأينا ذكر بعض الاقتراحات او التوصيات في شكل فقرات كالاتي:

- **على مستوى البحث و التحري:**
  - ضرورة تخصيص ضباط شرطة قضائية خاصة لمكافحة الجرائم المعلوماتية.
  - جعل القواعد الخاصة بالبحث والتحري سلسة ولا تتطلب إجراءات معقدة.
- **على مستوى الإجراءات التقاضي:**
  - ينبغي مواكبة قواعد الإجراءات الجزائية لتتلاءم مع هذه الجرائم.
  - استحداث اقسام خاصة بالجرائم المعلوماتية في المحاكم و المجالس.
  - ضرورة تخصص قضاة في هذا النوع من الإجرام.
- **على مستوى التعاون الدولي:**
  - ضرورة التنسيق والتعاون الدولي قضائيا وإجرائيا في مجال مكافحة الجرائم المعلوماتية.
  - تعزيز التعاون والتنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية، وخصوصا الإنتربول.

قائمة المراجع:

اولا : باللغة العربية

أ/ الكتب:

1 _كري يوسف بكري/التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية 2011.

2-خالد عياد الحلبي/ إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، دار الثقافة، الأردن، ط2011 .

3- خالد ممدوح إبراهيم/ أمن الجريمة الإلكترونية، دار الجامعية، الإسكندرية، الإسكندرية ، 2008.

4 _خالد ممدوح إبراهيم/ فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر،الإسكندرية ، 2009.

5-رشيد خلوفي/قانون العقوبات، كليك للنشر، المحمدية، الجزائر،2017.

(37) عبد الفتاح بيومي حجازي/ مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى،2006 ، ص:138.

6-عبد الفتاح بيومي حجازي/ الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت دراسة متعمقة في جرائم الحاسب الآلي والإنترنت، بهجات للطباعة والتجليد، مصر، 2009

7-عبدالفتاح بيومي حجازي/جرائم الكمبيوتر والأنترنت في التشريعات العربية "دراسة مقارنة مع التطبيق على نظام مكافحة جرائم المعلوماتية في المملكة العربية السعودية، ط1 ، دار . النهضة العربية، الإسكندرية، 2009 .

8-علي عبد الله القهوجي/الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية للطباعة والنشر، بيروت، 1999.

10-محمد عبيد الكعبي/الجرائم الناشئة عن الاستخدام الغير مشروع لشبكة الانترنت، دار النهضة العربية، القاهرة، 2006

ب _ الرسائل والمذكرات :

1-معتوق عبد اللطيف / الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة مكملة لنيل شهادة الماجستير في علوم الجنائية ،2011 -2012 .

2-سفيان سوير، جرائم معلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، سنة 2010-2011.

4-بلال بن جامع / المشكلات الأخلاقية و القانونية المثارة حول شبكة الانترنيت ، ماجستير في علم المكتبات تخصص إعلام علمي و تقني، جامعة منتوري، قسنطينة،
5-محمد بن نصير محمد السرحاني/ مهارت التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت- دارسة مسحية على ضباط الشرطة بالمنطقة الشرقية، رسالة لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، تخصص، القيادة الأمنية، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، قسم العلوم الشرطية، الرياض،2004 .

ج_ القوانين

1-الأمر رقم 04-15 المؤرخ في رمضان 1425الموافق ل:10نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات.

2-اتفاقية برن سنة 1971.
3-الاتفاقية الدولية للإجرام المعلوماتي.

4-معاهدة الأمم المتحدة النموذجية بشأن نقل الإجراءات في المسائل الجنائية 1990 .

5-اتفاقية تتعلق بالتعاون القضائي المتبادل في الشؤون المدنية والتجارية ج ر رقم 92، سنة 1970.

6-معاهدة منظمة المؤتمر الإسلامي لمكافحة الإرهاب الدولي 1999.

7-اتفاقية بودابست، في 23 نوفمبر/تشرين الثاني 2001.

ثانيا: المراجع بالغة الفرنسية

2-DEBRAY Stéphane, Internet face aux substances illicites : complice de la Une cooperation international estindespensable, carles paysqui ne se pas dotes de lois contrela cybercri minalite sont des paradisnumerique voir chernaouti heli slange

ثالثا: مواقع الأنترنت

https://ar.wikipedia.org/wiki
http://arblawinfo.com
http://www.eastlaws.com

جامعة الجزائر 1 يوسف بن خدة

كلية الحقوق

الملتقى الدولي الافتراضي الموسوم بـ:

القانون الجنائي في ظل التطور التكنولوجي –اشكالات ومعالجات–

يومي 29/28 سبتمبر 2022

مداخلة بعنوان: نحو صياغة قانونية جنائية جديدة في ظل التطور التكنولوجي

محور المداخلة: تأثير الوسائل العلمية الحديثة على الاثبات الجنائي

د/ علي غريبي

أستاذ بحث قسم ب

تخصص الدولة والمؤسسات العمومية–قسم القانون العام

المركز الوطني للبحث في العلوم الإسلامية والحضارة بالأغواط–الجزائر

a.ghribi@crsic.dz

الملخص:

إن مفرزات التقنية العلمية التي ظهرت في العصر الحديث أحدثت تغيرا جذريا في وسائل الاثبات الجنائية، وتعد هذه الأخيرة من أبرزها، و التي جاءت لتلائم الثورة العلمية والتكنولوجية والتقنية في عصرنا الحالي، و التي تطور معها الفكر الإجرامي الذي صاحب ظهور ما يعرف بالجريمة الإلكترونية ألقى على عاتق القائمين على مكافحة الجريمة في الدولة عبئا شديدا ومهاما جسيمة تفوق القدرات المتاحة لهم وفق أسس و قواعد و إجراءات البحث الجنائي والإثبات الجنائي التقليدي، نظرا لعدم كفاية وعدم ملائمة هذه النظم التقليدية في إثبات تلك الجرائم سواء من الناحيتين القانونية أو التقنية، الشيء الذي ألزمعلى المشرع التدخل بقوانين تتناسب مع مثل هذه الجرائم، وقد حملت ورقتنا البحثية هذه عنوانا يضم رؤى وتوصيات من شأنها أن تقدم الإضافة في هذا الموضوع.

الكلمات المفتاحية: الاثبات الجنائي، التطور التكنولوجي، الجريمة الالكترونية.

Abstract:

The detachments of scientific technology that have appeared in the modern era have brought about a radical change in the means of criminal proof, and the latter is one of the most prominent ones, which came to fit the scientific, technological and technological revolution in our current era, with which the criminal thought that accompanied the emergence of what is known as electronic crime threw on Those in charge of combating crime in the state bear a heavy burden and grave tasks that exceed the capabilities available to them according to the foundations, rules and procedures of criminal investigation and traditional criminal proof, given the insufficiency and inadequacy of these traditional systems

in proving those crimes, both legally and technically. Legislature interfering with lawscommensurate with such crimes, and our research paper carried a title that includes visions and recommendations that would provide an addition to this topic.

***Keywords**: criminal evidence, technological development, electronic crime.*

مقدمة:

لقد شهد العقد الأخير من القرن العشرين غزوا تكنولوجيا كبيرا، فتسارع إيقاع التقدم التكنولوجي والتقني، وظهر ما يسمى بالفضاء الالكتروني، ووسائل الاتصالات الحديثة كالفاكس، والانترنت، وسائر صور الاتصال الالكتروني عبر الأقمار الصناعية، لكن تم استغلال هذا التقدم من قبل مرتكبي الجرائم المعلوماتية في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة فقط، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية.

إن جرائم تقنية المعلومات أصبحت من مقتضيات الضرورة التشريعية في التجريم[1] مع الأخذ بعين الاعتبار تحقيق الهدف المرجو من ذلك، على اعتبار أن أي نقل للسلوك الإنساني من طائفة " المباح" إلى طائفة " التجريم" يجب أن يقتضيه هدف معين وهو حماية المصلحة العامة التي يؤدي ذلك السلوك المجرم للمساس بها بحيث تعرض المصلحة للخطر والضرر والتي يرى المشرع أنه لا بد من رفع ذلك من خلال توفير الحماية بتقرير التجريم والعقاب، وهذا يعني أن الضرورة يجب تنطوي على الالتزام بتحقيق الهدف الذي ينشده المشرع من خلال تبيان قاعدة قانونية مضبوطة لمعالجة وضع محدد بحيث تعالجه على نحو كاف وبغير مبالغة.

إن التوازن ما بين الفكر الفلسفي الاجتماعي المحدد لمضمون حق الدولة في العقاب وما بين الفكر الدستوري الذي بمقتضاه تحدد قيمة الحقوق والحريات يجب أن تقوم عليه سياسية التجريم والعقاب من خلال تحديد النمط السلوكي المُجرم ومن ثم تحديد مقدار العقاب، بما يكون متفقاً مع مفهوم السياسة الجنائية ضمن إطار المنظومة التشريعية في الدولة[2].

وبالتالي ولغايات حماية الحقوق والحريات فإنه من الواجب الموازنة ما بين الضرورة الاجتماعية والتناسب في تحديد أنماط السلوك المجرم، ومن ثم تنظيم العقوبة بما يتفق مع الهدف من التشريع العقابي والمصلحة العامة.

1- محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، 2010، ص 140 وما يليها.

2- أحمد فتحي سرور، القانون الجنائي الدستوري، دار الشروق ،القاهرة، 2004، ص 25 وما بعدها..

ونظرا لهذا التطور الذي عرفته الجريمة في الجزائر، قام المشرع الجزائري بتعديل قانونالعقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004م المتمم للأمر رقم 66-156 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر7.

لكل هذه الأسباب كان لا بد كذلك من الانشغال بوسائل الإثبات وتطويرها، بحيث أصبح ما يعرف بالإثبات الالكتروني أو الرقمي، متجاوزا تلك الإثباتات التقليدية واستبدال الملفات الورقية بالأسطوانات الضوئية أو الأقراص الممغنطة.

ومن خلال هذا كله نتساءل حول السياسة التشريعية الجنائية للمشرع الجزائري في ظل التطور التكنولوجي ومدى مسايرة الصياغة القانونية الجنائية لهذا التطور الحاصل؟

المبحث الأول: المفاهيم القانونيةالجنائية الجديدة المتولدة عن التطور التكنولوجي

مع انتشار الوسائل الحديثة للتكنولوجيا بين افراد المجتمعات وشيوع استخدامها والتوسع في التعامل من خلالها ، اضحى لدى كل فرد القدرة على التفاعل والتواصل دون مانع من حدود أو جغرافيا ، وذلك مع توافر القدرة على نقل وتلقي المعلومات والتقنيات والاضطلاع على البيانات والبرامج بكل سهولة و يُسر ، ومع وجود الحسنات والفوائد الجمة التي رافقت ظهور هذه الحقول الجديدة والمتطورة من العلوم والمعرفة ، إلا ان ذلك قد ترافق مع بروز العديد من المشكلات والسلبيات التي ظهرت على شكل جرائم يقترفها بعض مستخدمي التكنولوجيا والتي تتصف بخطورتها وسهولة ارتكابها ومعضلة عبورها للحدود الوطنية ، والتي يمكن ان يطلق عليها الجرائم الالكترونية أو المعلوماتية أو التقنية، ولأجل ذلك ظهرت مصطلحات ومفاهيم جديدو لم تكن معروفة من ذي قبل وسنتطرق الى ذلك فيما سيأتي.

المطلب الأول: في قانون العقوبات وقانون الاجراءات الجزائية

الفرع الأول: في قانون العقوبات

نص المشرع الجزائري في القسم السابع مكرر[3] من الفصل الثالث من الباب الثاني من الكتاب الثالث من الجزء الثاني من قانون العقوبات على نوع جديد من الجرائم اصطلح على تسميته بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، جاء ذلك في اطار مسايرة المشرع للتطور الحاصل فيفي مجال الاتصالات وتكنولوجيا المعلومات،والتصديق على اتفاقية بودابست[4] المتعلقة بمكافحة الجرائم الالكترونية.

تطرق المشرع الجزائري في القسم المذكور أعلاه إلى مجموعة من المفاهيم والمصطلحات الجديدة من خلال نصوص المواد من 394 مكرر إلى 394 مكرر7.

---

[3]- القانون 15/04 المؤرخ في 2004/10/10 ، ج ر 71، ص 11و12، يتمم الأمر 156/66 المتضمن قانون العقوبات المعدل والمتمم.

[4]- اعتمدت الاتفاقية وتقريرها التوضيحي من قبل لجنة وزراء مجلس أوروبا في دورتها 109 في 8 نوفمبر 2001. وفتح باب التوقيع عليها في بودابست في 23 نوفمبر 2001، ودخلت حيز التنفيذ في 1 يوليو / تموز 2004.

المادة 394 مكرر: "يعاقب ....كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير في معطيات المنظومة.إذا ترتب عن الأفعال المذكورة أعلاه، تخريب نظام اشتغال المنظومة تكون العقوبة....."

ورد في نص هذه المادة مجموعة مصطلحات تحتاج إلى ضبط وتوضيح وتمييز عما قد يشابهها من مصطلحات:

1- فعل يدخل:وهو سلوك يرتكبه المجرم المعلوماتي بشرط أن يكون عن طريق الغش، بمعنى أن هذا الفعل مرتبط بشكل أساسي بوجود نظام معلوماتي محمي الذي يمثل الركن المفترض في مثل هكذا جرائم، وعليه فإن ارتكاب فعل الدخول فقط إلى المنظومة المعلوماتية بطريق الغش تقوم الجريمة.

2- فعل يبقى: ومعناه بقاء الجاني في النظام المعلوماتي سواء لمدة محددة أو غير محددة عن طريق الغش، وهو سلوك قد يرتبط بفعل الدخول المذكور آنفا، وقد لا يرتبط به كأن يكون الدخول مصرحا به لكن الجاني يبقى في النظام المعلوماتي ويتجاوز المجال المخصص له عن طريق الغش.

3- عن طريق الغش: استعمل المشرع هذا المصطلح في جميع فقرات المواد ليؤكد على سوء نية مرتكب الجريمة

4- يحاول ذلك: يؤكد المشرع من خلال استعماله لهذا المصطلح أن مجرد المحاولة للدخول أو البقاء في منظومة معلوماتية فإن الجريمة تقوم في حقه.

5- منظومة للمعالجة الآلية للمعطيات: حاول المشرع الجزائري مجاراة التطور التكنولوجي الحاصل، فصدر بموجب ذلك القانون 09-04 الذي سنتطرق إليه بنوع من التفصيل في المطلب الثاني من هذا المبحث، حيث قام المشرع بتقديم تعاريف لبعض المصطلحات المستعملة في قواعد تكنولوجيات الاعلام والاتصال.

6- فعل حذف: القيام بحذف بيانات ومعطيات من المنظومة المعلوماتية ولا يمكن اعطاء هذا المصطلح تعريفا أو مرادفا آخر حتى لا نحمل النص أكثر مما يحتمل وحتى لا نقع في تكرار المصطلحات وهو يعتبر ظرف تشديد.

7- فعل تغيير: ومعناه قيام المجرم المعلوماتي بالمساس بمعطيات المنظومة المعلوماتية من خلال إضافة معلومات لم تكن في المنظومة، وفعل التغيير بهذا المعنى يحتمل عدة معاني من بينها الحذف، الإزالة، التعديل، التخريب...وهي كلها أفعال تؤدي إلى تغيير في معطيات المنظومة، واعتبره المشرع ظرف تشديد لجريمتي الدخول أو البقاء.

8- فعل تخريب: وينطوي هذا الفعل على قيام المجرم المعلوماتي بإتلاف نظام عمل المنظومة المعلوماتية وهو فعل يتطلب قصدا خاصا، بحيث تتجه ارادة الجاني ليس فقط إلى الدخول أو البقاء في المنظومة وإنما إلى تخريب نظام اشتغالها.

9- نظام اشتغال المنظومة: وهنا يجب التفريق بين نظام اشتغال المنظومة وتشغيل النظام المعلوماتي، فالأولى يقصد بها اشتغال النظام المعلوماتي ككل وكذا المعطيات الموجودة بداخله في حين يقصد بالثانية بدء تشغيل النظام فقط أي زر التشغيل.

المادة 394 مكرر 1:" يعاقب .....كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها."

1- فعل أدخل: ويقصد به ادخال معطيات لم تكن موجودة في الأصل في نظام المعالجة الآلية وهو سلوك غير سلوك الدخول، بمعنى أن الادخال هنا لا يعني الدخول بل أن كل جريمة مستقلة عن الأخرى.

2- معطيات: وهي مجموعة من المعلومات المتضمنة في نظام المعالجة الآلية.

3- فعل أزال: أي نزع وهو سلوك قد يأخذ معنى الحذف، وأزال معطيات من نظام المعالجة الآلية بطريق الغش تستوي فيها الازالة الكلية لمعطيات المنظومة والإزالة الجزئية.

4- فعل عدل: بتشديد حرف الدال وهو فعل يفيد معنى التلاعب بمعطيات النظام المعلوماتي، كما أنه يحتمل عدة معاني تتشابه في مضمونها كالإزالة والادخال والحذف..

5- بطريق الغش: يؤكد المشرع في كل مرة أن القيام بهذه الأفعال لابد أن يكون بطريق الغش أي استعمال طرق احتيالية للدخول الى النظام المعلوماتي وارتكاب الجريمة.

المادة 394 مكرر2:"يعاقب....كل من يقوم عمدا وعن طريق الغش بما يأتي:

- **تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.**
- **حيازة أو افشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في هذا القسم."**

1- يقوم عمدا وعن طريق الغش: أضاف المشرع في هاته المادة مصطلح "عمدا" ليؤكد على اتجاه ارادة المجرم المعلوماتي الى ارتكاب الفعل المجرم.

2- تصميم:تنظيممعطيات وفقًالنموذجقاعدةالبيانات،يحددالمصممالبياناتالتييجبتخزينهاوكيفيةترابطعناصر هذهالبيانات بغرض استخدامهافي ارتكاب جريمة من الجرائم المنصوص عليها في هذا القسم.

3- بحث: وهي محاولة الحصول على أية معطيات سواء كانت مخزنة أو معالجة أو مرسلة تسهل ارتكاب جريمة من الجرائم المنصوص عليها في هذا القسم.

4- تجميع:وضعمجموعةمنعناصرِالمعطيات والبياناتالمنطقيةالمرتبطةمعبعضهاالبعض.

5- توفير: والقصد منه ايجاد معطيات ووضعها تحت تصرف المجرم المعلوماتي من أجل تسهيل ارتكاب الجريمة.

6- نشر: وهو استخدام شبكة المعلومات كوسيلة لعرض المعطيات وبذلك تتاح الفرصة للقارئ للاطلاع عليها أو تحميلها أو نسخها أو طباعتها.

7- الاتجار: وهو جعل معطيات النظام المعلوماتي عبارة عن سلعة تباع وتشترى وذلك عن طريق إما طباعتها أو نسخها على دعامة مادية.

8- معطيات مخزنة: أي موجودة داخل نظام المعالجة الآلية للمعطيات.

9- معطيات معالجة: أي خضعت لتجميع وتصنيف وأصبحت جاهزة للاستعمال.

10- معطيات مرسلة: أي هونقلمعلوماتمرمزة بأمانةبينمصدرمعلوماتمحددووجهةمحددة،ويمكنأنتمثلالمعلوماتالمرمزةأحرفاًهجائيةأوأعداداًأوأشكالاًقدتنتج منضغطمفتاحطرفيةأوصورةنصأوإشارةكهربائيةصادرةعنجهازقياس.

11- حيازة:وهي امتلاك عن طريق الغش لمعطيات متحصل عليها من جريمة من الجرائم المنصوص عليها في هذا القسم.

12- افشاء:وهي امتلاك عن طريق الغش لمعطيات متحصل عليها من جريمة من الجرائم المنصوص عليها في هذا القسم.

13- نشر:وهو استخدام شبكة المعلومات كوسيلة لعرض المعطيات والسؤال هنا هل هناك فرق بين مصطلح "نشر" الوارد في الفقرة الأولى من هذه المادة والفقرة الثانية من نفس المادة.

14- استعمال: وهي استخدام عن طريق الغش لمعطيات متحصل عليها من جريمة من الجرائم المنصوص عليها في هذا القسم.

من خلال ما تم التطرق إليه يظهر جليا أن المشرعالجزائريلم يضعتعريفامحددا لـ " أنظمة المعالجةالآليةللمعطيات" ذلكأنهولغاياتالبحثفيتوافرالجريمةالمعلوماتيةفلابدمنالبحثفيمسألة " المعالجةالآليةللمعطيات"

كشرطلازمللقولبتوافرأوعدمتوافرأركانأيجريمةمنجرائمالمعلوماتية،فإذاثبتعدمتوافرهذاالشرطفإنهلايمكنالبحثفيقياماالجريمةعلىماجاءفيالقسم السابع مكرر 1؛ذلكأنشرط " المساس بأنظمةالمعالجةالآليةللمعطيات" يعتبرعنصرالازمالكلجريمةمنالجرائمالتيتمبيانهافيهذاالقسم؛وبالتاليلايكونمنالضروريتحديدمفهوم " أنظمةالمعالجةالآليةللمعطيات"

والذييعتبرمفهوماتقنياًفنياومتطورابتطورالتقدمالعلميفيمجالالمعلوماتية،وبالتاليفإنعدمتبنيالمشرعمفهوماًمحدداًلهذاالتعبير يروتركهالأمرللفقهوالقضاءأمرقد يشكل عقبة أمام القاضي الجزائي في تطبيق نصوص التجريم.

ولعلهفعلحسناًفيبياناالنماذجالإجراميةالمبينةفيالنصوصالسابقة(394 مكرر-394 مكرر2)،حيثتناولتقسيمجرائم المساس بأنظمة المعالجة الآلية للمعطياتمنجانبين؛الجانبالأولوهوبيانمدلولالجريمةالمعلوماتيةبالمعنىالموضوعيلهامنخلالتحديدأنهذاالسلوكيكونبصورمتعددةوهوسلوكغيرمشروعيكونموجهبواسطةعملياتالكترونيةيكونالهدفمنهاأمننظمالحواسيبوالبياناتالتيتعالجها.

والجانب الثاني هو بيان العقوبة المقررة لكل جريمة من هذه الجرائم.

ومن جهة أخرى وهو أمر على قدر كبير من الأهمية ألا وهومدى إمكانية إخضاع هذه الجرائم الواردة على النظام المعلوماتي للنصوص التقليدية، لأن مجرد القراءة الأولية لهذه النصوص تبين افلات العديد من

السلوكات من التجريم كالنصب الالكتروني والسرقة والاختلاس الالكترونيين...إلخ، وبالتالي فإن ورود هذه النصوص بهذا الشكل دونما تحديد وتفسير واضحين سيكون عقبة أمام القاضي الجزائي خاصة وأن هذا الأخير مقيد بمبدأ الشرعية.

الفرع الثاني : قانون الاجراءات الجزائية

في اطار التطور التكنولوجي الحاصل في مجال القانون الجنائي صدر الأمر رقم 20-04 المؤرخ في 30 أوت 2020 [5]المعدل والمتمم لقانون الاجراءات الجزائية، حيث استحدث من خلال الكتاب الثاني مكرر المعنون بـ: "استعمال وسائل الاتصال المسموعة والمرئية أثناء الاجراءات"، تقنية جديدة اسماها بتقنية المحادثة المرئية عن بعد أو ما اصطلح الفقه القانوني على تسميته بالتقاضي الالكتروني.

وفي الواقع أن التقاضي الالكتروني[(6)]، ظهر عند بداية الألفية الثالثة كمصطلح، ويعد أخر ما توصل إليه العقل البشري من إبداع في فقه القانون في ظل التقدم التكنولوجي المعاصر، لما له من انعكاس إيجابي على عملية التقاضي بصورة عامة، من خلال استثمار الوقت بإتباع إجراءات حديثة ومتطورة من أجل تحقيق العدالة بين المواطنين بأقصر الطرق وأسرعها، كما ينجم عنه توسع دائرة التقاضي لشمل أقاليمخارج نطاق الاختصاص المقرر سابقا بموجب القانون ليصل إلى أقاليم دولية، ومنه يمكن وزارة العدل من تجاوز مشكلة البعد الجغرافي بين الدول والمدن وتكاليفها الباهضة[7].

ونظرا لما تتمتع به هذه التقنية الحديثة من إيجابيات، وأهمية بالغة، تسعى حاليا معظم الدول لتبنيها، ونظرا لحداثة الفكرة فقد وجدنا تعاريف عدة لها سنحاول عرض أهمها لمحاولة تحديد مفهومها الصحيح، كما أن هذه التقنية تقابلها فكرة التقاضي التقليدية، والتي تختلف عنها في طرق التنفيذ باستخدام وسائط، مما يجعلها تنفرد بجملة من الخصائص.

أولا: تعريف التقاضي الالكتروني

---

[5]- الأمر رقم 20-04 المؤرخ في 30 أوت 2020 ، ج ر عدد 51 ، ص 9، يعدل ويتمم الأمر 66-155 المتضمن قانون الاجراءات الجزائية.

[6]- تعود التجربة الأولى لإيجاد تسوية الخصومات عبر الفضاء الالكتروني إلى عام1996 عندما قام معهد قانون القضاء وجمعية التحكيم الأمريكية والمركز الوطني لأبحاث المعلوماتية ومركز القانون وقواعد المعلومات بإدارة برنامج القاضي الافتراضي والإشراف عليه وكان الهدف الرئيسي منه إعطاء حلول سريعة للمنازعات المتعلقة بالإنترنيت عن طريق وسيط يتمثل في قاض محايد يكون خبيرا في التحكيم والقوانين التي تحكم أنشطة الانترنيت أو قانون القضاء الالكتروني ، ويتحقق هذا الهدف بقيام مستخدم الانترنيت بإرسال شكواه إلى تلك الهيئة عن طريق البريد الالكتروني وبعد ذلك تقوم الهيئة باختيار قاضي محايد ليفصل في النزاع ، ويكون قرار القاضي مجردا عن القيمة القانونية إلا إذا قبلت به الأطراف وتكون هذه الخدمة مجانية دون مقابل, أنظر: صلاح المنزلاوي، القانون الواجب التطبيق على عقود التجارة الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص ص 163-164.

[7]- صفوان محمد شديفات، "التحقيق والمحاكمة الجزائية عن بعد عبر تقنية ال Videoconfe،ence"،دراسات، علوم الشريعة والقانون، المجلد 41، العدد 1، 2015، عمادة البحث العلمي، الجامعة الأردنية، ص 353.

إن فكرة التقاضي الالكتروني مستمدة من فكرة الإدارة الالكترونية، والتي تعني الانتقال من تقديم الخدمات والمعلومات إلى الأشخاص بشكلها التقليدي الورقي،إلى الشكل الالكتروني عبر الأنترنت، فهي عبارة عن تطوير لأداء أجهزة القضاء سواء من حيث الخدمات الإدارية أو القضائية.

ولقد تطرق الفقه في العديد من المحاولات إلى إعطاء تعريف لتقنية التقاضي الالكتروني، ولعل أهم هذه التعاريف، كونه:"سلطة لمجموعة متخصصة من القضاة النظاميين بنظر الدعوى ومباشرة الإجراءات القضائية بوسائل الكترونية مستحدثة، ضمن نظام أو أنظمة قضائية معلوماتية متكاملة الأطراف والوسائل،تعتمد منهج تقنية شبكة الربط الدولية (الانترنيت) وبرامج الملفات الحاسوبية الالكترونية بنظر الدعاوى والفصل بها وتنفيذ الأحكام بغية الوصول لفصل سريع بالدعاوى والتسهيل على المتقاضين."[8]

كما عرفه جانب آخر من الفقه، على أنه:"الحصول على صور الحماية القضائية، عبر استخدام الوسائل الالكترونية المساعدة للعنصر البشري، من خلال إجراءات تقنية تضمن تحقيق مبادئ وضمانات التقاضي، في ظل حماية تشريعية لتلك الإجراءات تتفق مع القواعد والمبادئ العامة في قانون المرافعات مع مراعاة الطبيعة الخاصة للوسائل الالكترونية[9] ."

ويعرف بأنه:"عملية نقل مستندات التقاضي إلكترونيا إلى المحكمة عبر البريد الالكتروني حيث يتم فحص هذه المستندات بواسطة الموظف المختص وإصدار قرار بشأن القبول أو الرفض وإرسال إشعار إلى المتقاضين علما بما تم بشأن هذه المستندات".[10]

ولقد عرفه د. أسعد فاضل منديل على أنه:"سلطة المحكمة القضائية المتخصصة للفصل الكترونياً بالنزاع المعروض أمامها من خلال شبكة الربط الدولية (الانترنت) وبالاعتماد على أنظمة الكترونية وآليات تقنية فائقة الحداثة بهدف سرعة الفصل بالخصومات والتسهيل على المتخاصمين[11] ."

فهو تنظيم تقني معلوماتي يتيح للمتقاضين تسجيل دعواهم، وتقديم أدلتهم، وحضور جلسات المحاكمة، تمهيداً للوصول إلى الحكم، وتنفيذه، من خلال وسائل الاتصال الإلكترونية، والتي هي جزء من نظاممعلوماتي يمكن القضاة من الاتصال بالمتقاضين دون حضورهم الشخصي، ومباشرة التقاضيإجراءات التقاضي، من خلال هذا النظام، كما يتيح هذا النظام من خلال المحكمة الإلكترونية شفافية، وسرعة في الحصول على المعلومات.

---

[8]حازم محمد الشرعة، التقاضي الالكتروني والمحاكم الالكترونية، دار الثقافة ، الأردن،2010، ص57؛ عصمت عبد المجيد بكر، دور التقنيات العلمية في تطور العقد، دار الكتب العلمية، بيروت، لبنان، 2015، ص 514.

[9]أسعد فاضل منديل، التقاضي عن بعد ،دراسة قانونية، كلية القانون، جامعة القادسية، العراق، 2014، ص 04.

[10]خالد ممدوح إبراهيم، التقاضي الالكتروني: الدعوى الالكترونية وإجراءاتها أمام المحاكم، دار الفكر الجامعي، الإسكندرية، 2008، ص13.

[11]أسعد فاضل منديل، المرجع السابق، ص 04.

والواضح من هذه التعاريف، أن أصحابها أسهبوا في بيان مفهوم التقاضي الالكتروني وإجراءاته، وكان من الأفضل لو أنهم اكتفوا بالتعريف على اعتبار أن المسألة مسألة فقه القانون، واختصروا العبارات ليكون التعريف أشمل لمفهوم التقاضي الالكتروني وأوضح لمعناه.

وعليه، يمكننا أن نعرف التقاضي الالكتروني كالآتي:" **استخدام وسائل تقنية الاتصال المرئية والسمعية الإلكترونية في مباشرة الدعوى القضائية وحتى الفصل في المنازعات القضائية عن بعد**".

ثانيا: خصائص التقاضي الالكتروني.

يتميز نظام التقاضي الالكتروني بجملة من الخصائص تجعله يختلف عن التقاضي بالطرق التقليدية ويواكب التطور في ظل ثورة تكنلوجيا المعلومات، هذه المميزات نوجزها في الآتي:

1- الانتقال من النظام الورقي إلى النظام الالكتروني: إن أهم ما يميز إجراءات التقاضي الالكتروني، هو عدم استعمال الوثائق الورقية في كافة الإجراءات والمراسلات بين طرفي التقاضي، حيث تتم بينهم الكترونيا، وهو ما يتفق مع الغرض من إنشاء الوسائط؛ بمعنى خلق مجتمع المعاملات اللاورقية[12]،لذلك نجد بأن الدعائم الالكترونية سوف تحل محل الدعائم الورقية بصفة نهائية، بحيث تصبح الرسالة الالكترونية هي السند القانوني الذي يمكن طرفي النزاع من اعتماده في حالة نشوئه،ودليل من أدلة الإثبات الالكترونية[13].

كما أن استخدام المستندات والوثائق الالكترونية يمكن من التخلص من الكميات الكبيرة للملفات الورقية للدعاوى، التي تكاد تمتلئ بها غرف المحاكم، وكذلك التخلص من عملية التخزين العشوائي لملفات الدعاوى وما يترتب عليها من ضياع وفقدان لها .

وبهذا يمكن تخفيض المساحات المخصصة لتخزين الملفات الورقية في الأجهزة القضائية، واستعمالها في نشاطات أخرى المحكمة،كما أن الوثائق والمستندات الالكترونية، يمكن الوصول إليها والاطلاع عليها بسهولة وبسرعة مما هو علية في الملفات الورقية.

2- السرعة في تلقي وإرسال المستندات والوثائق:تتيح شبكة الانترنت إمكانية إرسال المستندات والوثائق، وبعض الرسائل الكترونيا؛ بمعنى التسليم الفوري للوثائق الكترونيا، شأنها في ذلك شأن البحوث والتقارير الالكترونية، إلى جانب بعض الخدمات كالاستشارات القانونية وطلب الخبرة في مجال ما، والتي تعتمد على تقنية التنزيل"**do**ين**nload**"، وتقابله التقنية الثانية التي يطلق عليها بـ"**upload**"، والتي تعني التحميل عن بعد، أي إرسال ملف أو برنامج إلى جهة أخرى،لذلك نرى بأن أجهزة الإرسال الالكترونية، لها دور قانوني في تطبيق إجراءات التقاضي الالكتروني، بحيث يساعد هيئة القضاء في التجميع والتخزين

---

[12]خالد ممدوح إبراهيم، التقاضي الالكتروني: الدعوى الالكترونية وإجراءاتها أمام المحاكم، دار الفكر الجامعي، الإسكندرية، 2008، ص36.

[13]هادي حسين الكعبي ونصيف جاسم محمد الكرعاوي، مفهوم التقاضي عن بعد ومستلزماته، مجلة المحقق الحلى للعلوم القانونية، العدد الأول، السنة الثامنة، 2016، ص 284.

والحفظ،وكذا في الإعلاناتالإخطارات، وفي تبادل الوثائق بين الخصوم أو ممثليهم القانونيين[14]. وهذه الخاصية تسمح بالاستثمار في الوقت.

3- استخدام الوسائط الالكترونية في تنفيذ إجراءات التقاضي:يعد استخدام الوسائط الالكترونية في تنفيذ إجراءات التقاضي عبر شبكة الاتصالات الالكترونية، من أهم خصائص التقاضي الالكتروني،على اعتبار أن هذا الأخير، لا يختلف من حيث الموضوع أو الأطراف عن التقاضي التقليدي، وإنما الاختلاف يكمن في طريقة تنفيذه، حيث يتم باستخدام وسائط الكترونية؛ تتمثل في جهاز كمبيوتر متصل بشبكة الاتصالات الدولية(net،Inte)،أو شبكة اتصال خارجي خاصة (anet،Ext) التي تقوم بنقل التعبير عن الإدارة الالكترونية في نفس اللحظة رغم البعد المكاني لأطراف النزاع[15] ، سماع أقوالهم،تبادل المذكرات بينهم أو بين ممثليهم،الاستماع لأقوال الشهود أو استجواب الخصوم [16].

4- سرعة البت في القضايا وإنجاز إجراءات التقاضي:تتم عملية إرسال واستلام المستندات والوثائق في التقاضي الالكتروني دون الحاجة لانتقال أطراف الدعوى مرات عديدة لمقر المحكمة لذلك تساهم في اختصار الزمن وتوفير الجهد وتقليل النفقات، وهذا يؤدي إلى تقليل وامتصاص مشاكل ازدحام الجمهور في المحاكم وارتفاع جودة مستوى الخدمة المقدمة لأطراف الدعوى[17] . بالإضافة إلى ذلك نجد أن القضاء التقليدي الجاري حاليا، أن يعقد القاضي الجلسة الأولى، وقد يخصصها لاستماع أقوال المدعي، ثم يعطي الخصمين موعدا آخر، ربما يكون بعد شهر أو شهرين، وربما ثلاثة أشهر، للجلسة الثانية، فإذا وصل موعد الجلسة الثانية، يكون القاضي قد نسي القضية تماما، فيضيع نصف زمن الجلسة الثانية في قراءة القاضي لضبط الجلسة الأولى، وسؤال الخصمين عما دار فيها، بل ربما يعقد جلسة أخرى لسماع البينات بعد ثلاثة أشهر، وهكذا دواليك في سلسلة لا تنقضي، وأما في القضاء الإلكتروني، فإن ذلك سيختفي ذلك تماما، حيث أن القضية لن ترفع إلى القاضي، إلا بعد استيفاء جميع البيانات والإثباتات والأقوال التي يرغب الطرفان في إبدائها، ثم يرفع الملخص بعد موافقة الطرفين عليه للقاضي لينظر فيه، فالقضية هنا تكون ناضجة تمامًا حال رفعها للقاضي، وقد يحتاج القاضي بعد ذلك لبعض الأسئلة اليسيرة ثم يصدر حكمه مباشرة.[18]

المطلب الثاني: في القوانين الخاصة ذات الصلة

نص المشرع الجزائري في القانون رقم 09-04 المؤرخ في 05 اوت 2009 المتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيات الاعلام والاتصال ومكافحتها على قواعد قانونية جديدة تتماشى والتطور

---

[14]خالد ممدوح إبراهيم، المرجع السابق، ص 36.

[15]ليلى عصماني، "نظام التقاضي الالكتروني آلية لإنجاح الخطط التنموية"، مجلة المفكر، العدد 13، فيفري 2016، كلية الحقوق والعلوم السياسية، جامعة بسكرة، ص 218.

[16]سيد أحمد محمود ، دور الحاسب الالكتروني أمام القضاء ، دار النهضة العربية ،مصر، 2008،ص30.

[17]ليلى عصماني، مرجع سابق، ص 218.

[18]حسام محمد نبيل،" التقاضي الإلكتروني" والعدالة الناجزة"، مجلة لغة العصر ، 09- 12-2017، تاريخ الاطلاع: 2022/08/10 ساعة الاطلاع :21:44.لمttp://aitmag.a،لم،am.o،g.eg/Neينs/86774.aspx

الحاصل في مجال القوانين الجنائية تكملة لما ورد في القسم السابع مكرر 1 المذكور أعلاه، حيث تطرق في مادته الثانية إلى تعريف مجموعة من المصطلحات المستخدمة في مجال انظمة المعالجة الآلية للمعطيات نتناولها فيما سيأتي.

المادة الثانية:" يقصدفيمفهومهذاالقانونبمايأتي:

أ – الجرائمالمتصلةبتكنولوجياتالإعلاموالاتصال:جرائمالمساسبأنظمةالمعالجةالآليةللمعطياتالمحددةفيقانونالعقوباتوأيجريمةأخرىترتكبأويسهلارتكابهاعنطريقمنظومةمعلوماتيةأونظاماللاتصالاتالإلكترونية.

ب – منظومةمعلوماتية:أينظاممنفصلأومجموعةمنالأنظمةالمتصلةببعضهاالبعضأوالمرتبطةيقوموا حدمنهاأوأكثر بمعالجةآليةللمعطياتتنفيذالبرنامجمعين.

ج – معطياتمعلوماتية : أيعمليةعرضللوقائعأوالمعلوماتأوالمفاهيمفيشكلجاهزللمعالجةداخلمنظومةمعلوماتية بمافيذلكالبرامجالمناسبةالتيمنشأنهاجعلمنظومةمعلوماتيةتؤديوظيفتها.

د – مقدموالخدمات:

1 – أيكيانعامأوخاصيقدملمستعمليخدماتهالقدرةعلىالاتصالبواسطةمنظومةمعلوماتية و/أونظاماللاتصالات.

2 – وأيكيانآخريقوم بمعالجةأوتخزينمعطياتمعلوماتيةلفائدةخدمةالاتصالالمذكورةأولمستعمليها.

هـ – المعطياتالمتعلقةبحركةالسير: أيمعطياتمتعلقةبالاتصالعنطريقمنظومةمعلوماتيةتنتجهاهذهالأخيرةباعتبارهاجزءافيحلقةاتصالات توضحمصدرالاتصال،والوجهةالمرسلإليها والطريقالذييسلكهووقتوتاريخوحجومدةالاتصالونوعالخدمة.

و – الاتصالاتالإلكترونية:أيتراسلأوإرسالأواستقبالعلاماتأوإشاراتأوكتاباتأوصورأوأصواتأومعلوماتمختلفةبواسطةأيوسيلةإلكترونية".

المبحث الثاني: تأثير التطور التكنولوجي على السياسة التشريعية الجنائية

المطلب الأول: من خلال صياغة قواعد قانونية جديدة(أزمة المصطلحات وتحديد المفاهيم)

أولا :تطبيق نصوص قانون العقوبات التقليدي

إن واقع التطور التكنولوجي في العصر الحديث فرض نفسه على الساحة التشريعية والقضائية في معظم دول العالم ، بحيث أصبح هاجسا لكل المهتمين بالشأن العام . وفيالجزائر ومع انه لا يوجد تشريع خاص بالجرائم المعلوماتية إلا أن هذا الموضوع ونتيجة ضغط الواقع أصبح حائزا على اهتمامات كل القطاعات الناظمة للشأن التشريعي والإداري والاقتصادي.

إلا أن هذا الاهتمام مازال يبارح مرحلة المحاولات التي تهدف للوصول إلى صياغة أطر قانونية حديثة تقوم بتحقيق المواجهة الفاعلة للجرائم المعلوماتية، فبالنسبة للتجريم المطبق في الجزائر فإن المواجهة تقتصر على قواعد قانون العقوبات التقليدي بحيث يتم تطويع هذه النصوص والمفاضلة فيما بينها لتنطبق على السلوك المخالف لتخدم قطاع العدالة في معاقبة مرتكبي هذه الجرائم ، والتي في كثير من الأحيان لا تؤدي الغرض المرجو منها في مواجه هذا السلوك سواء كان ذلك بسبب عدم التكييف القانوني السليم لهذا السلوك وبالتالي افلات المجرم من العقاب أو بسبب عدم كفاية العقوبة المقررة وعدم تناسبها مع حجم الفعل والضرر اللذَينِ تحققا.

حيث انه يتم ملاحقة بعض الجرائم التي ترتكب بواسطة الكمبيوتر والانترنت عن طريق إسقاط نصوص قوانين العقوبات الساري في الجزائر، مثل نصوص الابتزاز والنصب ونصوص السرقة والإتلاف والتزييف وتقليد الأختام والتزوير وخيانة الأمانة والسب والقذف والتشهير وإفشاء الأسرار والحض على الفجور ، بحيث يتم تطبيق هذه النصوص عندما ترتكب هذه الجرائم بواسطة الكمبيوتر أو شبكة الانترنت ، وغني عن البيان بأن هذه النصوص تعتبر قاصرة عن الوفاء بالغرض وبالتالي تدق الحاجة إلى التجريم المعلوماتي الخاص بهذه الجرائم ، ذلك أن نصوص هذه الجرائم تنطبق عندما يكون الكمبيوتر وسيلة لارتكاب السلوك وفي بعض الأحيان عندما تقع على الكمبيوتر ذاته إلا أن المجرم في كثير من الأحيان يفلت من العقاب بسبب عدم وجود النص التشريعي المناسب للتجريم .

ثانيا : القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيات الاعلام والاتصال ومكافحتها .

حيث ان جهات الملاحقة قد تجد ضالتها التجريمية في نصوص هذا القانون عندما يتعلق السلوك المرتكب بوسائل الاتصال ، حيث أن هذا القانون يتعلق بعملية تنظيم الاتصالات وإنشاء وتشغيل الشبكات ومحطات البث واستخدام الموجات ، وكذلك يشتمل على الحماية الجنائية لتكنولوجيا الاتصالات في الجزائر، فمن ضمن ما نص عليه هذا القانون مراقبةالاتصالاتالإلكترونية والحالاتالتيتسمحباللجوءإلىالمراقبةالإلكترونية فمثلا المادّة4 تنص:" يمكنالقيامبعملياتالمراقبةالمنصوصعليهافيالمادة3أعلاهفيالحالاتالآتية:

أ – للوقايةمنالأفعالالموصوفةبجرائمالإرهابأوالتخريبأوالجرائمالماسةبأمنالدولة.

ب – فيحالةتوفرمعلوماتعناحتمالاعتداءعلىمنظومةمعلوماتيةعلىنحويهددالنظام العاموالدفاعالوطنيأومؤسساتالدولةأوالاقتصادالوطني.

ج–

مقتضياتالتحرياتوالتحقيقاتالقضائيةعندمايكونمنالصعبالوصولإلىنتيجةتهمالأبحاثالجاريةدونااللجوءإلىالمراقبةالإلكترونية.

د – فيإطارتنفيذطلباتالمساعدةالقضائيةالدوليةالمتبادلة.

لايجوزإجراءعملياتالمراقبةفيالحالاتالمذكورةأعلاهإلابإذنمكتوبمنالسلطةالقضائيةالمختصة.

عندمايتعلقالأمربالحالةالمنصوصعليهافيالفقرة "أ" منهذهالمادة، يختصالنائبالعاملدىمجلسقضاءالجزائربمنحضباطالشرطةالقضائيةالمنتمين للهيئةالمنصوصعليهافيالمادة 13أدناه، إذنا لمدةستة (6)أشهرقابلةللتجديدوذلكعلىأساستقريريبين طبيعةالترتيباتالتقنيةالمستعملةوالأغراضالموجهةلها".

علما أن هذا القانون يعتبر من القوانين الحديثة نسبيا في مجال تكنولوجيا الاتصالات كونه يتعلق بمعالجة الجوانب الفنية لعملية الاتصالات ذاتها وكذلك معالجة الإطار الرقابي وضبط المخالفات والجرائم التي ترتكب في إطار الإساءة لتقنية الاتصالات [19]. إلا أنه في نهاية المطاف ومع وجود بعض النصوص التي تجرم سلوكيات تدخل في إطار الجرائم الالكترونية إلا انه بالمجمل لا يشتمل على الحماية الجنائية الكافية التي يمكن أن تستوعب الأفعال التي ترتكب في إطار الجرائم الالكترونية .

المطلب الثاني:على صعيد التحري والاثبات

إن الاعتماد على نظم المعلومات والكمبيوتر والشبكات في الاعمال في ازدياد مستمر ولا تزال تثار مشكلة امن هذه النظم والشبكات، إذ أن المشكلة الحقيقية تكمن في حمايتها وحماية محتواها من انشطة الاعتداء عليها.

وإن المواجهة الحقيقة لأي نوع من الجرائم إنما تظهر للعيان عندما يكون هناك أجهزة مختصة وإجراءات مقننة تظهر من خلالها القدرة على الملاحقة والكشف وإحراز الأدلة وصولا إلى إثبات الجريمة او السلوك المخالف للقانون امام الجهات القضائية المختصة تمهيدا لمحاكمته وإقرار العقوبات الرادعة بحق مقترف السلوك .

أولا : انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال

وفي الجزائرتمإنشاءالهيئةالوطنيةللوقايةمنالجرائمالمتصلةبتكنولوجياتالإعلاموالاتصالومكافحته حيث تنص المادّة13

[19]– عبد الفتاح بيومي حجازي ، الجرائم المستحدثة ، ط1 ، منشأة المعارف ، الاسكندرية 2009، ص315.

:"تنشأهيئةوطنيةللوقايةمنالجرائمالمتصلةبتكنولوجياتالإعلاموالاتصالومكافحته.تحددتشكيلةالهيئةوتنظيمهاوكيفياتسيرهاعنطريقالتنظيم.

وتضطلع هذه الهيئة بالمهامالتالية:

أ – تنشيطوتنسيقعملياتالوقايةمنالجرائمالمتصلةبتكنولوجياتالإعلاموالاتصالومكافحته.

ب – مساعدةالسلطاتالقضائيةومصالحالشرطةالقضائيةفيالتحرياتالتيتجريهابشأن الجرائمذاتالصلةبتكنولوجياتالإعلاموالاتصال بمافيذلكتجميعالمعلوماتوإنجازالخبراتالقضائية.

ج –

تبادلالمعلوماتمعنظيراتهافيالخارجقصدجمعكلالمعطياتالمفيدةفيالتعرفعلىمرتكبيالجرائمالمتصلةبتكنولوجياتالإعلاموالاتصالوتحديدمكانتواجدهم.

فقد تم إنشاء هذه الهيئة بهدف مواجهة التحديات القائمة في هذا المجال لمكافحة الجرائم الالكترونية كظاهرة من الظواهر الإجرامية المستحدثة والتي تتطلب طواقم وإجراءات ومعدات خاصة والتي ترتكب إما عن طريق وسائل الاتصال المختلفة أو باستخدام الحاسوب والانترنت ، وتعمل هذه الوحدة جاهدة وباستخدام الطرق التكنولوجية الحديثة للكشف عن الجرائم ، وكذلك التعرف على الجناة بهدف تقديمهم إلى العدالة.

هذا وتسعى هذه الوحدة إلى توفير الأدلة اللازمة لإثبات الجرائم الالكترونية ، وتسعى وبالعمل مع النيابة العامة للخروج بآليات قانونية سليمة للتحصل على الأدلة الالكترونية التي يمكن استخدامها لإدانة المتهمين ، وكذلك تعمل على صياغة دليل إرشادي للعاملين يبين إجراءات البحث والتحري في الجرائم الالكترونية وذلك بهدف توضيح الإجراءات الواجبة الإتباع وتسهيل مهمات جمع الأدلة ' وذلك في اطار السعي المتواصل لتحسين مستوى المواجهة مع المحافظة على المشروعية الاجرائية في خضم ملاحقة هذه الجرائم ، وما يظهر ايضا هو عدم القدرة على الوصول بالإنجاز الى اقصى درجاته وهو الذي يعطي صورة واضحة عن حجم المعيقات سواء من المتعلقة بالإمكانات أو ما هو بالمعيقات الاجرائية من الناحية القانونية ومشروعية الاجراءات والادلة المستخلصة ، وهو الذي يستأهل معه الوقوف على اقرار القوانين سواء المتعلق بالتجريم أو الملاحقة والاثبات .

ثانيا:التحري والتفتيش وحجز المعطيات

يقصد بالتحري بالاصطلاح القانوني بحث واستقصاء الحقائق ، وهو عمل أمني وقانوني يقوم به المتحري للحصول على معلومات وبيانات تعريفية او توضيحية عن الاشخاص او الاشياء او الاماكن ، وذلك للحد من الجرائم أو ضبطها لتحقيق الامن والحفاظ على النظام العام[20]. ويمكن القول بان التحري الالكتروني إنما

[20]– مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، مصر (المحلة الكبرى) 2005م، ص23.

يتم عبر الحواسيب ونظم المعلومات وشبكة الانترنت وهو عمل امني وقانوني يتم بواسطة التقنيات الالكترونية والرقمية للحصول على المعلومات عن الأشخاص أو الأماكن أو الأشياء وذلك للحد من الجرائم أو ضبطها[21].

جاء في الفصلالثالث المعنون بالقواعدالإجرائية من القانون 09-04 ،تفتيشالمنظوماتالمعلوماتية حيث نصت المادّة 5 منه: "يجوزللسلطاتالقضائيةالمختصةوكذاضبّاطالشرطةالقضائية. فيإطارقانونالإجراءاتالجزائيةوفيالحالاتالمنصوصعليهافيالمادة 4أعلاه، الدخول،بغرضالتفتيش، ولوعنبعد،إلى :

أ – منظومةمعلوماتيةأوجزءمنهاوكذاالمعطياتالمعلوماتيةالمخزنةفيها.

ب – منظومةتخزينمعلوماتية.فيالحالةالمنصوصعليهافيالفقرة "أ " منهذهالمادة،إذاكانتهناكأسبابتدعوللاعتقادبأنالمعطياتالمبحوثعنهامخزنةفيمنظومةمعلوماتيةأخربوأنهذ هالمعطيات

يمكنالدخولإليها،انطلاقامنالمنظومةالأولى،يجوزتمديدالتفتيشبسرعةإلىهذهالمنظومةأوجزءمنهابعدإعلامالسلط ةالقضائيةالمختصةمسبقابذلك.

إذاتبينمسبقابأنالمعطياتالمبحوثعنهاوالتي

يمكنالدخولإليهاانطلاقامنالمنظومةالأولى،مخزنةفيمنظومةمعلوماتيةتقعخارجالإقليمالوطني،

فإنالحصولعليهايكونبمساعدةالسلطاتالأجنبيةالمختصةطبقاللاتفاقياتالدوليةذاتالصلةووفقالمبدأالمعاملةبالمث ل.

يمكنالسلطاتالمكلفةبالتفتيشتسخيركلشخصلهدرايةبعملالمنظومةالمعلوماتيةمحلالبحثأوبالتدابير المتخذةلحمايةالمعطياتالمعلوماتيةالتيتتضمنها،

قصدمساعدتهاوتزويدهابكلالمعلوماتالضروريةلإنجازمهمتها".

أما بخصوص حجزالمعطياتالمعلوماتية فنصت المادّة6:"عندماتكتشفالسلطةالتيتباشرالتفتيشفيمنظومةمعلوماتيةمعطياتمخزنة

تكونمفيدةفيالكشفعنالجرائمأومرتكبيهاوأنهليسمنالضروريحجزكلالمنظومة،يتمنسخالمعطياتمحلالبحث وكذاالمعطياتاللازمةلفهمها،علىدعامةتخزينإلكترونيةتكونقابلةللحجزوالوضعفيأحرازوفقاللقواعدالمقررةفيقانونالإجراءاتالجزائية.

[21]– مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، مرجع سابق، ص22.

يجبفيكلالأحوالعلىالسلطةالتيتقومبالتفتيشوالحجزالسهرعلىسلامةالمعطياتفيالمنظومةالمعلوماتيةالتي يتجريبهاالعملية.غيرأنهيجوزلهااستعمالالوسائلالتقنيةالضروريةلتشكيلأوإعادةتشكيلهذهالمعطيات،قصدجعلهاقابلةللاستغلالللأغراضالتحقيق،شرطأنلايؤديذلكإلىالمساسبمحتوىالمعطيات."

وفي حالة الحجزعنطريقمنعالوصولإلىالمعطيات فنصت المادّة7 :

"إذااستحالإجراءالحجزوفقالماهومنصوصعليهفيالمادة

6أعلاه،لأسبابتقنية،يتعينعلىالسلطةالتيتقومبالتفتيشاستعمالالتقنياتالمناسبةلمنعالوصولإلىالمعطياتالتيتحتويهاالمنظومةالمعلوماتية،أوإلىنسخها،الموضوعةتحتتصرفالأشخاصالمرخصلهمباستعمالهذهالمنظومة.المعطياتالمحجوزةذاتالمحتوىالمجرم".

المادّة 8: "

يمكنالسلطةالتيتباشرالتفتيشأنتأمربإتخاذالإجراءاتاللازمةلمنعالاطلاععلىالمعطياتالتييشكلمحتواهاجريمة،لاسيماعنطريقتكليفأيشخصمؤهلباستعمالالوسائلالتقنيةالمناسبةلذلك".

وقد وضع القانون حدودالاستعمالالمعطياتالمتحصلعليها حيث نصت المادّة 9 :

"تحتطائلةالعقوباتالمنصوصعليهافيالتشريعالمعمولبه،لايجوزاستعمالالمعلوماتالمتحصلعليهاعنطريقعملياتالمراقبةالمنصوصعليهافيهذاالقانون،إلافيالحدودالضروريةللتحرياتأوالتحقيقاتالقضائية".

وقد نظم القانون قواعد التفتيش ودخول المنازل والانتقال إلى مسرح الجريمة وإجراء الكشف والمعاينة ، فقد نص القانون على عدم جواز تفتيش الشخص أو حبسه او الاعتداء على حريته إلا بأمر قضائي وفق أحكام القانون ، وكذلك نص قانون الاجراءات الجزائية على اجراءات الكشف والمعاينة والانتقال الى مسرح الجريمة وأقر كذلك قواعد دخول وتفيش المساكن وأقر لها حرمة خاصة بحيث لا يجوز دخولها او تفتيشها إلا بأمر من جهات الاختصاص [22].

ولكن ما يثور حول هذا الموضوع هو مدى انطباق هذه القواعد التقليدية الخاصة بالتفتيش والكشف والمعاينة على حالة تفتيش نظم الكمبيوتر وقواعد البيانات وتثور أيضا أهمية الاستعانة بالخبرة في هذه المجالات حيث أن الخطأ القانوني في تفتيش وضبط الدليل قد يفوت الفرصة في كشف الجريمة أو إدانة الجاني . حيث ان تفتيش الحواسيب ونظم المعلومات هو تفتيش لما يحفظه الجهاز أو الشبكة عندما يكون مزودا بحافظات الكترونية للعمليات التي تتم عبره ، وهو في نهاية الامر تفتيش للفضاء الافتراضي غير الملموس في كثير من الاحيان وبما يصعب معه تحريز الدليل الا من خلال تجميده على شكل مادي ملموس ، وكل هذا انما يتعلق بالقدرة على تحديد المطلوب مسبقا من أجل استحضار جميع الاجراءات القانونية اللازمة

[22]– وقد جاء ذلك في الباب الأول من قانون الاجراءات الجزائية.

للنفاذ الى هذه الفضاءات الافتراضية بناء على أمر مقنن من السلطات المختصة ذلك ان هذه الاجراءات قد تنطوي على كشف خصوصية البيانات المخزنة في النظام ، فإذا لم تكن ضمن الاطار المبين في أوامر التفتيش والضبط فإنها تذهب باتجاه الصيرورة الى بطلان الإجراء وبالتالي بطلان الدليل الذي استمد منه.

ولا بد من الاشارة إلى الهدف الاساسي من إجراءات التفتيش والضبط وهو كشف الاعتداءات والجرائم التي تقع على الافراد والمصالح العامة ، حيث أن البيانات المخزنة داخل الحواسيب والنظم ليس جميعها تتصل بجريمة الاعتداء موضوع التفتيش ، لهذا فلا بد من المحافظة على الخصوصية وحرمة الحياة الخاصة في معرض الكشف عن الدليل, أو في معرض الإقرار باستخدام دليل ذي طبيعة الكترونية ذلك أنه حق دستوري قد نص عليه الدستور[23]. وهذا عوضا عن أنه من ضمن الأهداف الأساسية للتجريم الالكتروني هو حماية الخصوصية وحرمة الحياة الخاصة بالإضافة إلى الأهداف الأخرى في حماية المصالح الإستراتيجية للجماعة والنظام العام أو المتعلقة بالحقوق الأساسية للأفراد .

الخاتمة:

في ختام هذ الورقة البحثية توصلنا إلى أنه من الضروري والأهمية بما كان إعادة النظر في قانون العقوبات بشكل أساسي والقوانين المتعلقة به من خلال التوجه نحو سياسة جنائية فاعلة في ظل التطور التكنولوجي، إنه لا بد من انتهاج سياسة جنائية واضحة وتكون كفيلة بمواجهة الجرائم المستحدثة، بحيث يتوفر لهذه السياسة مقومات النجاح من المناقشة المستفيضة والتخطيط الشامل والجهات التنفيذية القادرة والناشطة، والأدوات التشريعية والقضائية المتخصصة والفاعلة لتتكلل الجهود المبذولة بالنجاح في الإطار العام لهذه السياسة في مواجهة الجرائم بصورة شاملة متكاملة وقابلة للتطور بحيث تواكب مستجدات العصر وتتواءم مع مبادرات التعديل والتطوير.

[23]– فقد نص التعديل الدستوري لسنة 2020 في مادت 47 على أنه:" لكل شخص الحق في حماية حياته الخاصة وشرفه. لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية. حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي."

قائمة المصادر والمراجع:

1- التعديل الدستوري الجزائري بموجب المرسوم الرئاسي 20-442 لسنة 2020 .

2- الأمر رقم 20-04 المؤرخ في 30 أوت 2020 ، ج ر عدد 51 ، ص 9، يعدل ويتمم الأمر 66-155 المتضمن قانون الاجراءات الجزائية.

3- القانون 15/04 المؤرخ في 2004/10/10 ، ج ر 71، ص 11و12، يتمم الأمر 156/66 المتضمن قانون العقوبات المعدل والمتمم.

4- القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من جرائم تكنولوجيات الاعلام والاتصال.

5- محمد حماد الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، 2010.

6- أحمد فتحي سرور، القانون الجنائي الدستوري، دار الشروق ، القاهرة، 2004.

7- صلاح المنزلاوي، القانون الواجب التطبيق على عقود التجارة الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

8- صفوان محمد شديفات، "التحقيق والمحاكمة الجزائية عن بعد عبر تقنية ال Videoconfe،ence"،دراسات، علوم الشريعة والقانون، المجلد 41، العدد 1، 2015، عمادة البحث العلمي، الجامعة الأردنية.

9- حازم محمد الشرعة، التقاضي الالكتروني والمحاكم الالكترونية، دار الثقافة ، الأردن،2010.

10- عصمت عبدالمجيد بكر، دور التقنيات العلمية في تطور العقد، دار الكتب العلمية، بيروت، لبنان، 2015.

11- أسعد فاضل منديل، التقاضي عن بعد،دراسة قانونية، كلية القانون، جامعة القادسية، العراق، 2014.

12- خالد ممدوح إبراهيم، التقاضي الالكتروني: الدعوى الالكترونية وإجراءاتها أمام المحاكم، دار الفكر الجامعي، الإسكندرية، 2008.

13- هادي حسين الكعبي ونصيف جاسم محمد الكرعاوي، مفهوم التقاضي عن بعد ومستلزماته، مجلة المحقق الحلى للعلوم القانونية، العدد الأول، السنة الثامنة، 2016.

14- ليلى عصماني، نظام التقاضي الالكتروني آلية لإنجاح الخطط التنموية، مجلة المفكر، العدد 13، فيفري 2016، كلية الحقوق والعلوم السياسية، جامعة بسكرة.

15- سيد أحمد محمود ، دور الحاسب الالكتروني أمام القضاء ، دار النهضة العربية ،مصر، 2008.

16- عبد الفتاح بيومي حجازي ، الجرائم المستحدثة ، ط1 ، منشأة المعارف، الاسكندرية 2009.

17- مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية، مصر (المحلة الكبرى) 2005.
18- مصطفى محمد موسى، دليل التحري عبر شبكة الانترنت، دار الكتب القانونية ،المحلة الكبرى، مصر ،2005.
19- حسام محمد نبيل،" التقاضي الإلكتروني" والعدالة الناجزة"، مجلة لغة العصر ، 09- 12- 2017، تاريخ الاطلاع: 2022/08/10 ساعة الاطلاع 21:44: http://aitmag.aلم،am.o،Ne/eg.gينs/86774.aspx.

شريفة سوماتي

أستاذ محاضر أ جامعة الجيلالي بونعامة – قسم الحقوق–

بريد الكتروني : c.soumati@univ-dbkm.dz

محور المداخلة : المحور الأول

عنوان المداخلة

متطلبات التحول الرقمي لتحقيق مجتمع المعرفة

مقدمة :

لقد تعددت التصنيفات المتعلقة بالمجتمع من فترة لأخرى وعبر مراحل تاريخية متعددة، فهناك من يقسمها بناءا على السيرورة التاريخية فيصنفها إلى مجتمعات كلاسيكية وأخرى حديثة، وهناك من يفضل تنميطها بناءا على نمط المعيشة السائد فيها. ثم أن هناك من يضع تصنيفا اخر يرتبط بصورة كبيرة مع وسائل وأدوات العمل السائدة فيها وكذا الموارد المستعملة فيها، فانتقلت من الصيد إلى الزراعة ثم إلى الصناعة هذه الأخيرة التي ساهمت في ظهور الاختراعات والابتكارات التي سهلت من حياة الأفراد نسبيا ، غير أننا نشهد اليوم مجتمع جديد يشتغل على موارد أخرى جديدة لم تكن مستغلة من قبل أو أن الاهتمام بها كان ذا طابع فلسفي أكثر منه عملي ويتعلق الأمر بالمعرفة[1] .

وفي هذا الصدد شهدت المجتمعات المعاصرة في العقدين الماضيين تطورات متسارعة في شتى مجالات الحياة: الاجتماعية، والسياسية، والاقتصادية، والثقافية، والمعلوماتية، وقد أفرزت تلك التطورات العديد من المفاهيم الجديدة، منها :مجتمع المعرفة، والثورة المعرفية، والثورة التكنولوجية، والتعليم الرقمي، وغيرها من المفاهيم ذات الدلالات والأبعاد، التي تعبر عن التقدم العلمي والتكنولوجي[2].

ويعد مصطلح مجتمع المعرفة من أهم المصطلحات التي برزت في هذا الصدد، وعرف تطورا كبيرا لاسيما بعد الطفرة التكنولوجية التي يشهدها العالم المعاصر لاسيما في مجال

تكنولوجيات المعلومات والاتصالات الحديثة التي قادت إلى زيادة كم المعارف والمعلومات كمتطلع إلى تعزيز الامكانات المعرفية والعمل على توظيفه والاستفادة منها في تطوير المجتمعات الانسانية عامة، المتقدمة منها والنامية، كما أن التوجه نحو بناء المعرفة يلقى اهتماما كبيرا لدى خطط المنظمات الدولية التي تسعى إلى التقريب بين كافة الدول والحد من الفجوة المعرفية القائمة بينها [3]

ولقد أدى تبادل المعارف والمعلومات بشتى الوسائل، ولا سيما من خلال تكنولوجيات المعلومات والاتصالات، إلى تحويل الاقتصاد والمجتمعات ومختلف النظم الادارية والصحية والعدلية .... وغيرها .في سبيل بناء مجتمعات معرفة جامعة وتمكين المجتمعات المحلية عن طريق زيادة الفرص المتاحة للانتفاع بالمعلومات والمعارف .

وعليه فإن أهمية هذه المداخلة تكمن في كونها جاءت من أجل الاحاطة بأهمية التحول الرقمي في تحقيق مجتمع المعرفة، وإبراز أهم متطلبات تحقيق التحول الفعال بناءا على التجارب الرائدة في هذا المجال . وتبعا لذلك فإن الاشكالية الأساسية التي سنحاول معالجتها من خلال هذه المداخلة هي : كيف يسهم التحول الرقمي في تحقيق مجتمع المعرفة ؟ وما هي المتطلبات الأساسية لضمان تحقيق فعال لمجتمع المعرفة بعيدا عن تلك الصعوبات والمعوقات التي تعترضه ؟

وسيتم الاجابة عن هذه الاشكالية في محورين أساسين باتباع منهج وصفي واخر تحليلي يتناسب وطبيعة الدراسة

المحور الاول : تأصيل مفاهيم الدراسة سنحاول من خلاله تأصيل مفهوم مصطلحين أساسين في عنوان هذه الدراسة وهي **التحول الرقمي ومجتمع المعرفة**

المحور الثاني : المتطلبات الأساسية لنجاح التحول الرقمي في تحقيق مجتمع المعرفة وسيتم التفصيل في هذا المحور بناءا على التجارب الرائدة في هذا الصدد

المحور الأول : تأصيل مفاهيم الدراسة

يعد مجتمع المعرفة، والتحول الرقمي من المفاهيم الحديثة والاليات المستحدثة التي راجت في الاونة الأخيرة وأفرزتها ظاهرة العولمة، لتكون عونا لنا ودليلا هاديا نسترشد به في التخطيط على بصيرة لتحقيق التحول المنشود لإقامة مجتمع معلومات ناجح في بلادنا.

وقبل الولوج في تحديد معنى المصطلحين ينبغي بنا الاشارة الى أن)الرقمية) و (المعرفة) .. يمثلان دعامتين أساسيتين في بناء مجتمع واقتصاد قائم على المعرفة، وفي الخلفية تقبع الإنترنت بما لها من تداعيات في الاتصال وحشد المعلومات وحصاد المعرفة[4] .

أولا: مفهوم التحول الرقمي

أ- تعريف التحول الرقمي :

يعد التحول الرقمي اتجاها عصريا يتوافق وطبيعة متغيرات العصر ومتطلباته، وشرطا لازما لبناء المعرفة في المجتمع.

وهو عملية تحويل مصادر المعلومات على إختلاف أشكالها (من الكتب والدّوريات والتسجيلات الصوتية والصور المتحركة..) إلى شكل مقروء بواسطة تقنيات الحاسبات الالية عبر النظام الثنائي (البيتاتBytes–) والذي يعتبر وحدة المعلومات الأساسية للنظام المعلوماتي بالإستناد للحاسبات الالية وتحويل المعلومات إلى مجموعة من الأرقام الثنائية ويتم القيام بهذه العملية بفضل الاستناد إلى مجموعة من التقنيات والأجهزة المتخصصة[5]

ويذهب البعض إلى أن التحول الرقمي أعمق من مجرد استخدام الأشخاص الحاسب الالي أو الأنترنت وبعض التطبيقات البسيطة في أعمالهم اليومية، بل هو استخدام الأشخاص للتقنية في إدارة أعمالهم ونشطاتهم وفي معالجة وتحليل بياناتهم وفي التواصل بينهم وفي أداء تعاملاتهم الالكترونية بشكل كامل ولابد أن يتم كل ذلك في بيئة رقمية مؤمنة لقواعد بيانات محمية [6] وبمعنى أوسع، يشير المفهوم إلى التغييرات التي تحدثها التكنولوجيا الجديدة بشكل عام حول كيفية العمل والتفاعل معها وكيفية تكوين الثروة ضمن هذا النظام. إذن فالتحول الرقمي هو فكرة أن التقنيات الحديثة يمكن أن تغير بشكل جذري الطريقة التي

نتعامل بها مع القضايا التقليدية. إذ يؤثر على كل مستوى من مستويات العمل, وغالبًا ما يحدد كيفية اختيار للتقدم في المشكلات التي تواجهها.

وبهذا المعنى يصبح التحول الرقمي المرحلة الثالثة من تبني التكنولوجيات الرقمية؛ حيث الكفاءة أو المهارة الرقمية ثم الاستخدام الرقمي ثم التحول الرقمي، فمرحلة التحول تعني أن الاستخدامات الرقمية تمكن بطبيعتها الإبداعات في مجال معين، بد من تعزيز ودعم أنواع جديدة من الابتكارات و الطرق التقليدية، إذ يشير مفهوم "التحول الرقمي" إلى "الذهاب غير الورقي" بما يؤثر على كل من الأعمال الفردية، وشرائح المجتمع ككل، مثل الحكومة، والاتصالات الجماعية، والفن، والطب، والعلوم[7]

ب- خصائص وأهداف التحول الرقمي

للتحول الرقمي مجموعة من الخصائص يتميز بها نوجزها فيما يلي[8]:

- التفاعلية: حيث يتبادل القائم بالإتصال والمتلقي الأدوار، وتكون ممارسة الإتصال ثنائية وتبادلية، وليست في إتجاه أحادي بل يكون هناك حوار بين الطرفين
- اللاتزامنية : وهي إمكانية التفاعل مع العملية الإتصالية في الوقت الذي يناسب الفرد، سواء كان مستقبلا أو مرسلا.
- المشاركة والإنتشار : يسمح التحول الرقمي لكل شخص يمتلك وسوائل بسيطة أن يكون ناشرا لرسالته ويشاركها مع الأخرين
- المرونة: تتسم الشبكة الرقمية بالمرونة حيث تخضع النظم الرقمية عادة للتحكم من جانب برامج Software بالحاسوب مما يسمح بقدر عال من جودة الإستخدام.
  - الذكاء: تتسم الشبكات الرقمية بقدر عال جدا من الذكاء، حيث يمكن أن يصمم النظام الرقمي لكي يراقب تغير أوضاع القنوات الاتصالية بصفة مستمرة ويصحح مسارها
- تجاوز عامل الزمان والمكان فتااتحول الرقمي يتيح امكانية الاتصال عن بعد وبالتالي لا يفترض فيه وجود طرفي الاتصال في مكان واحد.

- إندماج الوسائط: فالوسائل الرقمية الجديدة تيتح إمكانية إستخدام كل وسائل وطرق وتقنيات االإتصال، مثل النصوص، الصوت، الصورة الرسوم البيانية الثنائية والثلاثية الأبعاد
- التخزين والحفظ: حيث يسهل على المتلقي تخزين وحفظ الرسائل الإتصالية واسترجاعها كجزء من قدرات الوسيلة في حد ذاتها.

و تكمن أهداف التحول الرقمي على المستويين الاجتماعي والاقتصادي في النقاط الآتية[9] :
- تعزيز تطوير نظم تكنولوجية وثقافة مالية أكثر ابتكار على مستوى المؤسسات والمجتمع.

-تغيير نظام التعليم لتوفير مهارات جديدة وتوجيه مستقبلي للأشخاص حتى يتمكنوا من تحقيق التميز في العمل الرقمي والمجتمع.

- إنشاء وصيانة البنية التحتية للاتصالات الرقمية وضمان إدارتها وإمكانية الوصول إليها، وتحقيق التوازن بين جودة الخدمة وتكاليف تقديمها.

-تعزيز حماية البيانات الرقمية، والشفافية، وضمان متطلبات الاستقلالية، وتعزيز الثقة.

- تحسين إمكانية الوصول إلى الخدمات، وإرساء ضوابط وآليات وجودة الخدمات الرقمية المقدمة للمجتمع.

- تطبيق نماذج أعمال جديدة ومبتكرة وتحسين الإطار التنظيمي والمعايير الفنية.

- تقليل التكاليف ذلك أن خفض التكلفة يبقى أمر مرغوب فيه للغاية خاصة في الأعمال التجارية..

- **ت**حسين أداء الموظف :يمكن أن يخلق التحول الرقمي بيئة عمل حيث يستطيع للموظفين تحسين الإنتاجية في حياتهم العملية اليومي ة.وأدوات تعاون المؤسسة هي أمثلة رائعة على ذلك, فمثلا يمكن لأدوات Microsoft Teams تقليل الخسائروزيادة الإنتاجية في المؤسسات الكبيرة.

-كما يهدف الى توفير كم هائل من المعلومات وأتاحتها وتحديثها على وسائط رقمية وتوفير خدمات معلوماتية بتقنيات جديدة،كالخدمة المرجعية الرقمية والترجمة و إتاحة المعلوموات

الأكبر عدد من المتفيودين والمتعاملين من خلال المنصات الرقمية وأرشفتها كموارد رقمية يمكن الوصول إليها من بعد وعن بعد[10]

ثانيا: مجتمع المعرفة

أ- تعريف مجتمع المعرفة

لا يوجد تعريف محدد أو متفق عليه للمقصود بمجتمع المعرفة اذ يعد هذا المصطلح من أكثر المصطلحات التي لم تتمخَّض الدراسات عن تعريف واضح، ودقيق له، إلّا أنّ هناك من حاول تعريفه من المُختصِّين؛ بهدف تقديم تعريف شامل يتعلَّق به في مجال اختصاصه،حيث جاءت التعريفات في بدايتها شاملة ومختلفة الجوانب في ذات الوقت .

فقد ذهبت إسراء عبد القادر إلى القول أن مجتمع المعرفة بأنه: " المجتمع الذي يضم مجموعة من الأفراد الذين تتقارب اهتماماتهم، ويجمعون المعرفة المرتبطة بهذه الاهتمامات، ويضيفون العديد من الأفكار إليها، وبذلك فإنهم يضيفون معرفة جديدة إلى المعرفة التي حصلوا عليها مسبقا"[11]

وذخب الوناس إلى أن مجتمع المعرفة يقصد به : " القدرة النوعية على التنظيم وإيجاد الآليات الراقية والعقلانية في مجال التسيير وترتيب الحياة والتحكم في الموارد المتاحة وحسن استثمارها وتوظيفها وخاصة إيلاء الموارد البشرية الموقع المناسب. كما يعِني هذا المفهوم كذلك تطوير أنماط التصرف والتحكم في القدرات المتنوعة "[12]وعرَّفه التركماني على أنّه: "ذلك المجتمع الذي يتَّخذ المعرفة هدفاً رئيسيّاً، تخطيطيّاً، وتطبيقيّاً، في شتّى مجالات حياته، ويُحسِن استعمال المعرفة في تسيير أموره، وفي اتِّخاذ القرارات السليمة، والرشيدة، وهو ذلك المجتمع الذي ينتج المعلومة؛ لمعرفة خلفيّات، وأبعاد الأمور بمختلف أنواعها، ليس في بلده فقط، بل في أرجاء العالَم كلّه"[13] عرَّفه (تقرير برنامج الأُمَم المُتَّحِدة الإنمائيّ لعام 2003م) على أنّه: "ذلك المجتمع الذي يقوم أساساً على نشر المعرفة، وإنتاجها، وتوظيفها بكفاءة في جميع مجالات النشاط المجتمعيّ: الاقتصاد، والمجتمع المدنيّ، والسياسة، والحياة الخاصّة، وصولاً لترقية الحالة الإنسانيّة باطِّراد؛ أي إقامة التنمية الإنسانيّة[14]

غير أنه نظرا لارتباط مجتمع المعرفة بالثروة التكنولوجية وما توفره من معلومات ومعارف ولما كان مجتمع المعرفة مجتمع الثورة الرقمية بامتياز فقد ارتبط مفهوم مجتمع المعرفة

بالتطور القمي الذي نعيشه فأصبح يعني بذلك : المجتمع الذي يُتيحُ لأفراده حُرّية امتلاك المعلومات، ونقلها، وبثّها، وتبادلها، عن طريق التقنيات الحاسوبيّة، والمعلوماتيّة، والفضائيّة المُتعدِّدة، وتوظيفها؛ لتحسين مستوى حياة الإنسان، وخدمته ومن التعاريف التي ذهبت الى ذلك نذكر :

- تعريف منظمة اليونيسكوUNESCO بأنه: المجتمع الذي تقوم فيه عمليات النمو والتطور والابتكار على الاستعمال الأمثل للمعلومات وتكنولوجيا الاتصال[15]
- تعريف(المؤتمر الإقليميّ الأوروبّي لعام 2002م) على أنّه: "المجتمع الذي يُتاح فيه للأشخاص جميعاً، بدون تمييز من أيّ نوعٍ كان، ممارسة حقّهم في حُرّية الرأي، والتعبير، بما في ذلك حُرّية اعتناق الآراء بدون تدخُّل، وحُرّية التماس، وتلقّي، وإصدار المعلومات، والآراء، من خلال أيّ وسيلة اتِّصال، وعَبر الحدود الجغرافيّة[16]"
- وعرف مجتمع المعرفة على أنه: "ذلك المجتمع المستند إلى تكنولوجيا المعلومات والاتصالات عن بعد، وما يرتبط بهما من تطورات اجتماعية واقتصادية وسياسية وثقافية، تزيد من إتاحة سلع المعلومات الجديدة وخدماتها وتأثيراتها الإنتاجية، ويظهر فيه قطاع المعلومات قطاع ا رائد ا وقائدا من قطاعات الاقتصاد[17]."

وهناك تعريف اخر لمجتمع المعرفة تبناه التقرير العالمي لليونسكو حيث يرى أن " مفهوم مجتمعات المعرفة أكثر غنى ويسهل الاستقلالية أكثر من مفهوم التكنولوجيا والاتصالية الذي نجده في أغلب الأحيان في قلب النقاشات حول مجتمع المعلومات " وما يميز هذا التعريف أنه يحاول أن يزيل لبس كبير في المفاهيم ذات الصلة بمجتمع المعرفة وتحديدا مجتمع المعلومات، حيث أن في العادة هناك من يطابق بين المفهومين ويرى بأنهما شيء واحد على الرغم من الفروقات الواضحة بينهما[18] فغالبا ما يستعمل مفهوم مجتمع المعرفة للإشارة إلى مرحلة أكثر تقدما من مراحل التنمية، أو إلى مجتمع معلومات من الجيل الثاني، وإذا كان مجتمع المعلومات يهدف إلى توفير المعلومات والتكنولوجيا اللازمة، فإن مجتمع المعرفة يهدف إلى إنتاج المعرفة، وإنتاج ثقافة قوامها تقاسم المعرفة وتشاركها، مع التركيز على استخدامات تطبيقات الإنترنت، وبالتالي تلبية الحاجات المجتمعية من المعرفة، وبناء القوة والثروة، والارتقاء بنوعية الحياة بصفة عامة[19]، وبالتالي فإن مجتمع المعرفة أبعد من مجتمع المعلومات الذي يعتمد على تقاسم المعلومات عبر تكنولوجيا المعلومات [20]

تبعا لما سبق يمكن القول أن مجتمع المعرفة هو أحد المجتمعات التي تمّ استحداثها في الآونة الأخيرة كأحد المتطلبات الرئيسية للتغيرات التي طرأت على المجتمعات المعاصرة، وكنتيجةٍ للتطور التكنولوجي، حيث لا يقتصر هذا المجتمع على هذا الجانب فقط، بل يشمل العنصر البشري، ويسعى إلى التنمية الشخصية، ويركز على الإبداع، ويدعم المشاركة في المعرفة، حيث يهدف إلى تطور المعلومات والمعارف وانتقالها بين الأجيال، كما يتطلب مجتمع المعرفة تحديداً من الأشخاص أن يكونوا ملتزمين كمعرفين[21].

يضم مفهوم مجتمع المعرفة العديد من المعاني والتفسيرات، حيث يمكننا القول أيضاً أنّه ذلك المجتمع الذي يقوم بإنتاج المعلومات والمعارف وتوظيفها بالأسلوب الأمثل بهدف الإنتاج، حيث تكون الأفكار أو المعرفة أساساً للثروة، ويطلق على ذلك أيضاً اسم رأس المال الفكري[22]، الذي يضم (**العقل، والمعلومة، والبحث والتطوير، وصناعة الأفكار، والمعلومات**) ويسعى بكل طاقاته وبكل جدية إلى إنتاج المعرفة ونشرها وتوظيفها؛ للإفادة منها في المجالات كافة؛ وبخاصة المجالات الحياتية [23]

ب- السمات الأساسية لمجتمع المعرفة[24]

يمكن ايجازها فيما يلي :

- المسار الجديد للاقتصاد العالمي " اقتصاد المعرفة "
- تنامي قطاع المعلومات وتراجع القطاعات الأخرى (صناعة المعلومات والمعرفة)
- اعتبار المعرفة سلعة ومادة خام وعنصر أساسي من هناصر الانتاج
- الاهتمام بالتعليم والمعرفة والبحث العلمي
- التحول إلى أنماط العمل التي تعتمد على الذكاء والعقل والقدرة على التحليل والتوظيف
- التحول إلى العمل والدراسة عن بعد
- التحول من العمل الفردي إلى العمل الجماعي
- الذاكرة الرقمية التي تسمح بالاحتفاظ واسترجاع المعلومات

ت- علاقة التحول الرقمي بمجتمع المعرفة

إن أبرز مقومات المجتمع الرقمي، كما سبق وأن أشرنا، هي المعلوماتية والرقمنة التي أفرزت واقعا جديدا، صاغ مقومات المجتمع الرقمي وفصلت في طبيعته. والتي حاول ياسر خضر البياتي[25] حصرها من خلال النقاط الآتية:

- إن الطفرة التقنية الرقمية قد أدت إلى نقل مركز سلطة القرن العشرين بمؤسساته السياسية والثقافية والاقتصاية إلى (الفرد) في القرن الحادي والعشرين.
- المستقبل الذي ينتظر التقنيات الحديثة لا زال في مراحل النمو الأولى وخاصة تطوات شبكات الانترنت وتقنيات أجهزة الكمبيوتر والهواتف الذكية ولقد تجاوزت الإنترنت فجوات التواصل وأصبحت أكثر انتشارا وهيمنة على مستوى العالم بشكل أسرع من أية وسيلة تواصل أخرى في تاريخ البشر[26].
- بفضل القوة الهائلة للتكنولوجيا الرقمية، سقطت الحواجز الصماء التي كانت تفصل بين البشر، كالبعد الجغرافي واختلاف اللغات والافتقار المزمن للمعلومات، وتحررت القدرات الكاملة لبني البشر على شكل موجة هادرة جديدة تزداد قوة من دون انقطاع، وأصبحت هذه القدرات الضخمة تحت تصرف كل البشر وباتوا قادرين على تحريرها بروس أصابعهم.

ولقد كان للتطورَ المتنامي والمتدفق للتكنولوجيا، سبباً في إدراكِ وبلورةِ دورِ المعرفةِ في النمو الاقتصادي والاجتماعي على حد سواء، الذي أدّى إلى ظهورِ مصطلح «اقتصادِ المعرفة» ثم ظهور مصطلح " مجتمع المعرفة" ، حيث تساهم تكنولوجيا المعلومات والاتصالات بدور هام في تعزيز الانتاج المعرفي من خلال تمكين أفراد المجتمع من مختلف الفئات وإشراكهم بشكلٍ إيجابي في البيئة الرقمية بالاعتماد على مهارات التواصل الفعّال والإبداع لممارسة أشكال المشاركة الاجتماعية التي تحترم حقوق الإنسان وكرامته من خلال الاستخدام المسؤول لتكنولوجيا المعلومات والاتصالات، وبهذا تساهم تكنولوجيا المعلومات في تطوير التنمية بمختلف مستوياتها. وتعتبر عاملا مهما في تطوير الحركة الاقتصادية و العلمية، كما تساهم في تنمية الحركة الاجتماعية و من هنا يأتي الاهتمام بها من طرف الدول، والمؤسسات

المحور الثاني : المتطلبات الأساسية لنجاح التحول الرقمي في تحقيق مجتمع المعرفة

يقصد بالمتطلبات، تلك الاحتياجات اللازمة لإنجاز عمل ما والقيام به وفق معايير محددة مسبقا/ و تعد متطلبات التحول الرقمي في الدولة مطلب أساسي لتحقيق مجتمع المعرفة وقدرتها على التطبيق والتجديد والنماء، سنحاول من خلال هذا المحور ان نتطرق إلى أهم هذه المتطلبات

أولا: وجود إرادة سياسية حقيقية لدعم التحول الرقمي

سبق لنا وأن أشرنا في عدة مناسبات علمية[27] على أهمية هذا المتطلب الذي يعد المحرك الأول لتحقيق تحول رقمي ناجح، لدعم الهياكل وإدخال التغيرات الجوهرية على أساليب العمل في الإدارة بصفة عامة .

كما سبق لنا القول أيضا أنه بالنسبة للجزائر لا نشكك أبدا في وجود هذه الارادة، اذ سعت السلطات العليا في الجزائر إلى تبني فكرة التحول الرقمي والادارة الالكترونية منذ سنة 2005 بإصدار مجموعة من التشريعات والنصوص القانونية التي رافقت هذا التحول، كما تظهر هذه الارادة أيضا من خلال تبني الجزائر لمشروع الجزائر الالكترونية 2013 صمن المبادرات والمشاريع التنموية التي تتبناها الحكومة الجزائرية لتحقيق التنمية المستدامة في مختلف جوانب الحياة، وتأتي الاشارة الأولى لهذا المشروع في الوثيقة التي قدمتها الجزائر لقمة مجتمع المعلومات التي عقدت في سويسرا سنة 2003 حيث أبرزت نيتها للولوج إلى مجتمع المعلومات في زمن أصبح فيه النفاذ إلى شبكة المعلومات والتحكم فيها شرطا أساسيا لكل تقدم سياسي واقتصادي واجتماعي وثقافي ..[28]

ثم تلتها تصريحات رسمية أخرى نذكر من أهمها تصريح رئيس الجمهورية السابق في أطار الاجتماعات السنوية التي يخصها لمختلف القطاعات، حيث ترأس اجتماعا مصغرا خصص لتقييم قطاع البريد وتكنولوجيا الاعلام والاتصال صرح فيه على أهمية ولوج الجزائر لشبكة المعلومات، ووجه في هذا الصدد تعليمات للحكومة من أجل توحيد المسعى وتثمين المؤهلات التي تتوفر عليها الجزائر في الجعود الرامية الى ترقية تحويل التكنولوجيا والمعرفة إلى مجال تكنولوجيا الاعلام والاتصال الحديثة [29]

ثانيا: وضع استراتيجة للتحول الرقمي

يعد أول متطلب أساسي، وذلك من خلال وضع خطة استراتيجية لتطوير الكفاءات والقدرات داخل مؤسسات الدولة والقطاع الخاص ويجب ان تشمل استراتسجية التحول الرقمي ما يلي:

- دعم السلطات العليا للتحول الرقمي
- تشجيع مشاركة المواطنون والأفراد بجميع فئات المجتمع ومختلف مستوياتهم والقطاعات التي ينتمون إليها استعمال التقنيات التكنولوجية
- تحديد مدة الفجوة الرقمية في المجتمعات
- رعاية الأفراد المبدعين في مجال التقنية العلمية
- رسم سياسة التحول الرقمي وتحديد المسؤوليات و إدارته ومراقبته
- بناء رؤية للتحول الرقمي [30]

ثالثا: وضع تشريعات تساير التحول والتطبيق الفعلي للتحول الرقمي وتحديثها وفق المستجدات:

يعد توفير البيئة التشريعية المناسبة لللتحول الرقمي مطلب أساسي لنجاح تطبيق مشروع التحول الرقمي والادارة الالكترونية وذلك من أجل وضع تشريعات حديثة تتوائم و تساير التحول والتطبيق الفعلي للتحول الرقمي وتنظم علاقة المواطن بالادارة وحماية التعاملات الالكترونية من مخاطر التجسس والقرصنة وإصدار اللوائح التي تضمن سرية تبادل المعلومات في نظام الادارة الالكترونية، بالإضافة إلى تغيير التشريعات التي تتلائم والسياسات التقليدية المتعلقة بالعمل إلاداري بما يتناسب مع إلادارة إلالكترونية سواء في ظل الظروف العادية أو في ظل الأزمات[31]

رابعا : نشر ثقافة التحول الرقمي[32]

تعد ثقافة التحول الرقمي أحد المناهج الحديثة في أدارة التغيير والتطوير ببعديها الأول وهو التقنيات المختلفة والبعد الاخر اخلاقي وهو الالتزام بأخلاقيات التعامل مع هذه التقنيات من المحافظة عليها واحترام الملكية الفكرية وغيرها، وتشمل ثقافة التحول الرقمي مايلي :

- تأكيد حق الفرد في التدريب لتكون لديه القدرة على استخدام التكنولوجيات الحديثة

- إنشاء وحدات لإدارة المعرفة في مختلف المؤسسات والقطاعات
- توفير المناخ المناسب للعمل والتعلم

خامسا: تطوير البنية التحتية لتكنولوجيا المعلومات والاتصال (الشبكات الرقمية نموذجا)[33]

يحتاج التحول الرقمي الى توفير بنية تحتية لتكنولوجيا المعلومات والاتصال وتقويتها وتدعيمها لاسيما منا الشبكات الرقمية للقيام بعملية الاتصال والنفاذ الى المعلومات، إن الشبكة عموما تعني مجموعة من الأماكن و العلاقات بين عدة وحدات سواء كانت تلك الوحدات إجتماعية أو تكنولوجية .....، أما الشبكة الرقمية فتتمثل في شبكات الاتصال بين الأجهزة الرقمية وعلى رأسها الكمبيوتر، وتعني الربط بين الأجهزة وبعضها كما لو كانت جهازا واحدا، وهناك نوعان من شبكات الاتصال هما:

- الشبكة محلية: **Network Area Local** :

وهي الشبكة التي تربط بين مجموعة من الحواسويب في نطاق جغرافي ضيق ومحدود مما يتيح للمستخدمين إمكانية مشاركة إستخدام الموارد المتاحة كأجهزة الطباعة والمسح الضوئي... وغيرها

- شبكة واسعة النفاذ: Network Area Wide :و

هي الشبكة التي توفر إمكانية التعامل والإتصال بين مختلف محطات العمل المتباعدة جغرافيا فهي يمكن أن تغطي مودينة أو دولة أو مواقع منتشرة في جميع أنحاء العالم

ومن أبرز المعدات المستخدمة في التحول الرقمي مايلي – :

- الحاسبات الالية ذات المواصفات الملائمة لعملية الرقمنة؛ –
- الماسحات الضوئية المرقمنة Scanner لفحص أنواع المعلومات المكتوبة، المطبوعة، المصورة،...؛ –
- الكميرات الرقمية لرقمنة المواد التالفة التي لا يمكن نقلها؛ –
- أجهزة الحماية من الزيادة المفاجئة في الكهرباء) تفاديا لإتلاف الأجهزة وبالتالي فقدان المعلومات

- أجهزة النسخ الاحتياطية، وتضمن هذ الأجهزة تخزين وحفر الملفات الرقمية في أمان في حالة حدوث خطر ويفضل حفظها خارج المؤسسة؛ –
- الطابعات التي تساعد في طباعة المعلومات المرقمنة في حامالت ورمية؛
- –البرمجيات المستخدمة في عملية الرقمنة وبرامج الإدخال، من بينها: محرر HTMLويسمح بتحرير أو كتابة أي أبواد HTML عن طريق عملية الترميز/ محرر XML يعمل هذا المحرر بشكل كبير بطريقة محرر)HTML الترميز) محرر النص أو معالج الكلمات الذي يسمح بإنشاء النص وكتابته وياغته وتحرير . محرر الصور الذي يسمح بانتاج الصور وتحريرها لأغراض الحفر والعرض بالاضافة الى البرمجيات بمختلف أنواعها و اشكالها..... الخ

سادسا: إدارة وتمويل التحول الرقمي

يحتاج التحول الرقمي على بنية تنظيمية حديثة ومرنة وقيادات إدارية الكترونية واعية تساند التطوير والتغيير وتدعمه وتتعامل بكفاءة مع تكنولوجيا المعلومات وتكون قادرة على الابتكار وهندسة ثقافة التحول الرقمي، مع توفير الاموال اللازمة لكي تتحقق للتحول الرقمي الاستمرارية والنجاح ويلوع الاهداف المنشودة [34]

ولتحقيق ذلك لابد من مراعاة مايلي :

- رصد موازنة لخطة تطبيق التحول الرقمي
- توفير الدعم المالي الكافي لشراء الاجهزة الحاسوبية والبرامج والتطبيقات الحديثة
- تطوير البرامج والتطبيقات المستخدمة
- توفير المخصصات المالية اللازمة للربط الشبكي
- .تخصيص حوافز ومكافآت مناسبة للعاملين في البرنامج .
- توفير المخصصات المالية اللازمة لبرامج تدريب وتأهيل العاملين داخلي

سابعا : الهيكـل التنظيمـي

يتطلب تطبيق التحول الرقمي إحداث تغيير على مستوى الهياكل التنظيمية التقليدية، التي كانت في الغالب تأخذ الشكل الهرمي الملائم لطبيعة الأعمال الصناعية، و عليه يتطلب الأمر التحول إلى هياكل تنظيمية أكثر مرونة كالمصفوفات والشبكات والخلايا الحية

المرتبطة بنسيج الاتصالات، إضافة إلى ذلك يجب استحداث إدارات جديدة، ودمج إدارات أخرى مع بعضها البعض، وإعادة الإجراءات والعمليات الداخلية بما يكفل توفير الظروف الملائمة لتطبيق إدارة إلكترونية تتميز بالكفاءة والفاعلية وسرعة الإنجاز، وعليه تجدر الإشارة إلى أن هذا التحول أو التغير يجب أن يكون تدريجا وعبر مراحل متعددة .من خلال ما سبق يمكن القول أن التحول إلى الإدارة الإلكترونية يتطلب إحداث جملة من التغيرات على مستوى الإدارة باعتبارها المحرك الأساسي لعمل المنظمة، وعليه فالهياكل التنظيمية والوظائف الإدارية وحتى القوانين والتشريعات مرتبطة ارتباط وثيقا لتغيرات التي تحدث في البيئة الخارجية، لما لهذه الأخيرة من تأثير على المنظمة ككل، بما في ذلك الجانب الإداري الأمر الذي يتطلب الإعداد لهذا التغيير من قبل القيادة الإدارية التي يجب أن تتعامل بكفاءة وفعالية مع تكنولوجيا المعلومات والسعي دوما إلى التشجيع على التعلم لأن الإدارة الإلكترونية تستلزم تطويرا واضحا ومعرفة متجددة، إضافة إلى غرس الوعي بضرورة التكيف مع هذه المستجدات[35].

ثامنا : توفير أمن المعلومات

بالرغم من التقدم التكنولوجي والمعرفي الذي تم التوصل إليه إلا أن التحدي الكبير يكمن في المحافظة على سرية المعلومات وتخزينها إلكترونيا وإتاحتها للجميع بشكل متساوي ومن بين الإجراءات التي تستلزمها التحول الرقمي لتحقيق هذا المطلب ما يلي[36]:

- وضع السياسات الأمنية لتقنيات المعلومات بما فيها خدمة الإنترنت– .
- وضع القوانين واللوائح التنظيمية والعقوبات الأمنية التي تحد من السطو الإلكتروني وانتهاكات خصوصية المعلومات في الإدارة الإلكترونية
- تطوير أدوات تشفير البرمجيات الحديثة للمحافظة على الخصوصية، وخاصة في البرمجيات المتعلقة بخدمات الإنترنت لتمكين المستخدم من المحافظة على سرية شخصيته وتعاملاته عبر الشبكة
- وضع سياسة حماية عامة لأمن نظم المعلومات المحاسبية، تحدد حسب طبيعة عمل وتطبيقات المنشاة
- يجب على الإدارة العليا في المنشأة دعم أمن المعلومات لديها.
- يجب أن توكل مسؤولية أمن المعلومات في المؤسسة لأشخاص محددين

- تحديد الحماية اللازمة لنظم التشغيل والشبكات الحاسوبية.
- الاحتفاظ بنسخ احتياطية لنظم المعلومات بشكل آمن
- تشفير المعلومات التي يتم حفظها وتخزينها ونقلها على مختلف الوسائط.

خاتمة :

في الختام، نقول أن التحول الرقمي في عصرنا الحالي لابد منه، وأن ضرورة التوجه نحو تطوير الياته ومناهجه وتحسينها أمر ضروري جدا في جميع الأوقات العادية من أجل تحقيق مجتمع المعرفة

ولقد تبين لنا من خلال هذه المداخلة أن التحوّل الرقميّ عبارة عن عمليةِ إعادة تنظيمٍ في العمق لسير عمل الوظائف القائمة، مع تعميم استخدام الأدوات الرّقمية لتنفيذها، وهو ما يؤدّي إلى تحسين كبير بأضعاف مضاعفة لخصائصها (تقليص وقت التنفيذ، اختفاء مجموعات كاملة من العمليات الفرعية، تقليل الموارد المستهلكة من أجل تنفيذ العمليات) وظهور صفات وخصائص جديدة جوهرياً. وعلاوة على ذلك؛ فإنّ التحوّل الرقميّ يشكّل قاعدة الانتقال إلى الاقتصاد الرقميّ وتكوين مجتمع المعلومات وانتاج المزيد من المعرفة التي تساهم في تطوير المجتمعات وتحقيق التنمية

وحسب دراسة وردت في صحيفة الشعب الالكترونية بتاريخ 10 مارس 2022 لمؤلفها كما بداري يقول فيها أن : الجزائر تمتلك مظاهر للتحول الرقمي، فقد اتّخذت بعض القطاعات إجراءات رقمية لتحسين جودة حياة المواطنين خاصَّةً من خلال تطوير تكنولوجيات الإعلام والاتّصال واستخدامها. وفي الوقت الرّاهن، يتمّ إيصال الإنترنت إلى أقصى حدود مناطق الجمهورية كما تمّ تأسيس خطوط اتّصالٍ بالألياف البصرية يتجاوز طولُها 160000 كيلومتر، ويملك المواطن بطاقة هوية ورخصة قيادة بيومترية، وكذلك جواز السّفر، ناهيك عن خدمات البطاقة الذهبية النقدية، ورقمنة بعض الخدمات العامة (الحالة المدنية، وصحيفة السوابق العدلية، وبطاقة الشفاء...) وقد كشف مخطّط عمل الحكومة المصادق عليه في الاجتماع الاستثنائي لمجلس الوزراء في 30 أوت 2021 في الملحق المخصّص للبيانات والمؤشرات، أنّه في نهاية الربع الأول من عام 2021 بلغ معدّل وصول الإنترنت عن طريق الاتصالات الثابتة في الجزائر 39%، ومعدل الاتّصال بالإنترنت عن طريق

الاتّصالات المتنقّلة ما يغطّي نسبة 90% من السكان، أمّا عدد مستخدمي الهاتف المحمول، فقد بلغ 46 046 797 مليون شخص، أي ما يُعادل نسبة 105% من مجموع السكان. ودون أن نتطرّق إلى جميع المبادرات، فقد تمّ تقديم مشروعٍ لمبادرة التحوّل الرقمي إلى مجلس الوزراء في 22 مارس 2020، يشمل رقمنة الإدارة المركزية، والوثائق والاستمارات الإدارية، وتعميم قواعد البيانات على أساس رقم التعريف الوطني، وجمع البيانات الاقتصادية، وإنشاء سجل لمراقبة المشاريع الحكومية وصنع القرار، وإنشاء منصة خدمات رقمية للشعب ..ومع ذلك نلمح من خلال السنوات العشر الأخيرة أن المهمّة غير مكتملة أمام التوجّهات العالمية للتحوّل الرقمي ذلك أن التحول الرقمي يتطلب عدة متطلبات متضافرة ومجتمعة نوجزها في شكل اقتراحات على النحو التالي:

- وضع استراتيجية رقمية للدولة، ووضع استراتيجيات رقمية خاصة بكل مؤسسة
- توفير الظروف الضرورية والكافية ذات الطابع المؤسّساتي والبنى التحتية والسيادة الرقمية الوطنية،
- التفاعل الفعال بين المؤسّسات والأوساط العلمية والتعليمية وبين الدولة والمواطنين،
- إعادة النظر في تنظيم العمل. ومن ناحية أخرى، فإنّ التأخير في عملية التحوّل الرقمي في فترة معّينة، يمكن أن يصبح تاريخيا لا رجعة فيه ولا يُمكن تعويضه.
- الاستعانة بالتجارب الرائدة في تطوير التحول الرقمي كالتجارب الأوروبية والاسيوية أوالتجارب العربية كتجربة دولة الإمارات
- نشر ثقافة تقبل التحول الرقمي ورفع من سياسات الترويج لاستخدام الخدمات الالكترونية والتشجيع على توظيف التكنولوجيا بأوساط المجتمع للحصول على هذه الخدمات.
- وضع خطة من أجل محو الأمية الرقمية وذلك لا يتأتى إلا بمعرفة كيفية استعمال الأدوات والخدمات الرقمية المتاحة والمعاملات وحدود استخدامه لها ما سيكسبه مهارة في الاستعمال.

الهوامش وقائمة المراجع

[1]- عادل عزالي " مجنمع المعرفة " مطبوعة بيداغوجية موجهة لطلبة السنة أولى ماستر علم اجتماع التنظيم والعمل ، 2017-2018 ،ص 1

[2]– مصطفى أحمد أمين " التحول الرقمي في الجامعات المصرية كمتطلب لتحقيق مجتمع المعرفة " مجلة الادارة التربوية ، العدد التاسع ، 2019 . ص 11

[3]– عبد الوهاب جودة الحايس ، عبيدة أحمد صبطي " مجتمع المعرفة الرقمي ودوره في اتنمية الابداع العلمي ، رؤية حديثة للتعلم والبحوث "المجلة العربية للاداب والعلوم الانسانية عدد 2 يناير 2019 ، ص 3

[4]– كيف نبني مجتمع المعرفة العربي حديث ' نحو مجتمع المعرفة من سلسلة اصدارات يصدرها مجلس البحث العلمي " جامعة الملك عبد العزيز ، متوفر على الموقع التالي: https://www.kau.edu.sa/Files/862/Files/147636 ص 5

[5]– الرقمنة وحماية التراث الرقمي مركز هردو لدعم التعبير الرقمي، القاهرة، 2016. ص6 على الموقع الالكتروني التالي:www.herdoegypt.org.

[6]–

[7]– مصطفى أحمد أمين " التحول الرقمي في الجامعة المصرية كمتطلب لتحقيق مجتمع المعرفة " مجلة الإدارة التربوية ، عدد 19، سبتمبر 2018 ، ص 43

[8]– فاطمة الزهراء فرحات " دور التحول الرقمي في تحسين اداء وظائف العلاقات العامة في المؤسسة العمومية الجزائرية " مذكرة ماستر في علوم الاعلام والاتصال ، جامعة العربي بن مهيدي أم البواقي 2019-2020 ، ص 65

[9]– سناء محمد عبد الغني "انعكاسات التحول الرقمي على النمو الاقتصادي في مصر " مجلة كلية السياسة والاقتصاد ، المجلد 15 ، عدد 14 أفريل 2022 ، ص 56 متوفر على الموقع الالكتروني التالي : https://jocu.journals.ekb.eg/article_229977

[10]– فاطمة الزهراء فرحات المرجع السابق /ص 66

[11]– إسراء عبد القادر " تعريف مجتمع المعرفة " على الموقع الالكتروني التالي : https://mawdoo3.com اخر تحديث 31 ماي 2017 على الساعة 7:37 أطلع عليه في 2022/08/05 على الساعة 20:06

[12]– المنصف الوناس ، " مجتمع المعرفة و الاعلام " القاهرة ، 2020 ،ص17

[13]– نهلة عبدالقادر إبراهيم قيطة (2011م)، دور الجامعات الفلسطينية في بناء مجتمع المعرفة و سبل تفعيله، غزّة: الجامعة الإسلاميّة، صفحة 28، 22-21

[14]– ابراهيم العبيدي " مفهوم مجتمع المعرفة ' على الموقع الالكتروني التالي : https://mawdoo3.com اخر تجديث 11 جانفي 2022 على الساعة 6:57 ، اطلع عليهفي 2022/08/05 على الساعة 19:37

[15]– علي عوض حاج، منظومة مجنمع المعرفة ودورها في دعم الدخل القومي وتحقيق الأمن الشامل، مجلة أفكار جديدة، 13 ديسمبر 2015 ص25

[16]–المرجع نفسه

[17]– مصطفى أحمد أمين " التحول الرقمي في الجامعة المصرية كمتطلب لتحقيق مجتمع المعرفة " مجلة الإدارة التربوية ، عدد 19، سبتمبر 2018 ، ص34

[18]– عادل عزالي ، المرجع السابق ، ص 14-15

[19]– مصطفى أحمد أمين المرجع السابق ص 32 .

[20]– عادل عزالي المرجع السابق ، ص 15

[21]– محمد مروان " ماهو مجتمع المعرفة " على الموقع الالكتروني التالي : https://mawdoo3.com/ اخر تحديث 10 أكتوبر 2021 على الساعة 13:05 اطلع عليه في 2022/08/05 على الساعة 19:58

[22]– محمد مروان المرجع نفسه .

[23]– مصطفى أحمد أمين المرجع السابق ، ص 36

[24]– فتحي زرنيز " الجزائر في مجتمع المعرفة الواقع وسبل الاندماج " مجلة افاق العلوم المجلد 5 عدد 3 2020 ، ص 195.

[25]– – ياسر خضر البياتي/ الاتصال الرقمي: أمم صاعدة وأمم مندهشة، ط1، عمان: دار البداية، 2014، ص ص 352-351

[26]– فلة بن غريبة " محاضرات في اتصال تنظيمي " موجهة لطلبة سنة اولى ماستر ، ص 4

[27]– أنظر : شريفة سوماتي " الادارة الالكترونية في ظل الكوارث والأزمات " أزمة كوفيد 19 نموذجا " مداخلة ألقيت بمناسبة الملتقى الدولي حول تسيير الموارد البشرية في الادارات والمؤسسات العمومية الواقع الرهانات الافاق في تاريخ 27 جوان 2022 بكلية الحقوق جامعة محند أولحاج اكلي ص 2

[28]– – عيسات عيني " التوجه نحو الادارة الالكترونية في الجزائر من خلال مشروع الجزائر الالكترونية 2013 " المجلة الجزائرية للدراسات السياسية / الجزء 4 ، العدد 2 ، ص 26

[29]– عيسات عيني، المرجع نفسه.

[30]– انظر : مصطفى أحمد أمين المرجع السابق ، ص96

[31]– شريفة سوماتي المرجع السابق ص 3

[32]– هبة ابراهيم الشحات بنوان " المتطلبات التعليمية للتحول الرقمي بتامجتمع المصري " التعليم الأساسي نموذجا " مجلة البحث العلمي في التربية مجلد 23 ، عدد 3 ، 2022 ، ص 23

[33]– فاطمة الزهراء فرحات المرجع السابق ، ص 74/ 75

[34]– هبة ابراهيم الشحات بنوان، المرجع السابق ، ص 24

[35]– وعيبة حارش ، سمير يوسف خوجة " متطلبات تطبيق الادارة الالكترونية ومعوقاتها في الادارة الجزائرية " مجلة رؤى للدراسات المعرفية والحضارية ، مجلد 7 عدد 2 ديسمبر 2021 ، ص 172

[36]– المرجع نفسه ، ص 176

استمارة المشاركة

الاسم واللقب: سعيدة رحامنية.

الوظيفة: أستاذة جامعية

الدرجة العلمية: أستاذ محاضر –ب–

مؤسسة الانتماء: جامعة الشهيد عباس لغرور خنشلة.

البريد الالكتروني: 3aida25@gmail.com

رقم الهاتف: 06 97 63 16 65

المحور الأول: التطور التكنولوجي والظاهرة الاجرامية

2–العلاقة بين الظاهرة الاجرامية والتطور التكنولوجي

عنوان المداخلة: تأثير التطور التكنولوجي على زيادة الجريمة

ملخص:

شهد العالم ثورة تكنولوجية هائلة غيرت من وجه العالم، هذا الغزو التكنولوجي الذي مس كل القطاعات والمجالات السياسية والاقتصادية والاجتماعية والثقافية والدينية...الخ.

وأصبح العالم قرية صغيرة على حد تعبير "ماك لوهان"، فالفرد اليوم يعيش ويسمع ويرى كل أحداث العالم في نفس اللحظة والساعة والدقيقة عبر العالم الافتراضي الرقمي أو عبر مواقع التواصل الاجتماعي والقنوات الفضائية الرقمية وغيرها من الوسائط التكنولوجية الحديثة.

غير أن مواقع التواصل الاجتماعي تعتبر أكثر الوسائل الإعلامية تفاعلا، وتتميز بغزارة المعلومات، وكما هو معروف فان أي وسيلة تكنولوجية متطورة هي سلاح ذو حدين يوجد فيها السلبي والايجابي، فمواقع التواصل الاجتماعي مثلما سهلت وبسطت طرق التواصل بين الأفراد، فإنها كذلك صعبت من معاقبة الأفراد المتعمدين استغلال هذه التكنولوجيا في الحاق الضرر بالأفراد والجماعات، حيث أنهم يستعملون الأسماء المستعارة والتحيل على الأخرين بسبب التواصل عن بعد الذي سهل عملية الجرائم بكل أنواعها.

لقد تزامن التطور التكنولوجي مع ظهور الفعل الاجرامي أو الظاهرة الاجرامية، حيث ارتبط الفعل الاجرامي بهذه الثورة التكنولوجية.

وأفرز التطور التكنولوجي الهائل في مجتمعات العالم ككل أفعال إجرامية متنوعة ومختلفة، حيث تنوع الاجرام وأصبح اجرام علمي أو كما يعرف حاليا بالجريمة الالكترونية.

فالجريمة ليست ظاهرة جديدة لكن الاجرام في حد ذاته تغيرت أركانه وطريقته وأصبح هناك جرائم كلاسيكية أو جرائم قديمة ان صح التعبير، وجرائم حديثة أو الكترونية تعتمد على التكنولوجيا الحديثة، بمعنى أن ظاهرة الاجرام تواكب التطور التكنولوجي الحديث.

تعمل كل دول العالم اليوم من أجل القضاء على الجرائم الالكترونية التي انتشرت انتشارا كبيرا، وأصبحت من أهم عيوب التكنولوجيا الحديثة، وتعمل على تهديد استقرار الشعوب والدول والأفراد.

وبات لزاما على المشرع القانوني وضع قوانين صارمة وفعالة للحد من الجريمة الالكترونية. وعلى الدولة كذلك تشكيل أجهزة أمنية متمكنة من التكنولوجيا تعمل على محاربة القائمين بهذه الجرائم الالكترونية.

الكلمات المفتاحية: التكنولوجيا–الجريمة –الجريمة الالكترونية.

Summary :

The world witnessed a huge technological revolution that changed the face of the world, this technological invasion that touched all sectors and fields, political, economic, social, cultural, religious...etc.

The world has become a small village in the words of "Mc Lohan". Today, the individual lives, hears and sees all the events of the world at the same moment, hour and minute through the digital virtual world or through social networking sites, digital satellite channels and other modern technological means.

However, social networking sites are considered the most interactive media, and are characterized by the abundance of information, and as it is known, any advanced technological means is a double-edged sword in which there is both negative and positive. Exploiting this technology to harm individuals and groups, as they use pseudonyms and deceive others due to remote communication that facilitated the process of crimes of all kinds.

The technological development coincided with the emergence of the criminal act or the criminal phenomenon, as the criminal act was linked to this technological revolution.

The tremendous technological development in the societies of the world as a whole has resulted in various and different criminal acts, where the diversity of crimes has become a scientific crime, or as it is currently known as electronic crime.

Crime is not a new phenomenon, but crime in itself has changed its elements and method, and there are classic crimes or old crimes, so to speak, and modern or electronic crimes that depend on modern technology, meaning that the phenomenon of crime keeps pace with modern technological development.

All countries of the world are working today to eliminate cybercrime, which has spread widely, has become one of the most important defects of modern technology, and is threatening the stability of peoples, countries and individuals.

And it became imperative for the legal legislator to put in place strict and effective laws to curb cybercrime. The state should also form technology-enabled security services to combat those responsible for these cyber crimes.

Keywords : technology - crime - electronic crime.

مقدمة:

ان التطور التكنولوجي الهائل الذي مس كل القطاعات والمجالات والأنشطة غير من خريطة العالم، فأصبح العالم كقرية صغيرة وهذا بفضل سهولة التواصل والاتصال بين مختلف القارات ودول العالم.

والفضل يعود للتطور التكنولوجي الهائل في مجال الاتصالات السلكية واللاسلكية، الذي سهل عملية الاتصال بين الناس في العالم ككل.

فالحاسوب أو الكومبيوتر المزود بشبكة الأنترنت أصبح أكثر وسيلة تستخدم في كل القطاعات والمجالات مما سهل عملية تدفق المعلومات وتبادلها بكل سهولة وسرعة وفعالية.

ان العالم اليوم يعيش ثورة تكنولوجية هائلة بأتم معنى الكلمة، سهلت من ظروف العيش والحياة في العالم، وقضت هذه التكنولوجيا على مختلف العراقيل والمشكلات الاتصالية. لكن كما هو معروف أن لكل شيء في الوجود له ايجابيات مثلما له سلبيات، فمن بين أهم سلبيات التكنولوجيا الحديثة هو استعمال هذه التكنولوجيا من طرف بعض الأفراد فيما يضر العباد والبلاد ويلحق بهم أضرار مادية ومعنوية تأثر على حياتهم واستقرارهم.

هذه الأفعال والتصرفات السلبية الناجمة عن التوظيف الخاطئ للتكنولوجيا الحديثة تعرف بالجرائم الالكترونية التي باتت حديث العام والخاص نظرا لأثارها النفسية والاجتماعية على الأفراد والمجتمعات.

يعتمد الفعل الاجرامي على الوسائل التكنولوجية الحديثة لتنفيذ الجرائم نظرا لسرعة الوسائل التكنولوجية في إيصال المعلومة وتسهيل التواصل بين الأشخاص، ونظرا لسرعة القيام بالفعل الاجرامي أصبحت الجرائم منظمة تحت ستار الوسائط التكنولوجية المختلفة مثل الفاسبوك والفايبر والتوتير والماسنجر وغيرها.

لمناقشة هذا الموضوع تم تناول عدة نقاط جوهرية في هذه الورقة البحثية يمكن عرضها كما يلي:

-تحديد المفاهيم.

-الموقف القانوني من الجريمة الالكترونية.

-تأثير التطور التكنولوجي على الانسان.

-العلاقة بين التطور التكنولوجي والجريمة الالكترونية.

خاتمة

1-تحديد المفاهيم:

سوف نتطرق في تحديد المفاهيم الى ثلاثة مصطلحات هامة تعتبر الكلمات المفتاحية لهذا البحث تتمثل في التكنولوجيا – الجريمة-الجريمة الالكترونية.

*تعريف التكنولوجيا:

تعددت تعاريف التكنولوجيا حيث نجد كم هائل من التعاريف لمصطلح التكنولوجيا يمكن رصد بعضها في مايلي:

أ-تعريف روث Root الذي يشير الى أنها: 'مجموع المعارف التي يمكن أن تساعد في انتاج المنافع، وخلق منافع جديدة'.[1]

يتضح من خلال التعريف السابق أن التكنولوجيا تعني في مضمونها التقدم والرقي والازدهار والابتكار وخلق أفاق جديدة، وحديثة ومتطورة تختلف عن ما هو تقليدي تماما.

[1]فضيلة سيساوي: **التكنولوجيا في البلدان النامية بين النقل والتحكم**، المجلة الجزائرية للدراسات السوسيولوجية، العدد 2و3، جامعة جيجل، جوان 2007، ص167.

ب–التكنولوجيا هي كلمة أعجمية ذات أصل يوناني، تتكون من مقطعين، كلمة تكنو والتي تعني حرفة أو مهارة أو فن، وكلمة لوجي التي تعني علم أو دراسة، ليصاغ الكل في كلمة تكنولوجيا بمعنى علم التطبيق.[1]

كما تعرف التكنولوجيا بأنها: 'مجموع التقنيات والمهارات والأساليب التقنية والعمليات المستخدمة في انتاج البضائع أو الخدمات أو في تحقيق الأهداف مثل البحث العلمي.'[2]

يتضح من خلال التعريف أن التكنولوجيا نستخدمها للدلالة على مفهومان، تعني التكنولوجيا كل ما هو آلات وأجهزة ومعدات وسلع، كما أنها نستخدمها كذلك للدلالة على كل ما هو مرتبط بالبحث العلمي والاكتشافات العلمية والمعرفة.

***تعريف الجريمة:**

تعددت تعاريف الجريمة واختلفت حسب تعدد وجهات نظر البحثين والدارسين، ومن الصعوبة إيجاد تعريف لمصطلح الجريمة، لكن على العموم يمكن تعريف مصطلح الجريمة من منظور قانوني واجتماعي من أجل الخروج بتعريف عام يتماشى مع أهداف الملتقى وأهداف هذه الورقة البحثية.

الجريمة في أساسها مفهوم قانوني يقصد به ذلك " الفعل أو الامتناع الذي نص القانون على تجريمه ووضع عقوبة جزاء على فعله".[3]

---

[1] ويكيبيديا : **تكنولوجيا**، Ar.m.wikipedia.org ، 2022/08/14، على الساعة 16:42.

[2] نفس المرجع.

[3] علي لوعناقة: **الشباب ومشكلاته الاجتماعية في المدن الحضرية**، ط1، مركز دراسات الوحدة العربية، بيروت، لبنان، 2007، ص37.

يتضح من خلال التعريف أن الجريمة في الأساس هي فعل يعاقب عليه القانون وذلك حسب نوع الجريمة، حيث وضعت قوانين ومواد حسب حجم الفعل الاجرامي، وخصصت محاكم لمحاكمة المجرمين.

وتصنف الجريمة الى ثلاث أقسام هي: الجنايات، الجنح، والمخالفات، تبعا لذلك قسم المشرع المصري والفرنسي الجريمة على النحو السابق بيانه، وعرفا الجريمة تعريفا قانونيا بأنها فعل أو الامتناع عن القيام بفعل يقرر له القانون عقابا.[1]

فالجريمة إذا تنطوي على الفعل وانعدام الفعل الذي يقرر له القانون عقابا، ويتحمل الشخص مسؤولية أفعاله لأهليته "توافر شروط السن، والعقل، وحرية الاختيار."[2]

أما المشرع الجزائري اعتبر الصبي الذي لم يبلغ سن الثالثة عشرة غير مسؤول قضائيا عن أفعاله لعدم أهليته وهنا " تنص المادة رقم 49 من القانون الجزائري" على أن الصبي الذي لم يبلغ سن الثالثة عشرة غير مؤهل للمسؤولية الجنائية ويعامل معاملة القاصر الذي يتخذ ضده تدابير إصلاحية وتربوية.[3]

"ورد في المادة رقم 444 من قانون الإجراءات الجنائية الجزائري، نص يجيز للقضاء الجزائري تحديد السن ما بين 13-18 سنة التي ينطوي تحتها القاصر ليودع مراكز الحماية والتأديب وهو ما سمي بالجزاء الوقائي أو الاجتماعي. "[4]

يتضح من خلال مفهوم الجريمة من الناحية القانونية أن المشرع وضع عقوبات محددة لكل جريمة، كما وضع شروط لكي يعاقب الشخص القائم بالجريمة حسب السن والعقل وحرية الاختيار وهي شروط تكاد تكون متشابهة في أغلب دول العالم سواء الدول العربية المسلمة أو الدول الغربية.

---

[1] نفس المرجع: ص39.

[2] نفس المرجع: ص39.

[3] نفس المرجع: ص39-ص40.

[4] نفس المرجع: ص40.

أما تعريف الجريمة من منظور اجتماعي، أو حسب علماء الاجتماع فيمكن رصد بعض التعريفات في مايلي:

–الجريمة هي:" أي سلوك ضار بالمجتمع وبرفاهية أعضائه، وهذا التعريف يجعل من الجريمة شيئا ثابتا ودائما بحسب هذا الرأي."[1]

– أما ميرتون ونسبت Merton and Nisbet "فقد ربطا الضرر بالفاعل، أي أن الاجرام ناجم عن الجماعة صاحبة الموقف، فالأفعال ضارة بفئة وليس بالمجتمع، لأنه كما يتصور أن الجريمة مظهر من مظاهر انهيار الجماعة لأن وشائل الضبط الاجتماعي والعدالة، لا تؤدي دورها الا بطريقة شكلية، فتحدث فجوة بين الجماعات".[2]

يتضح من خلال التعريف السابق أن الفعل الاجرامي ليس مسؤولية القائم بالجريمة فحسب، بل أن الفعل الاجرامي هو مسؤولية المجتمع أو الجماعة ومسؤولية العدالة، لأنها لم تؤدي دورها كما يجب من خلال تفعيل وسائل الضبط الاجتماعي وتشديد العقوبات.

***تعريف الجريمة الالكترونية:**

تعددت تعاريف الجريمة الالكترونية ولا يوجد تعريف موحد لهذا المفهوم لكن على العموم يمكن تعريفه من الناحية القانونية كما يلي:

–تعريفات القانون الجنائي: فقد عرفتها الدكتورة هدى قشقوش بأنها: " كل سلوك غير مشروع أو غير مسموح بهن فيما يتعلق بالمعالجة الألية للبيانات أو نقل البيانات".[3]

---

[1] نفس المرجع: ص38.

[2] نفس المرجع: ص38.

[3] مونة مقلاتي وراضية مشري: **الجريمة الالكترونية: دلالة المفهوم وفعالية المعالجة القانونية**، مجلة أبحاث قانونية وسياسية، المجلد 6 العدد 1، كلية الحقوق والعلوم السياسية، جامعة جيجل، جوان 2021، ص493.

كما عرفتها منظمة التعاون الاقتصادي والتنمية بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".[1]

يتضح حسب هذا التعريف أن الجريمة هي جريمة مهما تعددت طرقها سواء كانت بطريقة مباشرة أو غير مباشرة وذلك باستخدام الوسائل التكنولوجية فان القانون يتصدى لها بالمرصاد، ووضع لها عقوبات مثلها مثل الجريمة العادية.

ان تعريف الجريمة الالكترونية على العموم يقوم على ثلاث عناصر، السلوك ووصفه والنص القانوني على تحريم السلوك وايقاع العقوبة، ثم محل الاعتداء في الظاهرة الاجرامية المستحدثة متمثلا في معطيات الحاسوب، خلافا للجريمة عموما، إذا هي سلوك غير مشروع معاقب عليه قانونا.[2]

يتشابه هذا التعريف مع التعريف السابق الخاص بمنظمة التعاون الاقتصادي، حيث أن الجريمة سواء كانت بطريقة عادية أو عن طريق استخدام الوسائل التكنولوجية فهي فعل اجرامي وسلوك منبوذ اجتماعيا وقانونيا، ووضع المشرع عقوبات لكل فعل اجرامي مهما كان بسيطا.

2-تأثير التطور التكنولوجي على الانسان:

منذ أن وجد الانسان فوق الأرض وهو يحاول تطوير نفسه وتطوير الوسائل التي يستخدمها في حياته اليومية، فاكتشف كيف يشعل النار، وكيف يصطاد الحيوان لاستغلاله في طعامه، وكيف يطهو الطعام، وكيف يصنع أسلحة للدفاع عن نفسه من الحيوانات المتوحشة والمفترسة أو من أي معتدي أخر من البشر.

فمن أجل البقاء وتحسين ظروف العيش قام الانسان منذ القديم بتطوير نفسه في كل نواحي الحياة، الاجتماعية أو الاقتصادية أو الثقافية ...الخ، حتى وصل الى ماهو عليه اليوم من تطور وازدهار وأصبح يعيش ما يعرف

---

[1] نفس المرجع: ص494.
[2] نفس المرجع: ص494.

بالثورة التكنولوجية التي غيرت خريطة العالم بأكمله، وبات كل فرد يسمع ويرى ويعايش كل ما يجري في العالم وهو جالس في بيته، عبر العالم الافتراضي مستخدما الوسائط التكنولوجية فائقة التطور مثل: القنوات الفضائية الرقمية والهواتف المحمولة الذكية والحواسيب الالكترونية مزودة بشبكة الأنترنيت تتضمن مواقع مثل الفاسبوك و الفايبر والتوتير و الواتساب وغيرها من التطورات المذهلة.

ان العالم اليوم يعيش التطور التكنولوجي الهائل الذي يوفر للفرد كم هائل من المعلومات سريعة التدفق.

ان التكنولوجيا الحديثة أثرت على كل مجالات الحياة، السياسية والثقافية والاجتماعية والاقتصادية والتربوية وغيرها من مجالات الحياة المختلفة، فالتكنولوجيا الحديثة أحدثت تغيرات كبيرة في مجال التعليم، فانتشرت في العالم اليوم الجامعات الافتراضية والتعليم الافتراضي وإقامة ملتقيات وندوات عن بعد وانتشار مكتبات رقمية كله بفضل التكنولوجيا الحديثة.

ان التكنولوجيا الحديثة أحدثت تغييرات كبيرة في مجال الاقتصاد والصناعة والتجارة فأصبحت عمليات البيع والشراء والتصدير والاستيراد تنجز بفضل التكنولوجيا الحديثة.

غيرت التكنولوجيا كذلك في الوسط الثقافي، فأصبح الفرد الأن بإمكانه التعرف على ثقافات كل شعوب العالم في ظرف وجيز، باستخدام التكنولوجيا الحديثة. وبإمكانه السفر الى أي مكان في العالم، فالأنترنت قامت بتقريب المسافات والقضاء على التباعد الفيزيقي، فأصبح العالم اليوم يعيش ثقافة العولمة أو العالم الموحد ثقافيا واجتماعيا وسياسيا واقتصاديا.

في خضم هذا الغزو المعلوماتي الهائل، والتدفق السريع للمعرفة والمعلومات نشهد سلوكات وأفعال سلبية ترفضها كل الديانات والقوانين والأعراف، ألا وهي الاجرام العلمي أو كما تعرف بالمصطلح الأكثر تداولا وهو الجريمة الالكترونية.

حيث شهدت هذه الظاهرة انتشارا واسعا بين البشر في كل دول العالم، حيث انتشرت ظاهرة الانتحار وسط الأطفال والمراهقين بسبب بعض الألعاب الالكترونية ومشاهد العنف والاجرام مثل لعبة الحوت الأزرق التي سجلت عديد حالات الانتحار عند الأطفال والأحداث خلال السنوات الماضية وفي العديد من دول العالم والجزائر واحدة من الدول التي سجل بها حالات انتحار للأطفال والقصر بسبب هذه اللعبة الالكترونية.

كذلك انتشار جرائم التشهير والابتزاز والقذف عن طريق مواقع التواصل الاجتماعي، جرائم بيع وترويج المخدرات والمهلوسات والمؤثرات العقلية باستعمال التكنولوجيا الحديثة وغيرها من الجرائم الالكترونية التي انتشرت في السنوات الأخيرة.

وأصبح لزاما على الدول والحكومات والمشرع القانوني وضع قوانين وإجراءات لضبط وتقليل الاجرام الالكتروني الذي أصبح يهدد استقرار كل الشعوب والدول.

مثل انتشار القرصنة الالكترونية واختراق مواقع أمنية أو عسكرية أو سرية لأي بلد، الاحتيال والسرقة عبر الأنترنيت والتشهير والإساءة على مواقع التواصل الاجتماعي وانتهاك حقوق النشر والملكية وانتهاك سيادة الدول والحكومات عن طريق سرقة المعلومات واستخدامها لإثارة الفوضى أو الحروب أو أعمال إرهابية...الخ.

تكوين كذلك شبكات للإطاحة بالفئات الهشة في المجتمع مثل الأطفال والقصر والفتيات والنساء واستغلالهم جنسيا أو ماديا أو الحاق الضرر بهم لأغراض شخصية أو ذاتية عن طريق الاحتيال عليهم أو اغرائهم أو ابتزازهم أو تهديدهم وغيرها من الأعمال الاجرامية.

ان الجرائم الالكترونية تعتبر من أبرز وأكثر سلبيات التكنولوجية الحديثة، باعتبارها سلوكات مرفوضة دينيا وقانونيا وعرفيا، حيث يقوم بارتكابها فرد أو جماعة باستعمال الوسائل التكنولوجية الحديثة كالكمبيوتر أو الهواتف الذكية المزودة بالأنترنيت.

ان المجرم الالكتروني مجرم غير عادي وغير تقليدي، لأنه شخص متمكن من التكنولوجيا الحديثة، وله خبرة ومهارة في استخدام التكنولوجيا وله مهارة في مجال المعلوماتية، تؤهله للقيام بمهمته الاجرامية بكل دقة واحترافية.

حيث يقوم بكل طرق الابتزاز والاحتيال والتهديد وانتحال صفة الغير وغيرها من الطرق غير الشرعية المنافية للقانون من أجل استغلال الضحية أو الضحايا المستهدفين لتحقيق مكاسب معينة باستعمال الألم الافتراضي الرقمي الذي سهل من عملية ارتكاب الاجرام بشتى أنواعه.

3-العلاقة بين التطور التكنولوجي والجريمة الالكترونية:

تعتبر التكنولوجية الحديثة سمة العصر، حتى أصبح هذا العصر يعرف بعصر العولمة أو الرقمنة.

ان التكنولوجية الحديثة بكل وسائلها فائقة التطور مثل الحواسيب المحمولة والهواتف الذكية قد غزت كل دول العالم وكل البيوت، فأصبح كل فرد في المجتمع يمتلك وسيلة على الأقل من الوسائل التكنولوجية، ويعايش كل ما يجري في العالم عن طريق العالم الافتراضي.

رغم ان التكنولوجية الحديثة وفرت الجهد والوقت في انجاز الأعمال والوظائف، وتسهيل وصول المعلومات وتقصير المسافات، لكن الفرد اليوم يعيش تقارب افتراضي وتباعد فيزيقي وروحي وفراغ عاطفي وتشتت واغتراب نتيجة فقدان لكل القيم والمعايير الاجتماعية الأساسية في تكوين شخصية الفرد ووجدانه.

حيث لم تعد هناك الزيارات في الأعياد والمناسبات كما كانت من قبل، بل أصبحت المعايدات تتم عن طريق مواقع التواصل الاجتماعي المتوفرة على الهواتف المحمولة، مثل الفاسبوك والتوتير والفايبر والواتساب وغيرها من الوسائط التكنولوجية الحديثة المختلفة.

ان التكنولوجية الحديثة قضت على كثير من القيم والعادات والتقاليد وخاصة على صلة الرحم.

ان التأثير الإيجابي للتكنولوجية الحديثة على حياة كل شرائح المجتمع باديا للعيان، غير أن البعض لا يعي سلبيات هذه التكنولوجية الحديثة.

خاصة وأن ما أفرزته التكنولوجية الحديثة من مظاهر سلبية وخطيرة في تزايد مستمر، وأكثر ضحاياها هم الأطفال والمراهقين والفتيات وغيرهم من الفئات الهشة في المجتمع.

فأصبحنا اليوم نشاهد حالات انتحار الأطفال والمراهقين بسبب مشاهدتهم لأفلام العنف وبعض الألعاب الالكترونية مثل لعبة الحوت الأزرق التي تسببت في انتحار العديد من الأطفال في بعض دول العالم.

ومن بين كذلك الجرائم المسجلة بسبب الاستعمال الخاطئ للتكنولوجية الحديثة، الابتزاز والتهديد والتشهير عن طريق مواقع التواصل الاجتماعي، كأن يقوم زوج بتهديد وابتزاز زوجته في حالات الخلاف بينهما، أو يقوم شخص بنشر صور طليقته من أجل الضغط عليها من أجل النفقة، كلها سلوكات وجرائم مرفوضة دينيا وقانونيا، خاصة في البلدان العربية المسلمة.

هذه عينة بسيطة من بعض الجرائم الناجمة عن التطور التكنولوجي، للدلالة عن توظيف التكنولوجية بطريقة خاطئة من طرف بعض الأشخاص الذين يعتبرون خارجين عن الدين والقانون، والشاذ يحفظ ولا يقاس عليه.

ان توظيف التكنولوجية الحديثة من طرف بعض الأشخاص فيما يضر الناس أصبحت ظاهرة منتشرة بكثرة في كل المجتمعات، وتعمل كل الحكومات والدول للقضاء عليها بوضع قوانين وإجراءات ردعية وعقابية لهؤلاء المجرمين.

4-الموقف القانوني من الجريمة الالكترونية:

ان الجريمة الالكترونية تهدد اقتصاد الدول واستقرار الأفراد والجماعات، ولهذا فان المشرع القانوني وضع قوانين صارمة للحد من هذه الظاهرة.

تعتبر اتفاقية بودابست (2001) لمكافحة الجريمة الالكترونية الأداة الدولية الوحيدة الى حد الأن الملزمة بشأن الجرائم الالكترونية، كما تعد هذه الاتفاقية المصادق عليها من قبل 48 دولة، بمثابة الخطوط التوجيهية لكل دول العالم.[1]

فالجزائر كواحدة من دول العالم، كانت سباقة مقارنة بباقي الدول العربية، حيث جاء تعديل قانون العقوبات بالأمر رقم 10/97 المؤرخ في 06 مارس 1997، الذي نص على قمع الجرائم الالكترونية في المواد من 394 مكرر الى 394 مكرر 7، تحت عنوان: (المساس بأنظمة المعالجة الألية للمعطيات).[2]

غير أن المشرع الجزائري اعتبر كل الجرائم الالكترونية من فئة الجنح، مهما كانت درجة خطورتها،

كما جرم الشروع (المحاولة) بالنسبة لتلك الجنح.[3]

وهكذا نصت المادة 394 مكرر على أن: يعاقب بالحبس من 3 أشهر الى سنة وبغرامة من 50000 الى 100000 دج كل ما يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الالية للمعطيات أو يحاول ذلك، كما نصت المادة 394 مكرر 2 على أن: يعاقب بالحبس من شهرين الى ثلاث سنوات، وبغرامة من 1000000 الى 5000000 دج كل من يقوم عمدا وعن طريق الغش بما يلي:[4]

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

---

[1] محمود شرقي وصلاح الدين جبار: **تأثير تطور تكنولوجية المعلوماتية على تنامي الجريمة**، مجلة الأداب والعلوم الاجتماعية، المجلد 8، العدد01، جامعة البليدة 02، الجزائر، 2015، ص 11.

[2] نفس المرجع: ص09.

[3] نفس المرجع: ص 09.

[4] نفس المرجع: ص09-ص10.

2-حيازة أو افشاء أو نشر أو استعمال لأي غرض كان من المعطيات المتحصل عليها من احدى الجرائم المنصوص عليها في القسم.

كما نصت المادة 394 مكرر 7، على أن: يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها.[1]

ان الجزائر رغم أنها كانت سباقة بالنسبة للدول العربية في النص على الجريمة الالكترونية ومعاقبة مرتكبيها بالحبس والغرامة، وذلك سنة 1997، الا أنها اليوم في حاجة الى مراجعة تشريعاتها في هذا المجال بما يواكب التطور الملحوظ في الاجرام الالكتروني.[2]

ان العالم اليوم بصفة عامة، والجرائر بصفة خاصة في تحدي كبير لمواجهة خطر وسلبيات الوسائل التكنولوجية الحديثة بسبب التوظيف الخاطئ لهذه الوسائل، وكذلك الأثار النفسية والاجتماعية والاقتصادية والسياسية الناجمة عن الجرائم الالكترونية أصبح لزاما على كل الدول بما فيها الجزائر وضع إجراءات عقابية جديدة تتماشى مع التطور التكنولوجي أو بالأحرى تتماشى مع تطور الاجرام العلمي.

---

[1] نفس المرجع: ص 10.
[2] نفس المرجع: ص 10.

خاتمة:

أفرز التطور التكنولوجي الهائل في مجتمعات العالم ككل أفعال إجرامية متنوعة ومختلفة، حيث تنوع الاجرام وأصبح اجرام علمي أو كما يعرف حاليا بالجريمة الالكترونية.

فالجريمة ليست ظاهرة جديدة لكن الاجرام في حد ذاته تغيرت أركانه وطريقته وأصبح هناك جرائم كلاسيكية أو جرائم قديمة ان صح التعبير، وجرائم حديثة أو الكترونية تعتمد على التكنولوجيا الحديثة، بمعنى أن ظاهرة الاجرام تواكب التطور التكنولوجي الحديث.

يعتمد الفعل الاجرامي على التكنولوجية الحديثة لتنفيذ الجرائم نظرا لسرعة الوسائل التكنولوجية في إيصال المعلومة وتسهيل التواصل بين الأشخاص، ونظرا لسرعة القيام بالفعل الاجرامي أصبحت الجرائم منظمة تحت ستار الوسائط التكنولوجية المختلفة مثل الفاسبوك والفايبر والتوتير والماسنجر وغيرها.

تعمل كل دول العالم اليوم من أجل القضاء على الجرائم الالكترونية التي انتشرت انتشارا كبيرا، وأصبحت من أهم عيوب التكنولوجيا الحديثة، وتعمل على تهديد استقرار الشعوب والدول.

وبات لزاما على المشرع القانوني وضع قوانين صارمة وفعالة للحد من الجريمة الالكترونية. وعلى الدول كذلك تشكيل أجهزة أمنية متمكنة تعتمد على التقنيات الحديثة من أجل محاربة القائمين بهذه الجرائم الالكترونية ووضع حد لهم.

قائمة المراجع:

1-فضيلة سيساوي: **التكنولوجيا في البلدان النامية بين النقل والتحكم**، المجلة الجزائرية للدراسات السوسيولوجية، العدد 2و3، جامعة جيجل، جوان 2007.

2-ويكيبيديا : **تكنولوجيا**، Ar.m.wikipedia.org، 2022/08/14، على الساعة 16:42.

3-علي لوعناقة: **الشباب ومشكلاته الاجتماعية في المدن الحضرية**، ط1، مركز دراسات الوحدة العربية، بيروت، لبنان، 2007.

4-مونة مقلاتي وراضية مشري: **الجريمة الالكترونية: دلالة المفهوم وفعالية المعالجة القانونية**، مجلة أبحاث قانونية وسياسية، المجلد 6 العدد 1، كلية الحقوق والعلوم السياسية، جامعة جيجل، جوان 2021.

5-محمود شرقي وصلاح الدين جبار: **تأثير تطور تكنولوجية المعلوماتية على تنامي الجريمة**، مجلة الأداب والعلوم الاجتماعية، المجلد 8، العدد01، جامعة البليدة 02، الجزائر، 2015.

جامعة الجزائر 1 بن يوسف بن خدة

كلية الحقوق تنظم

الملتقى الدولي الافتراضي الوسوم ب:

القانون الجنائي في ظل التطور التكنولوجي

-إشكالات ومعالجات-

يومي 28و29 سبتمبر

استمارة المشاركة

الاسم: الدكتورة/ رحماني حسيبة

المؤهل العلمي: أستاذة محاضرة قسم "أ"

الوظيفة:أستاذة

مؤسسة الانتساب: كلية الحقوق والعلوم السياسية – جامعة أكلي محند أولحاج- البويرة

البريد الإلكتروني:rahmanihassibabouira@gmail.com

رقم الهاتف: 07 97 38 31 77

05 264661 31

محور المداخلة/ المحور الأول: التطور التكنولوجي والظاهرة الإجرامية

2/ العلاقة بين الظاهرة الإجرامية والتّطور التّكنولوجي

عنـــــوان المداخلـــــة:مسألة تفوق انتشار الإجرام الخطير عن سُبل الوقاية والمكافحةفيظلالتّطور التكنولوجي

ملخص

لقد انتشر الإجرام بشكل غير محدد، وأصبح المجتمع المعاصر اليوم يواجه ظواهرإجرامية خطيرة التي أفرزها التقدم والتطور الذي شهده العالم في كافة مناحي الحياة، وثورة وسائل الاتصال والمواصلات، والاكتشافات التكنولوجية، وللأسف هذا التطور والاستخدام المفرط للتكنولوجيا ساهم في ونمو سلوكاتمخالفة للقانون وشيوع الفساد،وإنتاج أنواع جديدة من الجريمة حسب رأي المختصين أنها باتت تشكل وضعا خطيرا يفوق حجمها الخطط والأساليب التي رسمت في مجال مكافحتها، بل أنها تفكك بأمن واستقرار الدول، مما يتطلب التركيز على تفعيل الاستراتيجيات وتعزيز آليات ذات طابع ردعي وقمعي لكل صور الاجرام.

الكلمات المفتاحية:التطور العلمي، الإجرام الخطير، الثورة التكنولوجية، استراتيجية مكافحةالإجرام، التغيرات الجيوسياسية، الاتفاقيات الدولية.

Abstract:

Crime has spreadindefinitely, and contemporary society todayisfacingdangerouscriminalphenomenaresultingfrom the progress and developmentthat the world has witnessed in all aspects of life, the revolution of means of communication and transportation, and technologicaldiscoveries. Unfortunately, thisdevelopment and excessive use of technologycontributed to the growth of illegalbehavior and the spread of corruption. The production of new types of crime, according to specialists, has become a dangerous situation thatexceeds the size of the plans and methodsdrawn up in the field of combatingit. Rather, itdisintegrates the security and stability of countries, whichrequiresfocusing on activatingstrategies and strengtheningmechanisms of a deterrent and repressive nature for all forms of crime.

Keywords:scientificdevelopment, serious crime, technologicalrevolution, anti-crime strategy, geopolitical changes, international agreements.

مقدمة:

ثمة علاقة وطيدة تربط ما بين التطور التكنولوجي والجرائم الخطيرة،فهناك العديد من الجرائم وأشكال مختلفة من الانحرافات والنشاطات الإجرامية وظهور العصابات الإجرامية متخصصة في التزوير، البغاء، وأخرى في المخدرات، وأخرى في القتل والاعتداءات، عصابات الأحياء، القرصنة على البرمجيات، الإتجار بالأعضاء والأجزاء البشرية، خطف الأشخاص، وغيرها من الأفعال غير مشروعة داخل منظومة جرائم الفساد ظهرت ليس من قبل الصدفة بل ساعد على ظهورها تنامي العولمة وانتشار التكنولوجيا المتطورة.

بل إن الإجرام الخطير والمعقد وجرائم الفساد بشكل عام أحد سمات التّطور التكنولوجي والتّقدم العلمي، فالعديد من الدول تعاني من ويلات الإجرام المنظم وارتفاع ملحوظ في معدل الجريمة، لدرجة أننا نتوقع حدوث جريمة منظمة عبر وطننا كل يوم أكثر من مرة، كما أصبح هناك تنفيذ لعمليات إجرامية كبيرة في منتهى السرعة وزيادتها المذهلة،إلى جانب احتلالها الأهمية في ظل نمو العولمة والشركات عابرة القارات، وازدياد التقدم العلمي والتكنولوجي وما يحمله في طياته من سرعة وسائل الاتصال والمواصلات(أنترنت– فاكس– تلكس– طائرات– هواتف محمولة– وغيرها)، حتى أضحى هناك ما يسمى بالجرائم الكبيرة. **les) grandes criminalités)**

هذه الجرائم التي تعد ناقوس يدق مُعلنا حرب على البشرية بسبب صعوبة كشفها أو معرفة مرتكبها، والتي تعني جرائم حضارية مرهونة بنظام الدول تندرج تحت طائفة الإجرام الخطير الذي يؤرق دول العالم كافة، ويدخل ضمن هذه الجرائم كل الجرائم التي ترتكب بعد التخطيط لها، والجرائم التي يرتكبها محترفي الإجرام والعصابات وفي مقدمتها انتشرت طائفة جديدة من الجرائم، وهي الجرائم التكنولوجية والقرصنة والاعتداء على الشبكات المعلوماتية بسبب تزايد التّقنيات الحديثة، وكثرة الابتكارات إضافة إلى استمرار عطاء الثورة التكنولوجية وشيوع استخدام وسائل تقنية المعلومات، والذي يعني في مجمل كل هذا ما يمكن أن نسميه النشاط الإجرامي التكنولوجي المتصل بالتقدم التكنولوجي الذي أصبح يشكل تهديدًا بالغًا لسائر الدول والمنظمات والمؤسسات والأشخاص.

إنّهوفي ظّل استمرارية التّطور التكنولوجي، مُلاحظ أن عالمنا المعاصر يعيش أزهى فتراته من خلال ما قدمته الثورة التكنولوجية من خدمات جليلة للإنسانية في كل المجالات انعكست على كافة أوجه النّشاط الإنساني وعلى العلاقات الدولية، وقد أحدثت هذه الثورة طفرة مذهلة في التّعامل مع التكنولوجيا والاستفادة منها، حتى باتت الثورة التكنولوجية بقوتها وقدرتها الفائقة تمثل العصب الرئيسي لكل التّغيرات الممكنة في

مختلف نواحي الحياة الحضارية، بل نشير إلى أنه قد تزايد الاعتماد على هذه الثورة في تسيير شؤون المجتمعات لكن مصحوبا بفرص جديدة لارتكاب أشكال وصور مستحدثة من الجرائم.

ولعلّ أهم ما يلاحظ علىظهور الجرائم المستحدثة أنها جرائم فيها إخلال بالنظام والإضرار المتعمد بالمصالح والأموالخاصةً، أو أنها تشكل أخطر أنواع الفساد الذي يسبب الضّرر للمجتمع في جميع الجوانب الاقتصادية والسياسية والاجتماعية والثقافية، ونظرا للآثار السلبية التي تترتب على سلوكات فاسدة ومتنوعة، على اعتبارها ظواهر إجرامية تتجاوز في تأثيرها العام حدود اللحظة الخاصة التي تمارس فيها، بل تتجاوز آثارها كافة حدود الزمن الماضي والحاضر ويمتد تأثيرها إلى المستقبل، فهي لهم تعد قاصرة على الإجرام المحلي بل امتدت إلى الإجرام المنظم الدولي لدرجة الإضرار وإفساد العلاقة بين الدول ومواطنيها وتفشي تصرفات إجرامية خبيثة.

لهذا تزايدت خطط مكافحة مختلف أشكال الإجرام وأنصبت جهود وطنية ودولية على دراسات معمقة،كذلك تتبع نهج وسياسات واستراتيجيات وخلق آليات قانونية للحماية من أخطار الجرائم، وبروز مُنظمات دولية وإقليمية وتحديات بشأن صك أدوات ناجحة لمكافحة مختلف جرائم الفساد والضرر والخطر في ظل وجود قناعة بعدم قدرة الدول فرادى على مكافحتها، وإدراكًا كذلك لقصور القوانين الجنائية بما تتضمنه من نصوص التّجريم التقليدية، وأنه لابد من وضع قوانين واستحداث تشريعات خاصة، أو العمل على تقدير القوانين الداخلية بما يتماشى ويتلازم مع مواجهة الجرائم بشكل فاعل.

لذا فإنّ إدراك لماهية مختلف الجرائم ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية في ظل التّطور التكنولوجي، يتخذ أهمية استثنائية لسلامة التّعامل مع مختلف المظاهر الإجرامية بكل استراتيجية لمواجهة الخطر الجنائي، وإن كانت بعض الدول سواء الغربية أوالعربية ما زالت تبحث عن السّبل والآليات الإجرامية والتّقنية والتّشريعية، وحتى محاولة وضع استراتيجيات جديدة مناسبة للحد من خطر الإجرام المستحدث المنبعث من مختلف السلوكات المنحرفة، أي الخطر المنبعث من المجرم والذي يطلق عليه بالخطورة الإجرامية.

وتؤكد الدّراسات على أن هناك مساعي كثيرة وخطوات إلى الأمام في سبيل مواجهة سائر أشكال الجريمة، بل يوجد توجُّه نحو اعتماد خطط وآليات مختلفة ومتطورة من أجل الوصول إلى حلول موحدة تحد من انتشار الإجرام وتعمل على استئصاله، لكن قد أظهر الواقع أنه لم تَعد النّصوص العقابية قادرة على مسايرةِ ومواكبةِ جرائم متعددة ذات الخطر والضرر الكبير لعمق هذه الجرائم وانتشارها بشكل ملحوظ،وبسبب ضعف بعض أجهزة الإدارات العامة وعدم مواكبتهم التّطور التكنولوجي الحاصل.

كما أن الفساد والصورةالحديثةللإجرام صارت ثقافة العصر ونظاما للحياة في كثير من الدول، والخطورة تكمن في تناميه مما يجعل صعوبة في السيطرة عليه، لذلك يتطلب الوضع وجود تدخل تشريعي قوي أو خطط تشريعية للقضاء على خطورة بعض الأفعال الإجرامية،مع محاولة إعادة النظر في إيجاد استراتيجية شاملة وواضحة تقيس جودة المواجهة والمكافحة لأخطر الجرائم في ظل إن صح التّعبير مرور العالم بمرحلة انتقالية بين التّعامل الورقي والتّعامل الإلكتروني،وتطور شبكات التّكنولوجيا التي تكسو الكرة الأرضية، وفي ظل التطور التكنولوجي الذي أثّر على المجتمعات وخلق ما يسمى بالخطر المحتمل في كل دول العالم بسبب عمل الأذكياء والمتحايلون على القانون من خلال هذا التّقدم العلمي والتكنولوجي.

وإذا كان هناك دور فعال في بعض تشريعات الدول لتجريم مختلف صور الإجرام، كان من مقتضى الدّراسة أن نتعرض من خلال عنوان ورقتناإلى تحليل هذه الفكرة بتبيان خطورة تنامي الجرائم وانتشارها في ظل التكنولوجيا الحديثة،مع تركيزنا على إظهار الأساليب المستحدثة في بلدان مختلفة بشأن مواجهة مختلف صور الإجرام انطلاقا من النهج التشريعي الجنائي وتطبيقاتهفي إطار حركة التطور التكنولوجي والسريع وتأثيره على الظواهر الإجرامية، وهذا بطرحنا الإشكاليةالتالية:**فيم تتمثل استراتيجية الدول لمواجهة خطر الإجرام واحتمالات الضّرر في ظل التّقدم التكنولوجي، وهل هناك دور فعال يشمل تجريم مختلف صور الإجرام الخطير؟.**

وبغرض الإجابةعلى الإشكاليةسنقسم الدراسة كما يلي:

-انعكاسات التطور التكنولوجي على تطور الإجرام**(أولا)**.

-النهج القانوني والقضائي والأمني المتبع للحد من انتشار الظواهر الإجرامية**(ثانيا)**.

أولا-ملامح التّطور التكنولوجي وانعكاساتهعلى تطور الإجرام:

لقد احتل التطور التكنولوجي بإيجابياته وسلبياته مكانا متقدما في العقود الأخيرة لدى الباحثين والمفكرين، وذلك محاولة لفهم هذا التطور الذي أصبح واقعا يفرض نفسه، ظهر التطور التكنولوجي بسمات واضحة أهمها السمة الثقافية والاقتصادية والسياسية ولكن أدى بشكل أوضح الى افتتاح العالم وتمركز مجتمعاته نحو تحقيق مصالح مختلفة، بل أن هذا التطور أدى الى تقسيم العالم إلى شعوب مستفيدة وفاعلة في ظل النظام العالمي الجديد الذي يخدم مصالح الدول الغنية ولا يخدم مستقبل البشرية بشكل عام[1].

فبسبب التطور الهائل والمتنازع في التكنولوجيا، وسرعة التفاعل والإدمان على مختلف الوسائل التقنية، والانجذاب نحو استخدام الوسائل العلمية كالحاسبات الآلية وشبكة المعلومات الدولية والوطنية ظهرت

[1]نزيه نعيم شلالا، الجريمة المنظمة، دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، سنة 2010، ص18.

الممارسات غير المشروعة وكثرت المخططات الاجرامية والتي من أهمها الجريمة المنظمة، الجريمة الالكترونية والجرائم المتعلقة بالأخلاق العامة والآداب العامة وغيرها من الجرائم، حيث استفادت العصابات الإجرامية من سهولة التنقل والاتصال واستفادت كذلك من التقنيات الحديثة ساعدتها كلها على ارتكاب الجرائم[1]،بل أنها تتفوق بنشر الإجرام من خلال استخدام مختلف الوسائل الحديثة في كل المجالات بكل يسر وتَسَهُّل عليها حتى التنسيق بين المنظمات الإجرامية، مما ساهم في تفشي ظاهرة الفساد والجرائم الخطيرة بأنواعها في جميع أنحاء العالم.

1- فكرة التّطور التكنولوجي وعلاقته بظهور أخطر الجرائم:

يساهم التطور التكنولوجي في كل المجالات بطرق مختلفة في تطور أشكال الإجرام على كافة المستويات الاجتماعية والاقتصادية والثقافية والسياسية، ومما أضاف خطورة هذا التّقدم هو تجاوزه الحدود الوطنية التقليدية وانتشار شبكاته عالميا، فقد فأفضت حقيقة الثورة التكنولوجيا وانجازاتها إلى إسقاط الحواجز بين البشر وإلى اختزال المسافات، وبروز جرائم وتنظيم عمليات إجرامية خطيرة[2]،لاسيما الجرائم الإلكترونية، وجرائم القرصنة، وغسيلالأموال، وجرائم عديدة يرتكبها المتخصصون بطرق النصب والاحتيال من خلال وسيلة التكنولوجيا التي تتم بها العمليات.

في الواقع، وعمليا أمام اقتحام التكنولوجيا وفي ظل عصر الاقتصاد الرقمي طرحت مشكلة اللاأمن بسبب انتشار أنشطة الفساد بكل صوره المالي والإداري،...إلخ، وظهرت جهود شريرة من طرف مجرمين ومنظمات تقترف جرائم ذات ملامح عالية وعابرة للحدود.

فليس من قبل الصدفة أن تتغلغل الجرائم في نمط الحياة اليومية في كل المجتمعات، حتى أن هناك ملامح جديدة للجرائم، بحيث نكتشف أشكال كثيرة للانحراف الاجتماعي والاقتصادي في ضوء متغيرات جديدة[3] مرتبطة بعدد من الذرائع التي تبرر استقرار الفساد والإجرام، واتساع نطاق مفعوله في الحياة اليومية بأخطر أنواع الجرائم، والتي غالبا ما تسبب الضرر للمجتمع في جميع الجوانب الاقتصادية والسياسية والاجتماعية والثقافية[4]، بسبب أبرز التطوراتفي جميع مجالات الحياة.

---

(1) حسين حياة، "**انعكاسات التطور التكنولوجي على الجريمة المنظمة وآليات مكافحتها دوليا**"، مجلة الفكر القانوني والسياسي، العدد 1، 2022، ص 573.

(2)international federation of Accountants, Anti money laudering,2nd editions,WWW.ifac.org, March 2004, p11.

(3)فاديا قاسم بيضون، الفساد، أبرز الجرائم، الآثار وسبل المعالجة، منشورات الحلبي الحقوقية، لبنان، سنة 2013، 09.

(4) نسرين عبد الحميد، الجرائم الاقتصادية، التقليدية-المستحدثة، المكتب الجامعي الحديث، الاسكندرية، مصر، سنة 2009، ص212.

إن التطورات التكنولوجية تعد من بين المصادر الرئيسية للتغيير على المستوى الوطني والدولي، ولها تأثيرها على المجتمعات ايجابيًا أو سلبيًا، ويتجلى التطور التكنولوجي في مختلف المجالات، ويعني التقدم التقني وتكثيف المنافسة في ميادين أسواق المال مع تبادل للأموال والخدمات والاتصال، حيث أضحى هذا التطور خارج عن سيطرة دول العالم، بما في ذلك أكبرها وأغناها وأفرز فضاءات ملائمة ومساعدة لكل أنواع الإجرام، أو كما يقول بعض المفكرين في سياق الحديث عن النشاط الإجرامي أن " التطور التكنولوجي سَهَّل في ميلاد تطور آخر هو تطور الإجرام.

فمن المؤكد مع التقدم والتطور الذي يشهده العالم في كافة مناحي الحياة الاقتصادية والاجتماعية والسياسية وثورة وسائل الاتصال والمواصلات، والاكتشافات التكنولوجية والتغيرات الجيوسياسية الكبرى، وتعقيد وتشابك العلاقات الإنسانية في الداخل والخارج الناتج عن توسع الاعمال وتزايد حدة المنافسة ترعرعت الجريمة والخدمات غير المشروعة[1]، وبالتالي ازدياد المخاطر وتنامي السلوكات المخالفة للقانون وشيوع الفساد، وحتى انتهاك حقوق وحريات الإنسان الأساسية وانهيار القيم الخلقية[2].

فيمكن القول أن الصّفات الأساسية للتطور التكنولوجي والتي تعني استخدام أنظمة المعلومات، والشبكات واستخدام تقنيات الحاسب الآلي والأنترنت وغيرها في جميع المعاملات والأنشطة التي يقوم بها الإنسانوتمس حياة كل فرد، فلاشك أن اتساع نطاق استخدام التقنيات العالية في بيئة المعلومات العالمية في مختلف الميادين علمية، صناعية، تجارية،...إلخ، ومن خلال البنيات التحتية لنظم المعلومات الدولية والثورة التكنولوجية سوف يؤدي إلى تزايد الجرائم والأنشطة غير مشروعة، خصوصا في ظل ضعف قدرات أجهزة وتشريعات نظام العدالة الجنائية التقليدية، والاعتماد المفرط على استخدام التقنيات الإلكترونية والمواقع العالمية،أو ما يسمى بالاعتماد على الفضاء الإلكتروني بعقد عمليات وصفقات مهمة أو لنقل أموال ضخمة بين دول العالم، هذه الاعتمادية سببت في انتشار الكثير من الفرص لارتكاب مختلف جرائم الفساد ذات الخطر والضرر.

2-فداحة وتفاقم الإجرام في دواليب التّطور العالمي:

يتحمل المجتمع الدولي اليوم عبئا ثقيلا جراء تفاقم الجريمة ومختلف أشكال الإجرام والمخاطر الناجمة عن التطور التكنولوجي، فقد أصبح الإجرام اليوم مرعب والذي ميزه الانفتاح والسرعة في ارتكابه، هذا الإجرام مرتبط ارتباطا وثيقا بعالم الأعمال والتكنولوجيا، كما أن الوجه الجديد للإجرام في عصر التقدم التكنولوجي

---

[1] مختار شبيلي، الإجرام الاقتصادي والمالي الدولي وسبل مكافحته، دار هومة للطباعة والنشر والتوزيع، الجزائر، سنة 2012، ص18.

[2] علي محمد جعفر، مكافحةالجريمة، سياسة الوقاية والعلاج، المؤسسات الجامعية، بيروت، لبنان، سنة 2003، ص27.

كشف عن فداحة أنشطته اللاشرعية التي تفاقمت حتى أخذت أبعاد ضخمة في زمن العولمة ويبقى مرتكبوه غير مكترثين لا بالحدود ولا بالسلطات ولا بالقوانين[1].

من المفيد الذكر أن نشير إلى أن التطور التكنولوجي وعلاقته بالجريمة محور اهتمام عديد من الدّراسات، بحيث تتراوح الجريمة ما بين جرائم الفساد، التي تتمثل في العمولات، الاختلاسات، تبييض الأموال، التهريب، وممارسة أفعال غير مشروعة في المستويات الإدارية العليا والدنيا كالرشوة، كما توجد جريمة أخرى بكل أنواعها أطلق عليها بالجريمة الحاسوبية أو الجريمة(الإلكترونية)، والتي تمخضت عن انتشار التأثيرات المتعاظمة لثورة المعلوماتية.

كما هناك أبحاث ميدانية وإحصاءات عالمية تؤكد على أن التطور التكنولوجي وانتشار الاتصالات الحديثة وتفشيه بصورة سريعة وكبيرة على كافة الأصعدة بالجريمة[2]، بالإضافة إلى ظهور الإجرام الاقتصادي والمالي والمنظم والذي يوصف في مجمله بالإجرام الخطير–الإجرام الكبير– العابر للأوطان، إجرام يأخذ أنماط مختلفة، وكذلك يُرتكب بالمهارة والمعرفة العميقة واستعمال التكنولوجيا المتقدمة في مجال الاتصال والمعلوماتية، والأبعاد الدولية والتعاون بواسطة فروع وشبكات في مختلف البلدان، والعمل عبر الأوطان خارج نطاق النظم والقوانين واستغلال عولمة الجريمة[3].

وكحوصلة لما سبق والملاحظ هو كثرة اللجوء إلى التقنيات والعمليات المتطورة بما يشجع انتشار الإجرام والشبكات الإجرامية، ولا يمكن إجراء جرد دقيق لكل أشكال الإجرام في ظل التقدم التكنولوجي البارز، نظرا لخصوصية وخطورة بعض صور الإجرام الذي يتطور بتطور الحياة الاقتصادية ويستفيد من أدوات التقدم العلمي والتكنولوجي على المستوى العالمي[4].

كما نشير إلى أن ثمة واقعاً إجراميًا تشكل في كل أنحاء العالم، يتمثل في انتشار الجرائم الإلكترونية بسبب القوة التكنولوجية، ومما زاد من تطور هذه التكنولوجيا هو تجاوزها للحدود الوطنية التقليدية وانتشار شبكاتها عالميا، بالإضافة أن هذه القوة أدت إلى ارتفاع لم يسبق له مثيل في التغيرات الاقتصادية والاجتماعية وما صاحبه من ظهور أنواع خطيرة من الجريمة، واستفحال مرتكبو الجريمة واستغلالهم التطور المذهل في تكنولوجيا المعلومات والاتصالات، وذلك بابتكار أساليب جديدة للسلوك الإجرامي حتى يتمكنوامن ارتكاب

---

[1] مختار شبيلي، الإجرام الاقتصادي والمالي الدولي وسبل مكافحته، دار هومة للطباعة والنشر والتوزيع، الجزائر، سنة 2012، ص27.

[2] فادية قاسم بيضون، المرجع السابق، ص373.

[3] مختار شبيلي، الإجرام الاقتصادي والمالي الدولي وسبل مكافحته، ص30.

[4] مختار شبيلي، المرجع نفسه، ص45.

جرائمهم وهم بمنأى عن المراقبة والمتابعة والضبط، نظرا لصعوبة دور الجهات المكلفة بضبط الجرائم وتتبع مرتكبيها[1].

ثانيا- النهج القانوني والقضائي والأمني المتبع للحد من انتشار الظواهر الإجرامية:

تعتبر الجريمة منذ نشوء البشرية مشكلة متصفة بالخطورة، دون أن توفر لها العقوبة إلا حلا جزئيًا مؤقتًا، ومهما وفقت سياسة الوقاية من الإجرام في تخطيطها وتنفيذها فإنّها تظل عاجزة عن تطهير المجتمع من ذوي الميول الإجرامية، مما يقتضي اتخاذ وسائل وتدابير للحد ومنع ارتكاب الجرائم[2]، ولهذا عند الحديث عن النهج القانوني والقضائي والأمني المتبع للحد من انتشار الظواهر الإجرامية، واسع النّطاق يشمل المجالات وتقع مسؤولية تنفيذ طرق الحد من الإجرام على كل أجهزة الدولة، والفئات الشعبية والمجتمع المدني.

وينطوي النهج على استراتيجيات وخطط جامعة مدروسة بدقة وشفافية لمحاربة الإجرام والفساد، وسائر أشكال الجريمة التي تكمن خطورتها في المشاكل والمخاطر التي تُشكلها على استقرار المجتمعات وأمنها، ذلك أن الإجرام بات يُمثل تحديًا كبيرًا للحكومات والمجتمعات في جميع أنحاء العالم، ولم يعد شأنًا محليًا بل ملفا عالميا دوليا يسمى الأمن والاقتصاد[3].

فلا يمكن إنكار أن عالم اليوم، مميز بالحركة والتطور السريعين والتحولات الكبرى في مختلف قطاعات الحياة الاقتصادية والاجتماعية المسايرة لهذا التطور، وفي السنوات الأخيرة لعب التطور التكنولوجي ومنه بالخصوص تكنولوجيا الإعلام والاتصال les technologies del'information et de la communicationدورًا أساسيًا في عالم الاقتصاد والمال وحتى السياسة، ومن آثارها على الحياة الاقتصادية السرعة، المجال المتسع، اختصار الوقت،بالإضافة إلى تسهيل وتحسين محتوى الخدمات والأعمال والعمل بواسطة الشبكات عن بعد والمجموعات الافتراضية[4].

ولقد خلق هذا التغيير والتطور استغلال أشخاص ومنظمات هذا الوضع، وكذلك اندماج عصابات الإجرام بمختلف أنواعها وكذا المجرمين في محيط هذا التقدم، وهاهم يرتكبون مخالفات خطيرةذات طابع اقتصادي مالي سياسي[5]، والأخطر من ذلك يستغلون الثغراتالقانونية سواء الجنائية أو الدولية وعلى المستوى

---

(1) حسين حياة، المرجع السابق، ص27.

(2) أكرم نشأت ابراهيم، السياسة الجنائية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، الأردن سنة 2008، ص12.

(3) فاديا قاسم بيضون، المرجع السابق، ص27.

(4) Philippe Laurette, Technologies de l'information et de la communication : les enjeux européens, 2003, p25.

(5) Philippe Broyer, l'argent sale l'harmattan, France 2000,p 301.

الداخلي أو الوطني، وبالتالي فإن أحسن سبيل لمواجهة الإجرام والشبكات الخطيرة هو رسم وتتبع سياسة جنائية بتشريعات فعالة، وإنشاء نظم وهيئات إدارية ومالية عليها أشخاص دارسون لعلم الإجرام ومختصون فيه وقادرون بفضل نظام مرن يضمن الحوكمة، وكذلك يمكنهم بسهولة استغلال الوسائل المتطورة والتكنولوجيا المتقدمة من مواجهة وكشف نشاطات وشبكات المجرمين.

1-اعتماد أساليب خاصة وجديدة للكشف عن الجرائم ومواجهتها:

لا يختلف اليوم اثنان في أن الإجرام بكل أنواعه الوطني والدولي أخذ حجما وأبعاد لا يستهان بها، تملي ضرورة التفكير الواعي والجدي بنية الحد منه ومن آثاره الهادمة، فلا شك أن عبئ الإجرام في تزايد مستمر، وسلبياته وآثاره بادية للعيان، وليس بالأمر البسيط مواجهته بالنظر إلى التقدم العلمي والتكنولوجي البارز والمخيف في نفس الوقت، مما يجعل اعتماد أساليب جديدة ومتنوعة أمرا لازما لمكافحته بصورة فعالة، خصوصا أمام هذا التقدم في مختلف المجالات الذي أدى إلى ظهور أشكال إجرامية معقدة ومتعددة، وتعدد مجالات الفساد بشكل صارخ حتى أضحى أمر مكافحته والآليات العادية غير كافية للمكافحة، بالتالي سيستدعي الأمر ضرورة اعتماد أساليب حديثة تتماشى والطرق الإجرامية الحديثة المتبعة[1].

ونظرا للأثر السيء للجرائم في ظل تطور التكنولوجيا وانعكاس الخطر الإجرامي على حياة الأفراد ومستقبل وأمن الدول، مع العلم أن أكثر الجرائم مستترة عن تلك التي تنشرها الإحصائيات الرسمية، ويزيد تسترها بسبب ارتكابها من قبل ذوي النفوذ السياسي والاقتصادي، كما أن معظم الأبحاث تبين طغيان الجرائم الخطيرة وأن الطابع الاقتصادي والمالي في العالم بسبب عدم وجود استيعاب للقواعد التي يفرضها هذا التطور[2]، وهذه المسألةتدعو مواكبة بطبيعة الحال العصر الحديث في مجال الإجرام، وذلكمن خلال أساليب جديدة خاصة وقوية لمكافحة الإجرام.

---

[1] مختار شبيلي، المرجع السابق، ص127

[2] صلاح عبد المعتال، التغير الاجتماعي والجريمة، مكتبة وهبة، القاهرة، 1976، ص196.

وهذه الأساليب نصت الاتفاقيات الدولية على استخدامها، وتضمنت دعوة الدول الأعضاء إلى اتخاذ ما يلزم من تدابير على ضوء نظامها الداخلي لاستخدام ما تراه مناسبا، وتتمثل في التسليم المراقب، اعتراض المراسلات، تسجيل الأصوات والتقاط الصور، الترصد الالكتروني، وأخيرا التسرب، وهي السبل التي من خلالها يقدم لسلطة التحقيق كافة الإيضاحات الدقيقة عن الجرائم وكشفها من حيث ظروفها وشأنها والمتهمين بارتكابها[1].

كما تمثلأساليب التحري الخاصة طرق إثبات حديثة للكشف عن الجرائم الخطيرة أقرتها معظم الدول في تشريعها العقابية، ومن المهم أن نشير إلى أن رغم ما قيل عن هذه الأساليب في أنها تمس الحياة الخاصة إلا أن وجودها ضروريافي سبيل التحدي والكشف عن الجرائم الكبيرة ذات الخطر والضرر، ولا شك أن جرائم الفساد، والقرصنة والجرائم الالكترونية إحداها، هذا من جهة، ومن جهة أخرى تطوير الإجرام وأساليبه أدى إلى ظهور هذه الأساليب[2]، وتبني التشريعات ذلك للحد من الإجرام المنظم والفاسد الذي يهدد بالضرر للمصالح المحمية والأساسية بفعل الحياة العصرية الحديثة، وما واكبها من انطلاقات علمية هائلة تضعف أمامها القوة البشرية والأساليب التقليدية[3].

2-تزايد التّعاون الدوليفي البحث عن وسائل مكافحة الإجرام والحد منه:

يعتبر الإجرام العنوان الأول في مسيرات الإصلاح التي تسعى إليها الدول لتوفير أدوات تعزيز رفض الفساد والحد من الجرائم، والسعي إلى وضع مدونات تستطيع أن تكون بشكل كبير وفاعل في تطبيق قوانين وآليات لمنع أي محاولات للجريمة، وهذا من خلال تعاون الدول في إيجاد اتفاقيات دولية حول منع انتشار الجرائم ومكافحة الإجرام على كافة الأصعدة[4].

---

[1]ادريس عبد الجواد، عبد الله بريك، المركز القانوني للضبطية القضائية في الدعوى الجنائية، دراسة مقارنة، دار الجامعة الجديدة ، الاسكندرية، مصر ، سنة 2008، ص88.

[2]العربي نصر الشريف، "**أساليب التحري في جرائم الفساد**"، مجلة دراسات في الوظيفة العامة، عدد 4، ديسمبر 2017، ص148.

[3]حسنين المحمدي، المرجع السابق، ص81.

[4] أكرم نشأت ابراهيم، المرجع السابق ، ص21.

ولا أحد يساور الشك اليوم في الجهود التي تبذلها الدول على نطاق واسع لمواجهة مختلف الآفات والظواهر الإجرامية بمختلف أنواعها ودرجة خطورتها،فالوضع الحالي والتطور التقني والتحولات المتسارعة التي يشهدها العالم يفرض ضرورة إيجاد سبل التعاون فيما بينها بغية محاربة ظاهرة الإجرام.

ونلاحظ اليوم تزايد صدور الاتفاقيات والمعاهدات والمؤتمرات والتوصيات الدولية والتدابير المتخذة خيال الإجرام بمختلف أشكاله، لاسيما الإجرام الاقتصادي والمالي الدولي، وأن هناك نشاط أجهزة المكافحة المختلفة حقيقة قائمة عالميا اليوم لا يمكن إنكارها[1]،كما أنه من المفيد أن نذكر أن أغلب الجرائم قد أضحت في ظل التكنولوجيا المتطورة دولية الطابع، عالمية التخطيط والتقنية، ولذلك لابد أن تكون المكافحة ذات جهود دولية[2]، مما يجعل اقتناع الدول على أن الإجرام مسألة دولية، وبالتالي فإن مواجهته بمسؤولية جميع الدول أن تتعاون جنائيا مع بعضها في تبني منهجية شاملة ومتعددة الأساليب للنجاح بصورة فعالة[3].

فالنمو السريع والعولمة والتقدم العلمي والتكنولوجي المطرد أمور شكلت أساسًا لنمو الإجرام، وتُخفيه بوسائل مبتكرة وبالتالي بعيدا عن منال التشريع الجزائي التقليدي، فعلى الرغم من أن النصوص الجزائية في تشريعات الدول قد عالجت معظم الجرائم لكن هذا لا يعني أنها تحيط إحاطة كاملة بجوانب هذه الجرائم، لذا كان لابد من الحد من الجرائم والإجرام الخطير ليس من منظار القوانين الداخلية بل من منظار توحيد الجهود والوصول إلى قوانين متناسقة، عن طريق إنشاء معاهدات واتفاقات وعقد مؤتمرات تضع نظام صارم ضد الإجرام والفساد، وتتضمن في محتواها طرق وإجراءات وتدابير ملزمة كفيلة بحظر النشاطات غير المشروعة، وتقصي الجرائم.

---

[1] علي محمد جعفر، داء الجريمة، مناهج الأمم المتحدة والتشريع الجزائي، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان سنة 1988، ص150.

[2] مصطفى يوسف كافي، المرجع السابق، ص102.

[3] فاديا قاسم بيضون، المرجع السابق ، ص228.

لننستطيع عرض كل الجهود أو الاتفاقيات التي بلورت الأدوات والآليات القانونية لمكافحة الجرائم، لكن يمكن الإشارة إلى بعض منها، على سبيل المثال التي لعبت دورًا محوريًا في وضع التقارير والقواعد وتوصيات مهمة ضد الإجرام، نذكر ما يلي:

أ- مؤتمر نابولي الاقتصادي العالمي حول الجريمة المنظمة لعام 1995 الذي دعا إنشاء فريق دافوس كرابطة غير رسمية لدراسة كيفية محاربة الفساد بآليات عالمية[1].

ب-منظمة الأمم المتحدة واتفاقياتها في مكافحة الجريمة المنظمة عبر الوطنية 1996-1997-1998-2000، وكلها تضمنت تدابير واجراءات جديدة في مسألة الجرائم الخطيرة، ومسألة المسؤولية الجنائية عن الإجرام المنظم، والجرائم الجسيمة[2].

ت- منظمة التعاون والتنمية الاقتصادية O.C.D.Eالتي يتركز نشاطها حول مكافحة الممارسات المضرة بالاقتصاد، الإدارة العمومية، العلوم التكنولوجيا، الطاقة، السياسة الاجتماعية، وتبادر هذه المنظمة بجهود بارزة سريعة في مجال مكافحة الإجرام الاقتصادي والمالي، وقد صدرت من هذه المنظمة اتفاقيات متعددة أشهرها تلك المتعلقة بمكافحة الرشوة والمعاملات المالية غير المشروعة[3].

في هذا السياق نشير إلى وجود مجموعات دولية أخرى مختلفة بأنشطة وجهود كثيرة في مجال التّصدي للإجرام، كذلك وجود جهاز دولي واسع متمثل في اتفاقيات ومعاهدات كثيرة وهيئات ومنظمات متخصصة تشكل إطارًا ملائمًا ومعتبرًا لمواجهة الإجرام بكل صوره، إلا أنه يبقي واقع الإجرام والفساد الكبير يشكل خطورة كبيرة بتعدد الأفعال الإجرامية التي غالبا ما يصعب حصرها، وأن مهمة مواجهة مختلف الجرائم ليس بالأمر الهين رغم تحمل معظم دول العالم العربي والغربي عبئ الإجرام وانعكاس آثاره السلبية.

---

[1] نجار لويزة، التصدي المؤسساتي والجزائي لظاهرة الفساد في التشريع الجزائري، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر 2018، ص111.

[2] شبلي مختار، الجهاز العالمي لمكافحة الجريمة المنظمة، دار هومة، سنة 2013، ص247.

[3] مختار شبيلي، الإجرام الاقتصادي والمالي الدولي وسبل مكافحته، المرجع السابق، ص86.

فتقول أن الإجرام أضحى لغة العصر متنوع الأشكال مختلف الأوجه الذي يرتكب من طرف أذكياء ومتحايلين على القانون، ويرتكبون أفعال رهيبة باسم الثقافة وتكنولوجية العصر، فالنتيجة برأينا التي لا تُخفى على أحد هي أن جهود وإرادة مواجهة الإجرام تبقى محدودة سواء من جانب التعاون الدولي، أو من جانب سن القوانين المناسبة أو في مجال التنظيم القضائي وأجهزة المكافحة الميدانية، أو حتى الاهتمام به في جانب الدراسات والبحوث الأكاديمية.

خاتمة

بناء على ما سبق في دراستنا،يتضحجليا أن الإجرام موجود في كافة المجتمعات بأنماطٍ وأشكالٍ مختلفةٍ ومعقدةٍ، ولا أحد ينكر أنّه ينتشر بوتيرة متسارعة يهدد المجتمع الدولي والأنظمة القانونية جزاء الأنشطة الخطيرة وغير المشروعة رغم الوسائل المختلفة والعديدة في مواجهتها، كما أنه لا يمكننا إنكار أن هناك إرساء لقواعد وآليات على المستوى المحلي والدولي، ووجود مختلف المعاهدات والاتفاقيات التي جاء في محاورها دراسة الأنشطة الإجرامية ووضعت اجراءات على أساس التعاون في مجال مكافحة أخطر صور الجريمة، إلا أنه بقي خطرها يهدد المجتمعات في عصرنا الحديث، بل في الواقع أضحى الإجرام يفوق الخطط وأساليب الوقاية منه ومكافحته، وهذا لأسباب خاصة منها قانونية وقضائية كذلك بسبب الاكتشافات التكنولوجية والتغيرات الجيوسياسية الكبرى.

التوصيات

1. ضرورة معالجة الصّعوبات ذات الطّابع السياسي والقانوني التي تعترض جهود التّعاون الدّولي لمكافحة الجرائم، خصوصا وأنّ الظّواهر الإجرامية تتزايد وتتمدد وأصبحت بمختلف صورها خطيرة ومعقدة.
2. ضرورة المراجعة اللاّزمة للنّصوص القانونية فيما يخص مسائل كثيرة من جانب تجريم الأفعال والعقوبات،وهذا من أجل تكريس الرّدع اللاّزم في مجال المكافحة.

3. تكثيف الدّراسات للمشاكل المثارة حاليا على ساحة القضاء والواقع حول أسباب فداحة وتفاقم الإجرام وانعكاساته السلبية على الحياة الاقتصادية والاجتماعية وحتى السياسية للدول في زمن التكنولوجيا، مع وجوب دراسة الظواهر الإجرامية المعقدة والجديدة التي ساهم التطور التكنولوجي في بروزها إلى درجة اتخاذها أبعاد تركت آثار عميقة سلبية على مستوى غالبية الدول، وهذا بهدف تكريس تدابير مناسبة وفعالة على مستوى الهيئات الشريعة والقضائية الأمنية وحتى على مستوى المجتمع المدني للحد فعلا من حجم الجرائم الخطيرة المنتشرة.

قائمة المراجع

أولا–الكتب

1. علي محمد جعفر، مكافحة الجريمة، مناهج الأمم المتحدة والتشريع الجزائي، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، لبنان سنة 1988.
2. علي محمد جعفر، داء الجريمة، سياسة الوقاية والعلاج، المؤسسات الجامعية، بيروت، لبنان، سنة 2003.
3. أكرم نشأت ابراهيم، السياسة الجنائية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، الأردن سنة 2008.
4. ادريس عبد الجواد، عبد الله بريك، المركز القانوني للضبطية القضائية في الدعوى الجنائية، دراسة مقارنة، دار الجامعة الجديدة ، الاسكندرية، مصر، سنة 2008.
5. مختار شبيلي، الإجرام الاقتصادي والمالي الدولي وسبل مكافحته، دار هومة للطباعة والنشر والتوزيع، الجزائر، سنة 2012.
6. نسرين عبد الحميد، الجرائم الاقتصادية، التقليدية–المستحدثة، المكتب الجامعي الحديث، الاسكندري، مصر، سنة 2009.
7. نزيه نعيم شلالا، الجريمة المنظمة، دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، سنة 2010.
8. شبلي مختار، الجهاز العالمي لمكافحة الجريمة المنظمة، دار هومة، سنة 2013، ص247.
9. نجار لويزة، التصدي المؤسساتي والجزائي لظاهرة الفساد في التشريع الجزائري، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر 2018.
10. فاديا قاسم بيضون، الفساد، أبرز الجرائم، الآثار وسبل المعالجة، منشورات الحلبي الحقوقية، لبنان، سنة 2013.

11.صلاح عبد المعتال، التغير الاجتماعي والجريمة، مكتبة وهبة، القاهرة، 1976.

ثانيا– المجلات العلمية

1. حسين حياة، "**انعكاسات التطور التكنولوجي على الجريمة المنظمة وآليات مكافحتها دوليا**"، مجلة الفكر القانوني والسياسي، عدد 1، 2022، ص 573.
2. العربي نصر الشريف، "**أساليب التحري في جرائم الفساد**"، مجلة دراسات في الوظيفة العامة، عدد 4، ديسمبر 2017، ص148.

Ouvrages :

1-international federation of Accountants, Anti money laudering,2nd editions,WWW.ifac.org, March 2004.

2-Philippe Laurette, Technologies de l'informations et de la communication : les enjeux européens, 2003.

3-Philippe Broyer, l'argent sale l'harmattan, France 2000.

الأستاذة حبيب فطيمة

أستاذة محاضرة قسم "ب" كلية الحقوق سعيد حمدين الجزائر-1-

البريد الإلكتروني rimadach29@gmail.com

الملتقى الدولي الافتراضي الموسوم

" القانون الجنائي في ظل التطور التكنولوجي "

-إشكالات ومعالجات-

المحور الأول: التطور التكنولوجي والظاهرة الإجرامية

عنوان المداخلة: التطور التكنولوجي كآلية لارتكاب الجرائم المستحدثة

الملخص

إضافة إلى مساهمة التطور التكنولوجي في زيادة الاندماج والارتباط بين الدول نتيجة تحرير التجارة الدولية وظهور الشركات المتعددة الجنسيات وكذا إلغاء الحدود الإقليمية التي أصبحت صورية وشكلية بفضل شبكة المعلومات الدولية التي حولت العالم وجعلته مجتمعا واحدا، كان للتطور التكنولوجي إفرازات أخرى وهو ما يشكل الجانب السلبي له، حيث أدى هذا التطور إلى ظهور ما يعرف بالجرائم المعولمة أو الجرائم العابرة للحدود الوطنية أو الجرائم المستحدثة أو بالأحرى جرائم الشركات المتعددة الجنسيات التي تمارس نشاطات إجرامية على نطاق دولي كجرائم غسيل الأموال، جرائم ذوي الياقات البيضاء، الاتجار بالمخدرات ، الأشخاص، الأعضاء والجرائم الضريبية...إلخ.

أصبحت جرائم التطور التكنولوجي ظاهرة عالمية تهدد المجتمع الدولي وهذا بالنظر إلى خصوصية هذا النوع الخطير من الإجرام الذي يعتمد على أحدث الاختراعات والابتكارات التكنولوجية، حيث أنه يتصف بالخفاء يصعب اكتشاف مرتكبيه، كما أنه ينطوي على أسلوب الاحتيال والذكاء الخارق الذي يظهر في قدرة مرتكبيها على تنفيذ أعمالهم الإجرامية وفشل الأجهزة المتخصصة في الكشف عنهم،هذا إلى جانب

قصور وعجز التشريعات الجنائية على مواجهتها، وهو الأمر الذي يدفعنا للبحث عن خصوصية هذا النوع من جرائم التطور التكنولوجي وتحديد دور التكنولوجيا الحديثة والمتطورة كأداة وأسلوب في ارتكابها.

للإجابة على هذه الإشكالية تم تقسيم المداخلة إلى محورين أساسيين:

تناول المحور الأول معالجة خصوصية جرائم التطور التكنولوجي

بينما تطرق المحور الثاني إلى معالجة دور التكنولوجيا الحديثة كآداة لارتكاب الجرائم المستحدثة.

الكلمات المفتاحية: الجرائم المستحدثة ، التطور التكنولوجي، العولمة الإجرامية .

مقدمة

كان للتطور التكنولوجي الناجم عن استعمال الحاسوب الألي والأنترنت وكذا الهاتف الذكي وغيرها من وسائل الاتصال والمواصلات الدور الفعال في تسهيل وتنفيذ أخطر الجرائم وتحقيق النتيجة الإجرامية ، وحصول فاعليها على أموال وأرباح مادية من وراء ذلك، فأصبح الحاسوب الألي سلاح ذو حدين يتم استخدامه كوسيلة مادية لارتكاب مختلف الجرائم ذات الطابع الالكتروني كالدخول غير المشروع في أنظمة المعالجة الألية للمعطيات والقيام بتغيير البيانات أو نقلها أو إتلاف المعلومات الموجودة فيه هذا من جهة ، بينما من جهة أخرى يكون ضحية للجرائم التي تقع عليه كتعرضه لعملية القرصنة من أجل السرقة وابتزاز الأشخاص باستعمال تلك المعلومات.

وإن الارتفاع الهائل لعدد الجرائم المستحدثة الناتجة عن الاستعمال غير المشروع للتكنولوجيا الحديثة والذي مس مختلف الجوانب الاقتصادية والاجتماعية والمالية وحتى السياسية بالنظر إلى خصوصية هذا النوع الخطير من الإجرام المعولم والذي ينفرد بخاصية سرعة التنفيذ ومحو كل أثارالجريمة وصعوبة اكتشافها ومن ثمة صعوبة إبراز الركن المادي لها كدليل لإثبات الفاعل الأصلي لهذه الجرائم، وعليه سنتوقف عند أهم الخصوصيات التي تميز هذه الجرائم المستحدثة من خلال المحور الأول، ثم نتناول دراسة دور التطور الحديث كألية لارتكاب هذا النوع من الجرائم وهذا على النحو التالي:

المحور الأول: خصوصية الجرائم المعلوماتية المستحدثة

تتميز جرائم التطور التكنولوجي بمجموعة من الخصائص التي تنفرد بها وتميزها عن غيرها من الجرائم التقليدية تتمثل في كونها:

- جرائم ذات طابع خاص لارتباطها بنظام المعلومات والتكنولوجيا الحديثة.
- هي جرائم عابرة للحدود الوطنية وهو ما يستشف من عبارة " الشبكة العنكبوتية" التي تطلق على الأنترنت ، كما تنعدم الحدود الدولية فيها.
- صعوبة إبراز الركن المادي لها، وهذا يعود لكون المجرم المعلوماتي يتخلص من الدليل المادي الملموس في أقل من ثانية خاصة وأن هذا النوع من الجرائم يتم في عالم افتراضي مما يجعلها خفية بسبب التلاعب في التذبذبات الإلكترونية.
- سرعة التنفيذ الفائقة، حيث أنها تتم بمجرد الضغط على زر ، وهو ما جعل بعض الفقهاء يطلق عليها تسمية " الجرائم الناعمة" بسبب السرعة الفائقة في تنفيذها وعدم اعتمادها على العنف ، فالجريمة الالكترونية هي جريمة فنية هادئة.
- هذا النوع من الجرائم يتطلب إلى جانب السرعة ،الدقة والخبرة وعلى هذا الأساس نجد أن مرتكبي هذا النوع الخطير من الإجرام المستحدث يتمتعون بمهارات عالية وبالخبرة والذكاء الذي يسمح لهم بمحو أثار الجريمة في ثوان قليلة[1].
- عولمة هذه الجريمة تؤدي إلى تشتيت جهود التحري والتنسيق الدولي لتعقب هذا النوع من الإجرام الخطير ، فهي صورة صادقة من صور العولمة.

تجدر الإشارة إلى أن الركن المادي في هذا النوع من الجرائم يتحقق بمجرد الدخول غير المشروع إلى نظام معالجة البيانات ، أي أن السلوك الإجرامي يتحقق بمجرد الضغط على زر كوسيلة لتنفيذ الجريمة ما تتم ملاحظته من خلال معالجة خصوصية الإجرام المعولم أن طبيعة هذا النوع من الإجرام المتطور يقف حائلا أمام اكتشاف السلطات الأمنية والقضائية لركنه المادي بسهولة وفي كل الحالات ، كما أنه يعجز القوانين عن التصدي له لارتباطه بالتطور التقني والتكنولوجيا الحديثة وهو ما يتسبب في إهدار مبدأ الشرعية الجنائية الذي يتطلب إيجاد تكييف قانوني صحيح

[1]-عبد الصبور عبد القوي علي ، الجريمة الالكترونية والجهود الدولية للحد منها ، رسالة ماجستير في القانون ، جامعة بني سويف ، كلية الحقوق، الأردن ص 25.

للجرائم المعلوماتية وبالتالي نتوصل إلى أن مبدأ الشرعية الجنائية في مجال الجريمة المعلوماتية له خصوصية من حيث الركن المادي.

المحور الثاني: دور التكنولوجيا الحديثة كألية لارتكاب الجرائم المستحدثة

إن التطور المذهل للتكنولوجيا أدى إلى ظهور جرائم ناجمة عن الاستعمال غير المشروع للحاسوب الألي ومختلف وسائل الاتصال التي جعلت العالم في متناول اليد بفضل الشبكة العنكبوتية ، حيث أصبح جهاز الكمبيوتر وسيلة المجرم المعلوماتي يستخدمه لتنفيذ مشروعه الإجرامي كاختراق الشبكات أو تخريبها أو التحريف أو التزوير أو السرقة والاختلاس وسرقة حقوق الملكية الفكرية مما يجعل هذه الأفعال تشكل جرائم بأركانها المادية والمعنوية.

وعليه قبل التطرق إلى دور التكنولوجيا الحديثة كوسيلة تساهم في الإنتشار السريع للجريمة المستحدثة نتوقف بالدراسة عند تحديد المجرم المعلوماتي وتحديد أهم الجرائم المرتكبة بواسطة التكنولوجيا المتطورة

أولا – تعريف المجرم المعلوماتي:

هو الفاعل الرئيسي للنشاط الإجرامي الإلكتروني ، هو يتمتع بذكاء خارق ، كما أنه متخصص في مجال المعلوماتية والبرمجة وله قدرات فائقة في كسر الشفرات وكلمات المرور ومن ثمة يتمكن من الوصول إلى أدق المعلومات والحصول عليها،فهو يعمل في سرية تامة ويشغل أجهزته عن بعد من خلال الارتباط بشبكة الانترنت [2].

كما أن مسرح الجريمة هو الفضاء الرقمي ، وهو المسرح الذي لا يقبل إلا الأذكياء ، بينما أداة الجريمة تكمن في الحاسوب المرتبط بالشبكة العالمية مما يجعل هذا النوع من الجرائم هي جرائم عابرة للحدود الوطنية.

تجدر الملاحظة إلى أن الدراسات والأبحاث العلمية تؤكد وجود فئات مختلفة من الجناة في هذا المجال يمكن تقسيمها على النحو التالي:

[2]- حسين اليوسفي المغاري، التكنولوجيا الحديثة في خدمة الاجرام ، مقال منشور على موقع الجزيرة نات، بتاريخ 2017/04/19.

- مستخدمو الحاسوب بالمنازل
- الموظفون الساخطون على منظماتهم
- المتسللون أو العابثون بقصد التسلية
- العاملون في الجريمة المنظمة
- المحترفون الذين يتسللون إلى مواقع مختارة بعناية ويقومون بإتلاف النظام وسرقة محتوياته[3].

ثانيا – أهم الجرائم الناتجة عن استخدام التطور التكنولوجي:

أفرزت التكنولوجيا الجديثة جملة من الجرائم المستحدثة مست مختلف الجوانب الاقتصادية والاجتماعية والسياسية والعسكرية وحتى الثقافية، نتوقف بالدراسة عند الجرائم التي تمس الأشخاص وتلك التي تقع على الأموال وهذا على النحو التالي:

1- الجرائم المستحدثة الواقعة على الأشخاص:

هذا النوع من الجرائم يهدد بالخطر الحقوق ذات الطابع الشخصي ومن أبرزها :

-التحريض العمدي على القتل عبر الانترنت

- استخدام الانترنت لترويج الدعارة
- التحرش والمضايقة عبر وسائل الاتصال
- التوغل داخل البيانات الشخصية

2- **الجرائم المستحدثة الواقعة على الأموال:**

وهي الجرائم التي تمس الحقوق ذات القيمة المالية ومن أبرز هذه الجرائم نذكر:

-قرصنة البرامج وسرقة خدمات الحاسوب

- تزوير البريد الالكتروني أو الوثائق أو السجلات
- الاختلاس عبر الحاسوب أو بواسطته
- استعمال الحاسوب كوسيلة للحصول على البطاقات المالية واستخدامها دون ترخيص أو تدميرها
- إنشاء صفحة انترنت مماثلة لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة لتطلب من العميل ادخال بياناته أو تجديث معلوماته بقصد الحصول على بياناته المصرفية وسرقتها[4].

[3]-أمينة حمشاشي ، ماهية الجريمة المعلوماتية، مداخلت ألقيت في ملتقى منظم من طرف جامعة مصطفى اسطمبولي معسكر

– إدخال بيانات ومعطيات خاطئة إلى نظام الحاسوب.

يتبين لنا مما سبق مدى مساهمة التكنولوجيا الحديثة في إفراز هذا النوع الخطير من الإجرام العابر للحدود الوطنية، فهو يمس كل المجالات دون استثناء ولا يعترف بالحدود ، بل يجول عبر العالم بكل حرية ويمس المصالح الجديرة بالحماية القانونية، فهو يمتد ليمس إلى جانب الأشخاص المؤسسات العمومية كالبنوك والأجهزة الرسمية والشركات بمختلف أنواعها وأشكالها مستفيدا من التكنولوجيا الحديثة التي يستخدمها للحصول على مكاسب مالية ومادية بطريقة غير شرعية عن طريق تزوير بطاقات الائتمان وعمليات اختراق مواقع إلكترونية على الشبكة العنكبوتية.

[4]-محمود شرفي ، صلاح الدين جبار، تأثير تطور تكنولوجية المعلوماتية على تنامي الجريمة ، كلية الحقوق، جامعة لونيسي علي البليدة 02 ص 05.

الخاتمة

إن الجريمة المعلوماتية هي جريمة من نوع خاص تؤثر فيها التطور التكنولوجي المستمر حيث أفرز هذا النوع من الإجرام المستحدث إشكالات من حيث صعوبة النصوص القانونية في مواكبة خصوصية الجريمة المستحدثة

توصلنا من خلال هذه المداخلة إلى مجموعة من النتائج تتمثل في:

- إن الاستخدام غير المشروع للصناعات التكنولوجية من شبكة الأنترنت ، الحاسوب الألي ، الهواتف الذكية وغيرها من وسائل الاتصال عبر العالم أدى إلى ظهور طائفة جديدة من الجرائم تسمى بالجرائم المعلوماتية.
- طبيعة هذا النوع من الإجرام المتطور يعجز القوانين على مواجهتها لارتباطها بالتطور التكنولوجي مما يتسبب في إهدار مبدأ الشرعية الجنائية الذي يتطلب إيجاد تكييف قانوني صحيح للجرائم المعلوماتية وبالتالي نلاحظ أن مبدأ الشرعية الجنائية في المجال المعلوماتي له خصوصية من حيث الركن المادي.
- عجز السلطات القضائية في إثبات الركن المادي لهذا النوع من الإجرام والذي يعود إلى خصوصية وطبيعة الجريمة في حد ذاتها لعدم ظهور دليل مادي ملموس يمكن الوقوف عليه وقدرة المجرم المعلوماتي من محو الدليل بكل سهولة.

التوصيات:

- لمواجهة هذا النوع الخاص من الجرائم المستحدثة لا بد من وضع أليات حديثة تقوم على نفس عناصر قيام هذا النوع الخاص من الجرائم الخطيرة كإنشاء معاهد متخصصة تتشكل من أحدث التجهيزات التكنولوجية العالية المستوى تقوم على اكتشاف هذه الجرائم قبل وقوعها ومواجهتها.
- ضرورة تكوين قضائيين وقضاة تحقيق متخصصين في مجال التشخيص والتحقيق في هذا النوع من الجرائم.
- ضرورة الاستعانة بالخبرات الأجنبية المتخصصة في هذا المجال والوقوف عند تجاربها في مجال مكافحة الجرائم المعلوماتية.

الهوامش

1- عبد الصبور عبد القوي علي، الجريمة الالكترونية والجهود الدولية للحد منها ، رسالة ماجستير، جامعة بني سويف الأردن

2- حسين اليوسفي المغاري، التكنولوجيا الحديثة في خدمة الإجرام ، مقال منشور على موقع الجزيرة نات

3- أمينة حمشاشي ، ماهية الجريمة المعلوماتية ، مداخلة ألقيت في ملتقة منظم من طرف جامعة معسكر

4- محمود شرفي، صلاح الدين شرفي، تأثير تطور تكنولوجيا المعلوماتية على تنامي الجريمة ، كلية الحقوق، جامعة لونيسي علي 02، البليدة .

عنوان المداخلة:

التطور التكنولوجي و الجريمة الالكترونية

– سرعة التأثير و صعوبة التحدي–

مداخلة الدكتورة: قمار خديجة

عضو مخبر نظام الحالة المدنية

مقدمة

يساهم التطور التكنولوجي في مجال المعلوماتية بطرق مختلفة وأساليب منها المعقدة والسهلة، في تطور اشكال الاجرام على كافة المستويات الاجتماعية والاقتصادية والثقافية والسياسية ...، ومما أضاف خطورة هذه التكنولوجيا هو تجاوزها للحدود الوطنية التقليدية وانتشار شبكاتها عالميا، ورغم ما تقدمه تكنولوجيا المعلومات من خدمات عديدة إيجابية للبشرية في جميع المجالات، وما حققت من انفتاح عالمي لم يسبق له مثيل من قبل ، في هذا المقال سوف نتناول الأجراء القانونية والوطنية الدولية التي بدأت تتسع دائرتها نظرا لكون الجريمة الالكترونية أصبحت عابرة للحدود، ولا تعترف بعنصر المكان والزمان، فهي تتميز بالتباعد الجغرافيواختلاف التوقيتات بين الجاني والمجني عليهم وما نجم على هذا التطور من انعكاسات سلبية على الافراد والمجتمعات عبر العالم أجمع[1]

لقد شهد العالم تطورات كبيرة في جميع المجالات والميادين خاصة الميدان التكنولوجي، فمن الأبواب التي طرقتها هذه التطورات نجد تكنولوجيا وسائل الإعلام والاتصال، فبالرغم من حداثة العهد بهذه التكنولوجيا في مجتمعنا، إلا أنها ودون منازع استطاعت أن تفرض وجودها في حياة كل فرد، فقد ساهم التطور المعاصر في تبادل الأفكار والمعلومات إلى إحداث سلوكيات مقبولة وغير مقبولة، في جميع المجالات التي تتعلق بالفرد والمجتمع، وقد يؤدي الاستخدام المفرط لهذه المواقع، إلى تدني المنظومة القيمية نتيجة للتأثر بالثقافات المفتوحة، من أخطرها انتشار الجرائم

---

[1] جبار صلاح الدين ،شرقي محمود، تأثير تطور تكنولجية المعلوماتية على تنامي الجريمة، مجلة الآداب و العلوم الاجتماعية، المجلد 08،العدد 01 سنة 2015، ص ص 179–193

الالكترونية، أو كما تسمى أيضا جرائم الانترنت، أو جرائم الكمبيوتر، أو جرائم المعلوماتية والتي تطوّرت بالتزامن مع التطورات التي تطرأ على التقنيات والتكنولوجيا والتي لا يقتصر استخدامها على الإنسان الخير بل كذلك الإنسان الشرير الذي قد يوصف كمجرم لسعيه وراء أطماعه واقتناصه الفرص لتحقيق أغراضه غير المشروعة، ولا يتوانى عن استغلال التقنية لتطوير قدراته الإجرامية باستخدام شبكة المعلوماتية كوسيلة سهلة لتنفيذ العمليات الإجرامية، مما يلحق ضررا بالآخرين، ومن أجل ذلك لا بد من فهم ماهية هذه الظاهرة الإجرامية المستحدثة في الفضاء الرقمي، وفهم أدواتها وطبيعة مرتكبيها، وسنحاول في مقالنا هذا تعريف الجريمة الالكترونية والمجرم الالكتروني، أنواعها، خصائصها وأسبابها وأهدافها، وأهم تأثيراتها على نفسية الفرد وقيم المجتمع، وكذا أبرز أساليب مواجهة الجرائم الالكترونية[2].

أهمية الموضوع: ظهر جيل جديد من الجرائم اختلف عن الجرائم التقليدية واتسم بخطورته الكبيرة نظرا لصعوبة إثباتها إضافة إلى إشكالية الأمن المعلوماتي الذي مازال في بدايات ظهوره، إن الأمن السيبراني عبر مواقع التواصل الاجتماعي أصبح حتمية ضرورية و هاجسا أمام رجال القانون خاصة مع الوتيرة المتسارعة لتداول المعلومات و الاستخدام العشوائي لمواقع التواصل و قصور وسائل الرقابة وضعف التشريعات القانونية و فرض العقوبة لتحجيم تأثيرات هذا النوع من الجرائم التي تستهدف الأفراد والدول،إذ تسجل يوميا حالات انتهاكات لبيانات شخصية و قرصنة لقاعدة و بنوك البيانات و المعطيات لمؤسسات وطنية بحيث أصبح الأمن القومي مهدد بهذه الممارسات الإجرامية ، التي استوجبت تجنيد آليات مواجهة الجريمة الالكترونية عبر مواقع التواصل و تبيان أساليب الحماية المعلوماتية أو ما يعرف بالأمن السيبراني و دوره في قمع التجاوزات و الجريمة المعلوماتية التي استحضرتها الممارسات السيئة لتكنولوجيا الاتصال[3].

الأهمية العلمية للدراسة من الجدل الفقهي حول اعتناق تشريع خاص للحد من الجريمة المعلوماتية فالبعض يرى أن هناك حاجة ملحة لوجود تشريع خاص بالجرائم المعلوماتية يعالج الجانب الموضوعي من جهة و الجانب الاجرائي من جهة أخرى .

---

[2] طالة لامية، سلام كهينة، الجريمة الالكترونية، بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، مجلة الرواق، المجلد06،العدد2، سمة 2020، ص ص 62-91.

[3] حميدة راضية، الجريمة الالكترونية عبر مواقع التواصل الاجتماعي...نحو تفعيل دور الأمن السيبراني المعلوماتي، مجلة الإعلام و المجتمع، المجلد 05،العدد02، سنة 2021، ص ص 338-356.

كما تظهر **الأهمية العملية** للموضوع من خلال الخطورة التي تشكلها الجريمة الالكترونية على المجتمع و الأفراد و على المؤسسات و المنظمات و الشركات، حيث أنها باتت تطال كافة شرائح المجتمع ، و لابد من إيجاد حلول فعالة للحد منها و مكافحتها.

الإشكالية المقترحة:

ما هي آليات مواجهة الجريمة الالكترونية و ما هو دور الأمن السيبرياني في قمع انتشار هذا النوع من الجرائم ؟

الى اي مدى استطاع المشرع الجزائري اعطاء مفهوم دقيق للجريمة المعلوماتية ؟

ما هي خصوصة الجريمة المرتكبة عبر الانترنت في التشريع الجزائري؟

ما هي السياسة الجنائية لمكافحة ظاهرة الاجرام الالكتروني؟

ماهي استارتيجيات الحلول الواجبة على الدولة تسخيرها للقضاء على هذه الظاهرة السلبية؟

أهداف الدراسة:

تسعى هذه الدراسة إلى تشخيص واقع الجريمة الالكترونية، و التعرف على إمكانية مكافحتها و الحد منها ، من خلال استعمال أساليب تكنولوجية متطورة للبحث و التحري و التعرف على المجرمين الالكترونيين ، وتنقسم أهداف هذه الدراسة إلى التالي:

- تسليط الضوء على مفهوم الجريمة المعلوماتية.
- البحث طبيعة الجريمة المعلوماتية و خصوصيتها .
- التعرف على مختلف أبعاد و مخاطر هذا النوع من الجرائم.
- إبراز آليات مكافحة الجريمة المعلوماتية.
- دراسة كيفيات البحث و التحري و جمع أدلة الإثبات في هذا النوع من الجرائم.

منهج الدراسة:

من اجل بلوغ الأهداف المسطرة في هذه الدراسة قمنا باستخدام المنهج الوصفي التحليلي من خلال وصف مفهوم الجريمة المعلوماتية و تحديد أنواعها و طبيعتها و مختلف العوائق المعرقلة

لمكافحتها ، و مدى تأثير التكنولوجيا على انتشار هذا النوع من الجرائم، و تبيان صعوبة إيجاد أدلة الإثبات لهذا النوع من الجرائم، و تحليل النتائج المتوصل إليها للخروج بجملة من الاقتراحات.

خطة الدراسة :

تم تقسيم هذه الورقة البحثية إلى محوريين أساسيين:

المحور الأول : مفهوم الجريمة المعلوماتية

المحور الثاني : التنظيم القانوني للجريمة المعلوماتية

المحور الأول

مفهوم الجريمة المعلوماتية

إن الجريمة ظاهرة اجتماعية ارتبطت في طبيعتها وحجمها بالتحولات المختلفة سواء كانت اقتصادية، اجتماعية وثقافية، الوطنية منها أو الدولية. ومن التحولات الجذرية التي شهدها عصرنا الحالي والتي ساهمت و بطريقة قياسية في ارتقاء البشرية إلى مستويات عليا، ما يسمي بالثورة المعلوماتية و هي الثورة التي تزاوجت فيها شبكات الاتصال بما وصلت إليه من تطور مع الحاسوب ذاك الجهاز الذي يمتلك قدرات هائلة للقيام بالعديد من الوظائف وفي ظرف قياسي . هذا التمازج الذي مكن الملايين من البشر الاتصال يبعضهم البعض و أتاح لهم الفرص للاطلاع على المعلومات و تبادلها ،القدرة على التفاوض وإبرام العقود و الصفقات في ظل بيئة تحاكي واقع البشرية و هي البيئة الافتراضية أو الرقمية Kغير انه و في المقابل أنتجت هذه الثورة نمط جديد من الإجرام صنف في سياق الجرائم المستحدثة و هي الجرائم المعلوماتية أو الالكترونية و هي جرائم تمس في صميمها قيما جوهرية تخص الأفراد والمؤسسات، و حتى

الدول و في جميع مناحي الحياة ، الأمر الذي خلف شعورا بعد الثقة بخصوص التعامل و الاستفادة من ثمار الثورة المعلوماتية.[4]

تعد الجريمة المعلوماتية من الجرائم المستحدثة في الوقت الراهن التي ظهرت كرد فعل متوقع للتطور السريع الحاصل في مجال الثورة التكنولوجية و المعلوماتية،

اولا- تعريف الجريمة المعلوماتية: لقد تباينت التعريفات المتعلقة بالجريمة المعلوماتية تباين المصطلحات التي اطلقت عليها فهي نتيجة تطور ظاهرة الاجرام المرتبط بتقنية المعلومات[5]تتكون مصطلح الجريمة المعلوماتية من الجريمة و مصطلح المعلوماتية، فمصطلح الجريمة يستخدم للتعبير عن السلوكيات و الأفعال الخارجة عن القانون.

أما مصطلح المعلوماتية أو علم المعلومات فهو يهتم بالموضوعات و المعارف المتصلة باصل المعلومات و تجميعها و تنظيمها و تخزينها و استرجاعها و كذا تحويلها و استخدامها، و قد تعددت الاسماء التي اطلقت على هذا النوع من الجرائم فهناك من يسميها سيبر كرايم و البعض جرائم الهاكرز و آخرون جرائم الكمبيوتر أو جرائم الحسابات، و لكن التسمية الاكثر شيوعا هي جرائم الكمبيوتر "فهي تلك الجرائم التي ترتكب باستخدام الحاسوب و الشبكات و المعدات التقنية مثل الجوال"[6]

و قد ظهر اتجاهين كلاهما يعطيان تعريف للجريمة المعلوماتية كل حسب وجهة رايه

أ- الاتجاه الأول- الاتجاه الضيق لمفهوم الجريمة المعلوماتية:

و لقد اخذ هذا الاتجاه بمعيار وسيلة ارتكاب هذه الجريمة أي "الكمبيوتر"فهي كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية و لملاحقته من

---

[4] معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة المفكر، المجلد 13، العدد 01، سنة 2018 ص ص 397-417

[5] معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة الفكر، العدد 17 ،جوان 2018، ص 400 ()

[6] صليحة بوجادي، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، المجلد 07 العدد01، سنة 2021، ص ص 2526- 2543.

ناحية أخرى" بمعنى أنها كل جريمة :"تقع على جهاز الكمبيوتر أو داخل نظامه فقط أي كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب"[7]

و هناك فقه آخر ضيق مفهوم الجريمة الالكترونية في معيار النتيجة المحققة بقولهم أنها "تلك الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح" فهي "كل نشاط غير مشروع موجه للنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي بتغييرها أو حذفها"

و هناك من ركز على معيار موضوع الجريمة أي هي الدراية الكافية و الكفيلة لاختراق أي جهاز كمبيوتر و قرصنته و سرقة معلوماته المخزنة فهذه الجريمة مرتبطة بالمعرفة الفنية و التقنية للكمبيوتر[8]

و عليه فان هذا الاتجاه جاء قاصر للاحاطة بالجريمة المعلوماتية فمنهم من يركز على معيار الوسية فقط و البعض على معيار النتيجة و الاخرون على معيار موضوع الجريمة

ب- الاتجاه الثاني- الموسع لمفهوم الجريمة المعلوماتية :

لقد تباينت آراء انصار هذا الاتجاه في تعريف الجريمة المعلوماتية فحاول البعض تعريف اوسع لـ هذه الجريمة بحسب الدرجة التي يمكن أن تمتد اليها الجريمة المعلوماتية، فعرفها ان " كل سلوك اجرامي يتم بمساعدة الكمبيوتر" أو هي "كل جريمة تتم في محيط اجهزة الكمبيوتر"أي أنها "كل فعل أو امتناع عمدي ، ينشا عن استخدام غير المشروع لتقنية المعلوماتية، يهدف الى الاعتداء على الأموال المادية أو المعنوية" ، و قد جاء هذا التعريف موافقا للتعريف الذي جاءت به منظ مة التعاون الاقتصادي و التنمية في اوروبا التي عرفت الجريمة المعلوماتية :" كل فعل أو امتنا ع عن فعل من شانه الاعتداء على الأموال المادية او المعنوية، يكون ناتجا بطريقة مباشرة أو غ ير مباشرة عن تدخل التقنية المعلوماتية"[9] و منه فقد ركز انصار هذا التعريف بالافعال المتصلة بجرائم محتويات الكمبيوتر لتحقيق مكاسب شخصية او مالية او اي ضرر .

---

[7] نائلة عادل محمد فريد فورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، الاسكندرية، 2014، ص120.

[8] عادل يوسف، عبد النبي البشكري، الجريمة المعلوماتية و أزمة الشرعية الجزائية، العدد السابع،الكوفة،ص113.

[9] بوجادي صليحة ، المرجع السابق، ص 2529.

حيث تقوم ككل الجرائم على أركان و هي الركن المادي اي استخدام الانظمة الالكترونية بطريقة غير مشروعة كالتلاعب في البيانات المرتبطة بالحواسيب الآلية، او السرقة لبطاقات الائتمان ، كذلك الركن المعنوي فهو سوء نية مستخدم الكمبيوتر، و يبقى الركن الشرعي الذي يمثل الصفات غير المشروعة للفعل، حيث يكون هنالك قاعدة تجريم و عقوبات مفروضة على الجرائم الالكترو نية المرتبطة بانظمة المعلومات.

ت- موقف المشرع الجزائري من تعريف الجريمة الالكترونية :

تبنى المشرع الجزائري الجريمة المعلوماتية و اصطلح عليها ب :"الجرائم المتصلة بتكنولوجيا الا علام و الاتصال" اذ اعتبر ان النظام المعلوماتي في حد ذاته و ما يحتويه من مكونات غير ماد ية "محلا للجريمة" و يمثل نظام المعالجة الآلية للمعطيات الشرط الاول الذي لابد من تحققه حت ى يتوافر اركان الجريمة و بالرجوع الى قانون العقوبات الجزائري نجده لم يعرف جرائم الانترنت ب ل اكتفى على بتحديد العقوبة على بعض الافعال تحت عنوان": الجرائم الماسة بنظام المعالجة ا لآلية للمعطيات" و ذلك في المادة 394 مكرر الى 394 مكرر 7 منه، و بذلك يكون المشرع ال جزائري قد تعريفا موسعا للجرائم المعلوماتية في القانون 04/09 معتبرا اياها انها تشمل بالاضافة الى جرائم المساس بانظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات – المواد المش ار اليها سابقا- اي جريمة اخرى ترتكب او يسهل ارتكابها بواسطة معلوماتية او نظام للاتصالا ت الالكترونية" [10]و يجب التنويه هنا ان المشرع قد تطرق ايضا الى الجرائم الالكترونيى و العقوب ات المقررة لها من خلال قانون التجارة الالكترونية 05/18 و ذلك في الفصل الثاني من الباب ا لثالث منه تحت عنوان "الجرائم و العقوبات و شملتها المواد من 37 الى 48 [11]

ثانيا- الطبيعة الخاصة للجريمة الالكترونية :

لقد أضفى التطور الهائل لتقنية المعلومات واندماجها بتقنية الاتصالات فيما بعد طبيعة خاصة ع لى جرائم كانت تقليدية قبل ظهورها، وأدى إلى ظهور أنماط مستحدثة من الأفعال الجرمية تباين ت التعبيرات والاصطلاحات للدلالة على هذه الجرائم تباين رافق مسيرة ونشأة تلك التقنية، وأحاط

---

[10] صليحة بوجادي، المرجع السابق، ص 2530

[11] القانون رقم 05/18 المؤرخ في 10 مايو 2018 المتعلق بالتجارة الالكترونية ، الجريدة الرسمية عدد 28، الصادرة في 16 ماي 2 018.

بها الكثير من التساؤلات التي تتعلق بتحديد ماهيتها باعتبارها جريمة مستحدثة ومتميزة عن باقي الجرائم التقليدية من خلال موضوعها وخصائصها، وكذلك تعدد المحاولات الرامية إلى تصنيفها وتحديد صورها المختلفة[12].

و من ثم فان للجريمة المعلوماتية طبيعة خاصة قانونية تكمن في الخصائص التي تتميز بها هذه الجريمة، كما للجريمة الالكترونية خصوصية معينة قد تظهر على مستويات[13]:

أ- خصوصية على التجريم و العقاب:

فالجريمة الإلكترونية هي الجريمة ذات الطابع المادي، التي تتمثل في كل سلوك غير قانوني مرتبط بأي شكل بالأجهزة الإلكترونية ، يتسبب في حصول المجرم على فوائد مع تحميل الضحية خسارة ، ودائماً يكون هدف هذه الجرائم هو سرقة وقرصنة المعلومات الموجودة في الأجهزة، أو تهدف إلى ابتزاز الأشخاص بمعلوماتهم المخزنة على أجهزتهم المسروقة،والجريمة الإلكترونية لها مسميات عدة منها.

عندما نتحدث عن الجريمة الإلكترونية Cyber crime أو جرائم تقنية المعلومات، فإننا نقصد الفعل الإجرامي الجديد الذي ظهر مع التطور التكنولوجي والطفرة النوعية الرقمية التي بات يعرفها الفضاء التواصلي المفتوح عبر الإنترنت، وبالتالي صار الحديث عن وجود فعل جُرمي مرتبط أساسا بهذه الثورة حيث تدفُّقُ المعلومات وحيث المعطيات الخاصة والعامة أضحت مُشرعة وفي متناول الجميع!

ففي ظل التطور التكنولوجي، كان من الطبيعي أن يُفرز المجتمع فئات جديدة متطورة في تعاملها الإجرامي، ذاك الذي أسميه شخصيا بالإجرام العلمي الذي يستلزم معرفة علمية معلوماتية دقيقة ومتطورة جدا، مواكبة للتطور الحاصل في الفضاء الرقمي الافتراضي. فهو يتجه صوب المعلومة مباشرة، تلك التي تعتبر أساس الجريمة الإلكترونية.[14]

---

[12] بثينة حبيباتني، الطبيعة الخاصة للجريمة المعلوماتية، مجلة دراسات و ابحاث، المجلد 12، العدد 03،سنة 2020، ص ص 721-730

[13] نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، رسالة ماجستير في القانون العام، كلية الدراسات العليا ، جامعة النجاح الوطنية نابلس- فلسطين، سنة 2017، ص20.

[14] حسن يوسفي المغاري، التكنولوجيا الحديثة في خدمة الإجرام ، مقال منشور عبر الموقع التالي: https://www.aljazeera.net ساعة الاطلاع 19:53 تاريخ الاطلاع 2022/07/20

ب- خصوصية على مستوى التتبع و الملاحقة:

لا شك أن للجريمة الإلكترونية أبعادا مرتبطة بالحياة الخاصة والعامة للفرد. فمنها ما هو اقتصادي وما هو اجتماعي وما هو سياسي، وما دمنا نتحدث عن الجريمة الإلكترونية، فهي غالبا ما تكون مرتبطة بعالم الاقتصاد الرقمي بالدرجة الأولى، المعلومة إذن هي الهدف الأول والأخير، بحيث أن سمات العالم الافتراضي الرقمي يعتمد أساسا المعلومة كأداة للتعامل، ومسرح الجريمة نفسه هو العالم الرقمي، بل وأدوات الجريمة هي أيضا من وإلى العالم الافتراضي العلمي المعلوماتي،إن احدى اهم مميزات الجريمة المعلوماتية و اكثر ما يجعلها جريمة محنكة هي صعوبة اكتشافها باعتبارها نادرا ما يتم الكشف عنها، خاصة و انه اثناء ارتكابها لا يشوبها اي عمل من اعمال العنف، كما انها لا تترك اثرا خارجيا ملموسا او مرئيا، لقيام الجاني بحجب السلوك و اخفائه عن طريق التلاعب في البيانات او التصحيح و التعديل و المسح و التخزين و الاسترجاع و الطباعة.

صعوبة الاثبات : [15]

ت- جريمة عابرة للحدود: إن اغلب الجرائم الالكترونية يختلف فيها الجاني و المجني عليه في مقر السكن ، فنجد مثلا الجاني الجاني من روسيا و المجني عليه من امريكا، ما يعني تعارض المواد المنظمة للجريمة، و يعني وجود تعقيدات بخصوص الملاحقة القضائية ، و من امثلة هذه الخاصية عرفت باسم مرض فقدان المناعة المكتسبة "الايدز" المرتكبة من قبل الامركي جوزيف بيب، و الذي قام بارسال فيوس الى اشخاص من المملكة المتحدة، و قد القي القبض عليه في أوهايو و عرض اما القضاء الانجليزي الذي اطلق سراحه نظرا لتدهور حالته العقلية، و عليه فان هذه الحماية غير مقصودة تستدعي ضرورة التعاون الدولي لمواجهة هذه الجرائم، و وضع المجرمين عند حدهم[16]،المجرم الإلكتروني مُتخصص، يتوفر على مهارة عالية في مجال المعلوميات والبرمجة، مهارة في اختراق الشبكات، مهارة فائقة في كسر الشفرات وكلمات المرور، مهارة خارقة في الوصول إلى المعلومات الدقيقة والحصول عليها. يشتغل بسرية تامة ويُشَغّل أجهزة عن بُعد ومن خلال ارتباط بشبكة الإنترنت، و يمتكلك ذكاء وتجربة ودهاء في تطوير وتعديل الأنظمة الأمنية المعلوماتية، والمجرم الإلكتروني إذن هو مُجرمٌ عابر للحدود، إنه الإجرام المُعولم!،فالمُجرم المعلوماتي، وهو الفاعل الرئيسي للعملية الجُرمية الإلكترونية، يتمتع بذكاء

---

[15] بن شهرة شلول، مراد مشوش، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية و السياسية، المجلد الرابع، ا لعدد01، جوان 2020، ص 06 (01-21)

[16]صليحة بوجادي، المرجع السابق، ص 2532.

وبدراية معلوماتية وبدهاء،إذ أن مسرح الجريمة الإلكترونية هو الفضاء الرقمي، وبالتالي فإن ذلك المسرح هو مسرحٌ للأذكياء، وأداة الجريمة تكون هي الحاسوب المرتبط بالشبكة العالمية. وعليه فإننا بصدد الحديث عن الجريمة العابرة للحدود.

ث- جريمة خفية و سريعة الارتكاب: تتسم الجرائم الناشئة عن استخدام الانترنت بانها خفية و مستترة في اغلبها ، لان الضحية لا يلاحظ رغم انها تقع اثناء وجوده في الشبكة، لان الجاني يتمتع بقدرات فنية تمكنه من جريمته بدقة ، مثلا عند ارسال الفيروسات المدمرة و سرقة الاموال و البيانات الخاصة او اتلافها، و التجسس و سرعة المكالمات و غيرها من الجرائم، فجرائم الانترنت في اكثر صورها خفية لا يلاحظها المجني عليه[17]

المحور الثاني

التنظيم القانوني للجريمة المعلوماتية

إن تأخر المشرع الاجزئري مقارنة مع بقية التشريعات الوطنية الأخرى في معاجلة الجريمة الالكترونية والتصدي لها الا ان تطور وسائل الاتصال وتشعبها والاعتماد عليها في المعاملات و العلاقات الاجتماعية بشكل كلي سواء تلكبمواقع التواصل الاجتماعي أو الوسائل المعلوماتية وفي ضل تزايد خطورة هذه الجرائم على الدولة والمجتمع واستجابة لتوقيع اجلزائر على المعاهدات الدولية و االاقليمية التي تكافح هذه الظاهرة بادر المشرع اجلزائري الى سن مجموعة من االقوانين من أجل مكافحة الجرائم المتعلقة ببالحاسب الآلي، بما يساعد على مكافحة هذه الجريمة وتعاقب مرتكبيها وطنيا ودوليا[18].

رغم إيجابيات الحاسب الآلي و الشبكة المعلوماتية الدولية إلا أنه تولدت عنهما العديد من الأنماط السلبية أذكر منها الجريمة المعلوماتية ، حيث تنوعت أساليب ارتكابها و تزايدت مخاطرها و حجم الخسائر الناتجة عنها فباتت تشكل مصدرا من مصادر تهديد الاقتصاد و الأمن القومي ومساسا بحرمة الحياة الخاصة وكذا النظام والآداب العامة ، ومع ذلك فالتشريعات العربية لم تتطرق لها إلا فيما ندر، و عليه ولتصدي لهذا النوع المستحدث من الجرائم لابد من

---

[17] عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري و التشريع المقارن، مجلة الحقوق و الحريات ص 73

[18] بدر الدين خلاف، التنظيم القانوني للجريمة المعلوماتية في الجزائر، مجلة العلوم القانونية و الاجتماعية، المجلد السادس، العدد الثا ني، جوان 2021، ص 332 (331- 346)

الخوض فيها من كافة جوانبها. و قد اقتصرنا نحن على الجانب الأكثر قيمة وأهمية فيها و هو دليل إثباتها إذ به تثبت الإدانة أو البراءة، كما أن هذا الدليل يختلف تماما عن الدليل الجنائي في الجرائم التقليدية و ذلك من حيث طبيعته الخاصة ، المتمثلة في الكم الهائل من البيانات المدونة في جهاز الحاسب الآلي لذلك حددنا كيفية البحث و الكشف عن الدليل وكذا حمايته للوصول إلى الهدف الأسمى وهو القبض على مرتكبها[19].

اولا- اركان الجريمة المعلوماتية: تقوم الجريمة المعلوماتية على ثلاث اركان معينة مثلها مثل الجرائم التقليدية الا من حيث محلها تتمثل في :

أ- **الركن المادي:** ينصب على استعمال الحاسب الآلي في صورة تدمير معلومات او اتلاف عمدي للمعلومات المخزنة في هذا الحاسب، او سرقة هذه المعلومات او سوء استخدام الكمبيوتر بطريقة غير مشروعة من اقتحام و تدمير المعلومات ، او سرقة لبطاقات الائتمان او التزوير و التلاعب في البيانات المرتبطة بالحواسيب الآلية .

وقد أجمع فقهاء القانون الدولي على أن تزوير أو إتلاف مُستند، أو سجل أو توقيع إلكتروني أو نظام إلكتروني أو موقع، والاستيلاء على منفعة أو مال أو مُستند باستعمال طرق احتيالية، أو إعاقة أو تعطيل الوصول إلى موقع أو الدخول إلى الأجهزة أو البرامج أو مصادر البيانات، تعتبر كلها ضمن الجريمة الإلكترونية. وبالإجمال يبقى التعريف العام المتمثل في كون الجريمة الإلكترونية هي جميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات دورا أساسيا

ب- **الركن المعنوي:** اي توافر القصد الجنائي فيكون الجاني عالما بكافة عناصر الجريمة التي يرتكبها، و تكون لشخصية الجاني دور اساسي في ارتكاب الجريمة حيث لابد من ان يكون ذو دراية و معرفة بالنظام الآلي قصدا احداث ضرر للمجني عليهحيث يشترط المشرع ان يكون

---

[19] سحتوت نادية ، التنظيم القانوني للجريمة المعلوماتية أدلة إثبات الجريمة المعلوماتية، مجلة دراسات و أبحاث، المجلد 01، العدد 1، سنة 2009، ص ص 48-54

الجاني عالما بنشاطه الاجرامي، فهو الحالة النفسية و المزاجية لمرتكبي الجرائم الالكترونية مع اهمية التركيز بين ماديات الجريمة و شخصية الجاني.

ت- الركن الشرعي: يقوم على وجود الصفة غير المشروعة للافعال المادية الصادرة عن الجاني، حيث يقوم الركن الشرعي على مبدا الشرعية الجنائية الذي يمنع المساءلة الجنائية ما لم يتوفر النص القانوني لذلك، مع وجود نصوص قانونية قاصرة لمعالجة كافة الاشكالات المتعلقة بجرائم المعلومات لسرعة تطورها فالتعدي على حرمة الحياة الخاصة عبر الانترنت لا يعد جريمة لان قانون العقوبات يشترط ارتباطها بمكان خاص، كذلك تجميع المعلومات عن الافراد و تسجيلها في الكمبيوتر لا يخضع للتجريم وفقا للقواعد العامة، الى جانب التداخل في نظام الحاسب الالي و تغيير المعلومات تعد صور جديدة لا يعرفها قانون العقوبات، و هذا يعني قصور القواعد التقليدية في مكافحة هذه الجرائم[20]، حيث يكون هنالك قاعدة تجريم و عقوبات مفروضة على الجرائم الالكترونية المرتبطة بانظمة المعلومات.

أولا- أهمية أدلة الإثبات الالكترونية :

يعتبر التطور الذي مس مختلف المجالات في القرن الواجد والعشرين ، والذي بدوره أثر على مجال المراجعة بنوعيها سواء الداخلية او الخارجية ، حيث اصبحت تستخدم تكنولوجيا المعلومات والنظام الالكتروني لتتماشى الواقع العملي المعمول به في وقتنا الحالي، وبطبيعة الحال لا يمكن أن تتغير الاهداف والنتائج المراد الحصول عليها من القيام بعملية المراجعة وهذا عند استخدام التشغيل الالكتروني للبيانات بدلات من الأوراق والمستندات الورقية الملموسة أي الطريقة العادية. لان عند استخدام التكنولوجيا الرقمية والبرامج والتطبيقات المستعملة في عملية المراجعة فإنها تساهم بشكل كبير في فاعلية وكفاءة عملية المراجعة وكما تساهم في تطوير أداء وجودة عمل المراجعة[21].

---

[20] بدر الدين خلاف، المرجع السابق، ص 337.

[21] شاهد الياس، ادلة الإثبات في عملية المراجعة الالكترونية، دراسة مقارنة بين ادلة الإثبات العادية و ادلة الإثبات الالكترونية، مجلة الدراسات المالية و المحاسبية و الإدارية، المجلد 04، العدد 02، سنة 2017، ص ص 277-288.

الجرائم الالكترونية جرائم مستحدثة بلغ منها من التطور الحد الذي يجعل لمسة زر فقط كافية لاسقاط اقوى الانظمة الحماية و تشفير المعلومات الاكثر سرية، و بسبب اختلاف الاساليب المستعملة في خرق الحواجز الامنية، صعب تصنيف مجرمي المعلومات فهناك عدة انماط اهمهم القراصنة و هم نواعان قراصنة هواة و ما يطلق عليهم ب"**الهاكرز**" فهم اشخاص يدخلون النظام الالكتروني لارضاء رغباتهم بدون تخريب للمعطيات الموجودة داخل النظام" و هناك قراصنة محترفون او " **الكراكرز**" **ف**هؤلاء مجرمين مخربين للانظمة يسعون للاستلاء على بطاقات الائتمان و استخدامها و تدمير او تشفير الملفات المهمة، سرقة التفاصيل الشخصية و بيعها، و يطلق عليهم اسم العناكب " SPIDERS لانهم يعملون في الخفاء.

هناك صعوبة في اثبات وقوع الجريمة ،حيث ان في حال اكتشاف الجريمة فان اثباتها امر يحيط الكثير من الصعاب، فالجريمة المعلوماتية تتم في بيئة غير تقليدية حيث تقع خارج اطار الواقع المادي الملموس لتقوم اركانها في بيئة الحاسوب و الانترت مما يجعل الامور تزداد تعقيدا لدى الجهات المختصة، و تجدر الاشارة الى ان وسائل المعاينة و طرقها التقليدية لا تفلح غالبا في اثبات هذه الجريمة نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالاخيرة لها مسرح تجري عليها الاحداث، حيث تختلف آثار مادية تقوم عليها الادلة و هذا المسرح يعطي المجال امام السلطات الاستدلال و التحقيق و الكشف عن الجريمة، و ذلك عن طريق المعاينة و التحفظ على الآثار المادية التي خلفتها الجريمة، خاصة و ان الجريمة الالكترونية لا تخلف آثار مادية كما ان يعقل ورود الكثير من الاشغال مكان الجريمة في الوقت نفسه زمان وقوع الجريمة و حتى اكتشافها الامر الذي يعطي المجال للجاني ان يغيروا و يتلفوا و يعبثوا بالآثار المادية الامر الذي يورث الشك في دلالة الادلة المستسقاة من المعاينة في الجريمة المعلوماتية.[22]

ثانيا – دور المشرع الجزئري في مكافحة الجريمة المعلوماتية:إن تأخر المشرع الجزائري مقارنة مع بقية التشريعات الوطنية الأخرى في معالجة الجريمة الإلكترونية والتصدي لها إلا أن تطور وسائل الاتصال وتشعبها والاعتماد عليها في المعاملات والعلاقات الاجتماعية بشكل كلي سواء تلك المتعلقة بمواقع التواصل الاجتماعي أو الوسائل المعلوماتية وفي ضل تزايد خطورة هذه الجرائم على الدولة والمجتمع واستجابة لتوقيع الجزائر، على المعاهدات الدولية و

---

[22]بن شهرة شول، مراد مشوش، المرجع السابق، ص 2548.

الإقليمية التي تكافح هذه الظاهرة بادر المشرع الجزائري إلى سن مجموعة من القوانين من أجل مكافحة الجرائم المتعلقة بالحاسب الآلي، بما يساعد على مكافحة هذه الجريمة وتعاقب مرتكبيها وطنيا ودوليا[23].

لقد جرم المشرع الجزائري الافعال الماسة بنظام المعالجة الآلية للمعطيات ما سميت بالغش المعلوماتي ، بوجب القسم السابع مكرر من قانون العقوبات المعدل بالقانون رقم 06-23 المؤرخ في 20-12-2006 في المواد 394 مكرر الى 394مكرر 7 ، فقد عاقب بالحبس من 03 اشهر الى سنة و بغرامة من 50000دج الى 200000دج ، كما تطبق العقوبات ذاتها على المحاولة، و تضاعف العقوبة اذا ترتب عن ذلك حذف او تغيير لمعطيات المنظومة، اما اذا ترتب عنها تخريب نظام اشتغال المنظومة تكون العقوبة من ستة اشهر الى سنتين و الغرامة من 50000الى 300000دج، و تعاقب المادة 394 مكرر 1 على المساس بمنظومة معلوماتية بالحبس من ستة اشهر الى ثلاث سنوات و بغرامة من 50000دج الى 400000دج.

في حين نصت المادة 394 مكرر 02 على عقوبة الحبس من شهرين الى ثلاث سنوات و بغرامة من مليون الى عشرة ملايين دج لكل من يقوم عمدا و بطريق الغش بتصميم او بحث او تجميع او توفير ،او نشر ،او الاتجار في معطيات مخزنة او معالجة او مراسلة عن طريق منظرمة معلوماتية يمكن ان ترتكب بها احدى الجرائم المذكورة اعلاه، و قد عاقب المشرع الشخص المعنوي بموجب المادة 394 مكرر 4 بغرامة تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي عند ارتكابه لهذه الجريمة، و قد تضمنت نفس المادة مكرر 03 مضاعفة العقوبة المقررة للجرائم الغش المعلوماتي، اذا استهدفت الجريمة الدفاع الوطنياو الهيئات او المؤسسات الخاضعة للقانون العام.

اما اذا تمت الجريمة في شكل تجمع بغرض الاعداد للجريمة المعلوماتية و تجسد ذلك في فعل مادي او اكثر معاقب عليه بعقوبة الجريمة ذاتها، و اقرت المادة السالفة الذكر مكرر 06 بمصادرة الاجهزة و البرامج و الوسائل المستخدمة مع اغلاق المواقع التي تكون محلا

---

[23] خلاف بدر الدين، التنظيم القانوني للجريمة المعلوماتية في الجزائر، مجلة العلوم القانونية و الاجتماعية، المجلد 06، العدد02،سنة 2021، ص ص 331-346.

للجريمة من جرائم الغش المعلوماتي، علاوة على اغلاق المحل او المكان التي ارتكبت فيه الجريمة .

اما فيما تعلق بالجرائم الماسة بنظام المعالجة الآلية للمعطيات فنجد المشرع الجزائري قد عاقب هذه الجرائم و ادرجها ضمن القسم السابع مكرر من قانون العقوبات و ذلك في المادة 394 مكرر 7 و التي اعتبرت الشخص مجما من خالل:

– فعل الدخول او البقاء عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعلومات او محاولة ذلك، او متى ترتب عنه تغيير معطيات المنظومة او حذف نظام التشغيل او تخريبه.

– الادخار او الازالة بطريقة الغش لمعطيات في نظام المعالجة الآلية للمعلومات .

– القيان عمدا عن طريق الغش بتصميم او بحث او توفير ،نشر ، او الاتجار بمعطيات مخزنة او معالجة او مرسلة عن طريق منظومة معلوماتية يمكن ان ترتكب بها الجرائم الماسة بانظمة المعالجة الآلية للمعطيات.

– حيازة او افشاء او نشر او استعمال لاي غرض كان المعطيات المتحصل عليها من احدى الجرائم الخاصة بانظمة المعالجة الآلية للمعطيات.

– المشاركة في مجموعة او اتفاق بغرض الاعداد لجريمة من الجرائم المنصوص عليها الخاصة بانظمة المعالجة الآلية لمعطيات.

اما بخصوص مستجدات الاجراءات المتخذة لمكافحة جرائم المعلومات فقد اورد المشرع الجزائري جملة من الاجراءات للبحث و التحري عن الجريمة اهمها

– جواز التفتيش و المعاينة و الحجز لكل محل سكني او غير سكني طبقا للمادة 47 من قانون الاجراءات الجزائية.

– جواز التفتيش في كل وقت ليلا او نهارا باذن مسبق من وكيل الجمهورية المختص.

– جواز الاخلال بقواعد التفتيش في الجريمة المتلبس بها اذا كان الشخص الذي يتم تفتيش مسكنه موقوفا او محبوسا حالة عدم امكان نقله لمخاطر تتعلق بالنظام العام او احتمال الفرار او الخوف من اختفاء ادلة، و يتم تفتيش باذن وكيل وكيل الجمهورية او قاضي التحقيق و بحضور شاهدين او ممثل معين صاحب المسكن، حسب المادة 47 مكرر من قانون الاجراءات الجزائية.

– جواز تمديد الوقف تحت النظر لمدة 48 ساعة اخرى و فقا للمادة 51 من قانون الاجراءات الجزائية.

– جواز اتباع طرق اعتراض المراسلات عن طريق اذن من وكيل الجمهورية بالكيفيات المحددة في المواد 65مكرر 5حتى 65مكرر10 من قانون الاجراءات الجزائية.

– جواز اتباع طريقة التسريب وفقا للمواد 65 مكرر 11 حتى 65مكرر18 من قانون الاجراءات الجزائية.

خاتمة

ازدهار الحضارة وانتشار التقدم التقني ساعد في تسهيل الكثير والكثير من أمور حياتنا ولكنه في نفس الوقت جلب لنا العديد من المخاطر والأضرار المتعلقة بالحواسيب والشبكة العنكبوتية ، مما جعل الحكومات والمجتمعات تنتبه إلى ضرورة نشر التوعية والتعريف بهذه الجرائم عن طريق شرحها وتحليلها للناس وبيان وسائل وطرق الوقاية منها.

في ظل هذا النمو المستمر للثورة المعلوماتية الذي يعيشه عصرنا ويشهده حاضرنا أصبحنا نواجه العديد من الأخطار والمشاكل التي تنشأ بشكل تلقائي مع أي تطور حضاري وتقني . فدخول الإنترنت في عالمنا وتمكن الصغير والكبير والجاهل والمتعلم من استخدامه دون أي قيود أو رقابة أدى إلى زيادة هذه الأخطار وتفشى النهب والسرقات الإلكترونية بشكل ملحوظ ؛ ولحفظ الحدود وزيادة الحماية وجب سن القوانين التي ترغم المجرمين على التزام حدودهم ، ولكننا وجدنا أن أكبر عائق كان ولازال يواجه هذه القوانين هو تطبيقها على أرض الواقع وبشكل فعلي ؛ وذلك بسبب جهل الناس بها ؛ لأنها قوانين مستجدة وحديثة لجرائم غير معهودة وليست كغيرها من

الجرائم ، فكان من أهم خطوات تطبيق هذه القوانين هو توعية الناس بالجرائم الإلكترونية وما تسببه من أضرار .

لا شك أن للجريمة الإلكترونية أبعادا مرتبطة بالحياة الخاصة والعامة للفرد. فمنها ما هو اقتصادي وما هو اجتماعي وما هو سياسي، وما دمنا نتحدث عن الجريمة الإلكترونية، فهي غالبا ما تكون مرتبطة بعالم الاقتصاد الرقمي بالدرجة الأولى، ثم الحياة الشخصية والشأن العام والشأن السياسي.

التوصيات المقترحة:

– اجراء دورات تكوين لافراد مكافحة الجرائم الالكترونية، و تنمية وعي الثقافة المعلوماتية للعاملين في مجالات العدالة الجنائية من خلال عقد الندوات المتخصصة و الدورات التدبيرية لهم في هذا المجال.

– وجوب فتح تخصصات في الجامعات الجزائرية لدراسة الحماية القانونية للمعلوماتية او تحت مسمى آخر قنون الحاسب الآلي و الانترنت.

– تفعيل احدث التقنيات و الوسائل للكشف عن هوية مرتكبي الجرائم المعلوماتية.

– لابد للمشرع الجزائري من ضبط جميع نماذج الجريمة الالكترونية و تقرير صور العقاب عليها و كذلك توسيع دائرة الاجراءات الجزائية للبحث و التحري عن الجريمة تكون اوسع من تلك التقليدية.

– تطوير ثقافة الحاسب الآلي لدى رجال الامن للقدرة على السيطرة الامنية على الكراكز و الهاكرز و اكتشافهم.

– انشاء فرق متصصة من خبراء الكمبيوتر لمكافحة الجريمة المعلوماتية .

– العمل على توسيع اجهزة الرقابة الالكترونية في كافة المؤسسات و الهيئات و الشركات للكشف عن الجريمة في وقتها.

– تعزيز التعاون و التنسيق مع المؤسسات الدولية المعنية بمكافحة الجرائم المعلوماتية و العمل على دراسة و متابعة المستجدات على الساحة العالمية.

- **أهم المراجع المعتمدة:**

- **المؤلفات العلمية:**

1. نائلة عادل محمد فريد فورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، الاسكندرية، 2014
2. عادل يوسف، عبد النبي البشكري، الجريمة المعلوماتية و أزمة الشرعية الجزائية، العدد السابع،الكوفة

- **المجلات العلمية:**

1. جبار صلاح الدين ،شرقي محمود، تأثير تطور تكنولجية المعلوماتية على تنامي الجريمة، مجلة الآداب و العلوم الاجتماعية، المجلد 08،العدد 01 سنة 2015، ص ص 179-193
2. طالة لامية، سلام كهينة، الجريمة الالكترونية، بعد جديد لمفهوم الإجرام عبر منصات مواقع التواصل الاجتماعي، مجلة الرواق، المجلد06،العدد2، سنة 2020، ص ص 62-91.
3. حميدة راضية، الجريمة الالكترونية عبر مواقع التواصل الاجتماعي...نحو تفعيل دور الأمن السيبراني المعلوماتي، مجلة الإعلام و المجتمع، المجلد 05،العدد02، سنة 2021، ص ص 338-356.
4. معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة المفكر، المجلد 13، العدد 01، سنة 2018 ص ص 397-417
5. صليحة بوجادي، الإطار المفاهيمي للجريمة المعلوماتية، مجلة الدراسات القانونية المقارنة، المجلد.
6. بثينة حبيباتني، الطبيعة الخاصة للجريمة المعلوماتية، مجلة دراسات و ابحاث، المجلد 12، العدد 03،سنة 2020، ص ص 721-730
7. سحتوت نادية ، التنظيم القانوني للجريمة المعلوماتية أدلة إثبات الجريمة المعلوماتية، مجلة دراسات و أبحاث، المجلد 01، العدد 1، سنة 2009، ص ص 48-54
8. خلاف بدر الدين، التنظيم القانوني للجريمة المعلوماتية في الجزائر، مجلة العلوم القانونية و الاجتماعية، المجلد 06، العدد02،سنة 2021، ص ص 331-346
9. بن شهرة شلول، مراد مشوش، السمات الخاصة للجريمة المعلوماتية، مجلة المستقبل للدراسات القانونية و السياسية، المجلد الرابع، العدد01، جوان 2001، 2543- 3865.
10. عبد المومن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري و التشريع المقارن، مجلة الحقوق و الحريات ص ,
11. بدر الدين خلاف، التنظيم القانوني للجريمة المعلوماتية في الجزائر، مجلة العلوم القانونية و الاجتماعية ، المجلد السادس، العدد الثاني، جوان.
13. سحتوت نادية، أدلة إثبات الجريمة المعلوماتية، مجلة دراسات ،المجلد01،العدد01، 2009، ص ص 48 – 54.

الرسائل العلمية:

1. نداء نائل فايز المصري، خصوصية الجرائم المعلوماتية، رسالة ماجستير في القانون العام، كلية الدراسات العليا ، جامعة النجاح الوطنية نابلس– فلسطين، سنة 2017، ص20.

– المواقع الالكترونية:

1. حسن يوسفي المغاري، التكنولوجيا الحديثة في خدمة الإجرام ، مقال منشور عبر الموقع التالي: https://www.aljazeera.net ساعة الاطلاع 19:53 تاريخ الاطلاع 2022/07/20

الملتقى الدولي الافتراضي الموسوم

بـ :القانون الجنائي في ظل التطور التكنولوجي

– إشكالات ومعالجات–.

يومي : 28 و 29 سبتمبر 2022

المحور الثاني:

أثر استخدام التكنولوجية الحديثة على أحكام التجريم

عنوان المداخلة:

موقف بعض التشريعات العقابية من جرائم تكنولوجية المعلومات.

د:فغول عربية أستاذة محاضرة أ

(كلية الحقوق والعلوم السياسية "علي لونيسي"

– جامعة البليدة 2–

Email :fegholarbia@gmail.com

الملخص:

يعيش العالم حاليا عصر الثورة المعلوماتية،هذه الثورة التي يترتب عنها الفوائد والمكاسب وفي نفس الوقت المشاكل والمخاطر الناتجة عنها جرائم تكنولوجية المعلومات التي تستوجب نصوص عقابية صارمة توفر الحماية الجزائية الكافية لتكنولوجية المعلومات، وحتى نصل إلى البيئة المعلوماتية الآمنة لابد على الفقه والقضاء البحث فيما إذا كانت النصوص التشريعية القائمة حاليا كافية لمواجهة هذه الجرائم بمختلف أنواعها أم أن الوضع يستدعي استحداث نصوص تشريعية قادرة على احتوائها ومراعاة طبيعتها وخصوصيتها خاصة وان النصوص التشريعية العقابية التقليدية تبت عجزها في العديد من المرات مما أدى إلى إفلات الجناة من العقاب رغم ارتكابهم أفعال إجرامية تشكل اعتداء صارخ على تكنولوجية المعلومات.

مقدمة

سهل التطور التكنولوجي حياة الأفراد في مختلف المجالات ،ونظرا للدور الذي تلعبه التقنيات الحديثة التي لها علاقة بالتكنولوجية المتمثلة في الانترنت والحاسوب الآلي في الحياة اليومية للأفراد أدى إلى استحالة الاستغناء عنها حاليا،إلا أن بالمقابل تواجه الدول خطر الإجرام الناشئ عن الانترنت والحاسوب الآلي حيث أصبح هذا النوع من الإجرام يمثل ظاهرة إجرامية تهدد أمن الدول و حق الأفراد في الحياة الخاصة، لذلك هي تحتاج إلى مواجهة تشريعية عقابية وذلك بوضع ضوابط تحددها هده الأخيرة لأنها أصبحت تهدد مصالح كل الدول ،فعلى المشرع التدخل بمختلف الوسائل اللازمة لمنعها من الانتشار والاستمرار تحقيقا لغايات السياسة الجنائية وفي هذا السياق نطرح السؤال التالي :

- فيما يتمثل موقف التشريعات العربية والغربية من جرائم التكنولوجية؟
- وإجابة على هذا السؤال سوف نقسم الدراسة إلى أربعة(04) محاور هي:
  - أولا: مفهوم الجريمة التكنولوجية المعلوماتية
  - ثانيا: تحديد طبيعة الجريمة التكنولوجية المعلوماتية.
  - ثالثا:موقف بعض تشريعات الدول العربية من جرائم تكنولوجية المعلومات.
  - رابعا: موقف بعض تشريعات الدول الغربية من جرائم تكنولوجية المعلومات.

- أولا:مفهوم الجريمة التكنولوجية المعلوماتية

ترتبط جرائم تكنولوجية المعلومات ارتباطا وثيقا بالحاسوب والانترنت كمتطلبات تقنية هي أساس ظهور هدا النوع من الجرائم، ولدلك سوف نتطرق الى التعريف العام لتكنولوجية المعلومات ثم التعريف بجرائم تكنولوجية المعلومات.

أ. التعريف العام لتكنولوجية المعلومات

إن مصطلح تكنولوجية المعلومات مصطلح مركب من كلمتين، "تكنولوجية" و"معلومات"، الكلمة الأولى "تكنولوجيا"كلمة يونانية الأصل تتكون من مقطعين: "تكنو" (TECHNO)ويقصد بها الفن والصناعة والمقطع الثاني"لوجيا "(LOGIA)تعني علم، أما كلمة المعلومات(Information)،فهي مشتقة من العلم والمعرفة، وترتبط بالمعارف التي يمكن نقلها واكتسابها، وتعني في المجال التقني البيانات التي تمت معالجتها، بحيث أصبحت ذات معني، وباتت مرتبطة بسياق معين.

وتعرف الكلمة كلها "تكنولوجية المعلومات: "بأنها الأدوات والتقنيات والنظم التي يمكن استخدامها للحصول على المعلومات والبيانات ومعالجتها وتخزينها واسترجعها[1].

ب. التعريف الفقهي والتشريعي لجرائم تكنولوجيا المعلومات

للتعرف على مفهوم الجريمة التكنولوجية المعلوماتية، لابد من الإشارة إلى تعريفها من ناحية الفقه ثم تعريفها من ناحية التشريع.

1. التعريف الفقهي

عرف الفقيه الألماني "**بيادمان**" الجريمة التكنولوجية بأنها:«تشمل كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب» ، وعرف الفقيه "**ليسلي ديبار**"بأنها«فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية»، وعرف الفقيه "**ماس**" بأنها "الاعتداءات القانوني التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح " [2].

وقيل عن هذه التعاريف أنها تضيق من مفهوم جرائم تكنولوجية المعلومات لذلك وجدت تعاريف أخرى حاولت التوسع أكثر في مفهوم جرائم تكنولوجيا المعلومات ،فعرفتها بأنها «كل فعل أو امتناع عمدي، ينشا عن الاستخدام غير المشروع لتقنية المعلوماتية بهدف الاعتداء على الأموال المادية أو المعنوية[3].

ومن هذه التعارف توصل الفقه إلى عدم الاتفاق على تعريف موحد لهده الجريمة المستحدثة التي لا تعرف الخمول وهي في تطور مستمر، كذلك لم يتم الاتفاق على صور التجريم، مما أدى إلى وجود أزمة حقيقية في المصطلح الدال على هده الجرائم بالنظر إلى التسميات التي ظهرت لهده الجرائم في مختلف التشريعات.

---

(1)**عبد الاله النواسية**، "جرائم تكنولوجيا المعلومات"، دار وائل للشر والتوزيع، عمان، الأردن، طبعة الأولى ،2017، صفحة 33.

(2)**أحمد عبد اللاه المراغي**، "الجريمة الالكترونية ودور القانون الجنائي في الحد منها"، دراسة تحليلية تأصيلية مقارنة،المصدر القومي للإصدارات القانونية، القاهرة، مصر، الطبعة الأولى ،2017،صفحة 27.

(3)**عادل عامر**، الجريمة الالكترونية في ظل القانون المصري، تاريخ النشر: 2020/04/11،
http://pulpit.alwatanvoice.com

2. التعريف التشريعي

استخدمت العديد من التشريعات مصطلحين هما[1]:

مصطلح مرتبط بجرائم الحاسوب أو جرائم الانترنت للدلالة على الجرائم التي يكون للحاسوب دور في ارتكابها، ومن بين التشريعات التي استخدمت مصطلح جرائم الحاسوب، قانون جرائم الحاسوب الماليزي لسنة 1997، وقانون جرائم الحاسوب في جمهورية كونغو رقم 14 لسنة 2003 وفي انجلترا استعمل مصطلح قانون إساءة استخدام الحاسوب لسنة1991، وفي نيوزلندا أطلق على القانون اسم قانون جرائم استخدام الحاسبات وفي البرازيل استخدم المشرع مصطلح جرائم الكمبيوتر في قانون العقوبات.

بينما استخدمت بعض التشريعات مصطلح جرائم الانترنت أو الجرائم السيبيرية و كلمة (cyber) ومن التشريعات التي استخدمت مصطلح جرائم الانترنت القانون الاسترالي رقم 14 لسنة 2003.

أما المصطلح المرتبط بالمعلومات أو المعلوماتية ،من التشريعات التي استعملته نجد تعديل قانون جمهورية أرمينيا عام 2003 وتمت إضافة له بعنوان الجرائم ضد أمن المعلومات الانترنت، وفي البرتغال سمي قانون العقوبات المعلوماتية، وفي لفيتنام سمي قانون جرائم تكنولوجية وفي دولة الإمارات العربية المتحدة سمي بقانون مكافحة جرائم تقنية المعلومات رقم:(2) لسنة 2006، وفي المملكة العربية السعودية سمي نظام مكافحة جرائم المعلوماتية وفي جمهورية السودان قانون الجرائم مكافحة جرائم تقنية المعلومات رقم:(12) سنة 2011.

- ثانيا: طبيعة الجريمة التكنولوجية المعلوماتية:

عرف الانترنت كوسيلة للاتصالات واستعماله أصبح في كل المعاملات اليومية، مما أدى إلى ظهور سلبيات عديدة خاصة بعد استغلال الكثير من المجرمين هذا التغيير في نمط المعاملات مما أدى إلى ظهور جرائم لم يكن يعرفها القانون من قبل[2].

فالجريمة التكنولوجية المعلوماتية لها طابع خاص، يمكن استخلاصه من التعاريف السابقة ومن بيان أداة ارتكابها،فضلا عن كونها نتاج لتقنية المعلومات الأمر الذي أدى إلى اتساع إتباع نطاقها داخل المجتمع مما أكسبها لونا أو طابعا قانونيا خاصا جعلها تتميز بعدة خصائص أهمها:

([1]) **عبد الاله النواسية**، المرجع السابق، صفحة39.

([2]) **أحمد عبد اللاه المراغى**، المرجع السابق، صفحة69.

أ. ترتكب في بيئة تكنولوجيا المعلومات:

وهذا يدل على أنها ظاهرة إجرامية خاصة وأن المعلومات هي محل الحق المعتدي عليه وهي نفسها المعلوماتية، التي يقصد بها المعلومات المعالجة بطريقة آلية بواسطة الحاسب الآلي، حيث يمكن تصحيحها، وتعديلها، ومحوها، وتخزينها، واسترجاعها، وطباعتها، وحذفها، ونقلها وإتلافها، وهذه العمليات وثيقة الصلة بالجرائم التكنولوجية المعلوماتية المرتكبة[1].

ب. لا تتسم بالعنف.

هذه الجرائم لا تحتاج إلى ادني مجهود عضلي، بل تعتمد على الدراسة الذهنية، والتفكير العلمي المدروس والقائم عن معرفة تقنية الكمبيوتر، كذلك هدا النوع من الجرائم عبارة عن معطيات وبيانات تتغير أو تعدل أو تمحى من السجلات المخزنة في ذاكرة الحاسوب[2]

ج. عابرة للحدود.

يقصد بها جرائم لا تقتصر على بلد واحد،بل تتعدي لعدة دول جغرافية أخرى، ولا تعترف بفواصل أو حدود،فهذه الجرائم قد ترتكب في وقت واحد في عدة دول، خصوصا وان مجرمو الانترنت من اجل إفلاتهم من العقاب يميلون لممارسة أنشطتهم الإجرامية في المناطق الأكثر سماحا[3].

د. هناك صعوبة في اكتشافها وإثباتها.

تتسم هذه الجرائم بأنها غير مرئية في العديد من الحالات، ولا تعتمد التعاملات فيها أصلا على الوثائق والمستندات المكتوبة، بل على نبضات الكترونية لا يمكن قراءتها إلا بواسطة الحاسب والبيانات التي يمكن استخدامها كأدلة ضد الفاعل يمكن في اقل من لمح البصر العبث بها أو محوها بالكامل[4].

---

(1)**محمد عبد الرحمان عنانزه**، القصد الجرمي في الجرائم الالكترونية، دار الأيتام للنشر والتوزيع، الطبعة الأولى، 2017، عمان الأردن، الطبعة الأولى 2017، صفحة91.

(2)**محمد الصغير مسيكة**،مفهوم الجرائم المستحدثة وطبيعتها القانونية (**الجرائم** الالكترونية)، "مجلة الدراسات القانونية والسياسية"المجلد الثامن، العدد 01، جانفي 2022،صفحة139.

(3)**ميموني عبد الحفيظ**، الزجر الجنائي للجريمة الالكترونية التحديات والأفاق، مجلة قانونك، العدد13، يوليو–سبتمبر 2022، صفحة305.

(4)**الشحات إبراهيم محمد منصور**، الجرائم الالكترونية في الشريعة الإسلامية القوانين الوضعية، دار الفكر الجامعي، الإسكندرية، مصر، الطبعة الأولى، 2011، صفحة191.

- ثالثا:موقف بعض تشريعات الدول العربية من الجرائم التكنولوجية المعلوماتية

اختلفت التشريعات المقارنة في أسلوب تنظيمها للجرائم بصفة عامة و الجرائم التكنولوجية المعلوماتية بصفة خاصة فهناك من التشريعات التي تغلب المنطق القانوني فتتقيد بمبدأ الشرعية الجنائية وتعتمد أسلوب وحده الجريمة وذلك بتحديد نموذج إجرامي واحد وتنص على الأفعال والأنشطة الإجرامية في مواد قانونية مختلفة مثل: المشرع الأردني والمشرع السعودي وهناك تشريعات تغلب المنطق العملي حيث تعتمد على أسلوب تعداد الجرائم بحيث تحاول الإلمام بمختلف الأنشطة الإجرامية الممكن اقترافها دون أن تشرك في نموذج إجرامي واحد وهذا مثل المشرع المصري والمشرع المغربي والمشرع الجزائري.

أ. التشريعات التي اعتمدت على أسلوب وحدة الجريمة:

1. التشريع الأردني

لم يغفل المشرع الأردني عن معالجة الجرائم التكنولوجية ،فقد وردت صور لعدة جرائم في قانون الاتصالات لعام 1995، وجرم قانون المعاملات الالكترونية لعام 2001 باستعمال الوسائل الالكترونية في ارتكاب الجرائم، ووردت بعض الإشارات لهذه الجرائم في تشريعات أخرى غير جزائية كتشريعات الملكية الفكرية، ولكن البداية الحقيقية لدخول هذه الجرائم في التشريع الأردني كانت عام 2010 عندما صدر قانون جرائم أنظمة المعلومات المؤقت الذي جرم العديد من الأفعال التي تستغل تكنولوجيا المعلومات في ارتكابها، و بقي القانون ساري المفعول إلى أن صدر قانون الجرائم الالكترونية رقم 27 لسنة 2015، والذي يعد التشريع الأساسي لجرائم تكنولوجيا المعلومات و رغم ما شابه من قصور في بعض الأحكام و الصياغة كان بإمكان المشرع الأردني تلافيها، خاصة و أنه جاء متطابقا في اغلب نصوصه مع قانون جرائم أنظمة المعلومات المؤقت، وبعد مرور خمس سنوات على العمل بقانون جرائم أنظمة المعلومات كانت كافية للكشف عن عيوبه وتلافيها في قانون الجرائم الالكترونية[1].

([1])**عبد الاله النواسية**، المرجع السابق، صفحة19.

- في الأردن بلغت نسبة انتشار الانترنيت بين السكان عام 2015، 83% و كل هؤلاء الأشخاص في حيازتهم وسيلة أو أداة لارتكاب جريمة تكنولوجية المعلومات (أنظر نفس المرجع، صفحة20).

2. التشريع السعودي:

تعد المملكة العربية السعودية من الدول المتقدمة في مجال التكنولوجيا و مجال الحواسب و التعاملات الالكترونية وكلما كان المجتمع أكثر تقدم وانفتاح في العالم التكنولوجي أصبح أفراده أكثر تعرض لخطر جرائم الالكترونية الحديثة، و لذلك قام المشرع السعودي بتنظيم الجريمة الالكترونية التي تعد من الجرائم الحديثة بشكل رسمي فأقر مجلس الوزراء نظام يسمى نظام مكافحة جرائم المعلوماتية و الذي كان أحد أبرز أهدافه تحقيق الأمن الإلكتروني و الأمن ألمعلوماتي للمستخدمين في المملكة العربية السعودية[1].

ويهدف هذا النظام إلى تحديد ماهية الجرائم المعلوماتية وشرحها بشكل مفصل وإدراج البنود التي تعالج كل جزئية في مجال الجرائم الالكترونية وأيضا تحديد العقوبات التي يفرضها القانون والنظام السعودي، وكان هدف هذا النظام الرئيسي هو تنظيم ووضع حد إلى الجرائم الإلكترونية وجرائم تقنية المعلومات والحاسبات، حيث نظم المسائل المتعلقة بابتزاز الآخرين بأي شكل لدفعهم على القيام بفعل أو الامتناع عن فعل،أو التشهير بالأخريين عبر أي وسيلة من وسائل تقنية المعلومات، أو بناء مواقع إلكترونية متصلة بجهات إرهابية أو الدخول إلى أي موقع إلكتروني بهدف إتلافه أو إلحاق أي ضرر به، كذلك جرم هذا النظام الدخول إلى مواقع حكومية ومحاولة إتلافها أو تعطيل الخدمات،أو بث أي محتويات كذلك جرم إنشاء مواقع إلكترونية هدفها ترويج المواد الإباحية ولو بأي شكل ،أو الترويج للمواد الممنوعة قانونا كبيع المخدرات أو غيرها من خلال وسائل التواصل المعلوماتي، كما جرم الدخول إلى مواقع البنوك بقصد التلاعب والإتلاف أو التسلل والقرصنة، أو حتى الدخول إلى المواقع الحكومية للحصول على معلومات أو إحصائيات أو أي بيانات تتعلق بالأمن الداخلي ،كما جرم إنشاء المواقع الالكترونية التي تحرض على الإرهاب أو متصلة بجهات إرهابية ،أو مواقع تهدف إلى تعليم القرصنة والإضرار بالمواطنين فنظام مكافحة الجريمة في السعودية يعتبر نظام شامل ويحدد العقوبات على كل جريمة من الجرائم الواردة فيه[2].

([1]) الجرائم الإلكترونية والمعلوماتية في المملكة العربية السعودية، " فريق مكافحة الابتزاز والتهديد الالكتروني، صفحة4.

http://www.antiextortion.net

([2])نفس المرجع، صفحة5، جاءت إعادة 3/2 من نظام مكافحة جرائم المعلوماتية السعودي الصادر في 2007/03/07، و الهدف من هذا النظام الحد من وقوع جرائم المعلوماتية، و ذلك مما يؤدي على حماية المصلحة العامة و الأخلاق و الآداب العامة، (أنظر **عبد الاله النواسية**، المرجع السابق، صفحة336).

ب. التشريعات التي اعتمدت على أسلوب تعداد الجرائم:

1. التشريع المصري:

لم يأتي المشرع المصري بتشريع خاص بجرائم تقنية المعلومات، يقدم الحلول الناجعة لكافة المشكلات القانونية الناجمة عنها، على الرغم من وجود بعض النصوص القانونية التي تحتويها قوانين تنظم موضوعات مختلفة تناولت بعض صور التجريم الإلكتروني، نذكر منها قانون الأحوال المدنية المصري رقم 143 لسنة1994، وقانون حماية الملكية الفكرية رقم82 لسنة 2002وقانون تنظيم الاتصالات 10 لسنة2003، وقانون التوقيع الالكتروني 15 لسنة 2004، وقانون الطفل المعدل في 2008، إلا أن هذه القوانين لم تغطي كافة صور التجريم المعلوماتي وهو ما كان له أثره السيئ على المجتمع بسبب عدم توفير الحماية القانونية لأفراده، خصوصا في ظل وجود مبدأ دستوري يحكم التجريم في مصر هو مبدأ الشرعية الجنائية والذي ورد النص عليه في المادة 95 من الدستور المصري الصادر في سنة 2014 و التي جرى نصها على أن " العقوبة شخصية، ولا جريمة ولا عقوبة إلا بناء على قانون، ولا توقع عقوبة إلا بحكم قضائي ولا عقاب إلا على الأفعال اللاحقة لتاريخ نفاذ القانون، فمع وجود ذلك النص الدستوري وغياب النص التشريعي العقابي يصبح القاضي الجنائي في حيرة من أمره، متى عرض عليه فعل يشكل جريمة من جرائم تقنية المعلومات التي لم يكن لها مسبقا نصا صريحا يجرمها في قانون العقوبات أو القانون الخاص[1].

2. التشريع المغربي:

يعد المشرع المغربي من التشريعات التي اتبعت أسلوب إدراج التجريم في قوانين العقوبات، حيث أضاف المشرع المغربي عام 2003 للفصل607 من قانون العقوبات تسعة مواد مكررة عنوانها " جرائم المس بنظام المعالجة الآلية للمعطيات"، إلا أن المشرع المغربي لم يعرف المقصود بالجرائم الإلكترونية ولا المقصود بنظم المعالجة الآلية للمعطيات في القانون 2003، تاركا المجال إلى الفقه والقضاء لأنه

---

(1) **محمود رجب فتح الله**– جرائم تقنية المعلومات – القانون المصري الجديد،صفحة3.

https://www.ahewar.org/debat/show

صدر عن المنظمة العربية للتنمية الإدارية التابعة لجامعة الدول العربية توصيات من خلال ندوة الدليل الرقمي التي عقدت في القاهرة من 5–8 مارس 2006، وقد ركزت التوصيات على الجوانب الإجرامي والتدريبية في مجال جرائم تكنولوجية المعلومات، (انظر في ذلك **عبد الله عبد الكرم عبد الله**، جرائم المعلوماتية والانترنت، دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، 2007، ص140.

المكلف بتطبيق بنود الجريمة الإلكترونية ثم أن المجال المعلوماتي هو مجال حديث و متجدد وبالتالي فأي تعريف يتم وضعه قد يصبح متجاوزا في ضوء التطور الهائل لقطاع تكنولوجيا المعلومات[1].

وقد تم توجيه النقد إلى الفلسفة المعتمدة من طرف المشرع المغربي على أن نصوصه كانت غير واضحة و مبهمة أو متناقضة بالشكل الذي جعل القارئ أو الدارس لايميز بين مختلف هذه الجرائم،زيادة على ذلك هناك امتداد وتشتت للنصوص الزجرية لهذه الجرائم في قوانين خاصة(كقانون حقوق و الحقوق المجاورة، وقانون حماية المعطيات ذات الطابع الشخصي، قانون التبادل الالكتروني للمعطيات الالكترونية،وقانون الصحافة والنشر ....) وهذا ما جعل من المقتضيات المنظمة لها مادة ضخمة وغير متجانسة، ذلك أن الجرائم المنصوص عليها تبدوا وكأنها منفصلة عن بعضها البعض دون أن تقام بينها روابط قوية ومتينة تجعلها في مجموعات متناسقة، وهذا ما سيساهم في غياب نظرية قواعد عامة للجرائم الإلكترونية[2].

3. التشريع الجزائري:

أصدر المشرع الجزائري بعض التشريعات المتعلقة بجرائم المعلوماتية أو ترتبط بها، مثل القانون رقم24/96 سنة 1996 المتعلق بالبريد والمواصلات وخاصة ما يتعلق منها بمخالفات الماسة بالتجهيزات السلكية واللاسلكية والعقوبات الزجرية، والقانون15/04 لسنة 2004 المتضمن تعديل قانون العقوبات الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية للمعطيات ثم تلاه القانون04/09الذي تضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال ومكافحتها،و هو قانون يدخل في إطار القانون الجنائي للمعلومات أو القانون الجنائي المعلوماتي وبالنظر إلى أن الأفعال التي يجرمها تنصب على البيانات أو المعطيات بشكل أساسي، فهو بذلك يخرج عن التقسيم المتعارف عليه بالنسبة للجرائم التي تمس الأشخاص أو الأموال، وان كانت البيانات والمعطيات التي تتناول هذه الأعمال الإجرامية، قد تكون لها قيمة مالية أو اقتصادية [3] ، فهناك نصوص جنائية وقوانين تصدت لهذا النوع من الجرائم، خاصة المادة 394 مكرر إلى المادة 394 مكر7من القانون رقم 15/04فحدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات ، وكذلك بين كيفية المساس بأنظمة

([1])**ميموني عبد الحفيظ**، مرجع سابق، صفحة295.

– بتاريخ 2012/12/21 تم انعقاد اتفاقية بين الدول العربية والخاصة لمحاربة الجريمة المعلوماتية والتي احتوت على43 مادة جاءت شاملة للأحكام الموضوعية والإجرامية الخاصة بجرائم تكنولوجية المعلومات والتي صادق عليها المغرب في سنة 2017، (أنظر **عبد الاله النواسية**، صفحة53).

([2]) **ميموني عبد الحفيظ**، المرجع السابق، صفحة302.

([3])**أحمد عبد اللاه المراغي**، المرجع السابق، صفحة110،وصفحة 111.

المعالجة الآلية للمعطيات،والعقوبات المقررة لهذه الجرائم تتراوح ما بين الحبس من شهرين على الأقل إلى ثلاث سنوات على الأكثر مع مضاعفة هذه العقوبات في حالة ارتكاب الجريمة بهدف استهداف الدفاع الوطني أو الهيئات الخاضعة للقانون العام مع مصادرة أدوات الجريمة من أجهزة وبرامج ووسائل مستعملة فيها وإغلاق مواقع ومحلات إن وجدت[1].

وبذلك الجزائر كباقي دول العالم لجأت إلى التشريع في الجرائم التكنولوجية المعلوماتية بمختلف أنواعها، وحاولت الحد منها في عدة قوانين وتشريعات خاصة.

- رابعا:موقف بعض التشريعات الغربية من الجرائم التكنولوجية المعلوماتية

أ. تشريعات اعتمدت على أسلوب وحدة الجريمة

1. التشريع الأمريكي:

لقد شرعت الولايات المتحدة الأمريكية قانونا خاصا بحماية أنظمة الحاسب الألي (1976-1985) وفي عام 1985 حدد معهد العدالة القومي خمسة أنواع رئيسية للجرائم المعلوماتية وهي: جرائم الحاسب الألي الداخلية أو جرائم الاستخدام غير المشروع عن بعد، وجرائم التلاعب بالحاسب الألى، ودعم التعاملات الإجرامية، وسرقة البرامج الجاهزة و المكونات المادية للحاسب[2].

وفي عام 1986 صدر قانونا تشريعيا يحمل رقم (1213) عرف فيه جميع المصطلحات الضرورية لتطبق القانون على الجرائم المعلوماتية كما وضعت المتطلبات الدستورية اللازمة لتطبيقه، وعلى أثر ذلك قامت الولايات الداخلية بإصدار تشريعاتها الخاصة بها للتعامل مع هذه الجرائم ومن ذلك قانون ولاية تكساس لجرائم الحاسب الآلي.

([1])**بلعيد الهام**، الجرائم المستحدثة، مجلة الباحث للدراسات الأكاديمية، المجلد09،العدد02، السنة2022،صفحة527.

([2]) **أحمد عبد اللاه المراغي**، المرجع السابق، صفحة112.

تعد الولايات المتحدة الأمريكية الرائدة لصناعة البرمجيات وأنظمة التشغيل، لذلك نجد أن لها كم هائل من التشريعات القانونية، وعدد كبير من المحاكم يصل إلى سبعة عشر ألغ محكمة، تنظر في تسعون مليون قضية تقريبا في العام، (أنظر**حازم محمد الشرعة**، الثقافي الالكتروني والمحاكم الالكترونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى ،2010، الأردن، عمان، صفحة 126).

ب. التشريعات التي اعتمدت أسلوب تعداد الجرائم

1. التشريع الفرنسي:

تعتبر فرنسا من الدول التي قامت بتعديل تشريعاتها العقابية وجرمت الاعتداء على تكنولوجيا المعلومات في ثنايا النصوص العقابية التقليدية ،فقد تبنت أسلوب الإدراج في التجريم، فلم تفرض تشريعات عقابية خاصة بجرائم التكنولوجيا المعلومات[1]، وإنما اكتفت بتعديل النصوص العقابية، فالمشرع الفرنسي عالج جرائم التكنولوجيا في المادة323-1إلى 7 من قانون العقوبات بعنوان" الدخول الغير مصرح به للبيانات المعالجة الآلية"، كذلك نص في المادة 3/323 من نص القانون "فعل من يدخل بسوء النية بيانات في نظام معالجة البيانات أو أقام بإلغاء أو تعديل هذه البيانات[2].

كذلك جرمت المادة 227-22 منه القيام بتجنيد بإفساد الأطفال أو الشروع في ذلك وإذا تم ذلك برسائل عن طريقك استخدام شبكة الاتصالات لإفساد القاصر ظرفا مشددا، و هذا الشرط الأخير أضافه المشرع الفرنسي بموجب القانون المعدل لقانون العقوبات رقم 711 سنة 2013[3] في جريمة استغلال الجنسي للأطفال كذلك سوى بين عقوبة الشريك والفاعل الأصلي وكذلك عاقب على الشروع فيها مثل عقوبة الجريمة التامة[4].

كذلك قرر القانون الفرنسي رقم 2001-539 الصادر في يوليو 2001 أن للقاضي الجنائي حق اللجوء إلى محكمة النقض لتحديد معنى النص التي وجد صعوبة في تغييره.

---

(1) قد أدمجت فرنسا في قانون العقوبات الفرنسي نصوص تشير إلى الجرائم المعلوماتية وذلك في01/03/1994، (انظر عادل عامر، "الجرائم الالكترونية"، صفحة 14).

http://pulpit.alwatanvoice.com/article/2020/04/11

(2) **عبد الاله النواسية**، المرجع السابق،صفحة63.

(3)**عبد الاله النواسية**، المرجع السابق،صفحة331.

(4)**محمد عبد الرحمان عنانره**،"القصد الجرمي في الجرائم الالكترونية"، دار الأيام للنشر التوزيع، عمان ،الأردن، الطبعة الأولى،2017، صفحة139.

الخاتمة:

نظرا لخصوصية جرائم المعلوماتية وتجاوزها الحدود الجغرافية أصبح من الضروري سن قوانين من طرف الدول تجرم مثل هذه الأفعال وتحدد عقوبات تتلاءم مع خصوصياتها.

لكن مع تطور المتصارع تقنيا، أدى بمجهود الدول التي سنت قوانين لمواجهة هذه الجرائم باءت بالفشل نوعا ما في مكافحتها، لذلك استوجب تعاون دولي فعال لمواجهة الجرائم الإلكترونية بكل قوة وفعالية خاصة وأنها تتم في أماكن مختلفة من العالم فالتعاون أصبح ضرورة حتمية.

لذلك تم التوصل إلى التوصيات التالية:

- الاتفاق فيما بين الدول على تعريف موحد لجرائم التكنولوجية المعلوماتية.
- تعزيز التعاون الغربي والعربي في مواجهة خطورة التكنولوجية المعلوماتية.
- توجيه التشريعات الخاصة بالجرائم التكنولوجية المعلوماتية بصفة مواكبة لتطورها، وبصفة تتناسب مع جسامة الضرر والخطر التي تحدثه هده الجرائم بالنسبة للأفراد والمجتمعات.
- تشديد العقوبات على مرتكبي جرائم تكنولوجية المعلومات وخاصة بالنسبة للمجرمين العائدين.
- نشر الوعي في المجتمع وتعريف بخطورة هذه الجرائم التكنولوجية المعلوماتية في كل وسائل الإعلام والاتصال، كالملتقيات الفكرية والثقافية لتتاح الفرصة لتبادل الخبرات بين كافة المعنيين.
- تدريس مواد الأنظمة المعلوماتية في الجامعات والكليات خاصة كلية الحقوق والمعاهد القضائية.
- تحديث كل ماله علاقة بالتكنولوجية و بما يتماشى مع التطورات التكنولوجية الحديثة.

قائمة المراجـــع المعتمدة

أولا : المراجـــــع باللغـــة العربية :

1. **عبد الاله النواسية**، جرائم تكنولوجيا المعلومات، شرح الأحكام الموضوعية في قانون الجرائم الالكترونية، وائل للنشر والتوزيع، الطبعة الأولى 2017، الأردن، عمان.
2. **حازم محمد الشرعة**،الثقافي الالكتروني والمحاكم الالكترونية، دار الثقافة للنشر والتوزيع، الطبعة الأولى ،2010، الأردن، عمان.
3. **محمد عبد الرحمان عنانزه**، القصد الجرمي في الجرائم الالكترونية، دار الأيتام للنشر والتوزيع، الطبعة الأولى، 2017، عمان الأردن.
4. **أحمد عبد اللاه المراعي**، الجريمة الالكترونية ودور القانون الجنائي في الحد منها، دراسة تحليلية تأصيلية مقارنة المركز القومي للإصدارات القانونية، الطبعة الأولى، 2017، القاهرة، مصر.
5. **الشحات إبراهيم محمد منصور**، الجرائم الالكترونية في الشريعة الإسلامية القوانين الوضعية، دار الفكر الجامعي، الطبعة الأولى، 2011، الإسكندرية، مصر.

ثانيا: المراجع الالكترونية

1. **عادل عامر**، الجريمة الالكترونية في ظل القانون المصري، دنيا الرأي، http://pulpit.alvatan voice.com/
2. **محمود رجب فتح الله**، جرائم تقنية المعلومات في القانون المصري الجديد، http://www.ahwar.org
3. **فريق مكافحة الابتزاز والتهديد الالكتروني**، الجرائم الالكترونية والمعلوماتية في المملكة العربية السعودية ، http://www.antiextortion.net

ثالثا: المقالات

.1	**ميموني عبد الحفيظ**، الزجر الجنائي للجريمة الالكترونية التحديات و الأفاق، مجلة قانونك، العدد13،جويلية–سبتمبر 2022.
.2	**بلعيد الهام**، الجرائم المستحدثة، مجلة الباحث للدراسات الأكاديمية، المجلد09،العدد02، السنة2022.
.3	**قزران مصطفى**، **زرقين عبد القادر**، الآليات الدولية لمكافحة الجريمة الالكترونية، مجلة صوت القانون، المجلد08، العدد02،2022.

رابعا: القوانين

.1	القانون15/04المؤرخ في 10نوفمبر2004 يعدل ويتمم الأمر 156/66المؤرخ في 08يونيو1966المتضمن قانون العقوبات.
.2	القانون رقم 04/09المؤرخ في 05غشت 2009يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والاتصال.

مداخلة للمشاركة في فعاليات

الملتقى الدولي الافتراضي المنظم بكلية الحقوق جامعة الجزائر-1- الموسوم بـ

"القانون الجنائي في ضل التطور التكنولوجي"

-إشكالات و معالجات-

"""استمـــــارة المشـــــاركة"""

	المشاركة الأولى	المشاركة الثانية
الاسم و اللقب	**مامي هاجر**	**كودري فاطمة الزهراء**
الدرجة العليمة	دكتوراه علوم في الحقوق	دكتوراه علوم في الحقوق-أستاذة قسم ب-
التخصص	قانون الأعمال	القانون المدني
مؤسسة الانتماء	جامعة الجزائر -1-	جامعة الجزائر -1-
البريد الإلكتروني	hadjer.droitpriv2018@gmail.com	f.koudri@univ-alger.dz
الهاتف	06 99 47 17 51 /05 55 83 33 29	06 76 07 37 00

ضمن المحور الثاني: أثر استخدام التكنولوجيا الحديثة على أحكام التجريم

بـعنـــوان:

"المواجهة التشريعية للجرائم المتأثرة بالتطور التكنولوجي المتعلقة بالمصارف"

-جريمة تبييض الأموال نموذجا-

الملخص:

ازدادت جرائم الأموال وبالخصوص الجرائم المتعلقة بالمصارف عبر العالم ازديادا حاداً في السنوات الأخيرة، فأضعفت النُظم المالية العالمية وأعاقت النمو الاقتصادي وتسببت في خسائر فادحة على الشركات والأفراد في العالم أجمع. ويأتي التطور التكنولوجي بجانبه المُظلم ليعقّد المشاكل أكثر مما عليه إذ أنه يوفر الأرضية الخِصبة للأنشطة الإجرامية المنظمة المتأثرة بالتطور التكنولوجي.

إذ يستفيدُ المجرمون من ظاهرتي العولمة و الرقمنة، لتمكنهم ارتكاب جرائم مالية بمزيد من المهارة والحِنكة. لنهدف من خلال هذه الورقة البحثية إلى التعريف بالتطور التكنولوجي المصرفي وعلاقته بجريمة تبييض الأموال من جهة، ومن جهة أخرى التطرق إلى المواجهة التشريعية التي خصها المشرع الجزائري من أجل مكافحة هذه الجريمة من خلال القوانين المختلفة والآليات المخصصة لمتابعة ومحاربة مثل هذه الجريمة، التي تُعتبر من أكثر الجرائم ارتباطا و تأثُرا بما تحمله التكنولوجيا و تطوراتها الحديثة.

Abstract.

Money crimes, especially banking-related crimes, have increased sharply across the world in recent years, weakening global financial systems, impeding economic growth and causing huge losses to companies and individuals worldwide. Technological development comes with its dark side to complicate problems more than it is, as it provides the fertile ground for organized criminal activities affected by technological development.

Criminals take advantage of the phenomena of globalization and digitization, to enable them to commit financial crimes with more skill and sophistication. Let us aim through this research paper to introduce the technological development of banking and its relationship to the crime of money laundering on the one hand, and on the other hand to address the legislative confrontation that the Algerian legislator singled out in order to combat this crime through various laws and mechanisms dedicated to following up and fighting such crime, which is considered one of the most Crimes are linked to and affected by technology and its recent developments.

المقدمة:

نتيجة لظهور العولمة ولنمو فاعلية أسواق رأس المال الدولية وانتشار المراكز المصرفية في العديد من دول العالم، أصبح من السهل انتقال رؤوس الأموال عبر الدول المختلفة، وقد حمل هذا في طياته تنامي حركة الجريمة المنظمة، وتزايد حركة تداول أموال المنظمات الإجرامية على المستوى المحلي ابرز هذه الجرائم وأخطرها ظاهرة تبييض الأموال و التي تعد من أكبر التحديات الحقيقية أمام المؤسسات المالية والمصرفية والهيئات الحكومية والدولية .

ومما يزيد هذه الظاهرة خطورة، هو أن كل جهد يبذله القائمون على المكافحة والتصدي لعمليات تبييض الأموال، يقابله عمل مضاد ومنظم ، حيث تشهد عمليات تبييض الأموال دخول مجموعات من المهنيين الجدد ومن مستويات ثقافية عليا لتخصصات مختلفة (محاسبين، قانونيين، منظمي معلومات، إداريين ،.....) وغيرها من التخصصات يعتمدون بصفة أساسية على الأساليب التكنولوجيا الحديثة في إنجاز جرائمهم .

ومع ظهور العولمة و الرقمنة تفجرت ثورة تكنولوجية في مجال الاتصالات والمعلومات والأجهزة والمعدات الحديثة، التي تركز استخدامها في المؤسسات المالية والمصرفية كالانترنيت و الحوالات، و وسائل الدفع الإلكترونية وغيرها . استفاد منها غاسلو الأموال و طوروا وسائل جديدة لعملياتهم ، إلا أن الدول ممثلة بهيئاتها المعنية بمكافحة تبييض الأموال والهيئات الدولية المنبثقة عن المنظمات العالمية والهيئات الإقليمية لم تقف موقف المتفرج من جرائم تبييض الأموال التي أضعفت النُظم المالية العالمية وأعاقت النمو الاقتصادي وتسببت في خسائر فادحة على الشركات والأفراد في العالم أجمع خصوصا وان آثارها لم تقف ضمن إطار حدودي معين ولكنها أصبحت عالمية بسبب زوال القيود والحدود بين الدول في ضل العولمة . لذلك كرست الجزائر على غرار دول العالم مجموعة من القوانين لمواجهة هذه الجريمة للحدّ من آثارها على الاقتصاد الوطني، و من خلال ذلك نكرس هذه الورقة البحثية في التطرق إلى جرائم المصارف المتأثرة بالتطور التكنولوجي و على وجه الخصوص جريمة تبييض الأموال باعتبارها أكثر الجرائم تأثرا بالتطور التكنولوجي في مجال جرائم المصارف أو كما تسمى بجرائم الأموال و الأعمال، و كذا التطرق إلى التدخل التشريعي المتاح في الجزائر من أجل مواجهة هذه الجريمة. من خلال الإجابة على إشكالية قانونية تتمثل في: **ما هي النصوص التشريعية التي وضعها المشرع**

الجزائري لمواجهة جريمة تبييض الأموال والوقاية منها باعتبارها أكثر الجرائم المصرفية تأثرا بالتطور التكنولوجي؟

نجيب على هذه الإشكالية القانونية من خلال محورين أساسيين:

المحور الأول: التطور التكنولوجي المصرَفي و جريمة تبييض الأموال.

ارتبط تبييض الأموال عبر الزمن بالنظام المصرفي في محاولة من المجرمين لتوفير الغطاء الشرعي للأموال غير المشروعة وفي ظل التطور التكنولوجي تعَّد شبكة الانترنت المجال الخصب لمحترِفي الجريمة الالكترونية المالية المصرفية، كوسيلة لإخفاء مصدرها غير الشرعي كما وجد مُرتكبو جرائم تبييض الأموال في التطور التكنولوجي الحاصل في الخدمات المصرفية الحديثة واستفادة هذه الأخيرة من ما وفرته لها ثورة الاتصال والتطور التقني والاستفادة من خدمات الانترنت وسرعة تنفيذ العمليات المالية والمصرفية، بالإضافة إلى الحركة السريعة للنقود الالكترونية مقارنة بالاستخدام التقليدي للنقود الورقية أرضية خصبة لعملياتهم المشبوهة.

أولا: مفهوم التكنولوجيا المصرفية.

تُعتبر التكنولوجيا المصرفية جزءا من التكنولوجيا المالية، والتي تعتبر جزءا لا يتجزأ منها، كما تعتبر جريمة تبييض الأموال التي هي نفسها جريمة غسيل الأموال من ضمن جرائم الأموال. حيث يمكن اعتبار التكنولوجيا المالية الإناء الذي تصب فيه تكنولوجيا المصارف.

عرَّف مجلس الاستقرار المالي، التكنولوجيا المالية بأنها:"ابتكارات مالية باستخدام التكنولوجيا يمكنها استحداث نماذج عمل أو تطبيقات أو عمليات أو منتجات جديدة لها أثر مادي ملموس على الأسواق والمؤسسات المالية وعلى تقديم الخدمات المالية"، و تلخص السيدة "cristine lacam"، مدير عام صندوق النقد الدولي:" التكنولوجيا المالية بدأت بالفعل تلمس حياة المستهلكين والأعمال في كلّ مكان، بدأ من التاجر المحلي الذي يسعى للحصول على قرض ومرورا بالأسرة التي تخطط للتقاعد وانتهاء بالعامل الأجنبي الذي يرسل أمواله لبلده"[1]، و عليه فإن مصطلح التكنولوجيا المالية عبارة عن دمج الجانب المالي مع الجانب التكنولوجي لينتج عنه مجال جديد يهتم بالمعاملات والخدمات المالية واعتمادا على مخرجات التكنولوجيا الجديدة[2].

والتكنولوجيا المالية هو المصطلح المستخدم لوصف أية تقنية تقدم خدمات مالية من خلال البرامج مثل الخدمات المصرفية عبر الانترنت أو تطبيقات الدفع عبر الهدف المحمول أو حتى العملات المشفرة، كما تمثل فئة واسعة تشمل العديد من التقنيات المختلفة ولكن الأهداف الأساسية هي تغيير طريقة وصول المستهلكين والشركات إلى مواردهم المالية والتنافس مع الخدمات المالية التقليدية[3].

ومن خلال التعريفات السابقة للتكنولوجيا المالية، يتجلى بكل وضوح مفهوم التكنولوجيا المصرفية.

التكنولوجيا المصرفية هي رصيد المعرفة الذي يسمح بإدخال آلات ومعدات وعمليات وخدمات مصرفية جديدة و محصنة، وعلى ذلك يقدم مصطلح التكنولوجيا الحديثة في المجال المصرفي في مجالين، الأول هو التكنولوجيا الخفيفة وتشمل الإدارة والمعلومات والتسويق المصرفي، والثاني هو التكنولوجيا الثقيلة وتشمل الآلات والمعدات المصرفية[4].

وتتضمن التكنولوجيا الحديثة استخدام الطرق والوسائل اللازمة لتقديم الخدمة المصرفية بالاعتماد على المعارف و المهارات والخبرات المتاحة، وتهتم التكنولوجيا في المجال المصرفي بالاستفادة من الحقائق العلمية ووضعها موضع التنفيذ العلمي بحيث تساهم في:

- تطوير الخدمات المصرفية الحالية،
- تقديم خدمات مصرفية جديدة[5].

كما تعرف التكنولوجيا المصرفية على أنها كافة العمليات أو النشاطات التي يتم عقدها أو تنفيذها أو الترويج لها بواسطة الوسائل الالكترونية أو الضوئية وذلك من قِبل المصارف والمؤسسات المالية. وكذلك العمليات التي يجريها مصدِروا البطاقات الالكترونية وأيضا المؤسسات التي تتعامل بالتحويل النقدي الالكتروني[6].

ثانيا: الوسائل التكنولوجية الحديثة في جرائم تبييض الأموال.

لقد تطور القطاع المالي والمصرفي كغيره من القطاعات مع تطور التكنولوجيا المصاحبة للعولمة، فتطورت معه أساليب تقديم خدماته المالية والمصرفية وبالمقابل فإن عصابات الجريمة المنظمة وغاسلي الأموال استفادوا من هذه التكنولوجيا وبالتحديد من المخاطر المصاحبة لاستخداماتها، وبذلك فقد تطورت وتغيرت وسائل وطرق تبييض الأموال، وأصبحت تبتعد تدريجيا عن الأساليب التقليدية التي تكون

عرضة للاشتباه فيها وكشفها بسهولة، وفيما يلي توضيح لأهم هذه الأدوات و الأساليب الالكترونية الحديثة:

1- أجهزة الصرف الآلي:Automated teller machine

إن ماكينة الصرف الآلي (ATM) هي عبارة عن ماكينة مصرفية أوتوماتيكية تسمح للعملاء بإتمام المعاملات الأساسية دون أي مساعدة من ممثلي البنوك. هناك نوعان من ماكينات الصرف الآلي العنصر الأساسي يسمح للعميل بسحب الأموال فقط والحصول على تقرير رصيد الحساب. واحد آخر هو آلة أكثر تعقيدا والتي تقبل إيداع الأموال، ويوفر تسهيلات الدفع ببطاقة الائتمان ومعلومات حساب التقارير7.

تستخدم هذه التكنولوجيا من أجل إيداع و سحب الأموال القذرة من الحسابات المصرفية بهدف التخلص من الإجراءات المصرفية التي تتضمن تعبئة نماذج خاصة لعمليات الإيداع والسحب والتي قد تكشف عن عملياتهم الغير قانونية، ويتم استخدام هذه الآلات في غسيل الأموال من خلال إجراء العديد من عمليات الإيداع والسحب للأموال لضمان عدم الكشف ولفت الانتباه. وتحاشيا للالتزامات القانونية المترتبة على المصارف و المتمثلة في الإبلاغ عن عمليات الإيداع التي تتجاوز المبالغ المحددة رقابيا8.

2- بنوك الانترنت internet Bank:

و تسمى أيضا بالبنك الافتراضي أو البنك الالكتروني وهي "بوابات لكافة العمليات المصرفية والاستثمارية والمالية عبر الانترنت في بيئة افتراضية لا وجود فيها للمكان والحدود واللقاء المباشر بالموظف أو مشاهدة المال موضوع النشاط"9.

كما يمكن تعريفه على أنه إجراء عمليات المكتب بشكل إلكتروني والتي تُعد الانترنت من أهم أشكالها، وبذلك فهي بنوك افتراضية تنشئ لها مواقع إلكترونية على الانترنت لتقديم خدمات نفس خدمات موقع البنك من سحب ودفع وتحويل دون انتقال العميل إليها. كما تتيح هذه الوسيلة الفرصة لغاسلي الأموال نقل وتحويل مبالغ ضخمة من الأموال بسرعة و سرية تامّة، كون هذه البنوك تعمل بسرية تامة حيث يكون المتعاملين فيها غير معلومي الهوية، فضلا عن عدم خضوع هذه البنوك لأية لوائح أو قوانين10.

3-الخدمات المصرفية الالكترونية:

على اختلاف المصطلحات التي تطلق على هذا النوع من الخدمات فجميعها تشير إلى قيام العميل بإدارة حساباته أو انجاز أعماله المتصلة بالبنك عبر شبكة الانترنت سواء كان في المنزل أو المكتب وفي أي مكان ووقت يرغبه ويعبر عنها "بالخدمة المالية عن بعد".

وتختلف التسميات حول مفهوم خدمات المصارف الالكترونية ولكنها تصب في مفهوم واحد هو المصارف التي تعمل عن طريق شبكة المعلومات الدولية (الانترنت).

تستخدم الخدمات المصرفية الالكترونية بكثرة في عمليات غسيل الأموال، خاصة في مرحلتي التوظيف والدمج، كالتحويل الالكتروني للأموال ودفع الفواتير.....

4- الاتصالات الالكترونية:

تعد الاتصالات الالكترونية من الاتصالات غير الخاضعة للقيود والضوابط الرقابية والتي من أهمها البريد الالكتروني و غرف المحادثة...

حيث يستغل المجرمون في جريمة تبييض الأموال هذه الوسائل في اتصالاتهم وخططهم لتنفيذ عملياتهم الإجرامية، وفي طرح معلومات مضللة وغير دقيقة حول أسعار الأسهم بهدف تضليل المستثمرين فيستغلها غاسلي الأموال في تحقيق أموال طائلة من عمليات البيع والشراء والتي من شأنها أن توفر الغطاء القانوني واللازم للأموال القذرة التي يغسلونها.

5- النقود الالكترونية:

وهي من أهم الأدوات التي يستعملها مجرمي تبييض الأموال وذلك لاستحالة تعقبها وسرعتها وسريتها، حيث يمكن من خلالها تحويل أي مبلغ في فترة وجيزة من دون قيود قانونية أو جغرافية أو مصرفية وبدون الحاجة إلى وسيط مالي.

6- البطاقة الذكيةsmart card:

تمتاز هذه البطاقة بأنها تمكن مستخدميها الاستغناء عن الأوراق النقدية وذلك بإضافة القيمة النقدية على الشريحة الالكترونية الموجودة على البطاقة، حيث تعمل الرقاقة أو الشريحة على تتبُع رصيد البطاقة بعد كل عملية يتم القيام بها[11].

يستطيع غاسلي الأموال استخدام البطاقات الذكية في عملياتهم الإجرامية، إذ بمقدورهم تحريك القيم النقدية المشحونة على البطاقة إلى أي مكان في العالم، كما يمكنهم إضافة أي قيم نقدية على الرقاقة الإلكترونية المحملة على البطاقة، ونظرا لان القيمة موجودة على متن البطاقة فإن التاجر الذي يقبل الوفاء بها يقوم

بالاتصال بالمصرف أو الجهة المصدرة للبطاقة للحصول على موافقتها لأجراء قيد التسوية للعملية على البطاقة، مما يعني سهولة استخدامها كوسيلة الإلكترونية لغسيل الأموال، ومن جهة ثانية يمكن لهم تهريب النقود إلى أكثر من دولة باستخدام هذه البطاقة عوضا عن النقود الورقية عبر الحدود[12].

- تشمل مراحل تبييض الأموال ما يلي:

- الإحلال (نقل الأموال المرتبطة ارتباط مباشر بالجريمة)؛
- التمويه (إخفاء المسار لإحباط عملية التعقب) ؛
- الاندماج (إتاحة الأموال للمجرم، مرة أخرى، ومن مصادر تبدو في ظاهرها مشروعة).

وتمثل مرحلة الإحلال الإدخال الأولي لعائدات الجريمة في النظام المالي للمجرم. بشكل عام، تخدم هذه المرحلة هدفين: إنها تعفي المجرم من الاحتفاظ بكميات كبيرة من النقود التي يتم الحصول عليها بطرق غير قانونية، ويتم إيداع المال في النظام المالي الشرعي. وخلال هذه المرحلة، يكون غاسلو الأموال أكثر عرضة للقبض عليهم، وذلك لأن وضع مبالغ كبيرة من النقد في النظام المالي المشروع قد يثير الشكوك.
لتأتي مرحلة التمويه بعد مرحلة الإحلال ويشار إليها أحياناً باسم "الهيكلة". وهذه هي المرحلة الأكثر تعقيداً لغسل الأموال وغالباً ما تستلزم نقل الأموال غير المشروعة دولياً. والغرض الأساسي من مرحلة التمويه هو فصل الأموال غير المشروعة من مصدرها الأصلي. ويتم ذلك من خلال عملية معقدة تتضمن الكثير من العمليات المالية، والغاية منها إخفاء مسار الحسابات وقطع الصلة مع المصدر الأصلي للنشاط الإجرامي.
والمرحلة الأخيرة من عملية غسيل الأموال تسمى "الاندماج". وخلال هذه المرحلة، يتم إعادة الأموال إلى الجناة بعد إضفاء صفة الشرعية على مصدرها. وإذ إن العائدات الإجرامية، التي تم وضعها في البداية على شكل نقود وخضعت لعدة عمليات مالية، أصبحت الآن مدمجة بالكامل في النظام المالي للجاني ويمكن استخدامها لأي غرض مشروع[13].

المحور الثاني: الجهود التشريعية لمكافحة جريمة تبييض الأموال والوقاية منها في ظلّ التطور التكنولوجي.

وضع المشرع الجزائري العديد من النصوص القانونية التي من شأنها مكافحة جريمة تبييض الأموال، وذلك من خلال العديد من القوانين أهمها قانون المالية لسنة 2018، القانون رقم 06-01 يتعلق بالوقاية من الفساد ومكافحته، القانون رقم 15-01 يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها

و العديد من أنظمة وتعليمات بنك الجزائر التي تهدف إلى الوقاية من جريمة تبييض الأموال ومكافحتها. كما أقر على البنوك والمؤسسات المالية العاملة في الجزائر اتخاذ مجموعة من التدابير التي من شأنها الوقاية من جريمة تبييض الأموال قبل حدوثها من خلال نظام بنك الجزائر رقم 03/12 المتعلق بالتدابير الوقائية من جريمة تبييض الأموال المطبقة من قبل البنوك.

أولا: النصوص القانونية المُجرمة لعمليات تبييض الأموال.

- **الإجراءات الاحترازية في قانون المالية لسنة 2018.**

وقاية من جريمة تبييض الأموال وكتدبير احترازي للوقاية من هذه الجريمة، منع المشرع الجزائري التعامل بالنقود الافتراضية، وذلك في نص المادة 117 من قانون المالية لسنة 2018، حيث جاء فيها: " يمنع شراء العملة الافتراضية وبيعها وحيازتها، العملة الافتراضية هي تلك التي يستعملها مستخدمو الانترنت عبر شبكة الانترنت، وهي تتميز بغياب الدعامة المادية كالقطع والأوراق النقدية وعمليات الدفع بالصك أو بالبطاقة البنكية، يعاقب على كل مخالفة لهذا الحكم، طبقا للقوانين والتنظيمات المعمول بها"[14].

فالمشرع الجزائري منع التعامل بالنقود الافتراضية كإجراء احترازي لما تشكله من وسيلة فعالة بالنسبة للمجرمين المحترفين في جرائم تبييض الأموال، ولما تشكله هذه التعاملات الافتراضية من أرضية خصبة ومُتاحة لتبييض الأموال بسرعة وسهولة وصعوبة في التتبُع.

- **قانون الوقاية من الفساد و مكافحته.**

جرّم القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته، في نص المادة 42 عمليات تبييض الأموال، حيث جاء فيها: " يعاقب على تبييض عائدات الجرائم المنصوص عليها في هذا القانون، بنفس العقوبات المقررة في التشريع الساري المفعول في هذا المجال"[15].

- **قانون العقوبات.**

قرر المشرع الجزائري عقوبات خاصة لجريمة تبييض الأموال، بصفة صارمة، حيث اعتبرها جنحة مشددة وذلك من خلال نص المادة 389 مكرر 01 إلى 389 مكرر 07 من قانون العقوبات[16]، وقد فرق من خلالها بين العقوبات المقررة للشخص الطبيعي و تلك المقررة للشخص المعنوي.

- **العقوبات المقررة للشخص الطبيعي.** وهي نوعان، عقوبات أصلية وأخرى تكميلية، وهي كالآتي:

✓ **العقوبات الأصلية:** نص عليها المشرع في نص المادة 389 مكرر 1 من قانون العقوبات جاء فيها:" يعاقب كل من قام بتبييض الأموال بالحبس من خمسة (5) سنوات إلى عشرة (10) وبغرامة من 1.000.000د.ج 3.000.000د.ج"

بالنسبة إلى الأجنبي الذي يمارس هذه الجريمة فيعاقب إضافة إلى المنع من الإقامة على الإقليم الوطني بصفة نهائية أو لمدة عشرة (10) سنوات على الأكثر سنوات وهذا طبقا للمادة 389 مكرر 6".

✓ **العقوبات التكميلية:**

نصت عليها المادة 389 مكرر 5 قانون عقوبات، والتي أحالتنا إلى تطبيق إحدى العقوبات التكميلية المنصوص عليها في المادة 09 من ذات القانون وهي : الحجز القانوني، الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية، تحديد الإقامة، المنع من الإقامة، المصادرة الجزئية للأموال، المنع المؤقت من ممارسة مهنة أو نشاط، إغلاق المؤسسة، الإقصاء من الصفقات العمومية، الحضر من إصدار شيكات أو استعمال بطاقة الدفع، تعليق أو سحب رخصة السياقة أو إلغائها مع المنع من استصدار رخصة جديدة، سحب جواز السفر، نشر أو تعليق حكم أو قرار إدانة، بالإضافة إلى ذلك فإنه طبقا للمادة 389 مكرر 4 قانون عقوبات، فإنه يجوز أيضا للجهة القضائية أن تحكم بمصادرة الممتلكات والعائدات التي وقع تبييضها، وكذلك مصادرة الوسائل والمعدات التي استعملت في ارتكاب الجريمة، والفوائد الأخرى الناتجة عنها في أي يد كانت، كما ذهب المشرع إلى أبعد من ذلك حيث نص على جواز حجز حتى الممتلكات الخاصة بالجاني، وهنا يأخذ بعين الاعتبار حسن النية من عدمها، وفي حالة ما إذا تعذر حجز الممتلكات محل المصادرة فإن الجهة القضائية تحكم بعقوبة مالية تساوي قيمة هذه الممتلكات.

✓ **ظروف التشديد.**

نصت عليها المادة 389 مكرر2 قانون عقوبات، بحيث يتم تشدد العقوبة على الجاني في الحالات الآتية: إذا كان مرتكب الجريمة قد ارتكبها على سبيل الاعتياد، إذا ارتكبها باستعمال تسهيلات يمنحها له نشاطه المهني، إذا ارتكبها في إطار جماعة إرهابية، في هذه الحالات يعاقب بالحبس من عشر (10) سنوات إلى عشرين (20) سنة، وغرامة مالية من 4.000.000 دج إلى 8.000.000دج.

هناك ظرف مشدد آخر نصت عليه المادة 42 قانون عقوبات، وهو: إذا كان مرتكب الجريمة أحد الأشخاص المنصوص عليهم في المادة 48 قانون الفساد وهم: قاض أو موظف يمارس وظيفة عليا في الدولة أو ضابط عمومي أو عضو في هيئة مكافحة الفساد أو ضابط أو عون شرطة قضائية أو موظف في أمانة الضبط، وكان مصدر العائدات الإجرامية التي بيضها أي الجريمة الأصلية هي جريمة من جرائم الفساد، يعاقب بالحبس من عشر (10) إلى عشرين (20) سنة. مع نفس الغرامة.

✓ **العقوبات المقررة للشخص المعنوي.**

نص عليها المشرع الجزائري في المادة 389 مكرر 7 من قانون العقوبات وهي كالآتي:

- غرامة لا يمكن أن تقل عن أربع (4) مرات الحد الأقصى لغرامة الشخص الطبيعي.
- المصادرة وهي عقوبة تكميلية وجوبية، وتأخذ نفس أحكام المصادرة بالنسبة للشخص الطبيعي كما سبق قوله.
- وقد يحكم أيضا ب: المنع من مزاولة النشاط المهني أو الاجتماعي لمدة لا تتجاوز خمس (5) سنوات، أو حلّ الشخص المعنوي.

وتجدر الملاحظة أن الشروع في هذه الجريمة يعتبر كالجريمة نفسها، وله نفس العقوبة المقررة لها وهذا طبقا للمادة 389 مكرر 3 من قانون العقوبات.

- **قانون الوقاية من تبييض الأموال.**

تضمن القانون رقم 15-01 يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها، العقوبة التي يقع على مسيري البنوك والمؤسسات المالية الذين يخالفون تدابير الوقاية من جريمة تبييض الأموال، وذلك في نص المادة 34 حيث جاء فيها:" يعاقب مسيرو وأعوان البنوك والمؤسسات المالية، والمؤسسات المالية المشابهة الأخرى الذين يخالفون عمدا وبصفة متكررة، تدابير الوقاية من تبييض الأموال وتمويل الإرهاب المنصوص عليها في المواد 7 و 8 و9 و 10 و14 من هذا القانون بغرامة من 50.000 د.ج إلى 1.000.000 د.ج[17].

ثانيا: تدابير مكافحة جريمة تبييض الأموال والوقاية منها على مستوى المصارف.

تتبع البنوك مجموعة من التدابير ذات الطابع الوقائي، من أجل منع استغلال وتوريط النظام المصرفي في عمليات تبييض الأموال، باعتباره القطاع الأكثر تعرضا لهذا النوع من الجرائم خاصة لما يعرفه من تطور تكنولوجي واستعمال للأجهزة التكنولوجيا المتطورة التي تقوم على الانترنت والتواصل الافتراضي.

حيث ألزم القانون 01/05 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما والنظام 03/12 الصادر عن بنك الجزائر مجموعة من التدابير الوقائية على البنوك، والتي يمكن إيجازها في العناصر التالية:

1. الرقابة الداخلية:

يتوجب على البنوك والمؤسسات المالية وضع نظام للمراقبة الداخلية، مع ضرورة تناسب هذا النظام مع طبيعة نشاط المؤسسات وحجمها، بالإضافة إلى وجوب التلاؤم مع مختلف المخاطر التي تتعرض لها.[18] وتتمحور مستلزمات ومتطلبات نظام الرقابة الداخلية الواجب تنفيذه على مستوى جميع البنوك، في النقاط التالية: نظام الرقابة على العمليات والإجراءات الداخلية، التنظيم المحاسبي ومعالجة المعلومات، أنظمة قياس المخاطر والنتائج، أنظمة الرقابة والتحكم في المخاطر، نظام المعلومات والتوثيق. [19]

و لتحقيق نظام رقابي داخلي فعال من أجل الوقاية من هذه الجريمة لابد للبنك والمؤسسة المالية اتخاذ مجموعة من التدابير أهمها:

– **التحقق من هوية الزبائن (العملاء):** تطبيقاً لهذا المبدأ تعمل البنوك على عدم فتح حسابات بنكية بأسماء وهمية أو مجهولة الهوية سواء تعلق الأمر بالشخص الطبيعي أو الشخص الاعتباري، ففتح الحسابات البنكية تكون بالأساس قائمة على هوية العميل، والتعرف على المستندات الرسمية الخاصة بالعميل التي تثبت الهوية الحقيقية للزبون المتعامل مع البنك،[20] ولا يقتصر هذا المبدأ على التحقق من هوية العميل بل يجب أن يشمل أيضاً التعرف على العمل الذي يمارسه والعمليات المالية التي يجريها مع البنوك والمؤسسات المالية الأخرى ومدى مشروعيتها.

– **حفظ السجلات والمستندات:** وهذا نظراً لأهمية الاحتفاظ بالسندات كونها تسهل على سلطات المكافحة معرفة مصدر الأموال ومتابعة الجريمة. لذا على المصارف والمؤسسات المالية الاحتفاظ بهوية العملاء وعناوينهم وكذا العمليات التي تم إجراءها من طرف العملاء لمدة 5 سنوات على الأقل.[21]

– **التكوين المستمر لمستخدمي القطاع البنكي:** طبقاً لتوصيات مجموعة العمل المالي التي فرضت على العاملين في البنوك برامج التدريب المتطور والمستمر، بهدف معرفة العمليات المشكوك فيها،[22] فقد ألزم

بنك الجزائر البنوك والمؤسسات المالية أن تضع برنامج تكوين دائم لمستخدميهم لزيادة وعيهم ومعرفتهم بمختلف التدابير المتعلقة بمكافحة تبييض الأموال، على أن يتلاءم مضمون هذه الدورات التكوينية مع احتياجات كل مؤسسة مالية.[23]

– **أنظمة الإنذار**: يتوجب على البنوك والمؤسسات المالية أن تتوفر على أنظمة تسمح بالنسبة إلى جميع الحسابات باكتشاف النشاطات ذات الطابع الغير اعتيادي أو المشتبه فيه. ويجب أن تخضع العمليات المشتبه فيها إلى إخطار بالشبهة يرسل إلى خلية معالجة الاستعلام المالي.

– **الإخطار بالُشبهة**: يجب على البنوك والمؤسسات المالية إبلاغ خلية معالجة الاستعلام المالي بكل عملية تتعلق بأموال يشتبه أنه متحصل عليها من جريمة أو يبدو أنها موجهة لتبييض الأموال أو تمويل الإرهاب،[24] ويتعين القيام بهذا الإخطار بمجرد وجود شبهة حتى ولو تعذر تأجيل تنفيذ تلك العمليات أو بعد إنجازها.[25] إن البلاغات التي تتلقاها الخلية معظمها من البنوك .

2. **الرقابة الخارجية**: تتمثل الرقابة على البنوك والمؤسسات المالية في رقابة اللجنة المصرفية وكذا رقابة البنك المركزي.[26] وتسهر اللجنة المصرفية على أن تتوفر البنوك والمؤسسات المالية على سياسات وممارسات وتدابير مناسبة لاسيما في ما يخص المعايير المتعلقة بمعرفة الزبون وعملياته والكشف والمراقبة بالإضافة إلى الإخطار بالشبهة مما يضمن مستوى عال من الأخلاقيات والاحترافية في الميدان المصرفي،[27] أما البنك المركزي يعتبر الرقيب الأول على نشاطات القطاع المصرفي، وعليه يسعى في أداء وظيفته الرقابية على التأكد من أن جميع البنوك الخاصة منها والعامة، تتقيد في أعمالها بأحكام البنك المركزي وقرارات مجلس إدارته وكذا التوجيهات المبلغة إليها من أجهزته المختصة.[28]

الخاتمة:

من خلال ما تمّ تناوله في هذه الورقة البحثية، فالجرائم المتأثرة بالتكنولوجيا الحديثة المتطورة أصبحت في تصاعد كبير خاصة في الآونة الأخيرة، أين وُلدت أبعاد جديدة للجريمة المالية الإلكترونية التي باتت تُشكل ظاهرة دولية معقّدة، جراء التكنولوجيا الرقمية، في ظل حصول جرائم مالية كبيرة سابقاً من خلال الإحتيال على المستثمرين والتلاعب بالأسعار في البورصات العالمية وإفشاء معلومات مميّزة داخلية أدت إلى إفلاس الكثير من الشركات والأفراد. علماً أن المطلوب، في البلدان النامية، بغية تحسين

الأداء حيال مكافحة ومعاقبة الجرائم المعلوماتية، هو إجراء تعديلات على القوانين الحالية وإيجاد بعض القوانين الجديدة لتجريم الأنواع الجديدة من الجرائم.لذلك كان لابد من الأخذ بمجموعة من التوصيات التي من شأنها أولا الوقاية من جريمة تبييض الأموال ومكافحتها بالدرجة الثانية، باعتبار هذا النوع من الجرائم من أكثر الجرائم تأثرا بالتكور التكنولوجي الحاصل، نذكر أهم هذه التوصيات ونحصرها فيما يلي:

– ضرورة تطبيق البنوك الجزائرية التدابير الوقائية والاحترازية التي من شأنها الوقاية من الجريمة قبل وقوعها، تطبيقاً صارماً،

–تكوين كفاءات في مجال جرائم تبييض الأموال باستخدام الوسائط الالكترونية، وذلك من أجل تسهيل اكتشاف ومتابعة مثل هذه الجرائم،

–منح صفة الضبطية القضائية لموظفي البنوك والمؤسسات المالية المختصين في تتبع هذه الجرائم، لما لهم من خبرة واسعة في هذا المجال، وذلك لتعقب هذه الجرائم والتحقيق فيها واتخاذ الإجراءات القانونية اللازمة،

– تزويد البنوك بأنظمة معلوماتية متطورة، تسيرها كفاءات ذات خبرة في مجال الجرائم التكنولوجية الحديثة ومنها جرائم تبييض الأموال،

–تخصيص باب في قانون العقوبات يجرم جريمة تبييض الأموال ويحدد إجراءات متابعتها بموجب قانون الإجراءات الجزائية،

– تكاثف الجهود بين المختصين في مجال تقنية المعلومات و المجال القانوني و الاقتصادي حول إيجاد الحلول الجذرية لمكافحة جريمة تبييض الأموال،

-اتخاذ التدابير الكافية لمنع سوء استخدام التطورات التكنولوجية في عمليات تبييض الأموال.

❖ **قائمة المراجع والمصادر حسب ورودها في الورقة البحثية.**

[1]-قدور طارق/ زغدي باديس،" دور التكنولوجيا المالية في تطوير الخدمات المصرفية لتحقيق الشمول المالي في الجزائر"، مجلة الاقتصاد و التنمية المستدامة، جامعة الوادي، بتاريخ 2022/03/02، الصفحة 874.

[2]- محمد قوجيل/ عبد العزيز طيبة،"مخاطر التكنولوجيا المالية وادارتها في القطاع المصرفي-دراسة تنظيمية واحترازية-"، مجلة الاقتصاد والمالية، المجلد 08، العدد 02، السنة 2022، الصفحة 187 و 188.

[3]- محمد أمين زايخ/ محمد يونسي، "دور التكنولوجيا المالية في تعزيز الشمول المالي في الوطن العربي –تجربة المملكة العربية السعودية"، دفتر البحوث العلمية المركز الجامعي تيبازة ، مجلد 10، العدد 01، السنة 2022، الصفحة 749.

[4]-البنك المركزي المصرفي، "التطورات الاقتصادية العالمية وانعكاساتها على عمليات البنوك مع إشارة خاصة لمصر"، الصفحة 31.

[5]-سامي أحمد مراد، "دور اتفاقية تحرير الخدمات الدولية في رفع كفاءة أداء الخدمات المصرفية"، المكتب العربي للمعارف، طبعة أولى، 2005، الصفحة 179.

[6]- آسيا قاسمي، "آثار العولمة المالية على تطوير الخدمات المصرفية وتحسين القدرة التنافسية للبنوك الجزائرية"، أطروحة دكتوراه، كلية العلوم الاقتصادية والتجارية وعلوم التسيير، جامعة أحمد بوقرة بومرداس، الجزائر، 2015، الصفحة 213 و 214.

[7] - https://ar.wikipedia.org/wiki/LE 15/08/2022.

[8]- رافعة إبراهيم الحمداني، "اثر استخدام التكنولوجيا المصرفية على ظاهرة غسيل الأموال والجهود الدولية لمكافحتها"، المؤتمر العلمي الرابع، "استراتيجيات الأعمال في مواجهة تحديات العولمة"، جامعة فيلاديلفيا، آلية العلوم المالية و الإدارية، 16/15 مارس 2005، www.philadelphia.edu.jo

[9]-عصام عبد الفتح مطر،" التحكيم الالكتروني"،دار الجامعة الجديدة الإسكندرية –مصر- 2009، الصفحة 18.

[10]- بن نقي سفيان، "جريمة غسيل الأموال بين الوسائط الالكترونية والنصوص التجريمية"، مجلة الأبحاث القانونية والسياسية، المجلد 03، العدد 02، 2021، الصفحة 159.

[11]– فريد علوش، " جريمة غسل الأموال –المراحل والأساليب"، مجلة العلوم الإنسانية –بسكرة– ، العدد 12، 2007، الصفحة 257.

[12]– أشرف شمس الدين توفيق، " تجريم غسيل الأموال في التشريعات المقارنة"، دار النهضة العربية ،مصر، 2001، الصفحة 56.

[13]- https://www.unodc.org/e4j/ar/organized-crime/module-4/key-issues/money-laundering.html, مكتب الأمم المتحدة المعني بالمخدرات والجريمة، نشرت النسخة الإنجليزية لأول مرة في جويلية 2018؛ تمت مراجعتها في جانفي 2019، نشرت الترجمة العربية في شهر أفريل 2021.

[14]– المادة 117 من قانون المالية لسنة 2018، الصادر بتاريخ 2017/12/31، الجريدة الرسمية بتاريخ 2017/12/28، العدد 76، الصفحة 56.

[15]– قانون رقم 01/06 يتعلق بالوقاية من الفساد و مكافحته،الجريدة الرسمية لسنة 2006، العدد 14، المعدل و المتمم، بموجب القانون رقم 11-15 بتاريخ 2011/08/02، الجريدة الرسمية العدد 44، الصفحة 8.

[16]– القانون 06-23 الصادر بتاريخ 2006/12/20 المعدل و المتمم لقانون العقوبات، الجريدة الرسمية بتاريخ 2006/12/23، العدد 84.

[17]– المادة 34 من القانون رقم 05-01 بتاريخ 2005/02/06، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتها، الجريدة الرسمية بتاريخ 2005/02/09، العدد 11.

[18] موسى مبارك أحلام، "آلية رقابة البنك المركزي على أعمال البنوك في ظل المعايير الدولية – دراسة حالة بنك الجزائر–"، كلية العلوم الاقتصادية وعلوم التسيير، قسم: التسيير، مذكرة مقدمة ضمن متطلبات نيل شهادة ماجستير، فرع: نقود ومالية، جامعة الجزائر، 2005/2004، ص 159.

[19] نظام بنك الجزائر رقم 02-03، المؤرخ في 14 نوفمبر 2002، المتضمن المراقبة الداخلية للبنوك والمؤسسات المالية.

[20] عبد السلام حسان، "جريمة تبييض الأموال وسبل مكافحتها في الجزائر"، كلية الحقوق والعلوم السياسية، قسم: الحقوق، أطروحة دكتوراه، تخصص: قانون جنائي، جامعة لمين دباغين، سطيف، الجزائر، 2016/2015، ص 183.

21 نادية عبد الرحيم،" مكافحة تبييض الأموال في الجهاز المصرفي الجزائري"، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، قسم العلوم الاقتصادية، أطروحة دكتوراه، جامعة الجزائر 3، 2015/2014.ص 233.

22 عبد السلام حسان، "جريمة تبييض الأموال وسبل مكافحتها في الجزائر"، كلية الحقوق والعلوم السياسية، قسم: الحقوق، أطروحة دكتوراه، تخصص: قانون جنائي، جامعة لمين دباغين، سطيف، الجزائر، 2016/2015.، ص 188.

[23] نظام رقم 12-03، مرجع سبق ذكره، ص 27.

[24] نوفل سمايلي، محمد حسن رشم، فضيلة بوطورة، "تطور أساليب غسيل الأموال ودور إجراءات الرقابة في البنوك لتعزيز مواجهة الظاهرة (مع الإشارة لإجراءات البنوك في الجهاز المصرفي الجزائري)"، مجلة آفاق للعلوم، العدد 01، جامعة زيان عاشور، الجلفة، الجزائر، 2016، ص 19.

[25] مباركي دليلة، "غسيل الأموال، كلية الحقوق والعلوم السياسية"، قسم: العلوم القانونية، أطروحة دكتوراه، تخصص: قانون جنائي، جامعة الحاج لخضر، باتنة، الجزائر، 2008/2007، ص 116.

[26] المرجع أعلاه، ص 250.

[27] نوفل سمايلي، مرجع سبق ذكره، ص 20.

[28] موسى مبارك أحلام، مرجع سبق ذكره، ص 17-18.

جامعة الجزائر 1 بن يوسف بن خدة

كلية الحقوق

الملتقي الدولي الافتراضي الموسوم بـ.

القانون الجنائي في ظل التطور التكنولوجي

إشكالات ومعالجات

المنعقد في يومي 28 ، 29 سبتمبر 2022

البحث المقدم من

المستشار الدكتور

محمد جبريل إبراهيم حسن

نائب رئيس هيئة قضايا الدولة المصرية

كلية الحقوق – جامعة القاهرة

عضو الجمعية المصرية للاقتصاد السياسي والاحصاء والتشريع

gebrelmohamed865@gmail.com

ت 01010999796

البحث بعنوان

المواجهة التشريعية للجرائم الالكترونية

دراسة تحليلية مقارنة

المواجهة التشريعية للجرائم الالكترونية

دراسة تحليلية مقارنة

مستشار دكتور

محمد جبريل إبراهيم حسن

نائب رئيس هيئة قضايا الدولة المصرية

كلية الحقوق –جامعة القاهرة

عضو الجمعية المصرية للإقتصاد السياسي والإحصاء والتشريع

Email :gebrelmohamed865@gmail.com

مقدمة:

بظهور التقنيات الحديثة توازي مع ذلك أيضاً ظهور مظاهر إجرامية حديثة تحت مسمي الجريمة الالكترونية ، كجرائم إساءة استخدام الإنترنت ، أو استخدمه في أغراض إجرامية كانتهاك الخصوصية ، والقرصنة والانتفاع بدون حق بخدمات الشبكات ، أو الدخول غير المشروع لموقع إلكتروني غير مصرح بالدخول عليه ، فالجريمة الإلكترونية من الجرائم المستجدة التي تنتج عن الممارسات السيئة لثورة تقنية التكنولوجيا المعلوماتية والتي تختلف كثيراً عن الجريمة التقليدية في طبيعتها ومضمونها ووسائلها و أدواتها، وحتى في خصوصية مرتكبها.

ولذلك لاقت هذه الجريمة الاهتمام التشريعي والفقهي علي المستوي الدولي والداخلي ، للتصدي لها من خلال إصدار التشريعات المناسبة ، وإجراء التعديلات على القوانين العامة و الخاصة ذات الصلة و أهمها قانون العقوبات و قانون الإجراءات الجنائية ، ولقد كان حرص المشرع المصري في هذا المجال ملحوظاً بمواكبة المستجدات التي يعيشها العالم من خلال ثورة التكنولوجيا والمعلومات ، فتم إصدار التشريعات الحاكمة لذلك ومنها قانون تنظيم الاتصالات رقم 10 لسنة 2003 ، والقانون رقم 15 لسنة 2004 بتنظيم التوقيع الإلكتروني ، ثم إصدار القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات .

وتأتي أهمية هذا البحث بعد ازدياد الجرائم الالكترونية في ظل النظام القانوني العقابي والإجرائي المعمول به ، لقد شهدت السنوات الأخيرة تطورا علمياً وتقنياً في شتى مناحي الحياة، ومن بين ما يشهده العالم من مستجدات التكنولوجيا هو ما يعرف بالشبكة المعلوماتية التي استحوذت على أغلب مجالات الحياة، فلا تكاد أن تخلو أي دار من موبايل أو جهاز حاسب آلي ، ولا تكاد تخلو أي مؤسسة أو بنك أو جهة حكومية من حاسب آلي يتولى الدور الأساسي والفعال في تسيير حركه العمل داخل هذه الجهة، وقد أدى انتشار هذه الحواسيب إلى قيام ما يعرف بثورة المعلومات ودخول العالم إلى مرحلة جديدة من الحضارة تعتمد اعتمادا كبيراً على التكنولوجيا، وقد ساهم هذا التطور في انبعاث تجارة إلكترونيه عالمية، تتم فيها الصفقات المالية الضخمة.

ومع هذه الإيجابيات الموجودة في سهولة التعامل وكذا سرعة التعاقد، إلا أنه قد ظهرت بالتوازي معها أمور سلبية من بينها الجريمة الإلكترونية بكل أشكالها و صورها أو الجرائم التقنية العالية أو Cyber Crime ، أو جرائم أصحاب الياقات البيضاءWhite Collar ، فهي ظاهرة إجرامية مستجدة ، تدق لأجلها أجراس الخطر لتنبه المجتمعات بحجم المخاطر وهول الخسائر الناجمة عنها باعتبارها تستهدف الاعتداء على المعطيات بدلالتها التقنية

الواسعة، والقيم المجتمعية الراسخة ، فهي جريمة تقنية تنشأ في الخفاء يقترفها مجرمون من كافة الفئات ، صغار وكبار ، فقراء وأغنياء ، ولكنهم أذكياء يمتلكون أدوات المعرفة و التقنية.

وتظهر خطورة الجرائم الإلكترونية في أنها تطال الحق في المعلومات وتمس الحياة الخاصة للأفراد وكذا تهدد الأمن و السيادة الوطنية وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشري.

لذا فإن إدراك ماهية الجرائم الإلكترونية، واستظهار موضوعها وخصائصها و مخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والاجتماعية والثقافية وكذا الأمنية.

البداية التاريخية لجرائم تقنية العلومات :

بدأ ظهور الإنترنت في الولايات المتحدة الأمريكية ، حينما شرعت وزارة الدفاع الأمريكية في عام 1969 بالعمل في مشروع شبكة وكالة الأبحاث المتقدمة(APRANET) . Advanced Research Projects Agency Networkولقد تم تطوير هذا المشروع عن طريق مراكز الأبحاث الجامعية أثناء الحرب الباردة ، وكان الهدف منه إقامة شبكة بين خطوط الحاسبات طويلة المدي تقاوم التدمير الجئي وتربط بين مراكز الحاسبات المختلفة وأنظمة الراديو والأقمار الخاصة بالولايات المتحدة الأمريكية في أنحاء العالم ، بحيث إذا تم تدمير جزئي لهذه الشبكة استمر العمل دون توقف بفاعلية فائقة [1] .

ونتيجة لنجاح المشروع رأت وزارة الدفاع الأمريكية في عام 1983 فصل الجانب العسكري عن الشبكة والاستقلال بشبكة خاصة (MILNET) ، وأسندت للهيئة القومية للعلوم بإنشاء شبكة مستقلة (NSFnet) ، وذلك بتوصيل خمسة حاسبات رئيسية لخدمة مركز البحوث الأمريكية بحيث حلت هذه الحاسبات والتي تعمل بسرعة فاقئة محل النظام السابق .

---

[1] د/ مدحت رمضان : جرائم الاعتداء علي الأشخاص والإنترنت – دار النهضة العربية 2000 – ص 5 .

واعتباراً من عام 1987 بدأ السماح للأفراد العاديين باستعمال شبكات الإنترنت (NSF net) ، وتزايدت أعداد المستخدمين لهذه الشبكة ، وظهرت (بيتنت) ، ثم ظهر الإنترنت في صورته الحالية ، وما صاحبه من الجرائم المرتبطة به[1] .

الإنترنت والإجرام :

كان للإنترنت الفضل العظيم علي الإعلام والتواصل و المراسلة ، وكذلك علي التعليم والبحث العلمي حيث يمكن عن طريق شبكة الإنترنت الإطلاع علي أحدث ما وصل إليه العلم من أبحاث بكل سهولة ويسر ، وبأقل التكاليف ، وكذلك تسهيل وصول المعلومة والتعليم عن بعد ، إلا أن ذلك لم يمنع استخدام الإنترنت استخداماً سيئاً ، فلم يخلو هذا المجال من النصب والاحتيال ، والتخريب والإرهاب وغسل الأموال ، والتجارة غير المشروعة ، وكذلك التشهير والتنمر والسب والقذف حيث تيسر هذه الشبكة المظلمة ارتكاب الجريمة دون التواجد في مكانها ، مع سرعة إخفاء آثارها ووسائلها ، حتى أصبح الإنترنت كالغابة التي تكثر فيها الاعتداءات والضحايا ، ويتضاءل فيها دور القانون، وتقل فيها الأخلاقيات ، ويضعف فيها ردع العقاب [2] .

إطار المواجهة التشريعية للجرائم الالكترونية :

تمثل المواجهة التشريعية للجرائم الالكترونية الركن الشرعي الذي لا تقوم الجريمة إلا به ، وهو يعني السند القانوني لتجريم الفعل ؛ وذلك تطبيقاً لمبدأ شرعية الجرائم والعقوبات ؛ حيث لا جريمة ولا عقوبة إلا بنص وإعمالاً لذلك فإنه من غير الممكن بأي حال من الأحوال الاجتهاد من القاضي الجنائي بدون توافر هذا النص، فلا يجوز القياس في التجريم ولا في العقاب .

والجرائم الالكترونية حديثة النشأة وذات تقنية عالية، ولم يكن وضع نصوص خاصة بها بالأمر السهل، وعلى الرغم من ذلك فقد نجحت بعض الدول في وضع قوانين لمثل هذه الجرائم ، وتعد دولة السويد أول دولة تضع مثل هذا القانون ، حيث أصدرت في عام 1973 قانون البيانات، وبعد ذلك وبين عامي (1976-1985) سنت

---

[1] TORTELLO NICOLE , lointier Pascal , internet Pour LES Juristes,Dalloz 1996,P.2.

[2] د/ خالد عبد العظيم أبو غابة : التقدم التكنولوجي وأثره علي جرائم العرض –دراسة مقارنة – مكتبة الوفاء القانونية 2021 – ص 19 .

الولايات المتحدة الأمريكية قانون لحماية أنظمة الحاسب الآلي، فتبعتها فرنسا والتي قامت في عام 1988 بتطوير قوانينها الجنائية لتتوافق مع ما استحدث من جرائم، وأما فيما يخص الدول العربية فقد قامت بعضها بسن بعض القوانين في هذا المجال ، مثل السعودية التي أصدرت في العام 2007 نظامي التعاملات الالكترونية ونظام مكافحة الجرائم المعلوماتية والإمارات العربية المتحدة التي أصدرت القانون الاتحادي رقم [2] لسنة 2006 بشأن مكافحة جرائم تقنية المعلومات ، ثم أصدرت مصر القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

أهمية الدراسة :

تأتي أهمية الدراسة من أهمية موضوعها ، وما تتسم به الجرائم الإلكترونية من خطورة ، حيث تعد من أحدث أنواع الجرائم، ومسرحها العالم الافتراضي غير الملموس ، والبعيد عن أي مظهر من مظاهر الجريمة التقليدية فهي جريمة عابرة للحدود يرتكبها مجرمون ذو مستوى عالي في أي مكان ، ويتمتعون بالذكاء والتمّيز في المجال التقني، مما يؤدي إلى تشتيت الجهود الدولية في محاولة تعقبها و التحري عنها، أو الوصول إلى مرتكبها.

وتبدو أهمية الدراسة أيضاً في الأثر الواسع للضرر الناتج عن الجرائم الإلكترونية ، فهي قد تقف عن ضحية واحدة ، بل تتعدد الضحايا عن هذه الجرائم ، مع الإصابة بالضرر الفادح ، مع سهولة ارتكاب الجريمة ، وصعوبة اكتشاف مرتكبها الذي عادة ما يصعب معرفته و يفلت بسهولة من العقاب .

أما الأهمية البارزة لموضوع الدراسة فهو ارتباطه بجريمة الإرهاب الإلكتروني ، فلا شك أن الجريمة الإلكترونية ترتبط ارتباطاً وثيقاً بسلوكيات الإرهاب ، مما يكون له أكبر الأثر بأمن واستقرار الدول .

إشكالية الدراسة :

تتمثل إشكالية الدراسة في المصطلحات المستخدمة في عناصر هذه الدراسة ، و التي يجب نحتها بداية حتي نستطيع الإلمام بالبنيان القانوني للجريمة ، فالحكم علي الشيء فرع من تصوره ، ولم يعتاد الباحث القانوني كثيراً علي استخدام مصطلحات كالمستخدمة في الجريمة الإلكترونية ، كالتقنيات الإلكترونية ، وشبكات الإنترنت ، والمنصات الإلكترونية ، والأكواد والشفرات والحروف والرموز والإشارات ، وشبكة المعلومات والحساب الخاص

والبريد الإلكتروني والدليل الرقم والدعامة الإلكترونية ، فتتبع الإشكالية في دراسة هذه الجرائم من خصوصية المصطلحات المستخدمة للدلالة علي السلوك الذي تنشأ به الجريمة .

كما تتمثل إشكالية هذه الدراسة في صعوبة الإلمام والمتابعة لجرائم الحاسب الآلي و الإنترنت و كذا الكشف عنها، لتطلبها فنيات عالية في هذا المجال ؛ لأن هذه الجرائم لا تترك أثرا فليست هناك أموال أو مجوهرات مفقودة ،و إنما هي أرقام تتغير في السجلات و معظم جرائم الحاسب الآلي تم اكتشافها بالصدفة و بعد وقت طويل من ارتكابها ، كما أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف الشر عنها .

كما تبدو الإشكالية في هذا الدراسة أيضاً في أن هذا النوع من الجرائم يصعب إثباتها ، ويصعب معرفة توقيتها ، فهي جرائم لا تترك أثراً ظاهراً بعد ارتكابها ، كما يصعب الاحتفاظ بأثرها إن وجد، كما إنها تحتاج إلى خبرة فنية و يصعب على المحقق التقليدي التعامل معها ، لأنها تعتمد على الخداع في ارتكابها و التضليل في التعرف على مرتكبها، بالإضافة إلى أن ارتباط الجريمة الإلكترونية بجهاز الحاسب الآلي و شبكة الإنترنت أضفى عليها مجموعة من الخصائص التي تميزها عن الجرائم التقليدية ، كالسرية ، والتشفير والخفاء التام ، فهي أشبه ما يكون بالجرائم الصامتة .

الهدف من الدراسة :

نظراً لتزايد مخاطر الجرائم الإلكترونية وتهديدهاللحق الخصوصية ، والمساس بالحياة الخاصة للأفراد ، وكذا تهديد الأمن و السيادة الوطنية ، مما يؤدي إلي فقدان الثقة في كل ما يحيط بالفرد .

لذا كان من الضروري إلقاء الضوء علي الجرائم الإلكترونية ، إدراك ماهيتها، واستظهار موضوعها وخصائصها و مخاطرها وحجم الخسائر الناجمة عنها وسمات مرتكبيها ودوافعهم ، حتي يتم اتخاذ الاحتياطات التشريعية اللازمة والاستثنائية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والاجتماعية والثقافية وكذا الأمنية ، ومن ثم مواجهتها علي كافة المستويات الأمنية والتشريعية والتنفيذية .

منهج الدراسة :

أخذنا في البحث منهج استقراء وتحليل نصوص قانون العقوبات وإسقاط الجرائم الالكترونية المتنوعة على نصوصه لنرى ما إذا كانت تلك النصوص كافية للتصدي للجرائم الالكترونية، أم أن تلك الجرائم كلها أو بعضها بحاجة إلى نصوص خاصة بها حتى لا يفلت مجرمي هذا العصر ومفرزاته من العقاب، والبحث في المنظومة التشريعية عن قوانين قد تسعفنا لتكملة النقص التشريعي إن وجد.

وبما أن السلطات المنوط بها ملاحقة هذا النوع من الجرائم تستند في عملها ابتداء على القانون الموضوعي " العقابي " ومن ثم تسير وفق ما يرسمه لها القانون الإجرائي، فإن إشكالية أخرى قد تقع فيها تلك السلطات إذا ما كان القانون الإجرائي عاجز عن تقديم ما يلزم لتلك السلطات لملاحقة تلك الجرائم، فالقانون الإجرائي يعد وبحق المساعد الأول لتطبيق القانون العقابي.

لما تقدم فإننا سنركز دراستنا هذه على الإشكاليات الموضوعية والإجرائية في النظام القانوني فيما يخص التكييف القانوني للجريمة الالكترونية ومدى إمكانية ملاحقتها والتحقيق فيها للوصول إلى التكييف القانوني لها إن وجد، وإلا فإننا سنكون أمام قصور تشريعي يسمح لمرور الكثير من الجرائم الالكترونية دون ملاحقة ودون عقاب.

لذلك فإن هذا البحث سيعتنق المنهج الاستقرائي الاستنباطي القائم على دراسة النصوص القانونية لنرى مدى توافقها وانطباقها على الجرائم الالكترونية، ومدى صلاحيتها لملاحقة هذه الجرائم وتكييفها تكييفا قانونياً يتطابق مع أركان الجريمة الالكترونية بمفهومها العصري المستقر عليه في الفقه الحديث.

خطة الدراسة :

خطة بحثنا ستتكون علي النحو الأتي:

الفصل الأول : مفهوم الجريمة الإلكترونية وخصائصها

المبحث الأول : مفهوم الجريمة الالكترونية

أولا : المصطلحات المكونة لتعريف الجريمة الالكترونية .

ثانياً : تعريف الجريمة الإلكترونية .

المبحث الثاني : خصائص الجريمة الإلكترونية .

المبحث الثالث : مخاطر الجريمة الالكترونية .

الفصل الثاني : المواجهة التشريعية للجرائم الالكترونية .

المبحث الأول : المواجهة التشريعية لجرائم الاعتداء علي الشبكات وأنظمة وتقنيات المعلومات واستخداماتها غير المشروعة .

المطلب الأول : جرائم الاعتداء علي الشبكات وأنظمة وتقنيات المعلومات واستخدمها استخدام غير مشروع .

المطلب الثانى : الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات .

المطلب الثالث : الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصةوالمحتوى المعلوماتى غير المشروع .

المبحث الثاني : الجرائم المرتكبة من مدير الموقع ومقدم الخدمة .

أولاً : إنشاء أو إدارة أو استخدام موقع لهدف غير مشروع .

ثانياً : جرائم مُقدم الخدمة .

المبحث الثالث :الجرائم الالكترونية المرتكبة بمعرفة الشخص الاعتباري .

أولاً : مسئولية الشخص المسئول عن إدارة الشخص الاعتباري .

ثانياً : مسئولية الشخص الاعتباري الجنائية .

الفصل الثالث : الأحكام الإجرائية للجريمة الالكترونية في القانون المصري .

المبحث الأول : خصوصيةالضبط والتحقيق في الجريمة الالكترونية

أولاً : خصوصية الضبط في مرحلة جمع الاستدلالات :

ثانياً : خصوصية التفتيش في الجريمة الالكترونية.

ثالثا : مرحلة التحقيق الإبتدائي.

رابعاً : مرحلة الأوامر القضائية المؤقتة .

المبحث الثاني : مسرح الجريمة الالكترونية والاستعانة بالخبرة الفنية وحجية الدليل الرقمي

المطلب الأول : مسرح الجريمة الالكترونية .

المطلب الثاني : إجراءات الاستعانة بالخبرة الفنية .

المطلب الثالث : حجية الأدلة الرقمية في الجرائم الالكترونية .

المبحث الثالث : إجراءات المنع من السفر وترقب الوصول والصلح والتصالح في الجرائم الالكترونية

المطلب الأول :إجراءات المنع من السفر وترقب الوصول .

المطلب الثاني : الصلح والتصالح في الجرائم الالكترونية .

وعلي الله قصد السبيل،،،

الفصل الأول

مفهوم الجريمة الإلكترونية وخصائصها

تتميز الجريمة الالكترونية عن الجريمة التقليدية تميزاً واضحاً من حيث نطاقها ووسائلها وأطرافها ، وخصائصها سوف نتحدث في هذا الفصل عن مفهوم الجريمة الالكترونية وخصائصها، وذلك علي التفصيل الأتي :

المبحث الأول : مفهوم الجرائم الالكترونية .

المبحث الثاني : خصائص الجرائم الالكترونية .

المبحث الأول

مفهوم الجريمة الالكترونية

مصطلح الجرائم الالكترونية هو مصطلح جديد بالنسبة للباحث في المجال القانوني ، ولقد ابتعدت معظم التشريعات عن وضع تعريف لهذه الجرائم ، ولذلك فقد أختلف فقهاء القانون الجنائي في وضع تعريف للجرائم الالكترونية ، وإن كانت معظم التعريفات تدودر حول وسيلة ارتكابها وهي تقنية المعلومات .

وتتضمن الجريمة الالكترونية عدة مصطلحات تعد حديثة علي مسامع الباحث القانوني ، ونعرض فيما يلي لهذه المصطلحات من خلال عرض مفهوم الجريمة الالكترونية وتعريفاتها.

وإذا كان مفهوم الجريمة الالكترونية لا يخرج عن كونه فعلاً غير مشروع يرتكبه المجرم المعلوماتي باستخدام الحاسب الآلي عن طريق ، المعالجة الآلية للبيانات[1] ، فإن هذا المفهوم يستلزم أن نعرض في البداية للمصطلحات المكونة لتعريف الجريمة الإلكترونية ، ثم تعريف الجريمة وخصائصها ، فيما يلي :

أولا : المصطلحات المكونة لتعريف الجريمة الالكترونية :

تُعد الجريمة الإلكترونية من الجرائم المستحدثة التي أفرزتها الممارسة السيئة لثورة التكنولوجيا المعلوماتية التي تختلف كثيرا عن الجريمة التقليدية في طبيعتها و أنواعها وأدواتها، وحتى في خصوصية وتمييز مرتكبيها، ولذلك فهي تحتاج إلي نحت مصطلحات جديدة لتقريب مفهومها إلي الذهن ، حيث يتصور وجود مصطلحات قد تكون حديثة نسبياً بالنسبة لمسامع الباحث القانوني ، كالإنترنت والحاسب الآلي ، والمعلومات الإلكترونية ، وغيرها من المصطلحات المستحدثة[2] ، ولذلك وقبل الخوض في إعطاء تعريفات للجريمة الإلكترونية لابد من الإشارة إلي المصطلحات المتعلقة بهذه الجريمة والتي نذكر منها:

1- مصطلح الالكتروني:

---

[1] د/ علي عبد القادر القهوجي : الحماية الجنائية لبرامج الحاسب – بحث منشور بمجلة البحوث القانونية والاقتصادية التي تصدرها كلية الحقوق –جامعة الاسكندرية 1997 .

[2] القاضي / عمر محمود الحوتي : الوجيز في الحماية الجنائية من جرائم تقنية المعلومات وفق أحكام القانون 175 لسنة 2018 – دار النهضة العربية 2012 – ص 21 .

هذا المصطلح يشمل كل ما يرتبط بالحواسيب والشبكات ، فيقصد به تقنية استعمال وسائل كهربائية أو كهرومغناطيسية أو بصرية أو أي شكل أخر من وسائل التقنية المشابهة [1] .

2- **الحاسب الآلي :**

يعرف الحاسب الآلي بأنه أي جهاز إلكتروني ثابت أو منقول سلكي أو لاسلكي يحتوي على نظام معالجة البيانات أو تخزينها أو إرسالها أو استقبالها ، ويؤدي وظائف محددة بحسب البرامج و الأوامر المعطاة له[2].

و ويحتوي الحاسب الآلي علي مجموعة من الأجزاء المتداخلة المادية و المعنوية وبتكامل هذه الأجهزة يقوم الجهاز باستقبال البيانات ومعالجتها من خلال مجموعة من عمليات حسابية بسرعة عالية و تسلسل منطقي تظهر بعدها النتائج المطلوبة ويمكن تخزينها والاستفادة منها مرات عديدة [3] .

ومن ثم فإن الحاسب الآلي هو عبارة عن جهاز إلكتروني يحتوي علي مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة و إدارة المعلومات بطريقة ما، وذلك بتنفيذ ثلاث عمليات أساسية هي : استقبال البيانات المدخلة (الحصول على حقائق مجردة) ، ومعالجة البيانات إلى معلومات (إجراء الحسابات والمقارنات ومعالجة المدخلات)، وإظهار المعلومات المخرجة (الحصول على نتائج) .

3- **المعلومات الرقمية :**

المعلومات الرقمية هي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بوسائل تقنيه المعلومات بوجه خاص الكتابة والصور والصوت و الأرقام و الحروف والرموز والإشارات وغيرها[4] ، وهي ليست أرقام وكلمات فقط ، بل يمكن

---

[1] د/ نهلا عبد القادر المؤمني : الجرائم المعلوماتية – دار الثقافة – عمان 2012 – ص 51 .

[2] د/ أحمد محمود مصطفي : جرائم الحاسبات الآلية في التشريع المصري – دار النهضة العربية –الطبعة الأولي 2010 – ص 35

[3] د / هدي حامد قشقوش : جرائم الحاسب الإلكتروني في التشريع المقارن – دار النهضة العربية القاهرة 1992 – ص 5 .

[4] د/ محمد سامي الشوا :الغش المعلوماتي كظاهرة إجرامية مستحدثة – بحث منشور في مؤتمر الجمعية المصرية للقانون الجنائي – القاهرة في 28/25 أكتوبر 1993 – ص 516 .

رقمنة أي شئ يمكن سماعه أو رؤيته ، فيمكن أن تحتوي قواعد البيانات والإنترنت علي موسيقي أو صور أو أعمال فنية ، وكذلك المنتجات السمعية أو البصرية [1] .

4- **المجرم المعلوماتي:**

هو الشخص الذي يرتكب الجرائم الالكترونية باستخدام الحاسب الآلي كوسيلة أو كهدف أو كليهما معاً ، ويتمتع هذا الشخص بالمهارة والمعرفة و الحيلة وكذلك الباعث من أجل تنفيذ نشاطه الإجرامي ، فالجاني في جرائم التقنية شخص طبيعي، يتوافر لديه كشرط أساسي معرفة كافية بآلية عمل و تشغيل الحاسب الآلي، و لا نقصد هنا المستوى الرفيع العالي من المعرفة، فإن الجريمة وإن كانت ترتبط بتقنية نظم المعلومات والحاسب الآلي من حيث السعة و الأسلوب و النتيجة، إلا أن الحد الأدنى من المعرفة يكفي لظهور الجريمة وإمكان ارتكابها خصوصاً إذا ما اتسعت دائرة الإجرام ، فاستعان الفاعل ذاته بغيره ممن يساعده ويساهم معه في إيقاع الجريمة وارتكابها[2].

وقد وجد الباحثون صعوبة في إيجاد تصنيف منضبط لمجرمي هذه التقنية و السبب راجع إلي التغير السريع الحاصل في نطاق هذه الظاهرة المرتبطة أساساً بالتسارع الرهيب في ميدان الكمبيوتر والانترنت [3]، ويمكن تقسيم مجرمو المعلوماتية (Cyber Criminels) إلى ثلاث مجموعات من الطوائف المختلفة، وهذا التصنيف كان قائماً على أساس أغراض الاعتداء ،وذلك علي النحو الأتي :

(أ)المخترقون أو المتطفلون: وهذه الفئة من المجرمون ينطلقون من دوافع إثبات الذات و المقدرة التقنية علي اختراق الحسابات الشخصية للاستطلاع والاستكشاف ، وعادة ما يتسمون بصغر السن، و لا تتوافر لديهم دوافع حاقدة أو تخريبية أو ربحية فهم يسعون إلى الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها ،

---

[1] د/ عبد الله عبد الكريم عبد الله : جرائم المعلومات والإنترنت – الجرائم الإلكترونية – منشورات الحلبي الحقوقية بيروت 2011 – ص 53 .

[2] د/ هشام محمد فريد رستم : جرائم الحاسب المستحدثة – دار الكتب القانونية – مصر 1999 – ص 110 .

[3] د/ مدحت رمضان : جرائم الاعتداء علي الأشخاص والإنترنت – مرجع سابق – ص 11 .

أو اختراق الحسابات الشخصية ليطلعوا علي المعلومات الشخصية بها ، مثل النشاطات والمحادثات والمراسلات ، وغيرها من البيانات [1] .

(ب) مجرمو الحاسبات المحترفون: تتمتع هذه الطائفة بسعة الخبرة والإدراك للمهارات التقنية كما تتميز بالتخطيط والتنظيم للأنشطة التي يرتكبوها ؛ فهم يسعون من وراء ذلك إلى تحقيق الربح المادي بطريقة غير مشروعة، ويتم عمل هذه المجموعات في إطار منظم ينطبق على أفعالهم وصف الجريمة المنظمة وتعد هذه الطائفة الأخطر من بين مجرمي التقنية ، فهم يسيطرون علي الحسابات والمواقع وسرقة ما تحتويه من ملفات [2] .

وغالياً ما تتم هذه الجرائم عن طريق مجموعات متعاونة ومنظمة من المجرمين ، ومنهم المبرمجون الذين تكون مهمتهم كتابة البرامج المستخدمة في عمليات الاختراق ، والموزعون الذين يقومون بتوزيع وبيع البيانات والفوائد المسروقة من مجرمين أحرين ، وكذلك خبراء تكنولوجيا المعلومات الذين تكون مهمتهم صيانة وإصلاح الهياكل القاعدية كالخوادم وتكنولوجيات التشفير وغيرها[3] .

ومن مجرمي الحاسبات المحترفين أيضاً القراصنة ، ويكمن دورهم في استغلال نقاط الضعف في أنظمة المعلومات ، فيدخلون علي هذه الأنظمة ويعبثون بها ، ومن هؤلاء أيضاً المحتالين الذين يقومون بإنشاء المخططات ونشرها كالرسائل غير المرغوب فيها ، والاحتيال عبر الشبكة [4]

(جـ)الحاقدون: تسعى هذه الطائفة من المجرمين إلى الرغبة في الانتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية عندما لا يكونوا موظفين فيها، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات

---

[1] د/ جميل عبد الباقي الصغير : الجرائم الناشئة عن استخدام الحاسب الآلي – دار النهضة العربية 2010 – ص 105 .

[2] د/ محمد علي العريان : الجرائم المعلوماتية – دار الجامعة الجديدة – الإسكندرية 2009 – ص 170 .

[3] د/ علي عبد القادر القهوجي : الحماية الجنائية لبرامج الحاسب – مرجع سابق – ص 176 .

[4] انظر د/ مقناني صبرينة : تأثير الجريمة الإلكترونية علي المعلومات الرقمية – بحث منشور في المجلة الجزائرية للأبحاث والدراسات – المجلد 3– العدد 9 – 2020/1/15 .

زراعة الفيروسات والبرامج الضارة وتخريب النظام أو إتلاف كل أو بعض معطياته، وقد لا يقف الأمر عند ذلك بل قد يستخدم المجرم الحاقد الحساب المخترق في تنفيذ جرائم إلكترونية ويلصقها بصاحب الحساب المخترق[1] .

ثانياً : تعريف الجريمة الإلكترونية :-

اختلفت الاجتهادات في تعريف الجريمة الالكترونية اختلافاً كبيراً ، ويرجع هذا الاختلاف إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، و تباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى ، فمن نظر إليها من زاوية اعتبار الأداة الالكترونية وهي الوسيلة المستخدمة في ارتكاب الجريمة سواء كان جوال أو كمبيوتر أو فاكس أو كاميرا فعرفها على أنها" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي[2] .

ومن نظر إليها من زاوية وقوع الجريمة عليها أي أن الأجهزة الالكترونية تكون هي محل الجريمة فعرفها على أنها أفعال غير مشروعة، تهدف للوصول لمعلومات معينة أو حذفها أو نسخها أو تغييرها [3] .

ومن نظر إليها من زاوية تقنية الحواسيب ، فقد عرفها على أنها تعني كل الجرائم التي تكون المعرفة بتقنية الحواسيب أساساً لارتكابها [4] .

ولا نستطيع إغفال أهمية أي تعريف من التعريفات السابقة للجريمة الإلكترونية، نظراً لخصوصية الزاوية التي ينظر إليها كل تعريف في الجريمة الإلكترونية، ولذلك نستطيع أن نوسع من تعريف الجريمة الإلكترونية أو نضيق علي حسب الزاوية المنظور من خلالها ، من خلال الأدوات أو النطاق أو الأثر ، فهي جريمة ترتكب بواسطة نظام الكتروني أو شبكة الكترونية أو ترتكب ضد أي نظام الكتروني في البيئة الالكترونية ، وتؤدي إلي آثار متعددة ،ونعرض فيما يلي للتعريف الضيق أو الواسع للجريمة الإلكترونية :

أ – التعريف الضيق للجريمة الالكترونية

---

[1] د/ أحمد محمود مصطفي : جرائم الحاسبات الآلية في التشريع المصري – دار النهضة العربية –الطبعة الأولي 2010 – ص 35

[2] د / هشام محمد فريد رستم : قانون العقوبات ومخاطر تقنية المعلومات– مكتبة الآلات الكاتبة، 1995 – ص 29.

[3] د/ غنام محمد غنام : عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر – بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت – كلية الشريعة والقانون بجامعة الامارات المتحدة 2000 .

[4] د/ سامي علي حامد عياد : الجريمة المعلوماتية وإجرام الإنترنت – دار الفكر الجامعي 2007 – ص41 .

ما ذهب إليه الفقيه MERWE حيث يرى أن الجريمة المعلوماتية هي الفعل غير المشروع الذي يتم التورط في ارتكابه بواسطة الحاسب الآلي، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات[1] .

ويرى الأستاذ MASS أن المقصود بالجريمة المعلوماتية : الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح [2] .

كما أن مجرد استخدام الحاسب الآلي لا يضيف إلى السلوك غير المشروع جديدا، ولكن استخدام البيانات و المعلومات والبرامج هو الذي يمكن أن يضيف إلى الجريمة سمة الجريمة المعلوماتية[3] .

ومعظم هذه التعريفات تعرضت للنقد من قبل الفقه، لذلك حاول جانب أخر من الفقه تعريف الجريمة الإلكترونية على نحو واسع من أجل محاولة تفادي أوجه القصور التي شابت تعريفات الاتجاه المضيق في التصدي لظاهرة الإجرام المعلوماتي.

ب – التعريف الواسع لمفهوم الجريمة الإلكترونية :

من بين التعريفات الموسعة للجريمة المعلوماتية ما ذهب إليه من بعض الفقه من إنها عمل أو امتناع عن عمل يأتيه الإنسان إضرارا بمكونات الحاسب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات و يفرض للاعتداء عليها عقابا[4]، ويمتاز هذا التعريف بالمزايا التالية:

- أنه يحتوي على كل صور الاعتداء الإيجابية أو السلبية التي توقع أضرار بمكونات الحاسب الماديةأو المعنوية.

---

[1] انظر د/ خالد عبد العظيم أبو غابة : التقدم التكنولوجي وأثره علي جرائم العرض – مرجع سابق– ص 19 .

[2] انظر تفصيل ذلك د/ سامي علي حامد عياد : الجريمة المعلوماتية وإجرام الإنترنت – مرجع سابق – ص41 .

[3] د/ غنام محمد غنام : عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر – بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت – كلية الشريعة والقانون بجامعة الامارات المتحدة 2000 .

[4] انظر د/ جميل عبد الباقي الصغير : الجرائم الناشئة عن استخدام الحاسب الآلي – مرجع سابق– ص 10 ، د / هشام محمد فريد رستم : قانون العقوبات ومخاطر تقنية المعلومات– مرجع سابق– ص 29 ، و د/ علي عبد القادر القهوجي : الحماية الجنائية لبرامج الحاسب – مرجع سابق – ص 1 2 .

- أنه يتضمن الأثر الجنائي المترتب على العمل أو الامتناع غير المشروعين و الذي يتمثل في الجزاء الجنائي بشتى صوره و أنواعه .
- يحافظ على الشرعية الجنائية : حيث لا جريمة و لا عقوبة أو تدبير أمن بغير قانون .

و نظراً لخطورة هذه الجريمة و آثارها الممتدة التي قد تصل من دولة لأخرى، فإن بعض الهيئات الدولية المعنية بجرائم الكمبيوتر قد أرست قواعد لتعريف هذا النوع من الجرائم، من هذه الهيئات الـ OECD ، التي اتخذت التعريف التالي كتعريف لجريمة الكمبيوتر بأنها : أي سلوك غير قانوني أو غير قانوني أو غير أخلاقي أو غير مفوض يتعلق بالنقل أو المعالجة الآلية للبيانات يعتبر اعتداءٍ على الكمبيوتر[1] .

المبحث الثاني

خصائص الجريمة الإلكترونية

يصعب متابعة جرائم الحاسب الآلي و الإنترنت و كذا الكشف عنها؛ لأن هذه الجرائم لا تترك أثرا فليست هناك أموال أو مجوهرات مفقودة ،و إنما هي أرقام تتغير في السجلات [2] ، و معظم جرائم الحاسب الآلي تم اكتشافها بالصدفة و بعد وقت طويل من ارتكابها ، كما أن الجرائم للتي لم تكتشف هي أكثر بكثير من تلك التي كشف الشر عنها ، و تعود أسباب صعوبة إثبات هذا النوع من الجرائم إلى الأمور التالية:

أنها كجريمة لا تترك أثرا بعد ارتكابها ويصعب الاحتفاظ بأثرها إن وجدت تحتاج غلى خبرة فنية و يصعب على المحقق التقليدي التعامل معها[3].

---

[1] د/ غنام محمد غنام : عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر – بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت – كلية الشريعة والقانون بجامعة الامارات المتحدة 2000 .

[2] د/ جميل عبد الباقي الصغير : الجرائم الناشئة عن استخدام الحاسب الآلي – دار النهضة العربية 2010 – ص 105 .

[3] د/ رامي متولي القاضي : مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية ط 2011 – ص 76 .

كماأنها تعتمد على الخداع في ارتكابها و التضليل في التعرف على مرتكبها ، بالإضافة إلى أن ارتباط الجريمة الإلكترونية بجهاز الحاسب الآلي و شبكة الإنترنت أضفى عليها مجموعة من الخصائص التي تميزها عن الجرائم التقليدية ، ولعل من أهمها ما يلي:

الخاصة الأولى : جرائم الحاسوب ترتكب بواسطة الحاسب الآلي و كذلك عبر شبكة الإنترنت فهي حلقة الوصل الرئيسية بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك و الشركات وغيرها من الأهداف التي تكون غالبا الضحية لتلك الجرائم [1] .

الخاصية الثانية : أنها جريمة عابرة للحدود، فالمجتمع المعلوماتي لا يعترف بالحدود الجغرافية فهو مجتمع منفتح عبر شبكات تخترق الزمان و المكان دون أن تخضع لحرس الحدود، وهو خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة و كذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى شكليات تتعلق بإجراءات الملاحقة القضائية وغيرها من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام [2] .

الخاصية الثالثة : صعوبة التحري و التحقيق نظرا لارتكابها في الخفاء ، و عدم وجود أي أثر إيجابي لما يجري خلال تنفيذها من أفعال إجرامية، فالتحري عنها ينطوي على العديد من المشكلات و التحديات الإدارية و القانونية، و التي تتصل ابتداء من عملية ملاحقة الجناة، فإذا تحققت إمكانية الملاحقة أصبحت الإدانة صعبة لسهولة إتلاف الأدلة من قبل الجناة أو لصعوبة الوصول إلى الأدلة أو لغياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجريمة[3].

---

[1] د/ فتوح عبد الله الشاذلي : جرائم الكومبيوتر – منشورات الحلبي 2003 – ص 76 .

[2] د/ رامي متولي القاضي : مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية–مرجع سابق – ص 76 .

[3] د/ عمر الفاروق : المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية – طبعة 1995 – ص 14 .

الخاصية الرابعة : تتسم بالخطورة البالغة من عدة جوانب، فمن ناحية أولى نجد الخسائر الناجمة عنها كبيرة جدا قياسا بالجرائم التقليدية خاصة جرائم الأموال، ومن ناحية ثانية نجدها ترتكب من فئات متعددة تجعل من التنبؤ بالمشيئة فيه أمرا صعبا ومن ناحية ثالثة تنطوي على سلوكيات غير مألوفة[1] .

ولا أدل على ذلك من أن الخسائر المادية الناجمة عن هذه الجرائم تبلغ وفقا لتقديرات المركز الوطني لجرائم الحاسب في الولايات المتحدة الأمريكية في نهاية القرن الماضي حولي 500 مليون دولار في السنة، وذلك في نهاية القرن العشرين [2] .

الخاصية الخامسة : الصورة التقليدية للمجرم تكاد تختفي في هذه الجرائم بل و على العكس من ذلك فالمجرم المعلوماتي عادة ما ينتمي إلى مستوى اجتماعي مرتفع عن غيره من المجرمين و نادرا ما يكون محترفا للإجرام أو عائدا ، كما أنه لا ينظر إليه كمجرم بالمعنى المتعارف عليه لهذه الكلمة وذلك لكون الأسباب و العوامل التي تقف وراء ارتكاب الجريمة المعلوماتية تختلف بالمقارنة بالجريمة التقليدية[3] .

الخاصية السادسة : قلة الإبلاغ عن وقوع الجريمة المعلوماتية، و ذلك راجع لسببين أولهما الخشية و الخوف من التشهير، لذلك نجد أن معظم جرائم الإنترنت تم الكشف عنها بالصدفة أو بعد فترة طويلة من ارتكابها ، و السبب الثاني هو عدم اكتشاف الضحية للجريمة مما يعني أن الجرائم التي حدثت ولم يتم اكتشافها هي أكثر بكثير من الجرائم التي تم كشف الستار عنها [4] .

وعليه فالجريمة الإلكترونية تعتبر من أحدث أنواع الجرائم، ويكون مسرحها العالم الافتراضي غير الملموس ، وتكون مظاهرها بعيدة عن أي مظهر من مظاهر الجريمة التقليدية ؛ فهي جريمة عابرة للحدود يرتكبها مجرمون ذو مستوى عالي، أذكياء و متميزون في المجال التقني، مما يؤدي إلى تشتيت الجهود الدولية في محاولة تعقبها التحري عنها، أو الوصول إلى مرتكبها.

---

[1] القاضي / عمر محمود الحوتي : الوجيز في الحماية الجنائية من جرائم تقنية العلومات – مرجع سابق – ص 7 .

[2] انظر د/ فتحي محمد أنور عزت : جرائم العصر الحديث –دار الفكر والقانون 2010 – ص 88 .

[3] د/ عمر الفاروق : المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية –مرجع سابق – ص 17 .

[4] د/ جميل عبد الباقي الصغير : الجرائم الناشئة عن استخدام الحاسب الآلي – مرجع سابق– ص 105 .

المبحث الثالث

مخاطر الجريمة الالكترونية

سنتحدث في هذا المبحث عن مخاطرالجريمة الالكترونية والمجالات التي يمكن أن تكون محلاً للتهديد من مخاطر الجرائم الالكترونية متي توافر استخدام وسائل الاتصال الحديثة في شبكة الاتصالات وشبكة المعلومات الدولية الإنترنت كوسيلة رئيسة لارتكاب الجريمة السيبرانية [1] .

ونشير في البداية إلي أن ارتكاب الجرائم التقليدية، وغيرها من الجرائم بدون استخدام تقنية المعلومات ، وشبكة الاتصالات وشبكة المعلومات الدولية "الإنترنت" لا يعد جرائم إلكترونية ، فمناط الجرائم الإلكترونية هو استخدام هذه

---

[1] في القضية رقم 2341 لسنة 2020 أمن دولة طوارئ مركز المنصورة المقيدة برقم 268 لسنة 2020 أمن دولة طوارئ كلي جنوب المنصورة اعترف المتهمون بتواصلهم مع .....المُكنَّى (أبو عبد الله المجاهد) – القيادي بتنظيم داعش خارج البلاد – عَبر موقع التواصل الاجتماعي فيس بوك على شبكة المعلومات الدولية)الإنترنت) الذي كلفه بالدعوة لأفكار التنظيم بأوساط مُخالطيه وتأسيس خلية داخل مصر تتبع التنظيم يتولى المتهم الأول قيادتها، لارتكاب الجرائم الإرهابية، عن طريق الإرهاب، وذلك للإخلال بالنظام العام في مصر، وتعريض سلامة المجتمع ومصالحه وأمنه للخطر والإضرار بالوحدة الوطنية والسلام الاجتماعي والأمن القومي، وإيذاء الأفراد وتعريض حياتهم للخطر، وعرقلة السلطات العامة ومصالح الحكومة ودور العبادة وتعطيل أحكام الدستور والقوانين، وزعزعة الأمن في البلاد وإشاعة الفوضى، فعقد المتهم العزم على تأسيس تنظيم إرهابي يتولى إدارته وقيادته، لتنفيذ الأغراض السابقة، فظهرَ أمام المتهمَين الثاني والثالث بمظهر الأخيار، وهو لا يَحمل بين جنباته سوى عوامل الإفساد والمَضَرة، وعقد لهما لقاءات بمسكنه وعبر شبكة المعلومات الدولية (الإنترنت) أحاطهما فيها بأفكار وأهداف التنظيم الإرهابية، وأمدهم بمطبوعات وإصدارات مما تصدر عن التنظيم المذكور تُزكِّي ما دعاهما إليه، ولما اقتنعا واعتنقا ذات الفكر خلُصوا إلى بعضهم نَجيا، وخطط الأول من منطلق أنه قائد الخلية الإرهابية التي أنشأها من ثلاثتهم؛ لتنفيذ أغراض التنظيم الإرهابية، ولسبق علمه بخدمة المتهم الثاني في اللواء 182 مظلات بأنشاص بمحافظة الشرقية، كلفه برصد وإعداد رسم توضيحي لهذا الموقع العسكري موضحًا به أماكن تخزين الأسلحة والذخائر، وأماكن نقاط المراقبة، ومحال إقامة قادته لاستهدافه وسرقة الأسلحة والذخائر لنقلها إلى بئر السبع في سيناء لاستخدامها في عملياتهم الإرهابية المزمع ارتكابها، ولما جمعوا تلك المعلومات وأمدوا بها تنظيمه الإرهابي الذي أسسه، احتفظ بها على حاسوبه هي وصور للقادة المشار إليهم ولنقاط المراقبة، وتخابَر مع قيادي تنظيم داعش بالخارج – سالف الذكر – وأمده بها تمهيدا لربطه بعناصر أخرى تتبع التنظيم داخل مصر لمعاونته هو وتنظيمه في اقتحام المقر واستهداف قياداته، وبناء على تكليفه من قيادي داعش بالخارج برصد ارتكاز أمني بنطاق محافظة الجيزة وكذا ضابط بقطاع الأمن الوطني بغرض استهدافهما، تمكن المتهمون من رصد ضابط بقطاع الأمن الوطني وتحديد محل إقامته وعمله ومواعيد غدوه ورواحه، ورقم هاتفه، واسمه الحركي، لاستهدافه لسبق عمله في مكافحة العناصر المتطرفة.

التقنيات الحديثة ، ولا يمنع ذلك تجريم الجرائم التي تقع بدون هذه التقنيات إلا أنها تخضع لنصوص جنائية أخري تتضمنها القواعد العامة في القانون الجنائي [1] .

والملاحظ هو كثرة وتعدد المخاطر التي يمكن أن تنجم عن الجرائم الالكترونية ، كما تتعدد أشكالها و تتطور وتتخذ أشكالاً لا حصر لها تبعا لما يتوفر بين يدي الإنسان من وسائل لإيقاع الفعل وتحقيق نتائجه في الواقع العملي[2].

وانطلاقاً من ذلك فقد ظهرت للوجود سلوكيات سلبية خطيرة تبعاً لظهور تقنية نظم المعلومات والاتصالات التي وضعت بين يديك البعض الفاسد وسائل و طرق حديثة لإيقاع جرائمهم بسهولة وخفة، فكان أن أحدثت هذه السلوكيات المستحدثة ثورة هائلة في النظرية العامة للجريمة على اختلاف مستوياتها[3].

السلوك الإجرامي في كافة الجرائم الواقعة على الأشخاص والأموال هو ما يأتي به الشخص من فعل يؤدي إلى إحداث النتيجة التي يسعى إليها، ففي جرائم القتل وفق نص المادة من قانون العقوبات المصري فإن أي سلوك الجاني يهدف إلى إزهاق الروح هو سلوك جرمي وهذا واضح من مطلع المادة المذكورة بقولها "كل من قتل إنسان".

وقد يكون السلوك الإجرامي في جريمة القتل بالامتناع عن القيام بعمل معين واجب على الجاني القيام به بهدف إزهاق روح إنسان ، كامتناع الأم عن إرضاع طفلها بهدف التخلص منه[4].

وهنا هل السلوك الإجرامي هذا والذي ينصرف على كافة الجرائم التقليدية ينطبق على الجريمة الالكترونية محل البحث؟

بما أن الجاني في الجرائم الالكترونية يختلف عن الجاني في غيرها من الجرائم من حيث كونه ذو خبرة كافية في مجال استخدام التقنيات الحديثة ، فإن السلوك الإجرامي الذي سيصدر منه في مجال ارتكاب الجريمة الالكترونية حتما سيختلف عن الجاني التقليدي.

---

[1] د/ فتحي محمد أنور عزت : جرائم العصر الحديث – مرجع سابق – ص 88 .

[2] د/ أحمد محمود مصطفي : جرائم الحاسبات الآلية في التشريع المصري – مرجع سابق – ص 34 .

[3] د/ خالد عبد العظيم أبو غابة : التقدم التكنولوجي وأثره علي جرائم العرض – مرجع سابق – ص 20 .

[4] د/ عماد الفقي : المسئولية الجنائية عن القتل بالامتناع – دراسة مقارنة –دار النهضة العربية 2015 – ص 14 .

ففي جريمة الإرهاب الإلكتروني، فإن السلوك الإجرامي هنا يختلف عنه في بقية الجرائم ، هو إطلاق صفحات أو مواقع تدعو وتحرض على الانضمام لمثل هذه للجماعات الإرهابية ، أو مثلا تبين كيفية صنع قنابل.1 ، وتختلف الجريمة الإلكترونية علي حسب تصنيفها علي النحو الأتي :

المخاطر وفقاً لتصنيف الجرائم الإلكترونية:

يصعب تصنيف الجرائم نظرا لاختلافها من مجتمع لآخر من حيث تطوره، ومدى استخدامه للحاسوب ودرجة اعتماده عليه في مختلف جوانب الحياة، وقد أوجد مشروع اتفاقية جرائم الكمبيوتر و الإنترنت لعام 2001 (اتفاقية بودابست 2001) تضمن أربع طوائف رئيسية:

أ_ الجرائم التي تستهدف سلامة وسرية المعطيات و النظم : وتضم الدخول غير القانوني أو غير المصرح به ، الاعتراض غير القانوني، تدمير المعطيات، اعتراض النظم .

ب_ الجرائم المرتبطة بالكمبيوتر: تضم التزوير المرتبط بالكمبيوتر، الاحتيال المرتبط بالكمبيوتر.

ج_ الجرائم المرتبطة بالمحتوى : وهي تضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية وغير الأخلاقية .

د _الجرائم المرتبطة بالأشخاص و الأموال : وتضم السرقة و الاحتيال و التزوير و الإطلاع على البيانات الشخصية، المعلومات المضللة و الزائفة، أنشطة الاعتداء على الخصوصية إساءة استخدام المعلومات ، القرصنة ... وغيرها من الجرائم [2] .

وعليه ، فقد تعدد الجهود الفقهية التي بذلت على الصعيد الدولي أو الوطني من أجل وضع تقسيم يمكن الاعتماد عليه لجرائم المعلوماتية ، و في هذا المجال يمكن تقسيمها إلى مجموعتين أساسيتين:

المجموعة الأولى: الجرائم التي تقع على الانترنت

---

[1] http://droit.moontada.com/t622-topic

بحث عن الجرائم الإلكترونية منشور على الإنترنت بتاريخ 2012/12/7

[2] د/ جميل عبد الباقي الصغير : الجرائم الناشئة عن استخدام الحاسب الآلي – مرجع سابق– ص 108 .

أي أن شبكة العنكبوتية تكون عنصر سلبي في الجريمة أي محل للجريمة فقط ، فإن هدف المجرم ينصب حول البيانات و المعلومات المخزنة و المنقولة عبر قنوات الخاصة أو العامة و اختراق الحواجز الأمنية إن وجدت و الاعتداء على الأموال، و التي نذكرها على التوالي .

أ- سرقة المال المعلوماتي:

أضحى لبرامج المعلومات قيمة غير تقليدية لاستخداماتها المتعددة في كافة المجلات الاجتماعية و الاقتصادية فهذه القيمة المميزة لبرامج المعلومات تجعلها محلا للتداول ، و هنا تبدو أهمية الإنترنت بصفته مصدر المعلوماتية ، مما أدى إلى ظهور قيمة اقتصادية جديدة وأموال جديدة ، عرفت بالأموال المعلوماتية ، و صاحب ظهور هذا المال المعلوماتي جرائم جديدة عرفت بالجرائم المعلوماتية و هذه الجرائم يمكن تصورها من زاويتين:

أن تكون المعلوماتية أداة أو وسيلة للاعتداء ، و أن تكون المعلوماتية موضوعا للاعتداء رأي سرقة تلك المعلومات.

فالزاوية الأولى يستخدم الجاني المعلوماتية لتنفيذ جرائم سواء ما تعلق منها بجرائم للاعتداء على الأشخاص أو الأموال كالسرقة و النصب و خيانة الأمانة ، أما الجرائم من الزاوية الثانية يكون المال المعلوماتي موضوعا لها

ب- استخدام البروكسي للدخول المواقع المحجوبة:

البروكسي [1] هو عبارة عن برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز موحد وهذا البرنامج يستخدم لتجاوز المواقع المحجوبة ،والتي عادة ما تكون إما مواقع جنسية أو سياسية معادية للدولة .

ج – جرائم الاختراق:

---

[1]البروكسي إصطلاحاً يعني الوكيل فهو عبارة عن وسيط بين مستخدمي الإنترنت والمواقع علي الشبكة الإلكترونية وهو بمثابة الفلتر الذي يحد من القدرة علي الوصول إلي مواقع معينة وفي نفس الوقت قد يساعد علي الوصول إلي بعض المواقع المحجوبة من قبل الحكومات أو من قبل مزودي خدمة الإنترنت فتقوم الحواسيب بالإتصال بهذه الخدمة من أجل طلب صفحة أو موقع ما علي الإنترنت قد لا تستطيع الوصول إليه بشكل عادي وتعمل الخدمة علي توفيره .

يمثل الاختراق المعلوماتي تحديا على قدر كبير من الأهمية لإنجازات تكنولوجيا المعلومات، و يعرفه شراح القانون المعاصرون بأنه : " فعل مشروع يوظف المعرفة العلمية السائدة في ميدان ثقافة الحاسوب و المعلوماتية لاقتراف إساءة أو هجوم على الغير "

فهي عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك و سرقة كلمات السر ، يقوم المستخدمون المخولون بفتح حسابات الشركات أو المؤسسات للأغراض الشرعية مثل اللعب بالحسابات الشخصية و مزاولة بعض أنواع الألعاب في الحاسوب للوصول إلى الأسرار الخاصة بالمؤسسة عن طريق كسر كلمات السر الخاصة بالأنظمة خلال خطوط شبكات الهاتف

و من الأساليب المستخدمة في عمليات الاختراق ، عملية الاقتحام أو التسلسل ، وتصنيع وبرمجة الفيروسات ، وبرمجة المواقع المعادية ، التي يتم إنشائها لمعاداة سياسية أو معاداة الدين أو للأشخاص أو الجهات.

وهناك أيضاً أسلوب القرصنة ، حيث تواجه شبكة الانترنت ما يسمى بظاهرة القرصنة ، و التي تكون من قبل بعض الجماعات التي تؤمن بالحرية المطلقة في الرأي والتعبير و الاستخدام أيضاً ، و هي جماعات تستطيع أن تدخل عبر طرق خاصة تحترق أجهزة الحاسوب ، و كذا الأرقام السرية للأشخاص و إلى بريدهم الإلكتروني ، فهي تعتبر سرقة للخدمات أو الاستعمال غير المصرح به للنظام المعلوماتي .

د – جرائم التجسس الإلكتروني:

وهي الجرائم التي يتم بواسطتها اختراق أجهزة المستخدمين بطرق غير شرعية و لأغراض غير سوية ، من أجل سرقة المعلومات تتعلق بذلك المستخدم سواء على الصعيد الشخصي ،أو السياسي أو العلمي أو الاجتماعي حيث لم يعد هناك سرية يمكن الاحتفاظ بها من دون أن يقوم الشخص بعمليات كثيرة لتجنب عمليات التجسس أو " الهاكرز " فهي ممارسات غير مشروعة على شبكات الحاسب الآلي ، تستهدف التحاليل على نظام المعالجة الآلية للبيانات بغية إتلاف المستندات المعالجة إلكترونيا

هـ – الإرهاب الإلكتروني:

يعد الإرهاب المعلوماتي من أخطر أصناف الجرائم المرتبطة بتكنولوجيا المعلوماتية نظرا لأثرها و دوافعها فالإرهاب الإلكتروني هو تحطيم أو إتلاف أنظمة معلوماتية بهدف المساس ،أو إحداث خلل يمس باستقرار دولة أو بهدف الضغط على حكومة ما

فهو هجوم مع سبق الإصرار، ذو أهداف سياسية ضد المعلوماتية، ضد أهداف مسلحة تخص الشرطة، الدرك أو أهداف عسكرية، أو غير مسلحة كالإدارات المدنية الوطنية، من طرف جماعات وطنية أو خفية .

و خطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة التي تضار بنيتها التحتية بالحواسيب الآلية و الشبكات المعلوماتية، مما يجعلها هدفا سهل المنال فبدلا من استخدام المتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية و إغلاق المواقع الجوية و شل أنظمة القيادة.

المجموعة الثانية : جرائم تقع بواسطة الإنترنت :

أي أن الشبكة دورها إيجابي في ارتكاب الجريمة، فهي تسهل للمجرم المعلوماتي تحقيق غايته و يلاحظ أن أغلب صورها في هذه الحالة تشكل جرائم الواقعة على الأشخاص ، كالجرائم الجنسية و الممارسات غير أخلاقية[1] .

ومن هذهالجرائم أيضاً الجرائم المالية و التي تضم كلا من:

- جرائم السطوعلى أرقام البطاقات الائتمانية : و التي يتم ارتكابها باستخدام تكنولوجيا المعلومات سرقة الأقراص الصلبة و المرنة، بغرض الحصول على المعلومات التي تحويها و يتولى قراصنة المعلومات بيعها بعد الحصول عليها، نظير الحصول على عائد مادي، مثل ذلك : الوصول إلى أجهزة الحاسب الخاصة بمكاتب الائتمان الرئيسية و سرقة المعلومات الائتمانية، تم استخدامها بإعادة بيعها لأشخاص آخرين، و تدمير المشروعات المهمة للشركات بغرض ابتزازهم
- القمار عبر الإنترنت : مع الانتشار الواسع و التطور الكبير لشبكة الإنترنت على مستوى العالم ظهر إلى الوجود .صيحات القمار يتمثل في الكازينوهات الافتراضية، و هي عبارة عن مواقع ويب تم تصميمها على

[1] د/ خالد عبد العظيم أبو غابة : التقدم التكنولوجي وأثره علي جرائم العرض – مرجع سابق – ص 22 .

طراز كازينوهات " لأس فيغاس " الأمريكية وتتوفر كل أنواع القمار و ألعابه ابتداء من ألعاب الورق، و انتهاء بآلات المقامرة، و هي موجودة على الشبكة المعلوماتية.

- تزوير البيانات : لا تكاد تخلو جريمة من عملية تزوير للبيانات بشكل أو بآخر، و يتم تزوير البيانات الحاسب إما بإدخال بيانات مغلوطة إلى الموظفين المسموح لهم بإدخال البيانات، ثبت أنه كان لهم ضلع كبير في الكثير من جرائم نظم المعلومات .
- الجرائم المنظمة : هي عنف منظم قصد الحصول على مكاسب مالية، بطرق و أساليب غير مشروعة ،وتمارس الجريمة على شكل نصي و احتيال و تزوير و سطو و خطف من أجل الابتزاز والقتل.....الخ، إلا أنها تختلف عن الجرائم المعروفة كونها تنفذ عن بعد تدبير وتنظيم، لذا سميت بالجريمة المنظمة .

الفصل الثاني

المواجهة التشريعية للجرائم الالكترونية

تتضمن المواجهة التشريعية للجرائم الالكترونية تجريم كل الأفعال التي ترتكب بواسطة تقنية العلومات والتي يمكن تصنيفها وفقاً لما ورد في القانون رقم 175 لسنة 2018 بشأن جرائم تقنية المعلومات إلي ثلاث فئات ، وهي الجرائم المتعلقة بالشبكات بجرائم الاعتداء علي الشبكات وأنظمة وتقنيات المعلومات واستخدامها استخدام غير مشروع ، ثم فئة الجرائم المرتكبة من مدير الموقع ومقدم الخدمة، وأخيراً فئة الجرائم الالكترونية المرتكبة بمعرفة الشخص الاعتباري، سوف نتحدث في هذا الفصل عن المواجهة التشريعية لهذه الجرائم علي النحو الأتي :

المبحث الأول : المواجهة التشريعية لجرائم الاعتداء علي الشبكات وأنظمة وتقنيات المعلومات واستخدامها استخدام غير مشروع .

المبحث الثاني : المواجهة التشريعية للجرائم المرتكبة من مدير الموقع ومقدم الخدمة .

المبحث الثالث : المواجهة التشريعية للجرائم الالكترونية المرتكبة بمعرفة الشخص الاعتباري .

وذلك علي النحو الأتي :

المبحث الأول

المواجهة التشريعية لجرائمالاعتداء علي الشبكات وأنظمة وتقنيات المعلومات واستخدامها غير المشروع

لقد واجه المشرع هذه الجرائم ، حيث وضع العقوبة لكل نوع من الانتهاكات بحسب طبيعتها وأسلوب أرتكابها ، ومنها جرائم الدخول والانتفاع بالشبكات ، والاعتداء علي البيانات والاحتيال المالي ، والجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات ، ثم جرائم الاعتداء علي الحياة الخاص ،وذلك في المطالب الأتية :

المطلب الأول : جرائم الاعتداء علي الشبكات وأنظمة وتقنيات المعلومات واستخدمها استخدام غير مشروع .

المطلب الثانى : الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات .

المطلب الثالث : الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصةوالمحتوى المعلوماتى غير المشروع .

المطلب الأول

جرائم الاعتداء علي الشبكات وأنظمة وتقنيات المعلومات واستخدمها في أغراض غير مشروعة

وحيث استخدمت تقنية المعلومات علي نطاق واسع في كافة المجالات الحياتية ، مما نتج عنه الكثير من الانتهاكات ، وهو ما واجهه المشرع علي النحو الأتي :

أولاً : الانتفاع غير المشروع :-اعتبر المشرع المصري الانتفاع بدون حق بخدمة الاتصالات من قبيل الأفعال المجرمة وفقاً لنص المادة 13 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات التي نصت علي أنه :- " يُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه, أو بإحدى هاتين العقوبتين، كل من انتفع بدون وجه حق عن طريق شبكة النظام المعلوماتى أو إحدى وسائل تقنية المعلومات، بخدمة اتصالات أو خدمات قنوات البث المسموع والمرئى [1] .

---

[1] د/ جميل عبد الباقي الصغير : المواجهة الجنائية لقرصنة البرامج التليفزيونية المدفوعة –دار النهضة العربية – ص 9 .

ومن هذا النص يتضح أن المشرع يواجه جريمة الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات وتقنياتها، ويقصد بالانتفاع تحقيق قدر معين من الاستفادة سواء كانت مادية أو معنوية [1].

ولقد انتهج المشرع الاماراتي ذات النهج بتجريم الانتفاع بدون حق ونص علي ذلك في المادة 34 من مكافحة التقنية الاماراتي [2] .

ثانياً :- جريمة الدخول غير المشروع :

يجرم المشرع الدخول سواء عن عمد أو عن خطأ علي موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه ، والموقع قد يكون تجاري أو تعليمي أو ترفيهي أو حكومي أو عسكري أو غيرها من المواقع ، ونص المشرع في المادة (14) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات علي أنه :- يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه.

فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين.

ومفاد ما تقدم أن هذه الجريمة تُعد ذات طبيعة خاصة ، حدد لها المشرع محلاً أو شرطاً مفترضاً ، ولا بد من توافره وهو توافر نظام معلوماتي سواء كان هذا النظام موقع الكتروني أو أنظمة معلوماتية الكترونية أو شبكة معلومات ، كما حدد المشرع عناصر السلوك فيهاوهي الدخول إلي النظام المعلوماتي بدون تصريح ، وتجاوز حدود التصريح ، والبقاء بصورة غير مشروعة في النظام المعلوماتي [3] .

---

[1] المستشار بهاء المري : شرح قانون مكافحة جرائم تقنية المعلومات – مرجع سابق – ص 69 .

[2] د/ ماجد بن كريم الزراع : الركن المادي في الجرائم المعلوماتية – رسالة ماجستير جامعة نايف العربية للعلوم الأمنية 2014 – ص 71 .

[3] د/ إبراهيم محمد القاسمي : جرائم الدخول والقاء غير المشروع في نظام المعالجة الآلية للمعطيات الالكترونية – رسالة ماجستير جامعة الامارات المتحدة كلية القانون 2018 – ص 9 .

كما ذهب المشرع الاماراتي إلي تجريم فعل الدخول غير المشروع إلي المواقع أو شبكات المعلومات إذا كان بدون تصريح ، أو تجاوز هذا التصريح ، بل وتوسع المشرع الاماراتي إلي تجريم البقاء في هذه الأنظمة بصورة غير مشروعة [1] .

والعلة من هذا التجريم هي حماية شبكة المعلومات والمواقع والحسابات الخاصة من الدخول غير المشروع أو الدخول والبقاء بدون ترخيص [2] .

ثالثاً : جريمة تجاوز حدود الحق فى الدخول :

ويقصد بها الدخول المشروع في البداية ولكنه تعدي فيما بعد وتجاوز حدود الدخول من حيث الزمان أو مستوي الدخول ، وهي الجريمة الجريمة التي تضمنتها المادة (15) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :-يُعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو إحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتى مستخدمًا حقًا مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول[3].

رابعاً :- جريمة الاعتراض غير المشروع :

يقصد بهذه الجريمة كل فعل ينطوي علي اعتراض يتم بدون وجه حق لأي معلومات أو بيانات و كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي ، والاعتراض هو مشاهدة البيانات أو المعلومات أو الحصول عليها بطريق التنصت أو التعطيل أو التخزين أو تعديل المسار أو إعادة التوجيه لأسباب غير مشروعه وبدون وجه حق [4] ، ولقد وردت هذه الجريمة بنص المادة (16) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه ُيعاقب بالحبس مدة لا تقل عن سنة, وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين, كل من اعترض بدون وجه حق أى معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلى وما فى حكمها.

---

[1] انظر المادة 34 من التشريع الاماراتي بشأن مكافحة جرائم تقنية المعلومات .

[2] القاضي / عمر محمود الحوتي : الوجيز في الحماية الجنائية من جرائم تقنية المعلومات – دار النهضة العربية 2021 – ص 25

[3] انظر المستشار بهاء المري : شرح قانون مكافحة جرائم تقنية المعلومات – مرجع سابق – ص 108 .

[4] د/ راشد محمد المري : الجرائم الالكترونية في ظل الفكر الجنائي المعاصر –دار النهضة العربية 2018 –ص 78 .

ولقد جرم المشرع الاماراتي كل فعل ينطوي علي اعتراض غير مشروع ومتعمد للبيانات والمعلومات المتداولة بوسائل التقنية الحديثة [1] .

خامساً :- جريمة الاعتداء على سلامة البياناتوالمعلومات والنظم المعلوماتية :

وهي من أكثر الجرائم التي يتعرض لها الأشخاص ، حيث يتم اتلاف البيانات والمعلومات الالكترونية ، وهي الجريمة التي تضمنتها المادة (17) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :-يعاقب بالحبس مدة لا تقل عن سنتين, وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين, كل من أتلف أو عطل أو عدل مسار أو ألغى كليًا أو جزئيًا متعمدًا وبدون وجه حق البرامج والبيانات أو المعلومات المخزنة، أو المعالجة، أو المولدة أو المخلقة على أى نظام معلوماتى وما فى حكمه، أيا كانت الوسيلة التى استخدمت فى الجريمة[2] .

سادساً :- جريمة الاعتداء على البريد الإلكترونىأو المواقع أو الحسابات الخاصة :

وهي الجريمة التي تضمنتها المادة (18) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :-يعاقب بالحبس مدة لا تقل عن شهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه, أو بإحدى هاتين العقوبتين, كل من أتلف أو عطل أو أبطأ أو اخترق بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بآحاد الناس[3] .

ويكثر ارتكاب هذه الجريمة في صورة اختراق حساب خاص ، حيث يقوم الجاني بسرقة الحساب والتلاعب في بياناته [4] .

فإذا وقعت الجريمة على بريد إلكترونى أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه, أو بإحدى هاتين العقوبتين.

والاتلاف يعني التدمير أو التخريب، بجعله غير صالح للاستخدام نهائياً، أما الإبطأ أو التعطيل ، فهو التخريب الجزئي ، وإن كان يظل صالحاً للعمل [1] .

---

[1] انظر الفقرة الأولي من المادة الخامسة عشر من القانون الإماراتي بشأن مكافحة جرائم تقنية المعلومات رقم 5 لسنة 2012 .

[2] د/ ماجد بن كريم الزراع : الركن المادي في الجرائم المعلوماتية – مرجع سابق – ص 71 .

[3] د/ جميل عبد الباقي الصغير : جرائم الإنترنت – الأحكام الموضوعية والجوانب الإجرائية – ص 15 .

[4] تطبيقاً لذلك راجع حكم محكمة طنطا الاقتصادية في الدعوي رقم 1190 لسنة 2019 جنح طنطا الاقتصادية .

سابعاً :- جريمة الاعتداء على تصميم موقع :

يقصد بتصميم الموقع عملية تخطيط محتواه وطريقع عرضه ، تُعد هذه الجريمة من أحدث الجرائم التي رصدتها التشريعات المتعلقة بالتقنية ، ولقد وردت هذه الجريمة في نص المادة (19) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :-يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو شوَّه أو أخفى أو غيَّر تصاميم موقع خاص بشركة أو مؤسسة أو منشأة أو شخص طبيعى بغير وجه حق[2].والموقع هو مجال أو مكان افتراضي له عنوان محدد علي شبكة معلومات يهدف إلي إتاحة البيانات والمعلومات للعامة أو الخاصة [3] .

وفي التشريع الإماراتي جرم المشرع فعل إلتقاط أو اعتراض أي اتصال عن طريق أي شبكة معلوماتية ، وذلك عن طريق العند وبدون تصريح [4] .

ثامناً :- جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة :

وهي الجريمة التي تضمنتها المادة (20) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :-يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا, أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعًا أو بريدًا إلكترونيًا أو حسابًا خاصًا أو نظامًا معلوماتيًا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكًا لها, أو يخصها.

فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية, تكون العقوبة السجن, والغرامة التى لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه.

وفى جميع الأحوال، إذا ترتب على أى من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى أو البريد الإلكترونى, أو تدميرها أو تشويهها أو تغييرها أو تغييرها أو

---

[1] المستشار بهاء المري : جرائم السوشيال ميديا – دار الأهرام للنشر والتوزيع 2022 – ص153 .

[2] انظر د/ ماجد بن كريم الزراع : الركن المادي في الجرائم المعلوماتية – مرجع سابق – ص 76 .

[3] نص المشرع علي تعريف الموقع في المادة الأولي من القانون 175 لسنة 2018 بشأن مكافحة جرائم المعلومات .

[4] انظر نص الفقرة الأولي من المادة الخامسة عشر من القانون الإماراتي بشأن مكافحة جرائم تقنية المعلومات .

تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها, أو إلغاؤها كليًا أو جزئيًا, بأى وسيلة كانت، تكون العقوبة السجن والغرامة التى لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه.

ولقد وافق المشرع المصري المشرع الإماراتي في هذا الشأن حيث جرم قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012 الاعتداء علي أي نظام أو بيانات أو معلومات حكومية [1] .

تاسعاً :- جريمة الاعتداء على سلامة الشبكة المعلوماتية :

وهي الجريمة التي تضمنتها المادة (21) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :-يعاقب بالحبس مدة لا تقل عن ستة أشهر, وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه, أو بإحدى هاتين العقوبتين، كل من تسبب متعمدًا فى إيقاف شبكة معلوماتية عن العمل أو تعطيلها أو الحد من كفاءة عملها أو التشويش عليها أو إعاقتها أو اعتراض عملها أو أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة بها.

ويعاقب كل من تسبب بخطئه فى ذلك بالحبس مدة لا تقل عن ثلاثة أشهر، وبغرامة لا تقل عن خمسون ألف جنيه ولا تجاوز مائتى ألف جنيه, أو بإحدى العقوبتين.

فإذا وقعت الجريمة على شبكة معلوماتية تخص الدولة أو أحد الأشخاص الاعتبارية العامة أو تمتلكها أو تدار بمعرفتها تكون العقوبة السجن المشدد, وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه[2] .

عاشراً :- التعامل في البرامج والأجهزة والمعدات المستخدمةفى ارتكاب جرائم تقنية المعلومات بطريقة غير مشروعة :

وهي الجريمة التي تضمنتها المادة (22) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :-يعاقب بالحبس مدة لا تقل عن سنتين، وبغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه أو بإحدى هاتين العقوبتين، كل من حاز أو أحرز أو جلب أو باع أو أتاح أو صنع أو أنتج أو استورد أو صدر أو تداول بأى صورة من صور التداول, أى أجهزة أو معدات أو أدوات أو برامج مصممة أو مطورة أو محورة أو أكواد مرور أو شفرات أو رموز أو أى بيانات مماثلة، بدون تصريح من الجهاز أو

---

[1] راجع المواد 2 ، و3 ، و4 من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012 .

[2] انظر في التعليق علي الركن المادي لجرائم الاعتداء علي سلامة الشبكات المعلوماتية د/ خالد عياد الحلبي : إجراءات التحري والتحقيق في جرائم الانترنت – دار الثقافة للنشر والتزيع – ص 73 .

مسوغ من الواقع أو القانون، وثبت أن ذلك السلوك كان بغرض استخدام أى منها فى ارتكاب أية جريمة من المنصوص عليها فى هذا القانون أو إخفاء آثارها أو أدلتها أو ثبت ذلك الاستخدام أو التسهيل أو الإخفاء[1] .

ولقد اتفق المشرع المصري في نهجه مع نهج المشرع الإماراتي الذي تناول هذه الجريمة ، إلا أنه أغفل بعض السلوكيات التي تتمثل في الحيازة والإحراز والجلب والتصنيع علي الرغمن من أهميتها [2] .

المطلب الثانى

الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات

أولاً :- جرائم الاحتيال والاعتداء على بطاقات البنوكوالخدمات وأدوات الدفع الإلكترونى

وهي الجريمة التي تضمنتها المادة (23) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :-يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر والغرامة التى لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، فى الوصول بدون وجه حق إلى أرقام أو بيانات أو بطاقات البنوك والخدمات أو غيرها من أدوات الدفع الالكترونية.

فإن قصد من ذلك استخدامها فى الحصول على أموال الغير أو ما تتيحه من خدمات، يعاقب بالحبس مدة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين.

وتكون العقوبة الحبس مدة لا تقل عن سنة، والغرامة التى لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف، أو إحدى هاتين العقوبتين، إذا توصل من ذلك إلى الاستيلاء لنفسه أو لغيره على تلك الخدمات أو مال الغير[3].

ولقد ورد في التشريع الإماراتي إضافة في أفعال هذه الجريمة تمثل في النشر وكشف سرية البيانات والأرقام الائتمانية [4] .

---

[1] انظر د/ ماجد بن كريم الزراع : الركن المادي في الجرائم المعلوماتية – مرجع سابق – ص 78 .

[2] راجع الفقرة الثانية من المادة الرابعة عشرة من قانون مكافحة تقنية المعلوماتي الإماراتي رقم 5 لسنة 2012 .

[3] راجع المستشار / بهاء المري : شرح جرائم تقنية النعلومات – مرجع سابق – ص 92 .

[4] راجع الفقرة الأخيرة من المادة 12 من قانون مكافحة جرائم تقنية المعلومات الإماراتي .

ثانياً :- الجرائم المتعلقة باصطناع المواقعوالحسابات الخاصة والبريد الإلكترونى :

وهي الجريمة التي تضمنتها المادة (24) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :-يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر, وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى العقوبتين كل من اصطنع بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا ونسبه زورًا إلى شخص طبيعى أو اعتبارى[1] .

فإذا استخدم الجانى البريد أو الموقع أو الحساب الخاص المصطنع فى أمر يسئ إلى من نُسب إليه، تكون العقوبة الحبس الذى لا تقل مدته عن سنة والغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتى ألف جنيه, أو بإحدى هاتين العقوبتين.

وإذا وقعت الجريمة على أحد الأشخاص الاعتبارية العامة, تكون العقوبة السجن, والغرامة التى لا تقل عن مائة ألف جنيه, ولا تزيد على ثلاثمائة ألف جنيه[2] .

المطلب الثالث

الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصةوالمحتوى المعلوماتى غير المشروع

وتتضمن هذه الجرائم جرائم الاعتداء علي المبادئ والقيم الأسرية في المجتمع المصريوانتهاك حرمة الحياة الخاصة وغيرها من الانتهاكات ، وتتضمن أيضاً ربط الحسابات الخاصة بمحتوي مناف للآداب ، ونفصل ذلك فيما يلي :

أولاً : جريمة الاعتداء علي القيم الأسرية :

وهي الجريمة التي تضمنتها المادة (25) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :- يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكترونى لترويج السلع أو الخدمات دون موافقته, أو نشر

---

[1] انظر في التعليق علي الركن المادي لجرائم الاعتداء علي سلامة الشبكات المعلوماتية د/ خالد عياد الحلبي : إجراءات التحري والتحقيق في جرائم الانترنت – مرجع سابق – ص 76 .

[2] راجع المستشار / بهاء المري : شرح جرائم تقنية النعلومات – مرجع سابق – ص 94 .

عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة[1].

وكان المشرع الإماراتي قد جرم كل فعل يمثل اعتداء علي الخصوصية باستخدام وسائل تقنية المعلومات أو الشبكات المعلوماتية [2] .

ثانياً : جريمة تعمد استعمال برنامج معلوماتي في أعمال منافية للأداب :

وهي الجريمة التي تضمنتها المادة (26) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :- يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين كل من تعمد استعمال برنامج معلوماتى أو تقنية معلوماتية فى معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة, أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه.

ويتمثل السلوك في هذه الجريمة في استعمال برنامج معلوماتى أو تقنية معلوماتية فى معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة ، وعملية المعالجة ، وعملية الربط كلاهما عملية فنية تتعلق بتقنية المعلومات ، حيث يتاح ربط الحساب بموقع ويب ، لاستخدام هذا الحساب الخاص علي مواقع أخري للويب لتظهر فيها محتوياته ، فيظهر المحتوي المناف للأداب علي الحساب الخاص [3] .

المبحث الثاني

الجرائم المرتكبة من مدير الموقع ومقدم الخدمة

وتشمل هذه الجرائم جرائم إنشاء أو إدارة أو استخدام موقع لهدف غير مشروع ، وجرائم مقدم الخدمة المتمثلة في الامتناععن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه فى الفقرة الأولى من المادة (٧) من هذا القانون والذي يُبث داخل الدولة أو خارجها، بوضع أى عبارات أو

---

[1] انظر د/ ماجد بن كريم الزراع : الركن المادي في الجرائم المعلوماتية – مرجع سابق – ص 77 .

[2] راجع المادة 21 من قانون مكافحة جرائم تقنية المعلومات الإماراتي رقم 5 لسنة 2012 .

[3] د / أحمد خليفة الملط : الجرائم المعلوماتية –رسالة دكتوراه كلية الحقوق جامعة القاهرة فرع بني سويف 2018 –ص 176 .

أرقام أو صور أو أفلام أو أى مواد دعائية، أو ما فى حكمها بما يُعد جريمة من الجرائم المنصوص عليها بالقانون، وتشكل تهديدًا للأمن القومى أو تعرض أمن البلاد أو اقتصادها القومى للخطر[1] .

أولاً : إنشاء أو إدارة أو استخدام موقع لهدف غير مشروع :

من الجرائم الشائعة في مجال التقنيات الحديثةجرائم أنشاء أو إدارة أو استخدم موقعًا أو حسابًا خاصًا على شبكة معلوماتية بهدف ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانونًا ، وهي الجريمة المنصوص عليها في المادة (27) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :- فى غير الأحوال المنصوص عليها فى هذا القانون، يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه, ولا تزيد عن ثلاثمائة ألف جنيه, أو بإحدى هاتين العقوبتين، كل من أنشأ أو أدار أو استخدم موقعًا أو حسابًا خاصًا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانونًا[2].

يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن عشرين ألف ولا تجاوز مائتى ألف جنيه, أو بإحدى هاتين العقوبتين، كل مسئول عن إدارة موقع أو حساب خاص أو بريد إلكترونى أو نظام معلوماتى، إذا أخفى أو عبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها فى هذا القانون والتى وقعت على موقع أو حساب أو بريد إلكترونى بقصد إعاقة عمل الجهات الرسمية المختصة[3].

يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن عشرين ألف ولا تجاوز مائتى ألف جنية، أو بإحدى هاتين العقوبتين كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكترونى أو النظام المعلوماتى عَرَّض أيًا منهم لإحدى الجرائم المنصوص عليها فى هذا القانون[4] .

ويعاقب بالحبس مدة لا تقل عن ستة أشهر, وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه, أو بإحدى هاتين العقوبتين, كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكترونى أو النظام المعلوماتى تسبب بإهماله فى تَعرّض أى منهما لإحدى الجرائم المنصوص عليها فى هذا القانون, وكان ذلك بعدم اتخاذه التدابير والاحتياطيات التأمينية الواردة فى اللائحة التنفيذية لهذا القانون.

---

[1] المستشار / بهاء المري : شرح جرائم تقنية المعلومات – مرجع سابق – ص 101 .

[2] انظر في شرح وتفصيل ذلك انظر د/ ماجد بن كريم الزراع : الركن المادي في الجرائم المعلوماتية – مرجع سابق – ص 76 .

[3] المادة 28 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

[4] المادة 29 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

ثانياً : جرائم مُقدم الخدمة :

وهي الجريمة الجريمة التي تضمنتها المادة (30) من القانون رقم 175 لسنة 2018 من قانون مكافحة جرائم تقنية المعلومات والتي تنص علي أنه :- يعاقب بالحبس مدة لا تقل عن سنة, وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه, أو بإحدى هاتين العقوبتين, كل مُقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه فى الفقرة الأولى من المادة (٧) من هذا القانون. فإذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة, وفاة شخص أو أكثر, أو الإضرار بالأمن القومى, تكون العقوبة السجن المشدد والغرامة التى لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضى المحكمة فضلاً عن ذلك بإلغاء ترخيص مزاولة النشاط[1].

كما تنص المادة (31) من ذات القانون علي أنه :- "يعاقب بالحبس مدة لا تقل عن سنة, وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة خالف الأحكام الواردة بالبند (٢) من الفقرة أولا من المادة (٢) من هذا القانون، وتتعدد عقوبة الغرامة بتعدد المجنى عليهم من مستخدمى الخدمة[2] .

يعاقب بالحبس مدة لا تقل عن ستة أشهر, وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه, أو بإحدى هاتين العقوبتين، كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات المشار إليها فى المادة (٦) من هذا القانون[3] .

يعاقب بغرامة لا تقل عن خمسة ملايين جنية ولا تجاوز عشرة ملايين جنيه، كل مقدم خدمة أخل بأى من التزاماته المنصوص عليها فى البند (١) من الفقرة (أولاً) من المادة (٢) من هذا القانون. وتضاعف عقوبة الغرامة فى حالة العود، وللمحكمة أن تقضى بإلغاء الترخيص.

ويعاقب بغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتى ألف جنيه، كل مقدم خدمة خالف أحكام الفقرة (ثانيًا) و(رابعًا) من المادة (٢) من هذا القانون [4] .

---

[1] فيتفصيل ذلك انظر د/ ماجد بن كريم الزراع : الركن المادي في الجرائم المعلوماتية – مرجع سابق – ص 81.

[2] راجع المستشار / بهاء المري : شرح جرائم تقنية النعلومات – مرجع سابق – ص 95 .

[3] المادة 32 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

[4] المادة 33 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

ويعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبالغرامة التى لا تقل عن مائتى ألف جنيه ولا تجاوز مليون جنيه، كل مقدم خدمة خالف أحكام الفقرة (ثالثًا) من المادة (٢) من هذا القانون[1].

المبحث الثالث

الجرائم الالكترونية المرتكبة بمعرفة الشخص الاعتباري

الشخص الاعتباري يتمثل في الدولة ومديرياتها ومدنها ومؤسساتها ، وكذا المنشآت العامة التي يمنحها القانون شخصية اعتبارية[2] ، ونعرض فيما يلي لصورتين من صور المسئولية الجنائية وهما :

أولاً : مسئولية الشخص المسئول عن الإدارة :

حيث تنص المادة (٣٥) من ذات القانون علي أنه :- "يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن ثلاثين ألف جنية ولا تزيد عن مائة ألف جنية أو بإحدى هاتين العقوبتين، كل مسئول عن الإدارة الفعلية لأى شخص اعتبارى، إذا تعرض الموقع أو الحساب الخاص أو البريد الإلكترونى أو النظام المعلوماتى المخصص للكيان الذى يديره، لأى جريمة من الجرائم المنصوص عليها فى هذا القانون، ولم يبلغ بذلك الجهات المختصة وقت علمه بالجريمة.

ثانياً : مسئولية الشخص الاعتباري :

وفى الأحوال التى ترتكب فيها أى من الجرائم المنصوص عليها فى هذا القانون، باسم ولحساب الشخص الاعتبارى، يعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلى[3] .

---

[1] انظر المادة 31 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

[2] راجع حكم المحكمة الإدارية العليا في الطعن رقم 931 لسنة 3 ق جلسة 1985/1/4 س 3 – ص 466 .

[3] المادة 36 من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

وللمحكمة أن تقضى بإيقاف ترخيص مزاولة الشخص الاعتبار للنشاط مدة لا تزيد على سنة، ولها فى حاله العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتبارى بحسب الأحوال، ويتم نشر الحكم فى جريدتين يوميتين واسعتى الانتشار على نفقة الشخص الاعتبارى[1] .

ووفقا للمادة (37) من ذات القانون فإنه لا يترتب على تقرير مسئولية الإدارة الفعلية للشخص الاعتبارى استبعاد المسئولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التى تقوم بها الجريمة[2] .

الفصل الثالث

الأحكام الإجرائية للجريمة الالكترونية في القانون المصري

الأحكام الإجرائية للجريمة الالكترونية هي عبارة عن القواعد التي تنظم سير إجراءات وقائع الجريمة منذ لحظة ارتكابها وحتي تنفيذ العقوبة علي مرتكبها .

ومع تزايد ارتكاب الجرائم الالكترونية فقد وجب علي المشرع وضع القواعد الإجرائية التي تلائم هذه الجرائم وتناسبها ، من حيث جمع الأدلة والاستدلال ، وضبط وتفتيش ، وفي هذا الفصلسنقوم بعرض خصوصية القواعد الإجرائية في النظام القانوني، وفيما يلي سنعرض لخصوصية الضبط والتحقيق في الجريمة الالكترونية ، ثم نعرض لمسرح الجريمة الالكترونية والاستعانة بالخبرة الفنية وحجية الدليل الرقمي ، وأخيراً معرض لإجراءات المنع من السفر وترقب الوصول والصلح والتصالح في الجرائم الالكترونية وذلك علي النحو الأتي :

المبحث الأول :خصوصية الضبط والتحقيق في الجريمة الالكترونية .

المبحث الثاني :مسرح الجريمة الالكترونية والاستعانة بالخبرة الفنية وحجية الدليل الرقمي .

المبحث الثالث :إجراءات المنع من السفر وترقب الوصول والصلح والتصالح في الجرائم الالكترونية .

---

[1] راجع المستشار / بهاء المري : شرح جرائم تقنية النعلومات – مرجع سابق – ص 99 .

[2] انظر في شرح وتفصيل ذلك انظر د/ ماجد بن كريم الزراع : الركن المادي في الجرائم المعلوماتية – مرجع سابق – ص 82 .

المبحث الأول

خصوصيةالضبط والتحقيق في الجريمة الالكترونية

تتميز الجرائم الالكترونية بالتقنية العالية التي تحتاج إلي متخصصين في ذات المجال سواء في مرحلة الضبط أو التفتيش أو التحقيق أوإصدار الأوامر ، وذلك ما سنعرض له فيما يلي :

أولاً : خصوصية الضبط في مرحلة جمع الاستدلالات :

يتولى مأموري الضبط القضائي البحث والاستقصاء وجمع الأدلة عن الجرائم ومرتكبيها وجمع الاستدلالات التي تلزم للتحقيق في الدعوى الجنائيةوإثباتها ، ولقد نصت المادة الخامسة من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات علي أنه يجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص منح صفة الضبطية القضائية للعاملين بالجهاز أو غيرهم ممن تحددهم جهات الأمن القومى، بالنسبة إلى الجرائم التى تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم[1] .

والمقصود بالجهاز هو الجهاز القومي لتنظيم الاتصالات وقد أجاز القانون للوزير المختص وهو وزير الاتصالات وتكنولوجيا المعلومات أن يستصدر قراراً من وزير العدل بمنح صفة الضبطية القضائية للعاملين بالجهاز القومي لتنظيم الاتصالات أو غيرهم ممن تحددهم جهات الأمن القومي بالنسبة إلي الجرائم التي تقع بالمخالفة لأحكام هذا القانون والمتعلقة بأعمال وظائفهم .

والمقصود بجهات الأمن القومي في تطبيق أحكام هذا القانون رئاسة الجمهورية ووزارة الدفاع ووزارة الداخلية والمخابرات العامة وهيئة الرقابة الإدارية .

وفي مرحلة جمع الاستدلالات يقوم مأموري الضبط القضائي بمجموعة من الإجراءات التي أجاز لهم القانون القيام بها لجمع الأدلة قبل إحالة هذه الاستدلالات للنيابة العامة للقيام بتحقيقاتها، وهذه الإجراءات نصت عليها بوجه عام المادة 22 من قانون الإجراءات الجنائية وهي على النحو التالي:

1- قبول البلاغات والشكاوى التي ترد إليهم بشأن الجرائم وعرضها دون تأخير على النيابة العامة.

---

[1] د/ حسن ربيع : الإجراءات الجنائية في التشريع المصري – بدون دار نشر – ص 26 .

2- إجراء الكشف والمعاينة والحصول على الإيضاحات اللازمة لتسهيل التحقيق، والاستعانة بالخبراء المختصين والشهود دون حلف يمين.

3- اتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة.

4- إثبات جميع الإجراءات التي يقومون بها في محاضر رسمية بعد توقيعها منهم ومن المعنيين بها.

وهذه الإجراءات التي يحب على مأمور الضبط القضائي في حال وقوع جريمة أن يقوموا بها جاءت لكافة الجرائم دون تخصيص، مما يجعلنا نقرر أن الجريمة الالكترونية في حال وقوعها تقوم الشرطة المختصة بإجراءات جمع الاستدلالات فيما يخصها، فيحق لرجال الشرطة الاستعانة بالخبراء المختصين الكترونيا لكشف الجريمة واتخاذ جميع الوسائل اللازمة للمحافظة على أدلة الجريمة.

وفي الحقيقة فإن هذه المهام المنوطة بمأموري الضبط القضائي بالنسبة للجريمة الالكترونية لها خصوصية وخاصة في مرحلة جمع الاستدلالات، ومن ثم فكان لابد من البحث عن مفهوم عصري يتلاءم مع جريمة عصرية كالجريمة الالكترونية، فلا يكفي أن يستعين رجل الشرطة بخبير مختص للبحث في الجريمة الالكترونية، بل لا بد من أن يكون رجل الشرطة ذاته هو المختص وذلك من خلال إنشاء وحدات متخصصة في الشرطة مختصة في ملاحقة الجرائم الالكترونية وهو ما تسعى لتحقيقه كثير من الدول العربية حديثا ومنها فلسطين ، وإزاء ذلك فقد أجاز المشرع المصري في المادة الخامسة من قانون مكافحة جرائم تقنيات المعلومات لوزير العدل بالاتفاق مع وزير الاتصالات وتكنولوجيا المعلومات منح الضبطية القضائية للعاملين بالجهاز القومي لتنظيم الاتصالات[1].

ويرجع ذلك إلي أن مرحلة جمع الاستدلالات في الجريمة الالكترونية يتم عبر شبكة الانترنت وأجهزة الحاسب الآلي ، وهي تحتاج إلي التخصص الفني للحصول على كافة البيانات والمعلومات اللازمة المرتبطة بالجرائم التي تقع بواسطة الحاسب الآلي أو أية وسيلة الكترونية لضبط جرائم الكمبيوتر والانترنت ، وحيث أن مرحلة جمع الاستدلالات هي مرحلة جمع المعلومات والأدلة ، ومن ثم فإنه يلزم لها شخص متخصص في هذا المجال[2].

وهو ما يتطلب بالضرورة إعداد كوادر بشرية من رجالالشرطة أو العاملين بالجهاز القومي لتنظيم الاتصالات ليستطيعوا التعامل مع الجريمة الالكترونية وإلا تعرضنا لفقدان الدليل، لأن الشرطة هنا ستتعامل مع بيانات دقيقة

---

[1] المستشار / بهاء المري : جرائم السوشيال ميديا – مرجع سابق – ص 265 .

[2] د/ سعيد عبد اللطيف حسن : إثبات جرائم الكومبيوتر والجرائم المرتكبة عبر الانترنت – دار النهضة العربية 1999- ص 44 .

على الأجهزة الالكترونية وعدم التعامل معها بشكل فني دقيق سيؤدي إلى فقدانها، لا سيما وأن نوعية المجرم الالكتروني تختلف في أسلوبه الإجرامي عن المجرم التقليدي الذي يرتكب جريمته باستعمال أدوات مادية يسهل التعامل معها وضبطها والتحفظ عليها [1].

ولقد انتهج المشرع الاماراتي نفس النهج في منح وزير العدل مهمة تحديد مأموري الضبط القضائي ومنحهم الضبطية القضائية ، ولكنه لم يحدد مهامهم علي وجه الدقة [2] .

ثانياً : خصوصية التفتيش في الجريمة الالكترونية.

التفتيش إجراء من إجراءات التحقيق ، ولا يجوز القيام به إلا في حالة الجريمة المتلبس بها وإلا وجب إصدار إذن به من جهة التحقيق المختصة ، وإذا كانت الجريمة تتعلق بالمساس بأمن الدولة أو نشر مواد مناهضةلنظامها السياسي أو الاجتماعي أو الاقتصادي أو بالتحريض علي الارهاب أو بث الفتنة الطائفية وما شابه ذلك وكانت الجريمة غير متلبس بها فإن الأمر في هذه الحالة يتطلب إعداد محضر تحريات من الجهة المختصة لعرضه علي النيابة العامة أو جهة التحقيق المختصة للإذن بضبط المتهم وضبط جهاز الكومبيوتر الذي أرسلت منه المادة المجرمة قانوناً أو الدخول علي موقع الجاني أو شبكة الانترنت لاستبيان اتصالاته بها [3].

ومتي أذنت النيابة العامة بضبط وتفتيش الجهاز كان للمختص من رجال الضبط القضائي أو لمن يندبه إذا رخصت له النيابة في ذلك لدي إصدارها الأذن ، ومن ثم يكون له الدخول علي كومبيوتر المتهم للتفتيش فيه ، وكذلك تفتيش مكتبه أو مسكنه في الحدود التي صدر فيها الإذن لضبط ما يكون متصلاً بالجريمة من أوراق أو أجهزة أخري أو مخرجات جهاز الكومبيوتر الخاص به وخلافه .

والتفتيش في هذه الحالة يشمل جميع مكونات الحاسب الألي مثل برامج النظام والتطبيقات التي يستعملها صاحب الجهاز وكذلك الأجهزة المتصلة به مثل الطابعة وشبكات الاتصال الخاصة به .

---

[1] د/ جميل عبد الباقي الصغير : الجوانب الإجرائية للجرائم المتعلقة بالإنترنت –دار النهضة العربية 2001 – ص 46.

[2] راجع نص المادة 49 من القانون الاتحادي بالامارات العربية المتحدة الخاص بمكافحة جرائم تقنية المعلومات .

[3] د/ حسن ربيع : الإجراءات الجنائية في التشريع المصري – مرجع سابق – ص 26 .

أما إذا كانت الجريمة متلبساً بها فيكون ذلك من حق مأمور الضبط القضائي المختص بدون إذن من جهة التحقيق .

خضوع تفتيش الحاسب الآلي للقواعد العامة :

يخضع تفتيش المكونات المادية للحاسب الآلي لضبط ما عليه من أدلة رقمية سواء كانت مخزنة أو من خلال ما نسخ علي أنظمة المعلومات من معلومات لدي اتصاله بشبكة الانترنت يتوقف علي ما إذا كان الحاسب الآلي في مكان عام أم مكتن خاص ، فإذا كان في مكان عام جاز لمأمور الضبط القضائي تفتيشه بدون إذن من جهة التحقيق ، أما إذا كان في مكان خاص مثل مسكن المتهم أو مكان يأخذ حكم المسكن مثل سيارته الخاصة أو في أحدي ملحقات مسكنه المتصلة بالمسكن فلا يجوز تفتيشه إلا بإذن مسبب من جهة التحقيق بناء علي تحريات جدية ترجع وقوع جريمة فعلاً [1] .

وإذا كانت الأدلة الرقمية علي حاسب آلي أو هاتف محمول بحرز شخص في مكان عام بطبيعته أو بالتخصيص فإن تفتيش هذا الحاسب أو الهاتف لا يجوز إلا في الأحوال التي يجوز فيها تفتيش هذا الشخص .

وتفتيش الحاسب الآلي يشمل عنصرين :

المكونات المادية للحاسب الآلي : وهو المكان الموجود فيه الحاسب الآلي والتفتيش هنا لا يكون داخل النظام المعلوماتي وإنما في أية متعلقات أخري لها صلة بالحاسب مثل المخرجات الورقية التي تم طبعها منه ، أو الطابعة المتصلة به لا سيما إذا كانت مما يخزن معلومات عن المخرجات أو أقراص مدمجة أو وسائط تخزين مثل هارد ديسك إضافي أو ميموري[2] .

المكونات المعلوماتية للحاسب الآلي : وهي البيانات والمعلومات الرقمية الموجودة في ذاكرة الحاسب والقرص الصلب الداخلي ونسخ الكوكيز التي تنتج عن إتصاله بالمواقع الالكترونية

ثالثا : مرحلة التحقيق الإبتدائي:

---

[1] د/ جميل عبد الباقي الصغير : الجوانب الإجرائية للجرائم المتعلقة بالإنترنت –دار النهضة العربية 2001 – ص 46.

[2] د/ سعيد عبد اللطيف حسن : إثبات جرائم الكومبيوتر والجرائم المرتكبة عبر الانترنت – مرجع سابق– ص 51 .

وهنا يأتي دور النيابة العامة في التحقيق والاستجواب في الجريمة الالكترونية، وهي المرحلة الأهم ومنها نبدأ في تحريك الدعوى الجنائية ضد المتهم في الجريمة الالكترونية، ولقد أسند المشرع لجهة التحقيق المختصة مهمة تحديد المهام والاختصاصات التي يقوم بها مأموري الضبط المختص [1] .

ولذلك أجاز قانون الإجراءات الجنائية لسلطة التحقيق الاستعانة بالخبراء المختصين لإثبات حالة الجريمة المرتكبة تحت إشراف وكيل النيابة وبحضوره إذا قدر أن مصلحة التحقيق تستدعي ذلك.

وعلى الرغم من أن قانون الإجراءات الجنائية أجاز للنيابة المختصة بالتحقيق الاستعانة بمن يريد من الخبراء المختصين في عالم الالكترونيات، إلا أن ذلك لا يعني بأي حال من الأحوال عدم ضرورة إعداد كادر مختص من وكلاء النيابة للتحقيق في الجرائم الالكترونية، ذلك أن أخطر مرحلة من مراحل التحقيق التي يقوم بها وكلاء النيابة هي استجواب المتهم، فكيف سيتم استجواب المتهم في جريمة الكترونية دون أن يكون وكيل النيابة المحقق ملم بكافة جوانب وتفاصيل أركان الجريمة الالكترونية من ناحية قانونية من جانب، ومن ناحية فنية تقنية من جانب آخر فيما يتعلق بالأدلة التي بين يديه سواء في البيانات المخزنة على الأجهزة الالكترونية من أرقام وصور ودلالاتها في ارتكاب الجريمة.

رابعاً : مرحلة الأوامر القضائية المؤقتة :

تنص المادة السادسة من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات علي أنه لجهة التحقيق المختصة، بحسب الأحوال، أن تصدر أمرًا مسببًا، لمأمورى الضبط القضائى المختصين، لمدة لا تزيد على ثلاثين يومًا قابلة للتجديد لمرة واحدة، متى كان لذلك فائدة فى ظهور الحقيقة على ارتكاب جريمة معاقب عليها بمقتضى أحكام هذا القانون بواحد أو أكثر مما يأتى:

١ – ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات، وتتبعها فى أى مكان أو نظام أو برنامج أو دعامة إليكترونية أو حاسب تكون موجودة فيه.
ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة أن كان لها مقتضٍ.

---

[1] انظر المادة السادسة من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

٢ – البحث والتفتيش والدخول والنفاذ إلى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقًا لغرض الضبط.

٣ – أن تأمر مقدم الخدمة بتسليم ما لدية من بيانات أو معلومات تتعلق بنظام معلوماتى أو جهاز تقنى، موجودة تحت سيطرته أو مخزنة لديه، وكذا بيانات مستخدمى خدمته وحركة الاتصالات التى تمت على ذلك النظام أو الجهاز التقنى ، وفى كل الأحوال، يحب أن يكون أمر جهة التحقيق المختصة مسببًا.

ويكون استئناف الأوامر المتقدمة أمام المحكمة الجنائية المختصة منعقدة فى غرفة المشورة فى المواعيد، ووفقًا للإجراءات المقررة بقانون الإجراءات الجنائية.

لجهة التحقيق المختصة، متى قامت أدلة على قيام موقع يُبث داخل الدولة أو خارجها، بوضع أى عبارات أو أرقام أو صور أو أفلام أو أى مواد دعائية، أو ما فى حكمها بما يُعد جريمة من الجرائم المنصوص عليها بالقانون، وتشكل تهديدًا للأمن القومى أو تعرض أمن البلاد أو اقتصادها القومى للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيًا.

وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة منعقدة فى غرفة المشورة، خلال أربع وعشرين ساعة مشفوعًا بمذكرة برأيها. وتُصدر المحكمة قرارها فى الأمر مسببًا إما بالقبول أو بالرفض، فى مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرضه عليها[1].

ويجوز فى حالة الاستعجال لوجود خطر حال أو ضرر وشيك الوقوع, أن تقوم جهات التحرى والضبط المختصة بإبلاغ الجهاز، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط المذكورة فى الفقرة الأولى من هذه المادة وفقًا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه ، وعلى جهة التحرى والضبط التى قامت بالإبلاغ أن تحرر محضرًا تثبت فيه ما تم من إجراءات وفق أحكام الفقرة السابقة يُعرض على جهات التحقيق خلال ثمانٍ وأربعين ساعة من تاريخ الإبلاغ الذى وجهته للجهاز، وتتبع فى هذا المحضر ذات الإجراءات المبينة بالفقرة الثانية من هذه المادة، وتصدر المحكمة المختصة قرارها فى هذه الحالة، أما بتأييد ما تم من إجراءات حجب أو بوقفها .

---

[1] انظر نص المادة السابعة من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

فإذا لم يُعرض المحضر المشار إليه فى الفقرة السابقة فى الموعد المحدد، يعد الحجب الذى تم كأن لم يكن. ولمحكمة الموضوع أثناء نظر الدعوى أو بناءً على طلب جهة التحقيق أو الجهاز أو ذوى الشأن أن تأمر بإنهاء القرار الصادر بالحجب أو تعديل نطاقه.

وفى جميع الأحوال, يسقط القرار الصادر بالحجب بصدور أمر بألا وجه لإقامة الدعوى الجنائية, أو بصدور حكم نهائى فيها بالبراءة.

المبحث الثاني

مسرح الجريمة الالكترونية والاستعانة بالخبرة الفنية وحجية الدليل الرقمي

ترتكب الجريمة الالكترونية عبر شبكات المعلومات الدولية بواسطة الحاسب الآلي أو الموبايل ، ولكن لا يوجد مسرح مادي ملموس للجريمة فيما يعرف بمسرح الجريمة ، ولذلك استوجب هذا الوضع الجديد الاستعانة بالخبرة الفنية التي تتقن هذه المستجدات ، حتي تستطيع استخراج الأدلة والحفاظ عليها وتفريغها وتبيان دلالتها ، وذلك ما سنعرض له فيما يلي :

المطلب الأول : مسرح الجريمة الالكترونية .

المطلب الثاني : إجراءات الاستعانة بالخبرة الفنية .

المطلب الثالث : حجية الأدلة الرقمية في الجرائم الالكترونية .

المطلب الأول

مسرج الجريمة الالكترونية

يعرّف مسرح الجريمة بأنه المكان الذي شهد وقوع الجريمة ،و يشمل على العديد من الأدلة التي تسهل التحقيق الجنائي ، وتسهل الاستدلال على الجاني الذي ارتكب الجريمة .

ويُعد كل مكان اتصل بالنشاط الإجرامي الذي ترتب عليه وقوع الجريمة أو حوى دليلاً يتصل بها مسرحاً للجريمة ، وكما نعلم بأن أول مهمة لرجال الضبط القضائي بمجرد علمهم بوقوع جريمة الانتقال إلى مسرح الجريمة وتأمينه إلى حين حضور وكيل النيابة المختص لمباشرة عمله وإجراء كافة التحقيقات اللازمة في مسرح الجريمة من سماع شهود وتنظيم محضر كشف على مسرح الجريمة وتوصيفه بدقة وضبط أدوات الجريمة الموجودة في مسرح الجريمة لمواجهة المتهم بها حين استجوابه[1] .

وفي الجرائم العادية وفقاً لقانون الإجراءات الجنائية يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فوراً إلى مكان الجريمة، ويعاين الآثار المادية لها ويتحفظ عليها، ويثبت حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة ويسمع أقوال من كان حاضراً ، أو من يمكن الحصول منه على إيضاحات في شأن الجريمة ومرتكبيها، ويجب عليه أن يخطر النيابة العامة فورا بانتقاله، كما يجب على عضو النيابة المختص بمجرد إخطاره بجناية متلبس بها الانتقال فورا إلى مكان الجريمة[2].

وفي الجرائم التقليدية يكون مسرح الجريمة بسيط وواضح المعالم ، وكل ما يتطلب من مأمور الضبط القضائي وعضو النيابة المختص بالتحقيق معاينته وتحديد أوصافه وضبط ما فيه من أدوات مستخدمة في الجريمة، بينما يكون مسرح الجريمة الالكترونية في صورة مغايرة ، وعلي شكل مختلف كأختلاف طبيعة الجريمة الالكترونية ، فهو حتماً ليس ببساطة ووضوح مسرح الجريمة التقليدية العادية[3] .

ويمكن القول أن مسرح الجريمة الالكترونية يتمثل في عالم افتراضي لا حدود مكانية له ، وإنماالبحث سينصب علي وسائل وأدوات تتم بها الجريمة عبر أجهزة الكترونية وشبكات الكترونية ،وسيتم ذلك باستخدام الأجهزة الالكترونية أيضاً ؛ لأن الأدلة الالكترونية لها أشكال مختلفة، فقد تكون رسالة أو صورة محملة علي كمبيوتر أو علي هاتف خلوي .

---

[1] د/ سعيد عبد اللطيف حسن : إثبات جرائم الكومبيوتر والجرائم المرتكبة عبر الانترنت – مرجع سابق– ص 54 .

[2] د/ جميل عبد الباقي الصغير : الجوانب الإجرائية للجرائم المتعلقة بالإنترنت – مرجع سابق – ص 44 .

[3] د/ جميل عبد الباقي الصغير : الانترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالانترنت –دار النهضة العربية 1999– ص 76 .

كما أن طريقة فحص وسائل ارتكاب الجريمة الالكترونية في مسرح الجريمة بواسطة الأجهزة الالكترونية ليس بالأمر البسيط، فقد تكون جهاز كمبيوتر واحد وقد تكون عدة أجهزة، وقد يكون الجهاز في حالة تشغيل ، وعلي ذلك فقد يتضمن مسرح الجريمة وسائل ارتكاب الجريمة التي تتمثل في الموبايل ، أو الحاسب الآلي بما يشمله من مواقع الكترونية أو محتوي أو حساب خاص أو بريد الكتروني ، وكذلك يتضمن مسرح الجريمة شبكة الانترنت التي تربط الحاسبات الآلية ، وذلك ما سنفصله فيما يلي :-

الموبايل :

تعد البرامج التي يحتوي عليها الموبايل مسرحاً للجريمة ، فقد تقع الجريمة باستخدام صفحة فيس بوك أو أحدي برامج الموبايل سواء حال الاتصال به بمحمول آخر أو بشبكة الانترنت ، مثل إرسال عبارات تشكل قذفاً أو سباً أو إرسال صور إباحية أو تهديداً ، ويتم في هذه الحالة تفريغ هذه البرامج والتحفظ عليها ، وإثبات رقم الخط الذي تم الإرسال منه .

الحاسب الآلي :

هوكل جهاز أو معدة تقنية تكون قادرة على التخزين، وأداء عمليات منطقية، أو حسابية، وتستخدم لتسجيل بيانات أو معلومات، أو تخزينها، أو تحويلها، أو تخليقها، أو استرجاعها، أو ترتيبها، أو معالجتها، أو تطويرها، أو تبادلها، أو تحليلها، أو للاتصالات.

وقد تقع الجريمة باستخدام الحاسب الآلي ، فيقوم مأمور الضبط القضائي بمعاينة الجهاز وأجزائه المادية ، ومكوناته التي تخزن فيها المعلومات، وكذلك معاينة الصفحة التي تم التواصل من خلالها بشبكة الانترنت ، وتفريغ محتواها ، وإثبات رقم الخط الأرضي الذي تم الارسال منه ، وتوقيت ارتكاب ذلك .

الموقع الالكتروني :

وهو مجال أو مكان افتراضى له عنوان محدد على الشبكة المعلوماتية، ويهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة علي حسب نوعية البيانات والمعلومات .

الحساب الخاص:

وهو مجموعة من المعلومات الخاصة بشخص طبيعى أو اعتبارى، تخول له الحق دون غيره الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتى.

فهو موقع إلكتروني عبر الإنترنت خاص بالتواصل الاجتماعيّ، و يتمكّن المُستخدِم من خلاله من التواصل والتفاعل مع المُستخدِمين الآخرين للموقع، حيث يسمح هذا الموقع للمُستخدِمين بإنشاء ملفات شخصية تُحمّل من خلالها الصور ومقاطع الفيديو وتُشارك عبر الموقع، وإرسال الرسائل واستقبالها،بالإضافة إلى التحدّث عما يفعله المُستخدِم، وغيرها العديد من الخدمات الأُخرى التي يوفرها هذا الموقع .

البريد الإلكترونى:

وهو وسيلة لتبادل رسائل إلكترونية على عنوان محدد، بين أكثر من شخص طبيعى أو اعتبارى، عبر شبكة معلوماتية، أو غيرها من وسائل الربط الإلكترونية، من خلال أجهزة الحاسب الآلى وما فى حكمها.

المحتوى:

وهي أى بيانات تؤدى بذاتها، أو مجتمعة مع بيانات أو معلومات أخرى إلى تكوين معلومة أو تحديد توجه أو اتجاه أو تصور أو معنى أو الإشارة إلى بيانات أخرى.

الدعامة الإلكترونية:

تعني أى وسيط مادى لحفظ وتداول البيانات والمعلومات الإلكترونية ومنها الأقراص المدمجة أو الأقراص الضوئية والذاكرة الإلكترونية أو ما فى حكمها.

الشبكة المعلوماتية:

وهي مجموعة من الأجهزة أو نظم المعلومات مرتبطة معًا، ويمكنها تبادل المعلومات والاتصالات فيما بينها، ومنها الشبكات الخاصة والعامة وشبكات المعلومات الدولية, والتطبيقات المستخدمة عليها[1] .

---

[1] د/ جميل عبد الباقي الصغير : الانترنت والقانون الجنائي – الأحكام الموضوعية للجرائم المتعلقة بالانترنت –دار النهضة العربية 1999– ص 76 .

وهذه الشبكاتهي التي يرتبط بها الحاسب الآلي أو الموبايل المطلوب الاستحصال منه علي الدليل الرقمي ، وقد يكون مرتبطاً بجهاز آخر من خلال شبكة معلوماتية أي شبكة حواسيب مربوطة ببعضها البعض ، فإن هذه الشبكة حينئذ تكون مسرحاً للجريمة ، وهو ما يثير كثيراً من الإشكاليات كما لو كان أحد الأجهزة الأخري موجود في مكان آخر لا يخضع لاختصاص مأمور الضبط القضائي ، أو كان في دولة أخري ، وهو الأمر الذي يتمثل في الحالات الأتية :

الحالة الأولي : وهي حالة أن كومبيوتر المتهم متصل بكومبيوتر آخر داخل الدولة ، وفي هذه الحالة نري أن الاختصاص يمتد لمأمور الضبط القضائي بتفتيش الجهاز الآخر لتعلقه بالجريمة طبقاً للقواعد العامة في امتداد الاختصاص فيكون له امتداد التفتيش لي سجلات بيانات ومعلومات الجهاز الآخر الموجود في مكان آخر ورتبط بالجهاز الذي انعقد لمأمور الضبط القضائي الاختصاص بتفتيشه وذلك متي كان من الضروري الدخول علي سجلات ذلك الجهاز الآخر لكشف الحقيقة بمناسبة الجريمة محل البحث أو كان هناك احتمالية ضياع الادلة الرقمية الموجودة علي الجهاز الآخر مثل خشية محوها إذا شاع نا ضبط جهاز المتهم .

الحالة الثانية : وهي حالة أن يكون الحاسب الآلي الآخر المتصل به حاسب المتهم موجود في دولة أخري ، وكان المتهم قد قام بتخزين المعلومات المتعلقة بجريمة والتي سيتم الاستحصال من خلالها علي الدليل الرقمي في أنظمة تقنية خارج الدولة عبر شبكة الانترنت لا سيما الجماعات الارهابية أو عصابات غسل الأموال والاتجار في المخدرات عبر الانترنت فإن تفتيش الجهاز الآخر عبر شبكة الانترنت سيثير مشكلات تمس سيادة الدولة الأخري .

والتفتيش في هذه الحالة والذي يسميه الفقه التفتيش الالكتروني العابر للحدود بتطلب وجود اتفاقات معينة بين الدول لإمكانية القيام به ، ولذلك نص المشرع المصري في المادة الرابعة من قانون مكافحة جرائم تقنية المعلومات علي أن :- " تعمل السلطات المصرية المختصة على تيسير التعاون مع نظيراتها بالبلاد الأجنبية فى إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيق مبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادى ارتكاب جرائم تقنيه المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها ، على أن يكون المركز الوطنى للاستعداد لطوارئ الحاسب والشبكات بالجهاز هو النقطة الفنية المعتمدة فى هذا الشأن "

ومن ثم فإن هذه الحالة لا تجيز تفتيش الحاسب الآلي الموجود في دولة أخري إلا من خلال الاتفاقيات الدولية التي تتيح المساعدة علي ذلك ، وإلا لا يجوز تفتيشها في حالة عدم وجود مثل هذه الاتفاقيات أما إذا تعلق الأمر

بالتفتيش في بيانات متاحة للجمهور أو رضي صاحب الجهاز الآخر فإن التفتيش يكون جائز ويكون الدليل الالكتروني الناجم عنه صحيحا قانونا ؟

الحالة الثالثة : هو أن يتم اعتراضبيانات ومعلومات وسجل النظام المعلوماتي للجهاز الآخر الموجود في بلد أجنبي ، أي التنصت عليه ، ونشير إلي أن قانون مكافحة جرائم تقنية المعلومات المصري لم يتعرض لهذا الفرض .

ونري في هذا الفرض أن الجريمة المطلوب ضبط دليلها الرقمي إذا كانت تتعلق بأمر يهدد الأمن القومي أو أمن المجتمع أن تصدر جهة التحقيق أمر من القاضي بمراقبة الاتصالات وفقا للقواعد المعمول بها في قانون الاجراءات الجنائية ، حيث أن المشرع المصري قد اشار في ديباجة قانون مكافحة جرائم تقنية المعلومات إلي قانون الإجراءات الجنائية الذي يبيح مراقبة الاتصالات في حالة وجود جريمة تستخدم فيها وسائل الاتصال [1] .

ويجب علي مأمور الضبط القضائي الذي يقوم بمعاينة مسرح الجريمة الالكترونية أن يكون على دراية كافية في التقنيات الالكترونية حتى يتمكن من تحديد الدليل الذي يبحث عنه، وعليه يتوجب على المحقق في محضر الكشف على مسرح الجريمة مراعاة الأمور التالية :

1- تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.

2- العناية بملاحظة الطريقة التي تم بها إعداد النظام.

3- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.

4- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

5- التحفظ على معلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة، وفحصها، ويرفع من عليها البصمات ذات الصلة بالجريمة.

---

[1] د/ جميل عبد الباقي الصغير : الجوانب الإجرائية للجرائم المتعلقة بالإنترنت –مرجع سابق – ص 46.

6- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.

7- قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات.

المطلب الثاني

إجراءات الاستعانة بالخبرة الفنية

تناولت المادة الأولي من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات تعريف الخبرة بأنها كل عمل يتصل بتقديم الاستشارات أو الفحص أو المراجعة أو التقييم أو التحليل فى مجالات تقنية المعلومات. و تلعب الخبرة الفنية دوراً هاماً في عملية الاثبات وكشف طلاسم الجريمة الالكترونية ، حيث تتم معاينة مسرح الجريمة لتوفير أدلة الإثبات من قبل خبير بالتقنيات المعلوماتية ، فإذا وقعت الجريمة باستخدام التلفون المحمول سواء حال الاتصال منه بمحمول آخر أو بشبكة الانترنت ، مثل إرسال عبارات تشكل قذفاً أو سباً أو إرسال صورة إباحية أو تهديداً ، أو كان وسيلة لارتكاب أي سلوك مما يشكل جريمة من الجرائم المنصوص عليها في قانون مكافحة جرائم تقنية المعلومات ، فيتم معاينة الصفحة التي تم الاتصال بها من خلاله بشبكة الانترنت لاستبيان محتوي هذا السلوك الاجرامي .

فلا شك أن الجرائم الالكترونية يستلزم فحصها وجود خبراء فنيين لمعاونة رجال الضبط القضائي والتحقيق والمحاكمة وتقديم المشورة الفنية حال طلبها ، ولقد أحسن المشرع المصري بالنص صراحة في الفقرة الأولي من المادة العاشرة من قانون مكافحة جرائم تقنية المعلومات علي الاستعانة بخبراء فنيين في عملية البحث والتحري وجمع الاستدلالات[1].

ولأعمال الخبراء أهمية كبيرة في البحث عن الدليل الالكتروني ، فالخبرة تنير الطريق لجهة التحقيق والقضاء ، وخاصة في ظل الخصوصية التي تتميز بها الجرائم الالكترونية التي تعد من المسائل الفنية المعقدة والتي يصعب

---

[1] د/ جميل عبد الباقي الصغير : الجوانب الإجرائية للجرائم المتعلقة بالإنترنت – مرجع سابق – ص 65 .

علي أي شخص الإلمام بها ، ومن ثم لزم لكشف غموضها وتجميع أدلتها الارتكان إلي هؤلاء الخبراء لانجاح أعمال التحقيق وعمليات الاستدلالال ، فقد يؤدي الاستغناء عن الخبراء طمس الأدلة أو تدميرها أو عدم الإلمام بها وأهمالها ، بسبب جهل المحقق غير الخبير في هذه التقنيات وعدم العلم بها ، وتطبق علي الخبراء في ممارسة عملهم وتحديد التزاماتهم وحقوقهم القواعد والأحكام الخاصة بقواعد تنظيم الخبرة أمام جهات القضاء [1] .

ويعد الخبير تقريرا يضمنه خلاصة ما توصل إليه من نتائج بعد تطبيق الأسس والقواعد العلمية الفنية على المسألة محل البحث، ولم يوجب المشرع إتباع شكل معين في تقرير الخبير، فقد يكون شفوياً أو كتابيا وفقا لما تحدده طبيعة المأمورية، لكن الواقع العملي أثبت أن ما يتم في الغالب الأعم هو أن يطلب من الخبير تقديم تقريره كتابة .

وإذا كان الحال كذلك بالنسبة لموضوعات الخبرة التقليدية، فأن أهمية إعداد تقارير فنية مكتوبة وملاحق توضيحية مصورة، تصبح حتمية في حالة الجرائم المعلوماتية أو الرقمية، حيث يقتضي الأمر عرض وتوضيح وتحليل الدليل الجنائي الرقمي وكيفية اشتقاقه ، ومعلوم أن تقارير الخبراء شأنها شأن باقي أدلة الإثبات تخضع حجيتها لتقدير القاضي ومدى تأثير أعمال الخبرة في الاقتناع الذاتي للقاضي .

المطلب الثالث

حجية الأدلة الرقمية في الجرائم الالكترونية

الدليل الرقمي هو المعلومات الالكترونية التي يكون لها قوة أو قيمة في الاثبات مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب الألي أو الشبكات المعلوماتية وما في حكمها[2] .

---

[1] راجع الفقرة الثانية من المادة 10 من القانون 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

[2] المستشار : بهاء المري : شرح جرائم تقنية المعلومات – مرجع سابق – ص 380 .

وقد تكون هذه الأدلة من مخرجات جهاز الكومبيوتر كالأوراق أو الرسوم أو الصور أو الفديوهات أو المقاطع الصوتية ، كما قد تكون مخرجات رقمية ، وأكثر ما يعيق هذه الأدلة هي أنها في كثير من الأحيان يتم الحصول عليها بطريقة غير قانونية ، مما يعرضها للبطلان [1] .

ولقد تناولت المادة الأولي من القانون رقم 175 لسنة 2018 بشأن جرائم تقنية المعلومات تعريف الدليل الرقمى ، فعرفته بأنه أى معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما فى حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة.

ولقد اشترطت المادة الحادية عشر من القانون سالف الذكر أنيكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط الدعامات الإلكترونية، أو النظام المعلوماتى أو من برامج الحاسب، أو من أى وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية فى الإثبات الجنائى متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون[2] .

وتشير هذه الضوابط والشروط إلي ضرورة أن تستخرج هذه الأدلة بدون تحريف أو تحديث أو محو أو إتلاف للأجهزة أو المعدات ، أو تدمير للبيانات والمعلومات أو أنظمة البرامج أو الدعامات الالكترونية ، كما يشترط أن تكون هذه الأدلة ذات صلة بالواقعة محل الموضوع المطلوب إثباته أو نفيه وفقاً لقرار جهة التحقيق ، وأن يتم تحرير هذه الأدلة بمعرفة مأمور الضبط القضائي المخول له التعامل في هذه النوعية من الأدلة أو الخبراء أو المتخصصين ، وأن يتم توثيقها في محضر الإجراءات من قبل المختص ، وكذلك توثيق مكان ضبطه ومكان حفظه ومكان التعامل معه ومواصفاته[3].

فمن المتعارف عليه أن الأدلة التقنية هي أدلة معقدة وتحتاج إلي ضرورة توافر شروط ومواصفات معينة ومغايرة للأدلة المادية التقليدية ، وهو ما فطن إليه المشرع المصري ، ومن ثم فقد اشترط الشروط والضوابط المشار إليها

---

[1] القاضي / عمر محمود الحوتي : الوجيز في الحماية الجنائية من جرائم تقنية المعلومات – مرجع سابق – ص 181 .

[2] راجع المادة الحادية عشر من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات .

[3] الأستاذة / إلهام أبو الطمين : الإثبات الجنائي في مجال الجرائم الالكترونية – رسالة ماجستير جامعة العربي بن مهيدي –أم البواقي –كلية الحقوق 2018 – ص 60 .

سابقاً في الفقرة الأخيرة من المادة الحادية عشر سالفة الذكر لقبول هذه الأدلة التقنية في الإثبات ، وهي ضرورة أن يتوافر فيها الشروط والضواط والمواصفات الفنية التي تمنحها القوة الثبوتية حتي يعتد بها ، بأن يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الالكترونية أو من النظام المعلوماتي أو من برامج الحاسب أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة الجنائية المادية في الإثبات الجنائي متي توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون[1] .

المبحث الثالث

إجراءات المنع من السفر وترقب الوصول والصلح والتصالح في الجرائم الالكترونية

إجراء المنع من السفر وترقب الوصول هو إجراء وقائي لضمان تحقق الأمن العام وتأمين المصالح القومية والاقتصادية للبلاد ، فالمنع من السفر ليس عقوبة جنائية ؛ ولكنه يفرض عند وجود أدلة كافية على جدية الاتهام فى ارتكاب جريمة من الجرائم .

أما الصلح والتصالح في الجرائم الالكترونية

ونعرض فيما يلي لإجراءات المنع من السفر وترقب الوصول ، وكذلك الصلح والتصالح في الجرائم الالكترونية علي النحو الأتي :

المطلب الأول :- إجراءات المنع من السفر وترقب الوصول .

المطلب الثاني :- الصلح والتصالح في الجرائم الالكترونية .

المطلب الأول

إجراءات المنع من السفر وترقب الوصول

---

[1] لقد بينت اللائحة التنفيذية للقانون 175 لسنة 2018 بشأن مكافحة الجرائم الالكترونية أهم الشروط والضوابط الواجب توافرها في الدليل التقني ومنها أن تستخرج بدون تحريف أو تحديث أو محو ، وأن تكون ذات صلة بالواقعة محل الموضوع ، وأن يتم تحرير الدليل بمعرفة مأمور الضبط القضائي ، ويتم توثيقة في محضر الإجراءات .

نصت الفقرة الأولي من المادة التاسعة من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات علي أنه :- "يجوز للنائب العام أو من يفوضه من المحاميين العامين الأول بنيابات الاستئناف، ولجهات التحقيق المختصة، عند الضرورة، أو عند وجود أدلة كافية على جدية الاتهام فى ارتكاب جريمة من الجرائم المنصوص عليها فى هذا القانون أو الشروع فى ارتكابها، أن يأمر بمنع المتهم من السفر خارج البلاد أو بوضع اسمه على قوائم ترقب الوصول, بأمر مسبب لمدة محددة... "

ويتضح من ذلك أن المختص بإصدار الأمر بالمنع من السفر أو الوضع علي قوائم ترقب الوصول هو النائب العام أو من يفوضه من المحامين العامين الإول بنيابات الاستئناف وجهات التحقيق المختصة ، فلا يجوز لغير هؤلاءإصدار أياً من الأوامر السابقة فقد ورد تحديدهم علي سبيل الحصر .

ويشترط لصحة الأمر بالمنع من السفر صدوره من المختص بإصداره ، وأن تتوافر حالة من حالات ضرورة إصداره ، وأن يصدر بناء علي أدلة كافية تبين جدية الإتهام ، وأن يصدر مسبباً ، ومحدد المدة .

ولمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة خلال خمسة عشر يومًا من تاريخ علمه به، فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.

ويكون التظلم بتقرير يودع قلم كتاب محكمة الجنايات المختصة، وعلى رئيس المحكمة أن يحدد جلسة لنظر التظلم تُعلن بها النيابة العامة والمتظلم، وعلى المحكمة أن تفصل فى التظلم خلال مدة لا تجاوز خمسة عشر يومًا من تاريخ التقرير به، بحكم مُسبب بعد سماع أقوال المتظلم والنيابة العامة أو جهة التحقيق المختصة حسب الأحوال، ولها فى سبيل ذلك أن تتخذ ما تراه من إجراءات أو تحقيقات ترى لزومها فى هذا الشأن.

ويحدد القانون أصحاب الحق في التظلم ، حيث نص في المادة التاسعة علي أنه لمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر .

ويكون التظلم من أمر المنع من السفر أمام محكمة الجنايات المختصة خلال خمسة عشر يومًا من تاريخ علمه به، فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.

ولقد أجاز القانون اعادة تقديم التظلم في حالة رفض التظلم الأول ، حيث نصت المادة التاسعة سالفة الذكر علي أنه لمن صدر ضده أمر المنع من السفر أن يتظلم من هذا الأمر أمام محكمة الجنايات المختصة خلال خمسة عشر يومًا من تاريخ علمه به، فإذا رُفض تظلمه فله أن يتقدم بتظلم جديد كلما انقضت ثلاثة أشهر من تاريخ الحكم برفض التظلم.

المطلب الثاني

إجراءات الصلح والتصالح في الجرائم الالكترونية

من الأسباب الخاصة التي تنقضي بها الدعوي الجنائية التنازل عن الدعوي أو طلب الصلح فيها [1]، ولقد أجاز المشرع المصري الصلح والتصالح في جرائم تقنية المعلومات ، وهو اتجاه تتبناه معظم التشريعات ، ولقد تضمنت المادة 42 من قانون مكافحة جرائم تقنية المعلومات هذا الأمر حيث نصت علي أنه :- " يجوز للمتهم فى أية حالة كانت عليها الدعوى الجنائية، وقبل صيرورة الحكم باتا،إثبات الصلح مع المجنى عليه أو وكيله الخاص أو خلفه العام، أمام النيابة العامة أو المحكمة المختصة بحسب الأحوال .

ويلاحظ أن المشرع قيد الصلح والتصالح بنوع معين من الجرائم وهي جرائم الجنح الواردة في نصوص محددة وهذه النصوص هي المتعلقة بالجنح المنصوص عليها فى المواد (١٤، ١٥، ١٦،١٧، ١٨، ١٩، ٢٣، ٢٦، ٢٨، ٣٠، ٣١) من هذا القانون.

متي ينتج الصلح أو التصالح أثره :

ولا يُنتج إقرار المجنى عليه بالصلح المنصوص عليه بالفقرة السابقة أثره إلا باعتماده من الجهاز بالنسبة للجنح المنصوص عليها بالمواد (١٤، ١٧، ١٨، ٢٣) من هذا القانون.

كما لا يُقبل التصالح إلا من خلال الجهاز بخصوص الجنح المنصوص عليها بالمادتين (٢٩، ٣٥) من هذا القانون ، ولا يسقط حق المتهم فى التصالح برفع الدعوى الجنائية إلى المحكمة المختصة إذا دفع ثلثى الحد الأقصى للغرامة المقررة للجريمة أو قيمة الحد الأدنى أيهما أكثر، وذلك قبل صدور حكم نهائى فى الموضوع.

---

[1] د/ حسن ربيع : الإجراءات الجنائية في التشريع المصري – مرجع سابق – ص 26 .

وفى جميع الأحوال، يجب على المتهم الذى يرغب فى التصالح أن يسدد قبل رفع الدعوى الجنائية مبلغًا يعادل ضعف الحد الأقصى للغرامة المقررة للجريمة. ويكون السداد إلى خزانة المحكمة المختصة أو النيابة العامة بحسب الأحوال ، ويترتب على الصلح انقضاء الدعوى الجنائية، ولا أثر للصلح على حقوق المضرور من الجريمة أو على الدعوى المدنية.

خاتمة الدراسة:

بعد أن انتهينا من إعداد هذا البحث توصلنا إلى وجود مشكلة حقيقية في وقوع الجريمة الالكترونية في مصر، ذلك أن قانون مكافحة جرائم تقنية المعلومات لا يغطي كافة الجرائم المعلوماتية و الالكترونية الحديثة والمتوقع وقوعها في أي لحظة، كما أنه وعلى الرغم من وجود بعض الجرائم التقليدية المجرمة في هذا القانون ، إلا أن العقوبات المفروضة عليها لا تحقق الردع العام ، هذا من جهة ومن جهة أخرى وجدنا أن كثير من الجرائم لا يغطيها هذا القانون مثل جرائم السرقات والمقامرة والإرهاب الالكتروني، مما يعني وجود ثغرة تشريعية لا بد من تلافيها.

وبعد البحث في الجانب الإجرائي للجريمة الالكترونية من حيث التحقيق ومسرح الجريمة فيها والتفتيش والضبط وجدنا أن هذا النوع من الجرائم يحتاج رجال تحقيق مدربون وأصحاب خبرة واختصاص في الأجهزة الالكترونية، فهي تختلف كل الاختلاف من حيث التحقيق عن الجرائم التقليدية.

نتائج الدراسة:

تعتبر الجريمة الالكترونية من الجرائم المستحدثة لذلك فإن المعالجة القانونية يجب أن تتم في إطار شمولي ذلك أن اعتماد المحاور الرئيسية للحماية الجزائية فيما بينها لا يخلو من التكاملية حيث أن خصوصية التجريم يلزمها خصوصية في الاثبات وكذلك خصوصية في الملاحقة.

أما خصوصية التجريم فهي نابعة من وقوع غالبية هذه الجرائم على العالم الافتراضي دون المادي، وذلك حتى مع ملامسة بعضها للعالم المادي، فإنها تبقى من الخصوصية بما يجعلها متمايزة عن غيرها من الجرائم والتي تتطلب خصوصية في التجريم لئلا يفلت مقترفها من العقاب.

ومن ناحية خصوصية الإثبات في هذا النوع من الجرائم فإنها لا تخلو من الصعاب الجمة والتي تكتنف رصد واحتواء الدليل المتحصل من مسرح الجريمة سواء المادي أو الافتراضي ، وذلك كون الأدلة الرقمية صعبة الاحتواء وسهلة الاختفاء والمحو ، وكذلك يمكن التضليل بشأن كشفها أو الاطلاع على مضمونها .

وأما خصوصية الملاحقة فإنها تنبع من الجانب التقني لهذه الجرائم والتي تتطلب قدرات خاصة لدى الأشخاص المختصين بالمتابعة والملاحقة لمثل هذا النوع من الجرائم ، وكذلك الآليات القانونية التي يجب اقرارها للمساعدة في التنقيب عن الأدلة الالكترونية ، ومشروعية الإجراء الذي يمكن إتباعه للكشف عن الدليل وهذا عوضاً عن مشروعية الدليل نفسه.

وبناءً على ذلك تعتبرالجريمة الالكترونية اعتداء علي معطيات الكمبيوتر المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات وفي مقدمتها الإنترنت، فهي جريمة تقنية تنشأ في الخفاء يقارفها مجرمون أذكياء يمتلكون أدوات المعرفة التقنية ، وتوجه للنيل من الحق في المعلومات **وبالتالي يجب التركيز على حماية الآتي:**

سرية المعلومات:والذي يشمل ما يلزم من تدابيرلمنع الاطلاع غير المصرح به على المعلومات السرية أو الخاصة.

سلامة المعلومات: والذي يشمل التدابير اللازمة لحماية المعلومات من التغيير .

ضمان الوصول الى المعلومات والموارد الحاسوبية: والذي يشمل حماية إمكانية الوصول إلى المعلومات لمن له الحق بالاطلاع عليها.

توصيات الدراسة :

نوصي في البداية أنه يجب على الأفراد أخذ الحيطة والحذر عند التعامل مع وسائل الاتصال و التقنيات الحديثة وذلك بإتباع التالي :-

1- أخذ الحيطة والحذروعدم تصديق كل مايروج عبر الإنترنت والتأكد من صدق الإعلانات .

2- وضع الرقم السري بشكل مطابق للمواصفات الأمنية ويفضل الاحتفاظ ببرامج حماية سرقة الأرقام السرية.

3- المحافظة علي سلامة الأجهزة الحاسوبية والمعدات الالكترونية وما عليها من برامج ومعلومات ومعطيات خاصة.

ونوصي بوجه عام :

1- تدريب المحققين في الجرائم الالكترونية علي الفنيات الالكترونية حتى يستطيعون التعامل مع تلك الجرائم، لما تحتاجه من خبرة ومعرفة حتى يتمكن من يحقق في تلك الجريمة الوصول إلى الأدلة .

2- ضرورو العمل المستمر علي تحديث التشريعات المعلوماتية والالكترونية من الناحية الموضوعية والإجرائية لمواكبة التطورات التكنولوجية .

3- ضرورة إعادة النظر في النظم الإجرائية المتعلقة بالتحري والتحقيق في مجال الجريمة الالكترونية .

4- تفعيل التعاون الدولي علي المستوي التشريعي والقضائي والأمني في مجال مكافحة الجرائم الالكترونية .

5- إنشاء سلطات تحقيق متخصصة في الجرائم الالكترونية ، وكذلك نيابات ودوائر قضائية خاصة لنظر هذه الجرائم .

وعلي الله قصد السبيل ،،،

قائمة المراجع :

د/ أحمد محمود مصطفي : جرائم الحاسبات الآلية في التشريع المصري – دار النهضة العربية –الطبعة الأولي 2010

د/ أيمن ظاهر : شرح قانون الإجراءات الجزائية الفلسطيني، دراسة مقارنة مع القانونين المصري والأردني وفق اجتهادات محكمة النقض والتمييز، الجزء الأول، 2011 .

د/ إيمان فاضل السمرائي، د/ هيثم محمد الزغبي: نظم المعلومات الإدارية – الطبعة الأولى، دار صفاء للنشر والتوزيع. عمان. 2005.

المستشار بهاء المري : جرائم السوشيال ميديا – دار الأهرام للنشر والتوزيع 2022

د/ جعفر حسن جاسم الطائي : جرائم تكنولوجيا المعلومات، دار البداية، الطبعة الأولى، 2007.

د/ جميل عبد الباقي الصغير : الجرائم الناشئة عن استخدام الحاسب الآلي – دار النهضة العربية 2010 .

د/ حنان ريحان مبارك المضحكي : الجرائم المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، ط1، 2014.

د/ خالد الغثبر ومحمد القحطاني ، أمن المعلومات بلغة ميسرة، ط1، جامعة الملك سعود، الرياض 2009

د/ خالد عبد العظيم أبو غابة : التقدم التكنولوجي وأثره علي جرائم العرض –دراسة مقارنة – مكتبة الوفاء القانونية 2021 .

د/ رامي متولي القاضي : مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية ط 2011

د/ سامي علي حامد عياد : الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، 2007.

د/ عبد الله عبد الكريم عبد الله : جرائم المعلومات والإنترنت – الجرائم الإلكترونية – منشورات الحلبي الحقوقية بيروت 2011

د/ علي عبد القادر القهوجي : الحماية الجنائية لبرامج الحاسب – بحث منشور بمجلة البحوث القانونية والاقتصادية التي تصدرها كلية الحقوق –جامعة الاسكندرية 1997 .

د/ عمر الفاروق : المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية – طبعة 1995 .القاضي / عمر محمود الحوتي : الوجيز في الحماية الجنائية من جرائم تقنية المعلومات وفق أحكام القانون 175 لسنة 2018 –دار النهضة العربية 2012 .

د/ غنام محمد غنام : عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكومبيوتر – بحث مقدم لمؤتمر القانون والكومبيوتر والانترنت – كلية الشريعة والقانون بجامعة الامارات المتحدة 2000 .

د/ فتحي محمد أنور عزت : جرائم العصر الحديث –دار الفكر والقانون 2010 .

د/ فتوح عبد الله الشاذلي : جرائم الكومبيوتر – منشورات الحلبي 2003 .

د/ مدحت رمضان : جرائم الاعتداء علي الأشخاص والإنترنت – دار النهضة العربية 2000 .

د/ محمد سامي الشوا: ثورة المعلومات وانعكاساتها على قانون العقوبات – دار النهضة العربية. القاهرة 1994 .

د/ محمد سامي الشوا :الغش المعلوماتي كظاهرة إجرامية مستحدثة – بحث منشور في مؤتمر الجمعية المصرية للقانون الجنائي – القاهرة في 28/25 أكتوبر 1993 .

د/ محمد أحمد أمين الشوابكة: الجريمة المعلوماتية – دار الثقافة، عمان. طبعة 2004.

د/ محمد علي العريان: الجرائم المعلوماتية – دار الجامعة الجديدة للنشر. طبعة 2004 .

د/ نبيلة هبة هروال : الجوانب الإجرائية لجرائم الانترنت، دار الفكر الجامعي، ط1 – 2007.

د/ نهلة عبد القادر المومني : الجرائم المعلوماتية، ط1، دار الثقافة، عمان 2012 .

د/ هشام محمد فريد رستم : جرائم الحاسب المستحدثة – دار الكتب القانونية – مصر 1999

د/ هشام محمد فريدرستم : قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الكاتبة، 1995.

د/ هدى حامد قشقوش : جرائم الحاسب الالكتروني في التشريع المقارن، 1992، دار النهضة العربية، القاهرة.

د/ يوسف ابو فارة : الأعمال الالكترونية، جامعة القدس المفتوحة، رام الله 2012 .

د/ يونس عرب : إيجاز في المفهوم والنطاق والخصائص والصور والقواعد الإجرائية للملاحقة والإثبات، ورقة عمل مقدمة إلى مؤتمر الأمن العربي 2002 – تنظيم المركز العربي للدراسات والبحوث الجنائية – أبو ظبي 10-12 /2/ 2002.

ثانياً : المراجع الالكترونية:

بحث الجرائم الإلكترونية، بحث منشور على الإنترنت بتاريخ 2012/12/7، http://droit.moontada.com/t622-topic

في ظل غياب القوانين والتشريعات التي تحاسب المتورطين فيها، الجريمة الالكترونية في فلسطين مباحة" مقال منشور على الإنترنت، http://www.alqudsalraqmi.ps/atemplate.php?id=392

د/علي عدنان الفيل ، الجرائم الالكترونية، تم الاقتباس عن الموقع الالكتروني ستار تايمز، شؤون قانونية، 2011/2/1، http://www.startimes.com/?t=27016443

مديرية تكنولوجية المعلومات، قسم نظم المعلومة، شعبة أمنية المعلومات، http://www.ictmoi.com/elibrary/crime.pdf.

ظاهرة الإجرام الإلكتروني ومخاطرها ،أكاديمية شرطة دبي ، مركز البحوث والدراسات تاريخ الانعقاد: 26 نيسان 2003 تاريخ الانتهاء: 28 نيسان 2003 الدولة : دبي الإمارات العربية المتحدة.

(http://www.th3professional.com/2010/11/blog-post_5845.html

الفهرس

مقدمة:

البداية التاريخية لجرائم تقنية العلومات

الإنترنت والإجرام

إطار المواجهة التشريعية للجرائم الالكترونية

أهمية الدراسة

إشكالية الدراسة

منهج الدراسة

خطة الدراسة :

الفصل الأول : مفهوم الجريمة الإلكترونية وخصائصها

المبحث الأول : مفهوم الجريمة الالكترونية

أولا : المصطلحات المكونة لتعريف الجريمة الالكترونية :

ثانياً : تعريف الجريمة الإلكترونية

المبحث الثاني : خصائص الجريمة الإلكترونية

المبحث الثالث : مخاطر الجريمة الالكترونية

الفصل الثاني : المواجهة التشريعية للجرائم الالكترونية

المبحث الأول : المواجهة التشريعية لجرائم الاعتداء علي الشبكات وأنظمة وتقنيات المعلومات واستخداماتها غير المشروعة .

المطلب الأول : جرائم الاعتداء علي الشبكات وأنظمة وتقنيات المعلومات واستخدمها استخدام غير مشروع .

المطلب الثانى : الجرائم المرتكبة بواسطة أنظمة وتقنيات المعلومات .

المطلب الثالث : الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصةوالمحتوى المعلوماتى غير المشروع .

المبحث الثاني : الجرائم المرتكبة من مدير الموقع ومقدم الخدمة .

أولاً : إنشاء أو إدارة أو استخدام موقع لهدف غير مشروع .

ثانياً : جرائم مُقدم الخدمة .

المبحث الثالث :الجرائم الالكترونية المرتكبة بمعرفة الشخص الاعتباري .

أولاً : مسئولية الشخص المسئول عن الإدارة .

ثانياً : مسئولية الشخص الاعتباري .

الفصل الثالث : الأحكام الإجرائية للجريمة الالكترونية في القانون المصري .

المبحث الأول : خصوصيةالضبط والتحقيق في الجريمة الالكترونية

أولاً : خصوصية الضبط في مرحلة جمع الاستدلالات :

ثانياً : خصوصية التفتيش في الجريمة الالكترونية.

ثالثا : مرحلة التحقيق الإبتدائي.

رابعاً : مرحلة الأوامر القضائية المؤقتة .

المبحث الثاني : مسرح الجريمة الالكترونية والاستعانة بالخبرة الفنية وحجية الدليل الرقمي

المطلب الأول : مسرح الجريمة الالكترونية .

المطلب الثاني : إجراءات الاستعانة بالخبرة الفنية .

المطلب الثالث : حجية الأدلة الرقمية في الجرائم الالكترونية .

المبحث الثالث : إجراءات المنع من السفر وترقب الوصول والصلح والتصالح في الجرائم الالكترونية

المطلب الأول :إجراءات المنع من السفر وترقب الوصول .

المطلب الثاني : الصلح والتصالح في الجرائم الالكترونية .

خاتمة الدراسة:

نتائج الدراسة:

توصيات الدراسة

قائمة المراجع

الفهرس

==========

تم بحمد الله

ملخص البحث

في ظل التطور التكنولوجي برزت عدة ظواهر إجرامية حديثة تحت مسمي الجرائم الالكترونية ، ومنها جرائم إساءة استخدام الإنترنت ، أو استخدمه في أغراض إجرامية كانتهاك الخصوصية ، والقرصنة والانتفاع بدون حق بخدمات

الشبكات ، أو الدخول غير المشروع لموقع إلكتروني غير مصرح بالدخول عليه ، فالجريمة الإلكترونية من الجرائم المستجدة التي تنتج عن الممارسات السيئة لثورة تقنية التكنولوجيا المعلوماتية والتي تختلف كثيراً عن الجريمة التقليديـة في طبيعتـها ومضمونـها ووسائلها و أدواتها، وحتى في خصوصية مرتكبها.

ومع تزايد تطورات التكنولوجيا الحديثة تزايدات الإشكاليات القانونية التي تتعبق بهذه الجرائم ، ولذلك لاقت هذه الجرائم الاهتمام التشريعي والفقهي علي المستوي الدولي والداخلي ، للسعي نحو كفائة مواجهة هذه الجرائم عن طريقالعمل المستمر علي تحديث التشريعات الالكترونية من الناحية الموضوعية والإجرائية لمواكبة التطورات التكنولوجية ، وكذلك ضرورة إعادة النظر في النظم الإجرائية المتعلقة بالتحري والتحقيق في مجال الجريمة الالكترونية .

ويجب من جهة آخري العمل علي تفعيل التعاون الدولي علي المستوي التشريعي والقضائي والأمني في مجال مكافحة الجرائم الالكترونية ، إنشاء سلطات تحقيق متخصصة في الجرائم الالكترونية ، وكذلك نيابات ودوائر قضائية خاصة لنظر هذه الجرائم .

الكلمات المفتاحية : الجرائم , الالكترونية , مواجهة , تشريعية

Research Summary

In light of the technological development, several recent criminal phenomena have emerged under the name of electronic crimes, including the crimes of misusing the Internet, or using it for criminal purposes such as violating privacy, piracy and unrightful

use of network services, or illegal entry to an unauthorized website. The emerging that results from the bad practices of the information technology revolution, which differs greatly from the traditional crime in its nature, content, means and tools, and even in the privacy of the perpetrator.

With the increasing developments of modern technology, the legal problems associated with these crimes have increased, and therefore these crimes have received legislative and jurisprudential attention at the international and internal levels, to strive towards the efficiency of confronting these crimes through continuous work to update electronic legislation from an objective and procedural point of view to keep pace with technological developments, as well as the need to re-establish Examining the procedural systems related to investigation and investigation in the field of electronic crime.

On the other hand, it must work to activate international cooperation at the legislative, judicial and security levels in the field of combating cybercrime, establishing specialized investigation authorities in cybercrime, as well as special prosecutions and judicial departments to look into these crimes.

Keywords: crimes, electronic, confrontation, legislative

المواجهة التشريعية لجريمة الابتزاز الإلكتروني

Legislative confrontation of the crime of electronic extortion

م.د.صابرين يوسف عبد الله/ كلية القانون – جامعة البيان

sabreen.yoseif@albayan.edu.iq

sabreen.yousif.87@gmail.com

م.م.أوج عماد صبري/ كلية القانون – جامعة البيان

awj.emad@albayan.edu.iq

بغداد / العراق

الملخص:

يعد الابتزاز الإلكتروني من الجرائم الخطيرة التي تهدد حقوق الأفراد وحرياتهم، وتسبب لهم أضرار جسيمة من الناحيتين النفسية والمادية، وترتكب من خلال تهديد الضحية بنشر أسرارها في حال عدم الاستجابة لطلبات الجناة، سواء أكانت تلك الأسرار في شكل صور أو مقاطع فيديو أو تسجيلات صوتية أو محادثات، وتعد هذه الجريمة من الوسائل اليسيرة التي يعتمدها الجناة في الحصول على الكثير من الأموال، لاسيما وأنه لا توجد نصوص قانونية فعالة يمكن أن تحد منها.

وقد اتجهت الدول بعد تزايد خطر هذه الجرائم إلى مواجهتها، أما عن طريق إدخالها ضمن النصوص العقابية النافذة في الدولة، وإما بتشريع قوانين خاصة لمكافحتها ووضع عقوبات صارمة لها، ونأمل من المشرع العراقي أن يشرع قانون يكفل الحد من هذه الجرائم الخطيرة.

الكلمات المفتاحية: ابتزاز، تهديد، تسجيلات صوتية، أسرار شخصية، مواجهة، أضرار جسيمة.

Abstract:

Electronic extortion is a serious crime which threatens the rights and freedoms of individuals, and causes them severe psychological and financial damage, It is committed by threatening the victim to publish their secrets if the perpetrators' requests are not responded to, whether those secrets are in the form of photos, videos, audio recordings or conversations. This crime is one of the easy means that perpetrators use to obtain a lot of money, especially since there are no effective legal provisions which can limit it.

After the increasing danger of these crimes, states have tended to confront it, either by including it within the penal provisions in force in the state, or by legislating special laws to confront it and to determine strict penalties for it. We hope that the Iraqi legislator will legislate a law that ensure the confrontation of these serious crimes.

Keywords: extortion, threat, audio recordings, personal secrets, confrontation, severe damage.

مقدمة:

مع دخول الأجهزة الذكية واستخدام وسائل التواصل الاجتماعي بصورة دورية حتى لم يبقَ كل فرد من أفراد العائلة صغيراً كان أم كبيراً إلا ويتواصل مع ذويه وأصدقائه بواسطة تلك الوسائل، مما جعل العراق بل العالم اجمع مرتبط بشبكة واحدة تجمع البشرية في نفس الزمان على حدث واحد . ومع ان لهذا التطور ايجابيات فعلية لكنه في الوقت نفسه لم يخلو من السلبيات التي نجمت عن الاستخدام الغير صحيح لوظيفة الانترنيت ومواقع التواصل الاجتماعي. فأصبح بيئة مناسبة للعصابات الإجرامية التي تمتهن الابتزاز والتشهير، مستغلين سهولة القيام بأعمالهم عن طريق القيام بعمل حسابات وهمية على وسائل التواصل الاجتماعي، وبزيادة التطور في التكنولوجيا وبالأخص برامج الاختراق (Hacker Programs) عمد ضعاف النفوس، فضلاً عن العصابات الإجرامية المنظمة على اختراق الحسابات الشخصية للأفراد لجميع فئات المجتمع، وبالأخص الفتيات وسحب صورهن الشخصية والفديوهات العائلية ذات الخصوصية الكبرى، ومن ثم ابتزازهن مقابل غايات سواء مالية أو جنسية، فأصبحت هذه الجرائم ظاهرة خطرة دقت ناقوس الرهبة في دول العالم اجمع .

إن هذا التطور المذهل للكمبيوتر أدى إلى نشوء جرائم ناتجة عن ذلك الاستخدام، وهذه الجرائم أما أن تقع على الجهاز الإلكتروني كـ(الحاسوب أو الهاتف المحمول) ذاته، وإما أن تقع بواسطته، حيث يصبح أداة في يد الجاني يستخدمه لتحقيق أغراضه الإجرامية. والصورة الأخرى الأكثر شيوعاً حالياً والتي اعتاد على تسميتها بالجريمة الإلكترونية وهي الجريمة التي تتم باستخدام الجهاز الإلكتروني كـ(الحاسوب أو الهاتف المحمول) من خلال الاتصال بالانترنت ويكون هدفها اختراق الشبكات أو تخريبها أو التحريف أو التزوير أو السرقة والاختلاس أو قرصنة وسرقة حقوق الملكية الفكرية، حيث يشكل هذا السلوك الانحرافى جريمة بأركانها المادية والمعنوية ولا عبرة هنا بالباعث على ارتكاب هذه الجريمة.

بل عمد بعض المجرمون إلى طرق أسهل مما اعتادوا عليه في الماضي مثل سرقة بطاقات الائتمان أو البطاقات التعريفية للأشخاص واستعمالها في جرائمهم، فتوجهوا إلى الابتزاز الإلكتروني باستخدامهم لأسلوب تهديد الضحية بنشر ملفات شخصية عائدة له أما تكون محتوية على صوره الخاصة أو صور عائلته أو ملفات فيها قضايا لا يرغب الضحية أن تخرج أو تنشر للعلن، وهذا إما عن طريق

برامج القرصنة كما أوضحنا أو عن طريق ما يمكن نعته بجرائم الحب واللعب على المشاعر بإيهام الضحية بمشاعر تجاه المبتز فتنجذب إليه وتثق به فترسل له تلك الملفات الخاصة، وعندها ينتهي شروع جرمه ليبدأ بالتنفيذ من خلال التهديد والوعيد بفضح ونشر تلك الصور او الفيديوهات مقابل مادي يحدده المبتز وفترة زمنية للتنفيذ واستحصال مأربه الدنيئة. ولا ننسى بان ليس الأشخاص الطبيعية هم الفئات التي من الممكن أن تقع تحت طائلة هذه الجريمة بل هناك شركات عالمية ودول حتى قد وقعت في فخ جريمة الابتزاز الإلكتروني لفضح أسرارها العليا ومخططاتها الخاصة .

أهمية البحث :

إن أهمية هذا البحث في مراجعة النصوص القانونية التي تنص علي تجريم الاستخدام غير المشروع للأجهزة الإلكترونية وملحقاتها بشكل عام، وشبكات الانترنت بشكل خاص. وذلك من خلال تحليل هذه الجرائم المستجدة وتحديد العقوبات المترتبة عليها في التشريع العراقي والتشريعات المقارنة له.

ومما هو متصور أن تضيفه هذه النصوص من دعم في مجال مكافحة جرائم الابتزاز الإلكتروني وما ينتج عنها من جرائم مشابهة أو مستجدة، فالأمر بالتطور طالما التكنولوجيا نفسها في تطور، وهذا هو الوتر الذي يجيده المبتز الإلكتروني ليصنع من ثغرات التحديث للأنظمة أو الأجهزة وسبق معرفته دون عن الفئات الأخرى بهذا التطور منه آلية جديدة وحديثة لبدأ فعله الجرمي.

إن الأهمية من محور المؤتمر المقدم له بحثنا المتواضع هذا من وجهة نظر الباحثتان يكمن في خطورة هذه الجريمة حيث إن وقعت على فرد واحد من العائلة كأول خلية في مجتمعات الدول بل ولبنته الأساسية والمهمة، ستؤدي بالتالي أن تقع آثارها الوخيمة على باقي أفراد الأسرة، بل وحتى من الممكن أن تمتد تلك الآثار لفترات زمنية طويلة بحسب البيئة العرفية والعشائرية والدينية المتشكلة منها مفاهيم الأسر العربية، وما تمثله تلك الملفات التي تحمل أسرار تلك الأسر من خطوط حمراء من الكبائر المجتمعية أن تنشر أو تفضح . فلا بد أن يُنوه عن جريمة الابتزاز الإلكتروني ويُعرف بكونها جريمة ولها عقوبة خصص لها المشرع أقصى وسائل الردع، والهدف هو ليس فقط لتعلم الضحية بهذا بل كذلك ليرتد المبتز لكون من يَشرع في مثل هذه الجرائم شريحة لا باس بها من فئة المراهقين كذلك الذين لا يعلمون حق العلم بعواقب أفعالهم التي يرومون القيام بها .

إشكالية البحث:

انتشرت في الآونة الأخيرة ظاهرة خطيرة أخذت تتزايد وتعصف بحقوق الأفراد وحرياتهم، وترتب أضرارا بليغة لهم على المستويين النفسي والمادي، وتمارس على نطاق واسع وبالتحديد عبر مواقع التواصل الاجتماعي، دون أن تكون هنالك حلول قانونية كافية للحد منها أو التصدي لها، الأمر الذي زاد من تطاول الجناة وتماديهم في مهاجمة الضحايا، غير مكترثين لما يسببوه لهم من أضرار، خاصة وأنها وسيلة يسيرة لجني الكثير من الأموال والمنافع الأخرى، ويمكن أن نختصر الإشكالية بالأسئلة الآتية: ما هو مضمون الابتزاز الإلكتروني وكيف يرتكب؟ كيف يتعامل معه القضاء العراقي حاليا في ظل غياب نصوص قانونية صريحة تجرمه؟ كيف تصدت التشريعات المقارنة له، وهل كانت موفقة في تصديها له بتشريع خاص؟

منهجية البحث :

تعتمد منهجية بحثنا على الأسلوب النظري الاستقرائي والأسلوب التحليلي الوصفي للنصوص التشريعية التي عالجت موضوع الجريمة الإلكترونية سواء في التشريع العراقي أم التشريعات المقارنة له؛ لنستخلص جملة بعد هذا المزيج من الأسلوبين نختتم بها البحث ونضع بكل تواضع جملة من المقترحات التي نأمل أن تسعف المجتمع في التقليل من هذه الظاهرة أو تعمل على تقليله، وذلك سيقع كله ضمن مبحثين يبين الأول ماهية جريمة الابتزاز الإلكتروني، ويوضح الثاني النصوص القانونية المواجهة لهذه الجريمة سواء في قانون العقوبات أم القوانين الخاصة، وسنتطرق أولا إلى أركانها ثم نتعرف على عقوباتها في ضوء ما ورد في التشريعات المذكورة في أعلاه.

المبحث الأول

ماهية جريمة الابتزاز الإلكتروني

سيقسم هذا المبحث لبيان مفهوم الابتزاز الإلكتروني كمصطلح بشكل عام وباعتباره جريمة بشكل خاص، ثم سنوضح صور الابتزاز الإلكتروني التي تقع على الأشخاص، وذلك في المطلبين الآتيين:

المطلب الأول

مفهوم الابتزاز الإلكتروني

أولا: مفهوم الابتزاز :

بشكل عام يمكن القول بأنه التعريفات التي وضحت معنى **الابتزاز** اختلفت في الصياغة ولكنها تدور حول معنى واحد، فمنها من عرف الابتزاز بأنه "هو القيام بالتهديد بكشف معلومات معينة عن شخص، أو فعل شيء لتدمير الشخص المهدد، إن لم يقم الشخص المهدد بالاستجابة إلى بعض الطلبات هذه المعلومات تكون عادة محرجة أو ذات طبيعة مدمرة اجتماعي". وبعضهم من عرفه بأنه "كثرة المطالب غير المشروعة للوصول إلى الهدف الذي رسم له، وغالباً ما يكون هذا الهدف مدمر للحياة الاجتماعية، وقد يستخدم في أي لعبة قذرة للإيقاع بالضحية دون مخافة من الله، أو وازع ديني يجعله يحاسب نفسه قبل الوقوع في الخطأ".وقد أعطاه البعض الآخر تعريف وفقاً للغاية الأساسية منه، فعرفه بأنه "محاولة الحصول على مكاسب مادية أو معنوية، عن طريق الإكراه من شخص أو أشخاص أو حتى مؤسسات، ويكون ذلك الإكراه بالتهديد بفضح سر من الأسرار".[1]

ثانياً : مفهوم جريمة الابتزاز :

ومن الشائع في تعريف الابتزاز الإلكتروني –كونه يعد من الجرائم الإلكترونية– تعريف بعضهم بأن **جريمة الابتزاز الإلكتروني** هي تلك "المخالفات التي ترتكب ضد الأفراد، أو مجموعات من الأفراد بدافع الجريمة، وبقصد إيذاء سمعة الضحية أو أذى مادي أو عقلي للضحية مباشر أو غير مباشر باستخدام شبكات الاتصالات مثل الانترنت وغرف الدردشة، والبريد الإلكتروني، والموبايل". وتعرف بأنها "استغلال المبتز لمهاراته الإلكترونية، أو قربه الاجتماعي من الضحية، لغرض سرقة المعلومات السرية لتلك الضحية، فضلاً عن صورها ومستنداتها الشخصية أيا كان نوعها، وإجبارها على دفع الأموال، أو الإذعان لطلباته المخالفة للشرع والقانون".[2]

فيمكننا القول بأن جريمة الابتزاز الإلكتروني مجموعة من الأفعال المُجرمة والمُساومات التي يلجئ إليها المبتز بعملية أكراه تقع على الضحية بعد حصوله على معلومات والتهديد باستغلالها في أعمال مخالفة للقانون والحقوق الشخصية للضحية، بهدف الحصول على كسب مادي أو معنوي أو جنسي أو بهم كلهم. وعرف المرشد الفيدرالي الأمريكي منتهك الحاسوب بأنه "الشخص الذي يخترق حاسوباً محمياً

---

[1] ابتسام سالم بعيوي،جريمة الابتزاز الإلكتروني، بحث مقدم إلى مجلة ميسان للدراسات القانونية المقارنة، المجلد صفر، الإصدار 1، 2019، ص 119.

[2] بن ناصر،صالح بن سعد،2015،بناء نموذج لمهارات التحقيق الاستدلالي في جرائم الابتزاز الإلكتروني، أطروحة دكتوراه مقدمة إلى قسم الدراسات الأمنية، كلية العدالة الجنائية،جامعة نايف العربية للعلوم الأمنية،ص 86.

مشمولاً بالحماية القانونية دون أن يكون مصرحاً له بذلك"[3]، ومن التعريفات التي ركزت على إلمام الفاعل بتقنية المعلومات، تعريف (Thompson David)الذي عرف جريمة الحاسب الآلي بأنها "أية جريمة يكون متطلباً لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب".[4]

أما مشروع قانون الجرائم المعلوماتية العراقي الذي ننتظر ولادته الفعلية إلى الآن، فقد أشارت المادة السادسة منه بأن الجريمة الإلكترونية عبارة "استخدام شبكة المعلومات أو احد أجهزة الحاسوب أو ما في حكمها بقصد تهديد أو ابتزاز شخص أخر لحمله على القيام بفعل أو الامتناع عنه ولو كان هذا الفعل أو الامتناع مشروعاً".

وحسب الفقرة الثامنة من المادة الأولى من نظام مكافحة الجرائم الإلكترونية في المملكة العربية السعودية والتي تنص على أن المقصود بالجريمة الإلكترونية هي "أي فعل يرتكب متضمناً استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".

وبأتساع استخدام التقنية الإلكترونية وشبكات الانترنت برزت اصطلاحات جديدة تحاول التقارب مع هذه البيئة المجمعة للوسائط التقنية ولوسائط المعالجة وتبادل المعلومات، فابتداء من اصطلاح إساءة استخدام الحاسب مروراً باصطلاح احتيال الحاسب فالجريمة المعلوماتية فاصطلاحات جرائم الحاسب والجريمة المرتبطة بالحاسب وجرائم التقنية العالية وغيرها.

المطلب الثاني

أسباب جريمة الابتزاز الإلكتروني وصورها

أولا: أسباب جريمة الابتزاز الإلكتروني :

يمكن القول بأن هنالك أسباب مترسخة في أصل الطبيعة البشرية أما تعمل على دفع الضحية للانصياع للمبتز وتنفيذ طلباته، أو تلك التي تُفقد في ضمائر المبتزين فتدفعهم إلى ارتكاب جرائمهم ومنها

---

[3] ناصر بن محمد البقمي،فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية، الرياض، مكتبة الملك فهد الوطنية،2007، ص 44.

[4] عبدالفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006، ص 26.

ما يكون متمثل بتقنية الأجهزة الإلكترونية نفسها وبشبكة الانترنيت والمعاملات المالية الإلكترونية فيستغلها المبتز، وعلى النحو الآتي :

1. يعتبر الابتزاز جريمة مجتمعية أخلاقية في الأساس، ويوصف بكونه تعبير عن الانتهازية وانعدام للصفات السامية الفطيرة للإنسان.لا يمكن القول بأن الابتزاز يقل جرماً عن السرقة، حيث إن الفرق الوحيد بينها هو إن السرقة غالباً ما تتم باستخدام عامل التغافل أو القوة، ولكن الابتزاز يتم في اغلب الحالات بالتهديد والصريح منه بالعواقب الوخيمة التي من الممكن أن تقع مستقبلاً، ما لم ينصاع الضحية لمطالب المبتز. إذ وفر الانترنت مرتعاً خصباً لمن يريد أن يبتز، وتساعد المبتزين بأوجه عديدة وهي (توفر وسيلة اتصال آمنة بين المبتز والضحية وذلك طبعاً بسبب عامل انعدام الهوية، يمكن استخدام الانترنت كوسيلة لتحديد الهدف، وذلك لكون الانترنت ملئ بالمعلومات التي تساعد على ذلك).[5]
2. ضعف الوازع الديني لبعض أشخاص الابتزاز واللامبالاة في حدود الله التي رسمها لعباده وحذر من الاقتراب منها بالتالي يُسول لأنفسهم طريق الجريمة ومنها الابتزاز الإلكتروني، ومن أهم تلك الحدود هو عدم قذف المحصنات من النساء حيث يقول سبحانه في محكم كتابه المجيد "إِنَّ الَّذِينَ يُحِبُّونَ أَن تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالْآخِرَةِ وَاللَّهُ يَعْلَمُ وَأَنتُمْ لَا تَعْلَمُونَ".[6]
3. التفكك الأسري وتقصير الوالدين في القيام بواجباتهما تجاه الأبناء يعتبر عامل مهم في تفشي هذه الظاهر بالنسبة للمبتز والضحية، وخاصة الفتيات بمتابعة سلوكهن وعدم تأسيس فجوة اجتماعية بين الآباء والأبناء، لئلا تكون الفتاة فريسة سهلة للابتزاز.
4. كذلك تلعب البطالة دوراً أساسيا ترتبط بها جريمة الابتزاز،إذ إن الجرائم الإلكترونية شأنها شأن الجريمة التقليدية ترتبط بالبطالة والظروف الاقتصادية الصعبة .
5. يعد الانترنت وسيلة تهديد مرعبة للضحية بشكل واضح، فيكتفي المبتز أن يُهدد بنشر ملفات الضحية الخاصة أو العائلية بما تحتويه من (صور، فديوهات، محادثات خاصة، أسرار عائلية) على شبكة الانترنت ليدب الهلع في قلب الضحية، وذلك لان وضع شي على الانترنت يعني

---

[5] ابتسام سالم بعيوي، مرجع سابق، ص 124.

[6] سورة النور، الآية (19).

اطلاع الملايين من البشر عليه، وهو الأمر الذي يسبب ضرراً نفسياً وخوفاً يحمله على طاعة المبتز والامتثال لطلباته الغير مشروعة، وأكدت على العامل النفسي الذي يعتبر الأساس الذي يقيم له وزناً في هذه القضايا بالتحديد المحكمة البريطانية بكون "كانت التهديدات التي وجهت للضباط حقيقية ومحددة وعنيفة، ولم يكن هناك أي سجل يشير إلى أن التهديدات لا ينبغي أن تؤخذ على محمل الجد".[7]

6. يُمكن استخدام خدمات الشبكة لتحويل المبالغ المادية الناتجة عن الابتزاز مباشرة دون أن يعرف الضحية رقم حساب أو هوية المبتز.

ثانياً : صور جريمة الابتزاز الإلكتروني:

بتتبُع قضايا الابتزاز الإلكتروني عبر مواقع الجهات الأمنية المختصة بمكافحة هذا النوع من الجريمة في مختلف الدول، قد ظَهر بأن هنالك عدة طرق يتبعها المبتزون للوصول إلى غاياتهم الجرمية، والتي من صورها الصداقة القوية بين الفتيات عبر مواقع التواصل الاجتماعي، حيث من خلال هذه المواقع تقوم الفتاة بالتحدث لصديقتها عن جميع أسرارها الشخصية، وإرسالها صورها وفديوهاتها الخاصة أو العائلية كأخذ الرأي مثلاً بقصات الشعر وما إلى ذلك، مما يجعلها فريسة سهلة بالنسبة للمبتزة، إذ تستطيع الأخيرة بأن تجمع أدوات الجريمة بشكل كبير من الضحية نفسها لتشرع في عملية الابتزاز بعد فترة طويلة من الزمن .

وقد تحدث العديد من حالات الابتزاز الإلكتروني بتخفي شاب بشخصية فتاة عبر وسائل التواصل الاجتماعي، ثم تتطور العلاقة بين المبتز والضحية ليتم التواصل بينهم عبر التطبيقات الإلكترونية كـ(الماسنجر، الواتس اب،وغيرها الكثير) ليعمد الجاني بتسجيل وحفظ بعض الصور ومقاطع الفيديو التي يتم إرسالها من قبل الفتاة.[8]

---

[7] United States v. Vandevere.(2019) No. 1: 19-cr-63-MOC (W.D.N.C.), 16 September .seeIOANA VASIU , LUCIAN VASIU, CYBER EXTORTION AND THREATS: ANALYSIS OF THE UNITED STATES CASE LAW , Masaryk University Journal of Law and Technology , DOI 10.5817/MUJLT2020 , p 33.

[8] Navneet Kaur , introduction of cyber crime and its type, International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842, Issue 08, Volume 5 (August 2018) ,P 436

ومما استجد حالياً صورة للابتزاز الإلكتروني وهي ما يحدث من استغلال بعض المدعين بـ(محاربي الابتزاز الإلكتروني)، إذ يقوم المبتز هذا بالتواصل مع الضحايا واستدراجها من خلال تأسيس موقع الكتروني تحت عنوان محاربة الابتزاز، عندها يطلب من الضحايا البيانات الخاصة بهم وصورهم وهدفه بعد ذلك هو تهديدهم وابتزازهم لقاء مبالغ مالية .وهذا ما أكدته محكمة تحقيق الكرخ عبر موقع السلطة القضائية بتصديقها لاعترافات محارب الابتزاز الإلكتروني، بعد ابتزاز وتهديد فتيات عبر مواقع التواصل الاجتماعي، حيث تم اتخاذ الإجراءات بحقه وفقاً لأحكام المادة (456) من قانون العقوبات العراقي.[9]

يمكننا القول بأنه يمكن إجمال صور جريمة الابتزاز الإلكتروني بفئتين، وهي كالآتي:

الفئة الأولى: جرائم ابتزاز الكتروني تقع على الأفراد.

الفئة الثانية: جرائم ابتزاز الكتروني تقع على الأشخاص المعنوية (الدول، المنظمات، الشركات).

ومنها ما يمس الحالة المادية للشخص الضحية كالحسابات والملكية الفكرية له أو ما كان نتاج أفكاره وفنه المحمية قانوناً، ومنها ما يقع على الحالة المعنوية وتتمثل بكل ما يمس كرامة الإنسان وخصوصياته وحرماته العائلية وأسراره الشخصية. كل تلك الحقوق قد كفلتها دساتير دول العالم بأعلى حماية تشريعية بل وصنفت لها أحكام صارمة في قوانين سواء عامة أم خاصة، فيعاقب قانون العقوبات على جرائم التهديد بشكل عام، ليأتي قانون الجرائم المعلوماتية ليختص لنفسه بمثل هذه الجرائم وان دلَ الأمر فأنه يدل على وعي قانوني ومجتمعي لخطورة هذا الجرم الإلكتروني. الذي كما اشرنا سابقاً أثره ليس فقط مادي من خلال استحصال المبتز من الضحية على مقابل لتهديده وهو أما يكون أموال أو علاقات جنسية محرمة أو أفعال منحرفة، بل أثرا نفسياً يقع ويترسب في نفس الضحية؛ لنرى بعد أن يتم إيقاع التهديد أو تداركه أما بالرضوخ لرغبة المبتز وأما بالطريق الأكثر أمنا وهو التبليغ القضائي عن هذا التهديد والابتزاز، فتعمد الضحية إلى قتل نفسها أو أن تقتل من قبل احد ذويها وهذا ينطبق سواء كانت الضحية رجلاً أم أنثى وهو النتيجة الغير مباشرة لجرم المبتز الأكثر إيلاما للمجتمع.

[9] ينظر الموقع الإلكتروني (2022/7/24) https://www.hjc.iq/view.5056/

المبحث الثاني

النصوص القانونية المواجهة لجريمة الابتزاز الإلكتروني

سنتطرق في هذا المبحث إلى بيان النصوص القانونية التي تصدى بها المشرع لجريمة الابتزاز الإلكتروني، ونتعرف على أهم ما ورد فيها من عقوبات للوقوف على مدى فاعليتها في الزجر عنها، وللإحاطة بتلك النصوص ومعرفة أحكامها سنقسم هذا المبحث إلى ثلاثة مطالب: نبين في الأول منها أركان جريمة الابتزاز الإلكتروني، وفي الثاني نوضح النصوص القانونية التي عاقبت على الابتزاز وفقا لقانون العقوبات النافذ، وفي الثالث نبين النصوص الواردة في القوانين الخاصة بالنسبة للدول التي واجهتها بتشريع خاص.

المطلب الأول

أركان جريمة الابتزاز الإلكتروني

تتكون جريمة الابتزاز الإلكتروني وفقا للقواعد العامة في نطاق القانون الجنائي من ثلاثة أركان هي: الشرعي والمادي والمعنوي، ولا يتحقق للجريمة وجودها القانوني إلا بتوافر أركانها الثلاثة، وسنبين هذه الأركان على التوالي:

يراد بالركن الشرعي النصوص القانونية التي تنص على تجريم الابتزاز الإلكتروني تطبيقا لمبدأ "لا جريمة ولا عقوبة إلا بنص"، وبالنظر لما ينطوي عليه الابتزاز من خطورة على الفرد والمجتمع، وما يشكله من تعدي على المبادئ والقيم التي يجب أن تسود في المجتمع، تدخل المشرع وجرم الابتزاز حماية لتلك المصالح،[10]كالمشرع الكويتي والإماراتي والعماني الذي جرمه في قوانين خاصة مستقلة عن قوانين العقوبات النافذة، أما بالنسبة للتشريع العراقي فأنه لم ينص على تجريمه في قانون خاص واتجه القضاء العراقي إلى مواجهة خطر هذه الجريمة وفقا للنصوص الواردة في قانون العقوبات النافذ، وهو ما سنبينه في المطلب الثاني فنحيل إلى ذلك تجنبا للتكرار.

---

[10] د.ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجنى عليه من الابتزاز، المجلة العربية للدراسات الأمنية، المجلد 33، العدد (70)، الرياض، 2017، ص206-207.

أما الركن المادي فأنه السلوك الذي تظهر من خلاله الجريمة إلى العالم الخارجي، وبدونه تبقى مجرد أفكار في نطاق العقل ولا يحاسب عليها، وهذا السلوك يتحقق غالبا عندما يقوم الجاني بدخول المجال الافتراضي (الحاسوب، المواقع الإلكترونية، النظام ألمعلوماتي) الخاص بالضحية دون إذن منه والحصول منه على تسجيلات صوتية أو مرئية تتعلق بشؤون الخاصة بهدف استعمالها كوسيلة لتهديده وابتزازه للحصول منه على ما يرغب في انتزاعه من المجنى عليه سواء أكان مقابلا ماديا أم عملا مشروعا أو غير مشروع، ويتحقق التهديد بفعل يقوم به الجاني من شأنه أن يمس خصوصيات الضحية وحرياته، ويستوي أن يطال التهديد شخص الضحية أو احد أفراد عائلته أو من يهمه أمره، وهو قد يكون كتابة بإرسال رسائل إلكترونية عبر الهاتف أو مواقع التواصل الاجتماعي الأخرى بمضمون التهديد للضغط عليه وحمله على تنفيذ مطالبه أو شفاها بالتلميح أو الإشارة بشكل يجعله يفهم الغاية المقصودة من فعل الجاني، وسواء أكان التهديد بغرف الدردشة أم البريد أم تسجيلا صوتيا يتضمن التهديد صراحة أم ضمنا، ويتطلب لتحقق جريمة الابتزاز توافر شرطا مهما وهو أن يكون المبتز جادا في تهديده بحيث يترك أثرا في نفس الضحية بأنه سينفذ تهديده إذا لم يجيب طلباته، وفي هذا الشأن قضت محكمة جنايات واسط/ هـ1 بعقوبة السجن لمدة (21) سنة على متهم بثلاثة جرائم ارتكبها ضد ثلاثة مواطنين، إذ قام بابتزازهم من خلال تهديدهم بنشر أمور تخدش الشرف بعد أن اقتحم صفحاتهم الشخصية عبر مواقع التواصل الاجتماعي، وتم الحكم عليه وفقا للمادة (430) من قانون العقوبات بالسجن لمدة سبع سنوات عن كل قضية ابتزاز،[11] وقد يتحقق السلوك عندما يحصل المبتز بطريق الخداع على تسجيلات أو صور من الضحية نفسه مستغلا ثقته وغفلته ويهدده بها كما سنرى لاحقا في بعض القضايا الواقعية.

في حين يمثل الركن المعنوي العنصر النفسي في الجريمة، ويقوم على عنصري العلم والإرادة كون الابتزاز من الجرائم العمدية التي تتحقق بتوافر القصد الجنائي العام، وينصرف العلم إلى إدراك الجاني بأن ما يقوم به من أفعال من شأنها أن تثير الرعب لدى الضحية، وتجعله في حالة قلق نفسي في انتظار ما سينشأ عن فعل الجاني من أضرار مادية أو معنوية تلحق به أو أحد ممن له صلة به، بينما تنصرف الإرادة إلى تحقيق النتيجة الإجرامية التي يبغي الجاني الوصول إليها من وراء ابتزاز الضحية، وذلك بتخويفه لحمله على القيام بعمل أو الامتناع عنه، أي أن يتجه الجاني بإرادته إلى القيام بابتزاز

[11] د.أميل جبار عاشور، المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في مواقع التواصل الاجتماعي "دراسة مقارنة"، مجلة أبحاث ميسان، المجلد 16، العدد 31، 2020، ص122-123 و127.

الضحية على الرغم من إدراكه لماهية فعله، ولا يشترط لتحقق الابتزاز أن يقوم الضحية فعلا بالسلوك أو يمتنع عنه وإنما تتحقق بمجرد تهديده للضحية بذلك وتوافر العلم لديه، كون الابتزاز يعد من الجرائم الشكلية التي لا يتطلب أن تتحقق فيها النتيجة الإجرامية.[12]

المطلب الثاني

مواجهة جريمة الابتزاز وفق أحكام قانون العقوبات النافذ

أن المشرع العراقي لم ينص صراحة على تجريم الابتزاز الإلكتروني في قانون العقوبات النافذ، كما أنه لم يشرع قانون خاص يعاقب عليه كجريمة مستقلة عن الابتزاز التقليدي المنصوص عليه في المادة (452) من القانون المذكور[13]، وهو ما يعد نقصا تشريعيا كان ينبغي على المشرع أن يكمله لغرض الحد من هذا النوع من الأفعال الضارة، خاصة وأنه وضع مشروع قانون لمكافحة الجرائم المرتكبة عبر الوسائل الإلكترونية منذ العام 2011، ولم يصدر لغاية الآن وبالرجوع إلى نصوص تلك المواد نجد أنه عالج مشكلة الابتزاز الإلكتروني في المادة (6) المعنونة بـ(جرائم التهديد والابتزاز) التي نصت على: "يعاقب بالحبس مدة لا تقل عن ثلاث سنوات ولا تزيد على خمس سنوات وبغرامة لا تقل عن (5,000,000) خمسة ملايين دينار عراقي ولا تزيد على (10,000,000) عشرة ملايين دينار عراقي كل من استخدم شبكة المعلومات أو أحد أجهزة الحاسوب أو ما في حكمها بقصد تهديد أو ابتزاز شخص آخر لحمله على القيام بفعل أو الامتناع عنه ولو كان هذا الفعل أو الامتناع مشروعا".[14] ونأمل أن يبادر المشرع إلى إقرار هذا القانون لتوحيد الأحكام القضائية بخصوص هذه الجريمة وتجنب الاجتهادات.

وبالرجوع إلى الواقع العملي نجد أن هذه الجريمة ترتكب على نطاق واسع في المجتمع العراقي عبر مواقع التواصل الاجتماعي المختلفة، ففي بعض الإحصائيات البسيطة التي ذكرتها مديرية (مكافحة إجرام بغداد) بتاريخ (2020/1/22) عن الابتزاز الإلكتروني المرتكب ضد النساء، أشارت فيها إلى أن أعداد هذه الجريمة بلغت (16) ارتكبت من قبل (19) متهما عام (2018)، وارتفعت إلى (213) جريمة

---

[12] د.ممدوح رشيد مشرف الرشيد العنزي، مرجع سابق، ص212-213.

[13] تنص المادة (452) من قانون العقوبات رقم (111) لسنة 1969 المعدل على:"1- يعاقب بالسجن مدة لا تزيد على سبع سنين أو بالحبس من حمل آخر بطريق التهديد على تسليم نقود أو أشياء أخرى غير ما ذكر في المادة السابقة ...".

[14] مشروع قانون جرائم المعلوماتية العراقي لسنة 2011.

و(101) متهما في عام (2019)، وتزايدت أكثر في العام (2020)، إذ بلغت عدد الجرائم المرتكبة خلال أول شهرين فقط من هذا العام (30) جريمة و(11) متهما.[15]

في حين نجد هنالك تشريعات ساوت في قانون عقوباتها النافذ بين الابتزاز الإلكتروني والتقليدي ولم تفرق بينهما من حيث التجريم، كالقانون الفرنسي، إذ نصت أحكامه على تجريم أفعال الابتزاز أيا كانت الوسيلة المستعملة في ارتكابه إلكترونية أم تقليدية، ولكنه فرق بينهما من حيث الجزاء، إذ جعل للتهديد الذي يتضمن عنفا عقوبة أشد من التهديد الذي يكون مضمونه التشهير، وفي ذلك أشارت المادة (312/ 1) من القانون إلى عقوبة السجن لمدة سبع سنوات والغرامة بمبلغ (100000) يورو لما كان مصحوبا بعنف، والسجن لخمس سنوات وغرامة بمبلغ (750000) يورو لما يكون مصحوبا بتشهير دون عنف بحسب ما بينت المادة (312/ 10) من القانون ذاته، وقد شدد العقوبات إلى السجن الذي يتراوح بين (10–30) والغرامة التي تصل إلى (150) ألف يورو، وذلك بحسب توافر الظروف المشددة المنصوص عليها في المواد (312/ 3 – 7/312).[16]

أما عن موقف القضاء العراقي فأنه لم يبقَ صامتا تجاه هذا التنامي المتزايد لجريمة الابتزاز الإلكتروني، وإنما تصدى لها وفق النصوص الواردة في قانون العقوبات مكيفا لها بصور مختلفة وفق أحكام المواد (430–431–432–452–456) كلا بحسب واقعة ارتكابها، ففي أحدى الوقائع قام مجموعة أفراد متخصصين بتهكير مواقع التواصل الاجتماعي واستولوا على صور ونسخ من المحادثات الإلكترونية ومن ثم هددوا أصحابها بنشرها في حال عدم الدفع، وبعد القبض على هذه الشبكة الإجرامية واعترافهم صدّقت (محكمة تحقيق الكرخ المتخصصة بقضايا الإرهاب/ رئاسة محكمة استئناف بغداد الكرخ الاتحادية) أقوالهم، وأحالتهم إلى المحكمة المختصة وفقا لأحكام المادة (430) من قانون العقوبات، وفي قضية أخرى حكمت المحكمة على المتهمين وفقا للمادة المذكورة بالسجن لمدة سبع سنوات عن واقعة ابتزاز فتاة بعد استدراجها من قبل أحدهم بحجة الزواج وقيام الأخر بالتصوير ومن ثم تهديدها، وقد تم

---

[15] د.هديل سعد احمد العبادي، جريمة الابتزاز الإلكتروني للنساء، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد العاشر، العدد الثاني، 2020، ص541.

[16] تامر محمد صالح، الابتزاز الإلكتروني، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية– كلية الحقوق، عدد (1)، 2018، ص 649و655–656.

القبض عليهم عند تسلم المصوغات الذهبية من الفتاة، وفي قضية (محارب الابتزاز الإلكتروني) التي تمت الإشارة إليها سابقا اتخذت الإجراءات التحقيقية بحقه وفقا للمادة (456) من قانون العقوبات.[17]

وقضت محكمة جنايات واسط / هـ1 في واقعة قيام متهم بابتزاز فتيات وتهديدهن بنشر صور ومحادثات لهن عبر مواقع التواصل الاجتماعي إذا لم يدفعن المبالغ المطلوبة بالسجن لمدة ست سنوات وفقا لأحكام المادة (430) من قانون العقوبات النافذ،[18] وفي قضية أخرى حدثت لدى مكتب مكافحة الإجرام في الناصرية، إذ قدمت شكوى من فتاة عن شخص تعرفت عليه عبر تطبيق الانستغرام واستمر تبادل الرسائل والاتصالات والصور الشخصية لمدة سنتين بعدها انقطعت العلاقة، وبدأ يبتزها بتسليم مبالغ مالية في مقابل عدم نشر شي منها عبر مواقع التواصل أو إلى ذويها، وطلب مبلغ مليونين وبعد دفعها المبلغ بخمسة أشهر طلب أربع ملايين، وبعد تسليمه مبلغ ثلاثة ملايين، أتصل بها وطلب تسع ملايين وذلك قبل أسبوعين من تقديمها الشكوى، وقد أخبرته بتأمين مبلغ أربع ملايين فقط، وتم تشكيل فريق عمل للقبض عليه بالجرم المشهود عند تسلم المبلغ، ونجح فريق العمل في القبض عليه متلبسا، وعند التحقيق معه اعترف بجريمته وتم تصديق اعترافه قضائيا والأمر بتوقيفه وفقا للمادة (452) من قانون العقوبات.[19]

المطلب الثالث

مواجهة جريمة الابتزاز وفق أحكام القوانين الخاصة

بالرجوع إلى التشريعات المقارنة نجد أن البعض منها سعى إلى مواجهة هذا النوع من الجرائم في تشريعات عقابية مستقلة عن قوانينها العقابية النافذة، ولعل ذلك يرجع إلى تقدير تلك الدول لاختلاف طبيعة هذه الجرائم المرتكبة عبر التقنيات الحديثة عن الجرائم التقليدية، وعدم كفاية القواعد النافذة في القضاء عليها أو الحد منها، سواء أكان ذلك من ناحية التجريم بعدم إحاطتها بكل صور الجريمة المستحدثة أم من ناحية الجزاء وعدم كفايته للردع والزجر، ومن تلك التشريعات قانون رقم (63) لسنة

---

[17] رامي أحمد الغالبي، جريمة الابتزاز الإلكتروني وآلية مكافحتها في جمهورية العراق، دراسة قانونية مقدمة إلى دائرة العلاقات العامة في وزارة الداخلية العراقية، 2019، ص 22-23.

[18] د.أميل جبار عاشور، مرجع سابق، ص 127.

[19] سعاد شاكر بعيوي، جريمة الابتزاز الإلكتروني، مجلة ميسان للدراسات القانونية المقارنة، جامعة ميسان-كلية القانون، 132-133.

(2015) في شأن مكافحة جرائم تقنية المعلومات الكويتي، والمرسوم بقانون (5) لسنة (2012) بشأن مكافحة جرائم تقنية المعلومات الإماراتي، والمرسوم السلطاني رقم (12/ 2011) بإصدار قانون مكافحة جرائم تقنية المعلومات العماني.

ومن استقراء نصوص القانون الكويتي نجد أنه عدّ الابتزاز جنحة وعاقب عليها بالحبس المقيد الذي لا يتعدى الثلاث سنوات والغرامة المقيدة بين (3.000–10.000) آلاف دينار، أو إحداهما، أما من حيث التجريم فنجد أنه قد وسع من نطاقه، إذ نص على تجريم الابتزاز أو التهديد سواء تم ضد شخص طبيعي أم اعتباري، وسواء تم باستعمال شبكة المعلوماتية أو أي وسيلة من وسائل التقنية، وسواء أكان الغرض منه قياما بعمل أو امتناعا عنه، وقد شدد العقوبة إلى الحبس المقيد الذي لا يتعدى الخمس سنوات والغرامة المقيدة بين (5000–20,000) ألف دينار أو إحداهما، إذا موضوع التهديد ارتكاب جريمة من نوع الجنايات أو كان أمرا يمس الكرامة أو يخدش الشرف والاعتبار أو السمعة.[20]

أما عن المشرع الإماراتي فقد جاء بعبارات مقارنة لما نص عليه المشرع الكويتي من ناحية التجريم، أما من حيث العقاب فنجد أن المشرع الإماراتي كان أقل شدة في تحديد عقوبة الجريمة وأكثر شدة في تحديدها عند توافر الظروف المشددة التي جاءت مماثلة لما أخذ به المشرع الكويتي، إذ يلاحظ بأن عقوبة الجريمة غير المقترنة بالظرف المشدد كانت الحبس المقيد الذي لا يتعدى السنتين والغرامة المقيدة بين (250–500) ألف دينار أو إحداهما، في الوقت الذي حددها المشرع الكويتي بما لا يتعدى الثلاث سنوات، أما العقوبة المقترنة بالظرف المشدد فقد رفعها المشرع الإماراتي إلى السجن الذي لا يتجاوز (10) سنوات، وهي عقوبة واحدة وجوبيه بينما الكويتي جعلها اختيارية بين الحبس لا يتعدى الخمس سنوات والغرامة أو إحداهما.[21]

ويلاحظ أن القانون العماني قد جاء بنصوص مشابهة للقانونيين السابقين من حيث التجريم، ولكنه اختلف عنهما بإضافة عبارة "ولو كان هذا الفعل أو الامتناع عنه مشروعا" في الوقت الذي خلت منها تلك القوانين، أما من حيث العقاب فنجده أكثر شدة من كلا القانونين السابقين، لأنه وضع حد أدنى ينبغي أن لا تقل العقوبة عنه، إذ حددها بالسجن الذي لا يقل عن شهر واحد ولا يتجاوز ثلاث سنوات، والغرامة المقيدة بين (1000–3000) ريال عماني أو إحداهما، كذلك الحال عند تشديد العقوبة، إذ

---

[20] المادة (3/ 4) قانون رقم (63) لسنة (2015) في شأن مكافحة جرائم تقنية المعلومات الكويتي.

[21] المادة (16) والمرسوم بقانون (5) لسنة (2012) بشأن مكافحة جرائم تقنية المعلومات الإماراتي.

حددها بالسجن المؤقت الذي لا يقل عن الثلاث سنوات ولا يتجاوز العشر سنوات، والغرامة التي لا تقل عن (3000-10,000) آلاف ريال عماني.[22]

ومن استقراء ومقارنة النصوص المذكورة في أعلاه نجد أن غالبية الدول تتقارب في تقديرها لخطورة تلك الجريمة، إذ لم تحدد لها عقوبة أكثر من الثلاث سنوات ويستثنى من ذلك الظروف المشددة التي تقترن بها، إذ أن البعض من التشريعات تشددت معها إلى الحد الذي جعلها بمصاف الجنايات الخطيرة، ولعل ذلك يرجع إلى الأضرار الكبيرة التي يمكن أن تنشأ عنها والتي قد لا يمكن تعويضها بسهولة، فضلا عن رغبتها في وضع حد للحيلولة دون انتشارها ولاسيما في ظل اتساع نطاق استعمال مواقع التواصل الاجتماعي (مسرح ارتكاب الجريمة)، ليس على المستوى الشخصي وحسب وإنما على المستوى العلمي والعملي أيضا، فغالبية مؤسسات العمل والجامعات والمدارس باتت تعتمد تلك المواقع بشكل كبير، وتعدها جزء لا يتجزأ من نطاق عملها، كما يلاحظ على تلك التشريعات أنها تتقارب في تحديد صور التجريم إلى حد كبير، إذ حددت كل منهما الجريمة بالعبارات ذاتها وبالكيفية ذاتها، ولعل ذلك يرجع إلى الطبيعة التقنية لها، إذ إن مسرح ارتكابها وموضوعها وأدواتها هي نفسها أيا كانت الدولة المرتكبة فيها، وهذا التوافق في تحديد الجريمة من شأنه أن يصب في صالح الجميع، بالنظر لكونها جريمة عابرة للحدود يمكن أن ترتكب في دولة ويظهر أثرها في دولة أخرى، وبما أن الفعل معاقب عليه في كلا الدولتين وبالكيفية ذاتها، فأن من شأن ذلك أن يجعل المتهم خاضعا للعقاب في دولته نفسها، وهو ما يشكل وسيلة من شأنها أن تساهم في الحد من انتشارها، ونختم كلامنا بالقول أن التشريعات المقارنة كانت موفقة بالفعل في مجابهة تلك الجريمة بنصوص خاصة وعدم معالجتها بالقانون النافذ، ولاسيما أنها وضعت عقوبات تتناسب وخطورة الجريمة وراعت وجود ظروف مشددة لها، ونأمل أن يحذو مشرعنا العراقي حذوها في التجريم والعقاب.

[22] المادة (18) المرسوم السلطاني رقم (12/ 2011) بإصدار قانون مكافحة جرائم تقنية المعلومات العماني.

الخاتمة

وبعد أن انهينا بحث موضوع (المواجهة التشريعية لجريمة الابتزاز الإلكتروني) وتعرفنا على ماهيته وأوضحنا أسبابه وصوره، واستقرينا النصوص القانونية التي تصدت له على مستوى القوانين الخاصة والقوانين العقابية النافذة في كل من العراق وفرنسا والكويت والإمارات وسلطنة عمان، توصلنا إلى النتائج والمقترحات الآتية:

أولا- النتائج:

1. قد ظهرت أنماط جديدة من الجرائم لم تكن معهودة من قبل في العالم، وأصبحت تقنية الحاسوب بشكل عام وشبكة الانترنت على وجه الخصوص محل ارتكاب الجريمة وظهور محترف في نطاق الجريمة، فبرز ما ينعت بـ(بجرائم الابتزاز الإلكتروني) القائمة على الاستخدام الغير مشروع للأجهزة الإلكترونية او الشبكات الإلكترونية أو الإخلال بالأمن ألمعلوماتي بشكل عام مما شكلت خطراً هدد العالم اجمع.
2. اختلفت الاصطلاحات المستخدمة للدلالة على الظاهرة الإجرامية الناشئة في بيئة الحاسوب وفيها بعد بيئة الشبكات والبيئة الرقمية بشكل عام، ويعتبر هذا الاختلاف مرافقاً للمسيرة ونشأة وتطور ظاهرة الإجرام المرتبط أو المتصل بتقنية المعلومات الإلكترونية، لذلك فانه أمام هذا الواقع التقني، ظهرت مصطلحات عديدة دالة على أفعال الجريمة المتصلة بالتقنية الإلكترونية.
3. يمكن القول بأن الجرائم الإلكترونية هي تلك الجريمة التي تؤدي فيها بطريقة مباشرة أو غير مباشرة تقنية الحاسب دورا أساسيا في ابتزاز الضحية .
4. امن الشبكات هو الموضوع الشاسع الذي أصبح أكثر أهمية لان العالم أمسى مترابط للغاية، وقد ناقش هذا البحث النوع الأكثر ضراوة على المجتمع ألا وهو جريمة الابتزاز الإلكتروني. فهناك حاجة ملحة لإجراء تحليل بحثي للجرائم الإلكترونية لحماية البيانات الحساسة وعلى وجه الخصوص جرائم الابتزاز الإلكترونية. لذلك لابد من تكثيف التقنيات القانونية المحلية منها والدولية لمكافحة هذه الآفة على حد سواء، كون تلك الجرائم تعتبر من ضمن الجرائم العابرة للحدود.
5. بدأت غالبية الدول في التصدي لهذا النوع من الجرائم من خلال وضع تشريعات خاصة تكفل الحد منها، وقد تضمنت تلك القوانين عقوبات سالبة للحرية وغرامات مالية كبيرة تكفل تحقيق

الردع العام والخاص الهدف الأساس للعقوبة، في حين اتجهت دول أخرى إلى غير ما حذته التشريعات السابقة، إذ طبقت نصوص قوانين العقوبات النافذة لديها على جريمة الابتزاز الإلكتروني أسوة بالابتزاز التقليدي كما هو الحال في القانون الفرنسي، أما بالنسبة للوضع في العراق فأنه لغاية الآن لم يشرع قانون خاص لمواجهة الابتزاز الإلكتروني، ويتم التصدي لهذه الجريمة من خلال تطبيق نصوص قانون العقوبات النافذ وبالتحديد نصوص جريمة التهديد (430-432) والابتزاز التقليدي (452) والاحتيال (456) من قانون العقوبات النافذ.

ثانيا-المقترحات:

1-تشريع قانون خاص بالجرائم المعلوماتية يتضمن تجريما لكل الاعتداءات الإلكترونية التي ترتكب عبر مواقع التواصل الاجتماعي، وخاصة الابتزاز الإلكتروني الذي انتشر على نطاق واسع في المجتمع العراقي، وأن يتضمن عقوبات سالبة للحرية وغرامات رادعة تحقق الهدف المنشود من هذا التشريع.

2-إقامة ندوات تثقيفية واسعة النطاق لغرض توعية أفراد المجتمع -خاصة الشباب والفتيات- عن مخاطر الابتزاز، وتوضيح طرق الوقاية الواجب عليهم إتباعها عند استعمال مواقع التواصل الاجتماعي أو الهواتف النقالة أو الحواسيب لتجنب الوقوع في شباك المبتزين، وبيان السبل والوسائل التي ينبغي عليهم إتباعها في حال تعرضهم للابتزاز الإلكتروني.

3-إقامة دورات تدريبية للجهات الأمنية والقضائية حول كيفية التعامل مع هذا النوع من الجرائم، وضرورة تفعيل التعاون الأمني والقضائي على المستويين الدولي والإقليمي؛ لزيادة فاعلية المواجهة التشريعية للجريمة المذكورة خاصة وإنها من الجرائم القارية التي لا تتوقف عند حدود دولة معينة.

المصادر

القرآن الكريم

أولا–المصادر العربية

أ–الكتب

1. عبدالفتاح بيومي حجازي، مكافحة جرائم الكومبيوتر والانترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2006.
2. ناصر بن محمد البقمي، فاعلية التشريعات العقابية في مكافحة الجرائم المعلوماتية، الرياض، مكتبة الملك فهد الوطنية، 2007.

ب–الأطروحات

1. بن ناصر،صالح بن سعد، بناء نموذج لمهارات التحقيق الاستدلالي في جرائم الابتزاز الإلكتروني، أطروحة دكتوراه مقدمة إلى قسم الدراسات الأمنية، كلية العدالة الجنائية،جامعة نايف العربية للعلوم الأمنية، 2015.

ج–البحوث والدراسات

1. ابتسام سالم بعيوي، جريمة الابتزاز الإلكتروني، مجلة ميسان للدراسات القانونية المقارنة، المجلد صفر، الإصدار 1، 2019.
2. د.أميل جبار عاشور، المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في مواقع التواصل الاجتماعي "دراسة مقارنة"، مجلة أبحاث ميسان، المجلد 16، العدد 31، 2020.
3. تامر محمد صالح، الابتزاز الإلكتروني، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية– كلية الحقوق، عدد (1)، 2018.
4. رامي أحمد الغالبي، جريمة الابتزاز الإلكتروني وآلية مكافحتها في جمهورية العراق، دراسة قانونية مقدمة إلى دائرة العلاقات العامة في وزارة الداخلية العراقية، 2019.
5. سعاد شاكر بعيوي، جريمة الابتزاز الإلكتروني، مجلة ميسان للدراسات القانونية المقارنة، جامعة ميسان–كلية القانون
6. د.ممدوح رشيد مشرف الرشيد العنزي، الحماية الجنائية للمجنى عليه من الابتزاز، المجلة العربية للدراسات الأمنية، المجلد 33، العدد (70)، الرياض، 2017.

7. د.هديل سعد احمد العبادي، جريمة الابتزاز الإلكتروني للنساء، مجلة جامعة الانبار للعلوم القانونية والسياسية، المجلد العاشر، العدد الثاني، 2020.

د-القوانين

1. قانون العقوبات رقم (111) لسنة 1969 المعدل
2. مشروع قانون جرائم المعلوماتية العراقي لسنة 2011.
3. المرسوم السلطاني رقم (12/ 2011) بإصدار قانون مكافحة جرائم تقنية المعلومات العماني.
4. المرسوم بقانون (5) لسنة (2012) بشأن مكافحة جرائم تقنية المعلومات الإماراتي.
5. قانون رقم (63) لسنة (2015) في شأن مكافحة جرائم تقنية المعلومات الكويتي.

ثانيا –المصادر الأجنبية:

1. IOANA VASIU , LUCIAN VASIU, CYBER EXTORTION AND THREATS: ANALYSIS OF THE UNITED STATES CASE LAW , Masaryk University Journal of Law and Technology , DOI 10.5817/MUJLT2020 , p 33
2. Navneet Kaur ,introduction of cyber crime and its type, International Research Journal of Computer Science (IRJCS) ISSN: 2393-9842, Issue 08, Volume 5 (August 2018).

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة الجزائر 1 بن يوسف بن خدة
كلية الحقوق
الملتقى الدولي الافتراضي الموسوم بـ:" القانون الجنائي التطور التكنولوجي _ إشكالات ومعالجات _"

مداخلة بعنوان: المواجهة التشريعية لجرائم العملات الرقمية والمشفرة في نظر السياسة الجنائية

الدكتور: **لبيض بوبكر** جامعة عمار ثليجي الأغواط Labiedbobaker@hotmail.com

الدكتور: **بداوي كريم** جامعة عمار ثليجي الأغواط karimboudoui26@gmail.com

ملخص:

تعتبر ظاهرة العملات الرقمية المشفرة ناتجا من نواتج الثورة التكنولوجية الحديثة، حيث فرضت على مختلف المؤسسات البنكية وغير البنكية واقعا مختلفا تماما قد يخفف من أعباء السوق النقدية الحالية، لكنها في المقابل لا تخلو من مخاطر متعددة وذلك كاستخدام هاته العملات في جرائم غسل الأموال وتمويل الإرهاب، وسهولة التحايل على المنظومة النقدية الرسمية والتحايل على القوانين الجنائية.

ومع تزايد الإقبال على هاته العملات الرقمية كانت تساؤلات الدراسة تثور حول مدى إمكانية أن نجعل من العملات المشفرة مصلحة يحميها القانون الجنائي، أم أن المخاطر التي تحيط بها تحول دون النظر إليها كذلك؟

وقد اعتمدنا المنهج الوصفي التحليلي لكونه يناسب موضوع الدراسة، حيث وجدنا أن هاته العملات تحتوي على مخاطر ومفاسد عظيمة تفرض على القانون الجنائي مواجهتها بتجريمها ومعاقبة من يتعامل بها إلى حين وضوح هاته العملات والوصول إلى استقرار دولي يعترف بها ويضعها في إطارها التنظيمي والقانوني.

الكلمات المفتاحية: العملات الرقمية، جرائم، الثورة التكنولوجية، القانون الجنائي.

Summary:

The phenomenon of cryptocurrency is the result of the products of the modern technological revolution, as it was imposed on various banking and non -banking institutions a completely different reality that may reduce the burdens of the current monetary market, but in return it is not without multiple risks, such as using these currencies in money laundering crimes and terrorist financing, Easy to circumvent the official monetary system and circumvent criminal laws.

With the increasing demand for these digital currencies, the study questions arise about the extent of the possibility to make the encrypted currencies an interest protected by the criminal law, or whether the risks surrounded by it preventing them from looking at them as well?

We have adopted the descriptive analytical approach because it fits the subject of the study, as we found that these currencies contain great risks and spoilers that impose on the criminal law to confront them by criminalizing them and punishing those who deal with them until the clarity of these currencies and reaching international stability that is recognized and placed in its organizational and legal framework.

Key words: digital currencies, crimes, technological revolution, criminal law.

مقدمة:

تشهد المجتمعات المعاصرة حاليا الثورة الصناعية الرابعة، والتي ستؤدي إحداث التحول في مختلف المجالات ومن بينها مجال الاقتصاد العالمي، وقد أدى نشوء الأنترنت وتطور تقنيات الاتصالات إلى بدء عصر الاقتصاد الرقمي.

والاقتصاد الرقمي هو عبارة عن سلسلة من الأنشطة الاقتصادية والاجتماعية والثقافية والتي يتم أداؤها على شبكات المعلومات وترتبط أساسا باستخدام المعلومات وتقنيات الاتصال، وتتضمن أنشطة متنوعة وهامة مثل أعمل البنوك والبيع والشراء والاستفادة من التعلم عن طريق استخدام الأنترنت والأجهزة المتصلة فيما بينها.

ومن شأن الاقتصاد الرقمي أن يؤدي إلى إنشاء نماذج للتمويل والمعاملات المالية، وصناعة سبل جديدة بديلة لتداول رأس المال، وهذا ما لا يلبيه النظام الحالي للبنوك الأمر الذي جعل الطلب يتزايد يوما بعد يوم على سوق للتجارة الرقمية.

وهنا تبدو الحاجة واضحة لضرورة إنشاء وصناعة وسيلة سهلة وملائمة للمعاملات فائقة السرعة عن طريق النت تخدم ما يسمى اليوم بالعقود الذكية والتبادل السريع للسلع والنقود، وهو ما قد يخرج على حدود الولاية القانونية للدول، وهذا الدور هو الذي تشغله اليوم ما يسمى بالعملات الرقمية أو الافتراضية المشفرة.

وترجع أهمية الدراسة في كونها تعالج ظاهرة مهمة وخطيرة يجب على التشريع الجنائي أن يتصدى لها بكل الآليات والسبل القانونية المتاحة، ذلك أن العالم بأسره منساق نحو التحول الرقمي في شتى المجالات الاقتصادية والاجتماعية، وهو أمر وإن كان يحمل إيجابيات سلسة وسهلة على الناس في تعاملاتها المالية إلا أنه أيضا ينطوي على مخاطر تهدد مصالح وأمن الدولة واقتصادها ومستقبلها القريب والبعيد.

وترجع خطورة العملات الرقمية المشفرة إلى إمكانية استخدامها لإخفاء أو تمويه المصدر غير المشروع للمال أو الوجهة النهائية للمال، وهنا يمكن أن نقول بأن غسل الأموال وتمويل الإرهاب والاحتيال والابتزاز وجرائم الكمبيوتر وغيرها من الجرائم، يمكن أن ترتكب كلها باستعمال العملات الرقمية المشفرة.

وهنا يثور تساؤل الدراسة الأول والمهم ألا وهو: هل تصلح العملات الرقمية المشفرة أن تكون مصلحة يحميها القانون الجنائي، أم أن المخاطر التي تحيط بها والمفاسد التي تجلبها تحول دون النظر إليها كذلك؟

وقد استدعى البحث منا استدام المنهج الوصفي التحليلي لكونه يناسب هذا النوع من الدراسات القانونية التي تعمل على وصف الظاهرة أولا، ثم تحليل ما تظهره وتبينه من نتائج للوصول بعد ذلك إلى أحكام قانونية تساعدنا في الإجابة على إشكال البحث وتساؤله.

وعلى هذا الأساس فقد جاءت الدراسة مقسمة إلى مبحثين اثنين: درسنا في المبحث الأول حقيقة العملات الرقمية المشفرة وعلاقتها بالأعمال والأنشطة الإجرامية، ثم جاء المبحث الثاني تطبيقيا حيث درسنا فيه تجريم التعامل والتداول بالعملات الرقمية المشفرة عرضنا فيه بشكل بسيط إلى موقف الدول من هاته العملات ثم إلى النصوص التشريعية المجرمة لتداول العملات ثم بين أركان جريمة التعامل بالعملات الرقمية المشفرة.

المبحث الأول: ماهية العملات الرقمية المشفرة وعلاقتها بالأنشطة الإجرامية

لقد اتجهت غالبية الدول والهيئات لرقمنة جميع مؤسساتها ونظمها المالية مواكبة منها لعمليات التطور التكنولوجي[1]، حيث تسارع كل الدول إلى مواكبة التحول الرقمي الذي يحدث في كل قطاعات ومؤسسات الدولة، ومن ثم ظهرت الحاجة لاستحداث أدوات جديدة تحمل صفة الرقمية وتعمل على تسهيل معاملات الناس داخل هذا العالم الذي أصبح صغيرا جدا انطلاقا من العولمة الحديثة، ومن هنا كانت العملات الرقمية المشفرة والبلوكتشين أحد أحدث أدوات التعامل المالي على شبكة الأنترنت والتي تضم الكثير من التعاملات المالية المتنوعة.

ولكي نستبين حقيقة العملات الرقمية المشفرة وعلاقتها بالأنشطة والأعمال الإجرامية، لا بد لنا أن نبحث في تعريفها الاصطلاحي وكيفية نشأتها وأهم الخصائص التي تتميز بها هاته العملات لندرس بعد ذلك العلاقة المتواجدة بين العملات المشفرة والأعمال الإجرامية، وهو ما سوف نبحثه من خلال المطالب التالية:

المطلب الأول: نشأة وتطور العملات الرقمية المشفرة

يمكن القول بأن العملات الافتراضية قد ظهرت على يد عالم الرياضيات الأمريكي دافيد شوم (David Chaum) عام 1978، حيث إنه اخترع ما يسمى ديجي كاش Digi Cash وهي عبارة عن نقود إلكترونية مشفرة ، الأمر الذي لفت الأنظار إلى إمكانية وجود عملات مشفرة وغير مركزية ولا يمكن تعقبها بحال من الأحوال[2].

وقد بدأ ظهور العملات الرقمية ونشأتها تزمنا مع أزمة الرهن العقاري سنة 2008م، والتي أطلق عليها بالأزمة المالية العالمية. وهنا رأى مصمم العملات الرقمية المشفرة وجود جدوى كبيرة من إنشاء عملة رقمية مشفرة غير مركزية ولا تتبع أي جهة حكومية تعمل على انتشال الاقتصاد العالمي من حالة الكساد التي دخل فيها[3].

---

[1] – أيمن صالح، واقع العملات الرقمية، صندوق النقد العربي، الإمارات العربية المتحدة، 2021م، ص 5.

[2] – خالد محمد نور عبد الحميد الطباخ، العملات الافتراضية ودور في تمويل الإرهاب وغسل الأموال، دار النهضة، مصر، ط2، 2022م، ص 56

[3] – عبد اللطيف حاجي صادق، أثر سد الذرائع في التعامل بالعملات الافتراضية البتكوين نموذجا، مجلة الشريعة والدراسات الإسلامية، جامعة الكويت، عدد 16، 2019م، ص 479.

وقد طرح مبرمج سمى نفسه ساتوشي ناكاموتو (Satoshi Nakamoto) فكرة العملة الرقمية المسماة بيتكوين ((Bitcoin حيث قام في عام 2008 بنشر بحث بعوان: البيتكوين: نظام عملة الند للند الإلكترونية، وهنا كانت فكرة استخدام نقود الكترونية بوصفها نظام نقدي الكتروني، يعتمد في تعاملاته المالية المباشرة على عدم وجود وسيط [1]

وفي عام 2009 قام ساتوشي ناكاموتو بإنتاج أول عملة بيتكوين بطريقة التعدين وتمت أول عملية تحويل عملات بيتكوين من الند للند بين ساتوشي وبين هال فيني المبرج الفعلي لنظام البيتكوين، وتم بالفعل نشر أول سعر تداول بين هذه العملة والدولار حيث كان 1 بيتكوين يبلغ 0.001 دولار، وتم إنشاء بعد ذلك منصة لتبادل البطاقات التجارية وسوق الكتروني لصرف البيتكوين، ومن هذه المنصة انطلقت عمليات التبادل وتحويل وتخزين الأموال وتبادل العملات[2].

ومنذ عام 2014 قامت شركات كبرى بقبول التعامل بعملة البتكوين ومنها شركة (أوفرستوك) لتصبح أكبر شركة تقبل البيتكوين لبيع التجزئة، بالإضافة إلى شركة (تايجر دايركت) العملاقة والمتخصصة في بيع أجهزة الحاسوب والتي اعتمدت عملة البيتكوين في مداولاتها، كما أصبحت جامعة نيقوسيا في قبرص وجامعة كمبيريا في إنجلترا تقبل دفع الرسوم الدراسية بالبيتكوين[3].

وقد تعدد أشكال وأنواع العملات الرقمية المشفرة، فبعد ظهور البيتكوين كعملة رقمية ظهرت عملات رقمية أخرى مثل عملة الإيثريوم (Etherum) وعملة داش (Dash) والبعض يسميها بعملة النقد المظلم أو عملة أكس لكونها مجهولة المصدر، وعملة الريبل (Ripple) وغيرها من أنواع العملات الرقمية المشفرة

المطلب الثاني: تعريف العملات الرقمية المشفرة

تعد العملة الرقمية المظلة الرئيسية التي تضم جميع أشكال العملات الأخرى سواء تلك العملات الالكترونية أو الافتراضية أو المشفرة، وبغض النظر عن المصطلحات والمسميات التي أطلقت عليها فإن السمة الرئيسية لهاته العملات تتمثل في كونها متاحة بشكل رقمي وليس لها وجود

---

[1] – خالد محمد نور، العملات الافتراضية، مرجع سابق، ص 57.

[2] – أحمد هشام قاسم النجار، العملات الافتراضية المشفرة دراسة اقتصادية شرعية محاسبية، دار النفائس للنشر والتوزيع، الأردن، 2019م، ص 20–21.

[3] – خالد محمد نور، العملات الافتراضية، المرجع نفسه، ص 58.

مادي ملموس[1]، وبما أن هذا المصطلح مركب من عدة مصطلحات العملة والرقمية ومصطلح التشفير فإننا سنعرف كل مصطلح على حده ثم نعرفه تعريفا مركبا على النحو التالي:

أولا: تعريف العملة

العملة في اللغة مشتقة من العمل، والعمل بمعنى الفعل والمهنة، والعملة – بكسر العين وضمها– هي ما يُعطى أجرة على العمل والإجارة[2]، وأما العملة في الاصطلاح فهي تطلق على النقد المضروب من معدن أو ورق[3].

ثانيا: العملات الرقمية

تعد العملة الرقمية النموذج الإلكتروني للعملة الورقية والمعدنية التي يمكن تخزينها في محفظة رقمية، ويمكن تحويل العملة الرقمية إلى نقد في متناول اليد عن طريق سحب النقود من أي جهاز صراف آلي أو بنك [4]، وهذا يعني أنها نقود غير ملموسة لذلك يطلق عليها البعض بالعملات الافتراضية.

ثالثا: التشفير

يطلق على التشفير معنى التعمية وهو تحويل نص واضح ومقروء إلى نص غير مفهوم باستخدام طرق التشفير التي قد تكون غير سرية لكن يستخدم مفتاحا سريا يمكن من يمتلكه من أن يعيد النص المشفر إلى النص الواضح[5].

---

[1] – العملات المشفرة، البنك المركزي الأردني، 2020م، ص7.

[2] – الفيروز آبادي، القاموس المحيط، مؤسسة الرسالة، بيروت، من دون سنة النشر، ص 412.

[3] – خالد محمد نور عبد الحميد الطباخ، العملات الافتراضية ودورها في تمويل الإرهاب وغسل الأموال، مرجع سابق، ص 50.

[4] - FATF Financial Action Task Force. (2014). Report Virtual Currencies Key Definitions and potential AML/CFT Risks p 22.

[5] - Vejacka, Martin, Basic concepts about virtual currencies, Journal of Economy, Business and finance, 2017, p12.

والتشفير أو ما يسمى بالإنجليزية (cryptograhy) هو أحد فروع الرياضيات حيث يسمح لنا من خلاله إنشاء براهين رياضية تحمل مستوى عال جدا من الأمان[1].

وعلى ضوء ما سبق فقد عرفت العملات الرقمية المشفرة عدة تعريفات نذكر منها ما يلي:

1. عرف التشريع المصري العملات الرقمية المشفرة بأنها:" عملات مخزنة إلكترونيا غير مقومة بأي من العملات الصادرة عن سلطات النقد الرسمية، ويتم تداولها عبر شبكة الأنترنت "[2].
2. وعرفها البنك المركزي الأوربي بأنها عبارة عن:" التمثيل الرقمي للقيمة، التي لا تخضع للبنوك المركزية والسلطة العامة، ولا ترتبط بالعملات الورقية، ويقبلها الأشخاص العاديون، أو الاعتباريون، كوسيلة للدفع بها ويمكن تحويلها أو ادخارها وتداولها إلكترونيا"[3].
3. وأما صندوق النقد الدولي (IMF) فقد عرفها على أنها:" تمثيل رقمي للقيمة، صادرة عن مطورين خاصين ومقومة في وحدة الحساب الخاصة بهم"[4].
4. كما عرفت بأنها عبارة عن:" وحدة اعتبارية ليس لها وجود فيزيائي أو كيان مادي ملموس، ولا تصدر عن بنك مركزي أو هيئة نقد معينة، إضافة إلى أنها لا تقترن بأي عملة نقدية محلية كانت أو عالمية، ويمكن تحويلها وتخزينها إلكترونيا، وإصدارها يتم بواسطة حواسيب متطورة، ويتم التداول بها في الأوساط الإلكترونية وعبر المنصات المخصصة لها دون رقابة وإشراف حكومي"[5].

---

[1] – خالد محمد نور عبد الحميد الطباخ، العملات الافتراضية ودورها في تمويل الارهاب، مرجع سابق، ص 52.

[2] – المادة 01 من قانون البنك المركزي والجهاز المصرفي رقم 194 لسنة 2020.

[3] - European Central Bank (2018)، Report on electronic money , Frankfurt, Germany ,p 7

[4] - IMF Staff Discussion Note, Virtual Currencies and Beyond: Initial Considerations, January 2016, p7.

[5] – أحمد هشام قاسم النجار، العملات الافتراضية المشفرة دراسة اقتصادية شرعية محاسبية، دار النفائس للنشر والتوزيع، الأردن، 2019م، ص 32.

المطلب الثالث: خصائص العملات الرقمية المشفرة

تتعدد خصائص العملات المشفرة بشكل كبير ومن خلال التعاريف السابقة لهاته العملات يمكننا أن نستشف بعض السمات والمزايا، لكننا سوف نركز على تلكم الخصائص التي تعتبر مخاطرا أيضا أو على حد قول وتعبير كريستين لاجارد مديرة الصندوق النقد الدولي:" إن سبب جاذبية العملات المشفرة هو نفسه ما يجعلها أصولا خطرة"[1]. وعلى هذا الأساس فإن خصائص العملات الرقمية المشفرة تتمثل في الأمور التالية:

أولا: اللامركزية Decentralized

اللامركزية تعني هنا عدم تحكم مؤسسة بحد ذاتها بطرحها في السوق الالكتروني، فهي عملة بعيدة تماما عن نظام البنوك، وهذا يعني بالضرورة أن هاته العملات المشفرة مستقلة عن رقابة النظام المالي، وتعتبر اللامركزية الميزة الأشهر لإصدار العملات الافتراضية المشفرة، حيث استخدمت اللامركزية تحقيقا لمبدأ التشفير ودعما لقوة المعاملات المالية التي تتم من خلال الأنظمة المستخدمة للعملات الرقمية المشفرة[2].

ثانيا: سهولة الاستخدام

يتطلب تداول العملات الرقمية الالمام بمسائل تقنية بسيطة، حيث إنه بمجرد أن تتوافر لدى المستخدم القدرة على مع واجهة التطبيق الخاص بالعملة يستطيع بعد ذلك إعداد وتنفيذ كل العمليات التي يطلبها أي متعامل، مما يعني أنه سيكون من السهل عليه استخدام هاته العملات في الأعمال والأنشطة الإجرامية[3].

ثالثا: إخفاء الهوية

تتميز العملات المشفرة بمسألة كتمان الهوية وذلك من خلال السماح باستخدام اسم مستعار إلى القدرة على الإخفاء التام للهوية، وذلك أن الدفع من خلال بورصة العملة المشفرة لا يخضع

---

[1] – كريستين لاجارد، معالجة الجانب المظلم في العالم المشفر، مجلة الدراسات المالية والمصرفية، المجلد 26، العدد 01، 2018م، ص 33.

[2] - Deutsch Bank, (2018), Bitcoin: Myths, misconceptions and misunderstandings, Frankfurt, 12

[3] - J. (Everette) and others: Risks and vulnerabilities of virtual currency, cryptocurrency as a payment method: Public-privat Analytic Exchange Program , 2017, p 10.

لقاعدة: (اعرف عميلك) المطبقة في التعاملات المصرفية التقليدية، وهو ما ساهم في جاذبيتها بالنسبة للأعمال الإرهابية والإجرامية بشكل عام، فعملة البتكوين مثلا استخدمت في دفع الفدية في واقعة استخدام فيروس ضار أدى إلى تعطيل أجهزة الكمبيوتر وأنظمة التشغيل[1] .

رابعا: الأمان وسرعة إنجاز المعاملة

يوفر التعامل بالعملة الرقمية المشفرة الكثير من الوقت، حيث إنه يتم إنجاز المعاملة بسرعة كبيرة رغم بعد المسافة وتخطي الحدود بين الأطراف والدول، وهي ميزة جذابة جدا وتقدم فرصة رائعة لعولمة الجريمة والجماعات الإرهابية[2]. كما أن العملات المشفرة تتميز بكونها على درجة عالية من الأمان فقد تم إنشاء نظامه وفقا لخصائص: الصواب، إخفاء الهوية ومقاومة هجمات الانتحال[3].

رابعا: التعامل مع عالم الويب السفلي

تُستخدم العملات المشفرة أيضا كوسيلة للدفع على المواقع غير المشروعة فيما يطلق عليه بالشبكة العنكبوتية السوداء (الأنترنت المظلم)، حيث ساهمت بعض الخصائص التي تتمتع بها العملات الرقمية المشفرة مثل تعدد التوقيعات الإلكترونية والعقود الذكية في دعم عدم مركزية الضمان، وإلى كسر حاجز الثقة من مرتكبي الأفعال غير مشروعة قانونا[4].

المطلب الرابع: الأنشطة الإجرامية ذات الصلة بالعملات المشفرة

إذا كان تداول العملات المشفرة يتم بين الأشخاص دون مرور على البنوك المركزية ودون رقابة حقيقية من الدولة، وفي غياب لقواعد موحدة لعملية تحويل الأموال مثل التي يتم ابتاعها في العملات التقليدية، فإن تداول هذه العملات قد صاحبها الارتباط بعدد من الجرائم والصفقات غير مشروعة والمشبوهة كغسل الأموال والاتجار في المخدرات وتمويل الإرهاب وغيرها. وسنبين هنا وجه الصلة بين العملات المشفرة والأعمال الإجرامية عبر بحث الصور التالية:

---

[1] - J.(Everette) and others, p 10-11.

[2] - J.(Everette) and others, p 19

[3] - أحمد هشام قاسم، العملات الافتراضية المشفرة، مرجع سابق، ص 43.

[4] - MCKINNEY (Ralph E) / SHAO (Lawrence P) / SHAO (Dale H.) / ROSENLIEB (Duane C.)، The evolution of financial instruments and the legal protection against counterfeiting: a look at coin, paper, and virtual currencies, journal of Law Technology & Policy, Vol.2 , 2015, p303.

أولا: جرائم غسل الأموال

في هذه الجرائم يحاول الجاني أن يعثر على طريقة يسبغ فيها المشروعية على دخله، فيقلبه من دخل غير مشروع إلى دخل مشروع يمكنه من استخدامه لأجل غايات أخرى غير محدودة، فهذه الجريمة تتشكل من إخفاء الأصول ومصادر الدخل غير مشروعة ثم تمويه مصدرها حتى تبدو في الظاهر أنها مشروعة[1] .

ويؤكد الدكتور علي محمد الخوري أن الدراسات تشير إلى أن " الكيانات الإجرامية نقلت وقامت بتبييض أموال لما يقرب من 2.8 مليار دولار في عام 2019 من خلال استخدام العملة المشفرة بيتكوين إلى البورصات بزيادة من حوالي مليار دولار في عام 2018"[2].

ومع ظهور الاقتصاد الرقمي فإن دائرة ارتكاب جرائم غسل الأموال قد استع نطاقها حتى أدى إلى ظهور مصطلح جديد هو غسل الأموال الرقمي[3]. وعلى سبيل المثال لا الحصر حدث في سنة 2014 أن اتهم Robert Feiella بأنه خالف نص المادة 1960 من الفصل الثامن عشر من القانون الفيدرالي الأمريكي حيث إنه تلقى إيداعات نقدية وقام باستبدالها بعملة البتكوين ثم قام بعد ذلك بغسل هاته العملات[4] .

ثانيا: جرائم الابتزاز والتهديد في الفضاء الالكتروني

أشار تقرير للشرطة الأوربية الصادر في سنة 2016م إلى أن العملات الافتراضية وخاصة البتكوين منها تعد الوسيلة المفضلة لمخترقي الشفرات ومرتكبي جرائم السرقة والاحتيال في الفضاء الالكتروني[5].

---

[1] - DYNTU (Valeriia)، Cryptocurrency as a means of money laundering, Entrepreneurship, Economy and Law , the all-Ukrainian scientific and practical economic and legal journal, Mai 2018, p269.

[2] – علي محمد الخوري، المدفوعات الإلكترونية والعملات الرقمية، مجلس الوحدة الاقتصادية العربية، القاهرة، 2021م، ص 79.

[3] – خالد محمد نور عبد الحميد الطباخ، العملات الافتراضية ودورها في تمويل الإرهاب وغسل الأموال، مرجع سابق، ص 57.

[4] - DUROS (Staci) , Cryptocurrency and Blockchain: Background and Regulatory Approaches, Wisconsin Policy Project, Wisconsin Legislative Reference Bureau, Volum1 Number 2, September 2018, p14.

[5] - Europol: Internet Organised Crime Threat Assessment (2016), Carlisle, p 20.

والملاحظ أنه قد انتشر استخدام عملة البتكوين فيما يعرف بهجوم (برنامج الفدية) ومن الأمثلة على ذلك ما قام به بعض المجرمين في بداية سنة 2017 من اختراق نظام غلق الأبواب لأحد الفنادق في النمسا وتمكنوا من إغلاق كافة أبواب الفندق بما فيها حجرات النزلاء، وأجبروا بذلك إدارة الفندق على دفع مليون وثمانمائة ألف دولار سددت بعملة البتكوين كفدية نظير فك هذا الغلق[1].

ثالثا: جرائم الإرهاب والمساس بأمن الدولة

تؤكد الكثير من التقارير والدراسات على الارتباط الوثيق بين العملات الرقمية المشفرة وجرائم تمويل الإرهاب، وقد ساعد على ذلك السرية والكتمان التام التي تتميز به هاته العملات بالإضافة إلى كونها عابرة للحدود، وعلى سبيل المثال أشارت التقارير لمنظمات بحثية أنه في سنة 2014م استخدم منتسبو داعش هذه التقنية (العملات الرقمية المشفرة) [2].

يضاف إلى جرائم الإرهاب والمساس بأمن الدولة جرائم أخرى تتصل بالعملات المشفرة مثل: جرائم الاحتيال المالي وجرائم المساس بالأسواق المالية والمقامرة، وجرائم الاتجار بالبشر وجرائم التزييف والتزوير وتقلبات أسعار العملات الرقمية.

المبحث الثاني: تجريم التداول بالعملات الرقمية المشفرة

رأينا سابقا تلكم العلاقة الوثيقة بين الأعمال الإجرامية المتنوعة من غسل الأموال وتمويل الإرهاب وجرائم الابتزاز والفدية والاتجار بالبشر وغيرها من الجرائم وبين العملات الرقمية المشفرة، إذا يفضل هؤلاء المجرمين تلقي أموالهم عبر العملات الرقمية نظرا لما تملكه من خصائص يجعل تعقبهم صعبا جدا أو غير ممكن تماما.

وعلى هذا الأساس الذي ينبئ بمخاطر كبيرة تحوم حول كل من يتعامل بهاته العملات بالإضافة إلى كون هاته العملات مجهولة من حيث المصدر ولا تحمل في طياتها أي استقرار مالي يعود بالأمان المالي على متداوليها فإنها تشكل خطرا كبيرا يجب على المشرع مواجهته.

---

[1] - Carlisle, p 21.

[2] – كولن ب كلارك وآخرون، السيناريوهات المالية المستقبلية للدولة الإسلامية في العراق والشام، مؤسسة راند، كاليفورنيا، 2017م، ص13.

كما أنها ولحد الآن لا تحمل ولا تنبئ بأية مصلحة لا مالية ولا أمنية أو اقتصادية تحفز المشرع على حماية هاته العملات والعمل على تنظيمها تنظيما قانونيا، ولهذا سارعت الكثير من التشريعات العربية والغربية على تجريم التعامل بهاته العملات وبعضها منع التعامل بها لكنه لم يدخلها في حيز التجريم بعد.

ونحن هنا ندرس آلية المواجهة القانونية لجرائم العملات المشفرة من خلال تجريم التعامل بالعملات المشفرة، وذلك عبر المطالب التالية:

المطلب الأول: النص التشريعي الخاص بمنع تداول العملات الرقمية المشفرة

قبل أن نتطرق إلى النصوص التشريعية التي منعت وحظر تداول العملات الرقمية، لا بد لنا هنا ان نقف وقفة صغيرة حول الموقف الدولي عموما من العملات المشفرة حيث إنه يمكننا أن نميز بين موقفين اثنين الأول فيهما سمح بتداول هاته العملات وأول الدول التي سمحت بذلك كانت ألمانيا ثم تلتها بعد ذلك روسيا في سبتمبر 2017م، حيث أعلنت أنها تسعى إلى تقنين استخدام العملات المشفرة، ومن الدول العربية نجد كل من البحرين والإمارات العربية المتحدة التي سمحت بنشاط جزئي لهاته العملات[1].

وأما الاتجاه الثاني الذي حظر وتحفظ على استخدام العملات المشفرة فلا شك أن نظام اللامركزية والتشفير الذي ينبني عليه العملات الرقمية جعلها في معزل عن تحكم ورقابة أية جهة رسمية في العالم، وهو دفع الكثير من الدول تمنعها وتحظر التعامل بها، ونحاول هنا بيان النصوص التشريعية التي معنت التداول بالعملات الرقمية المشفرة على النحو التالي:

- نصت المادة 117 من قانون المالية الجزائري لسنة 2018 على أنه:" يمنع شراء العملة الافتراضية وبيعها واستعمالها وحيازتها..... يعاقب على مخالفة لهذا الحكم، طبقا للقوانين والتنظيمات المعمول بها"[2]، ويلاحظ هنا أن المشرع الجزائري قد أحال بخصوص العقاب على

---

[1] – رامي متولي القاضي، المواجهة الجنائية لجرائم العملات الرقمية المشفرة والذكاء الاصطناعي، دراسة تحليلية في التشريع المصري والمقارن، مجلة الشريعة والقانون، مجلد 89، عدد 06، 2020م، ص 271.

[2] – المادة 117 من القانون رقم 17 –11 مؤرخ في 09 ربيع الثاني 1439هـ المواق لـ 28 ديسمبر 2017م المتضمن قانون المالية 2018م، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد 76.

مخالفة هذا المنع على القوانين والتنظيمات المعمول بها في هذا الشأن، وهذه الإحالة تبدو في نظرنا غامضة جدا فهي تعني أن المشرع قد الأمر برمته إلى اجتهاد القاضي المختص في هذا المجال، كما أنها قد تعني أيضا أن المشرع يتطلع في المستقبل القريب إلى تنظيم هاته العملات بما يتلأم مع مقتضيات التحول الرقمي وما آلت إليه الثورة الصناعية الرابعة.

- وأما المشرع المصري فقد وضع القانون رقم 194 لسنة 2020 الخاص بإصدار قانون البنك المصري والجهاز المصرفي[1]، حيث نصت المادة 206 من هذا القانون على أنه :" يحظر إصدار العملات المشفرة أو النقود الالكترونية أو الاتجار فيها أو الترويج لها أو إنشاء أو تشغيل منصات لتداولها أو لتنفيذ الأنشطة المتعلقة بها دون الحصول على ترخيص من جلس الإدارة طبقا للقواعد والإجراءات التي يحددها".

والواضح من هذا النص التشريعي أن المشرع المصري كان يهدف ويقصد إلى تنظيم هاته العملات تنظيما قانونيا وهو أمر أولى عنده من منعها وحظرها حظرا تاما حتى يكون بذلك متماشيا مع تحولات العصر الحديث وما جلبه التطور الصناعي الحديث[2].

المطلب الثاني: أركان جرائم العملات الرقمية المشفرة

من خلال النصوص التشريعية السابقة وخاصة النص التشريعي المصري الذي يمكّننا من أن نستشف أركان جريمة تداول العملات الرقمية المشفرة بشكل واضح وصريح، ولا بد هنا من أن نقول بأن هناك عدة صور وأنواع لجرائم العملات المشفرة، فهناك جريمة إصدار العملات الرقمية المشفرة، وجريمة الاتجار في العملات المشفرة، وجريمة الترويج لهاته العملات، وجريمة إنشاء وتشغيل منصات لتداول العملات المشفرة والتعامل بها.

وسوف نتناول هنا صورة واحدة من هاته الصور الجرمية وهي :(جريمة الاتجار في العملات المشفرة) منعها التشريع الجزائري والمصري معا، نبين فيها محل الجريمة وركنها المادي والمعنوي ونبين العقوبة التي قررها التشريع على النحو التالي:

---

[1] – القانون رقم 194 منشور في الجريدة الرسمية لجمهورية مصر العربية، العدد 37 مكرر (و) بتاريخ 2020/9/15 والمعمول به من 9/16/ 2020م.

[2] – رامي متولي القاضي، المواجهة الجنائية لجرائم العملات الرقمية المشفرة، مرجع سابق، ص 275.

أولا: محل جريمة الاتجار بالعملات المشفرة

حظر التشريع الجزائري في المادة 117 من قانون المالية لسنة 2018 حيازة العملات الرقمية المشفرة والاتجار فيها كما هو الشأن أيضا بالنسبة للتشريع المصري حيث نصت المادة 206 من قانون البنك المركزي:" يحظر إصدار العملات المشفرة أو النقود الالكترونية أو الاتجار فيها.."

وهذا يعني أن محل الجريمة هنا هو العملات الرقمية المشفرة، حسب النصين التشريعيين الجزائري والمصري السابقين.

ثانيا: الركن المادي لجريمة الاتجار بالعملات المشفرة

الركن المادي هنا هو فعل الاتجار بالعملات الرقمية المشفرة، ومكننا أن نميز هنا في فعل الاتجار بين مدلولين اثنين[1]: المدلول الأول ضيق ويشمل البيع والشراء والوعد بالبيع والشراء، وأما المدلول الثاني فهو واسع يشتمل على عمليات السمسرة والوساطة التي تمس عملية البيع والشراء بشكل عام، ومكننا أن نقول بأن المدلول الثاني يدخل في نطاق جريمة الاتجار بالعملات المشفرة، فقد يسبق البيع عملية توسط وسمسرة ولذلك فإنه لا يدان البائع أو المشتري هنا فقط بل يجرم أيضا السمسار أو الوسيط الداخل في هاته العملية[2].

ثالثا: الركن المعنوي

تعد جريمة الاتجار في العملات الرقمية المشفرة من الجرائم العمدية، والتي يتطلب تحققها توافر القصد الجنائي العام بعنصريه الهامين: العلم والإرادة، وهذا يعني أنه يجب أن يكون الجاني عالما بتعامله في العملات الرقمية المشفرة بالبيع أو الشراء أو السمسرة، وأن تتجه إرادته إلى فعل هذا العمل الذي يرى فيه الكثير من الناس ربحا إضافيا [3].

---

[1] – رامي متولي القاضي، المواجهة الجنائية لجرائم العملات الرقمية المشفرة، مرجع سابق، ص 279.

[2] – إبراهيم محمد جبريل، جريمة التعامل في العملات المشفرة أو النقود الرقمية، دراسة مقارنة، جامعة المنصورة، مجلة البحوث القانونية والاقتصادية، عدد 79، مارس، 2022م، ض 1048.

[3] – رامي متولي القاضي، المواجهة الجنائية لجرائم العملات الرقمية المشفرة، مرجع سابق، ص 280.

رابعا: العقوبة

تقضي المادة 225 من قانون البنك المركزي والجهاز الصرفي المصري بأنه:" يعاقب بالحبس وبغرامة لا تقل عن مليون جنيه ولا تجاوز عشرة ملايين، أو بإحدى هاتين العقوبتين، كل من خالف أياً من أحكام المواد (63، 184، 205، 206) من هذا القانون. وفي حالة العود يحكم بالحبس والغرامة معا".

وعلى هذا الأساس فإن الجناة في جريمة الاتجار بالعملات الرقمية المشفرة يعاقبون بالحبس وبغرامة مالية لا تقل عن مليون جنيه ولا تتجاوز عشرة ملايين، أو بإحدى هاتين العقوبتين حسب تقدير القاضي لظروف وملابسات القضية والظروف الشخصية للمحكوم عليه.

والحبس عقوبة حدها الأدنى أربع وعشرون ساعة وحدها الأقصى ثلاث سنوات، كما تشدد العقوبة في حالة ما إذا عاد المجرم إلى جريمته السابقة لتصبح الحكم بالحبس والغرامة معا، بالإضافة إلى عقوبة نشر ملخص الحكم بالإدانة[1].

ويمكننا أن نلاحظ أن المشرع المصري قد جعل العقوبات على هاته الجرائم متقاربة كثيرا مهما تنوعت صور جرائم العملات المشفرة، وترك التقدير للقاضي يمحص كل نوع ويبحث في كل حالة والملابسات التي مرت بها كل قضية.

أما فيما يخص المسؤولية الجنائية للشخص المعنوي فقد أشارت المادة 235 من قانون البنك المركزي والجهاز المصرفي حيث نصت على أنه:" في الأحوال التي ترتكب فيها الجريمة بواسطة شخص اعتباري يعاقب المسؤول عن الإدارة الفعلية للشخص الاعتباري المخالف بذات العقوبات المقررة على الأفعال التي ترتكب بالمخالفة لأحكام هذا القانون، متى ثبت علمه به، وكانت الجريمة قد وقعت بسبب إخلاله بواجبات الوظيفة. ويكون الشخص الاعتباري مسئولا بالتضامن معه عن الوفاء بما يحكم به من عقوبات مالية وتعويضات إذا كانت الجريمة قد ارتكبت من أحد العاملين به باسمه نيابة عنه".

---

[1] – رامي متلوي القاضي، المرجع والموضع نفسه.

ومن خلال منطوق النص التشريعي السابق يتضح لنا أن القانون يقرر مسؤولية جنائية لكل من الشخص الطبيعي الذي هو مسؤول عن إدارة الشخص الاعتباري، كما أنه يقرر مسؤولية جنائية أيضا على الشخص الاعتباري بذاته[1]

وبالنظر الفقهي الدقيق والتمعن العميق في صور جريمة العملات الرقمية المشفرة وأركانها وما قرره التشريع المصري من عقوبات على هاته الجرائم يتضح لنا الأمور التالية[2]:

- قام المشرع بمعاقبة الجاني سواء حقق غايته من الجريمة أم لم يحققها، وهذا يعني أن العقاب كان منصبا على تجريم النتائج التي تهدد بالخطر وعدم الانتظار حتى يقع الضرر.
- تم التوسع هنا في فكرة الفاعل نظرا إلى التوسع في شمول نظرية المساهمة في الجريمة.
- يلاحظ أيضا أن المشرع قد عاقب الجاني عقوبة الجنحة بعقوبة سالبة للحرية وعقوبة مالية عبارة عن دفع غرامة مالية فنص على كلا العقوبتين، ثم شدد العقوبة في حالة العود لجريمة مرة أخرى لتطبق على الجاني العقوبتين معا في نفس الوقت.
- كما يلاحظ أيضا أن المشرع لم ينص على مصادرة الأموال المستخدمة في الجريمة ويرجه هذا ربما إلى أن هذه الأموال قد يدمجها المجرم في عملات مشفرة غير محسوسة وذات قيمة مجهولة، ومن الصعوبة بمكان تحصيلها أو مصادرتها، خاصة إذا علمنا ان الكثير من الجرائم في هذا المجال تقع خارج البلاد.

---

[1] – رامي متولي القاضي، المواجهة الجنائية لجرائم العملات الرقمية المشفرة، مرجع سابق، ض 284.

[2] – إبراهيم محمد جبريل، جريمة التعامل بالعملات الرقمية المشفرة، مرجع سابق، ص 1091–1093.

خاتمة:

تناولت الدراسة كيفية المواجهة التشريعية لجرائم العملات الرقمية والمشفرة من خلال السياسة الجنائية، حيث قمنا ببحث ماهية هاته الجرائم وحقيقتها العلمية والواقعية ثم عرضنا إلى جوانب الصلة بينها وبين الأفعال الإجرامية من غسل الأموال وتمويل الإرهاب والمساس بأمن الدولة وجرائم الابتزاز عبر الفضاء السيبراني، وغيرها من الجرائم.

وبعد أن تأكد لنا كيف أن هاته العملات تشكل خطرا حقيقيا يجب على التشريع الجنائي أن يتصدى له بكل ما تتيح السياسة الجنائية من آليات وسبل، وقد توصلت الدراسة إلى النتائج والتوصيات التالية:

أولا: نتائج البحث

1. تتميز العملات الرقمية المشفرة بسرعة وسهولة إنجاز العمليات المطلوبة منها، كما تتميز بقلة التكلفة في عملياتها، بالإضافة إلى كونها لا تخضع لأي سلطة مركزية ولا توجد عليها أية رقابة أو قيود.
2. تعتمد العملات الرقمية على خاصية التشفير والمعتمد بالأساس على تقنية البلوكتشين الذي يحفظ سرية التعامل وهوية المتعاملين أيضا.
3. أظهرت الدراسة أن هذه العملات غير مكفولة من الدولة وتخرج عن رقابتها فلا قيود على تداولها، وبالتالي فلا قيمة حقيقية في ذاتها إذ إنها لا تعدو أن تكون رموزا مشفرة اكتسبت قيمتها من خلال المضاربة وهو ما قد يؤدي إلى انهيار سعرها في أي لحظة تاريخية فارقة.
4. تشكل العملات الرقمية المشفرة تهديدا حقيقيا على الأمن الاقتصادي في كونها تعتدي على حق البنك المركزي في السيطرة على إصدار العملة والنقود الرسمية، وهو أمر يخلق فوضى اقتصادية كبيرة وينزع الثقة بين المواطن والبنك وعملة البلد الرسمية.
5. أظهرت الدراسة أن هناك صلة وثيقة بين استخدام العملة المشفرة وبين طائفة واسعة من الأنشطة الإجرامية، ويرجع ذلك لعدة أسباب منها: سهولة الاستخدام، واستقلال هاته العملات عن الرقابة المالية، والقدرة على الإخفاء التام لهوية المتعاملين، بالإضافة إلى فورية التعامل وسرعته الكبيرة.

6. تعد جرائم غسل الأموال وتمويل الإرهاب والمساس بأمن الدولة وسلامة المواطنين، وجرائم الابتزاز في الفضاء السيبراني، وجرائم الكمبيوتر وتقنية المعلومات من أكثر الجرائم صلة بالعملات الرقمية المشفرة، بالإضافة إلى جرائم الفدية وتزييف العملة والاتجار بالأسلحة والمخدرات وغيرها من الجرائم المتعددة.

7. إن تجريم التعامل بالعملات الرقمية المشفرة وحظر إصدارها والاتجار بها أو حتى ترويجها لم يعد كافيا للحد من مخاطرها في ظل عدم وجود إطار معلوماتي وقانوني لها، بدليل تزايد الإقبال عليها على الرغم من وجود عقوبات على التعامل بها.

8. هناك عدة صور لجريمة التعامل بالعملات الرقمية المشفرة أثبتها المشرع المصري في القانون رقم 194 وهاته الصور هي: جريمة إصدار العملات المشفرة، وجريمة الاتجار بالعلات الرقمية المشفرة، وجريمة الترويج لهاته العملات، وجريمة اشاء منصات خاصة بالعملات الرقمية المشفرة.

9. تميز التشريع المصري على التشريع الجزائري بكونه نص على عقوبات جرائم العملة الرقمية المشفرة والتي تنوعت بين عقوبة الغرامة والسجن أو كلاهما معا في حالة العود لمثل هذا الجرم الاقتصادي.

10. تخلص الدراسة من زاوية السياسة الجنائية أن العملات الرقمية المشفرة تحتوي على درجة عالية من الخطورة، كما أنها تنطوي على تهديد جسيم يمس مصالح الدولة واستقلالها وبالتالي في المصلحة العامة للدولة ككل تتطلب تجريم التعامل بها في الوقت الحالي، كما أن ضرورات التحول الاقتصادي الرقمي تتطلب دراسة هاته العملات من زوايا أخرى متنوعة نبينها في التوصيات الخاصة بهذا البحث.

ثانيا: توصيات البحث

بناء على سبق دراسته وبحثه حول المواجهة الجنائية والتشريعية لجرائم العملات الرقمية المشفرة، وتأسيسا على النتائج البحثية السابقة فإننا نوصي بالأمور والنقاط التالية:

1. نوصي المشرع الجزائري بضرورة الإسراع وبيان بالنص التشريعي الخاص بالعقوبات المقررة على مرتكبي جرائم العملات الرقمية المشفرة، وعدم ترك الأمر منوطا باجتهاد القاضي لوحده فقط.

2. ضرورة الإعلان من جانب الدول عن موقف واضح وصريح حول العملات الرقمية المشفرة، وضرورة أن يكون هناك تعاون دولي أو على الأقل تعاون إقليمي فيما يخص جرائم العملات الرقمية المشفرة.

3. وجوب وضع إطار قانوني محدد لاستخدامات العملات الرقمية المشفرة، هذا في حال الاستخدام الجزئي لهاته العملات، وهذا بهدف التصدي للاستخدامات غير المشروعة.

4. العمل على تبني استراتيجية إعلامية وأمنية متكاملة للتوعية من مخاطر استخدام العملات الرقمية المشفرة، وذلك من خلال إشراك كافة المؤسسات المعنية بهذا الأمر الخطير.

5. الدعوة إلى عقد دراسات علمية جادة تمس هذا الموضوع من زوايا أخرى كزاوية الأمن الاقتصادي والأمن المجتمعي وآليات المواجهة التكنولوجية الحديثة لمثل هذا النوع من الجرائم الخطير والحساس والحديث جدا في نفس الوقت.

6. أن تكون هاته الدراسات العلمية كمشروع تمهيدي من أجل وضع إطار قانوني الاقتصاد والأمن الوطنيين ويتماشى مع ضرورات التحول الاقتصادي الرقمي الحديث.

7. يجب السعي في إطار التعاون الدولي نحو إنشاء بنك مركزي دولي على غرار البنوك المركزية الدولية تعمل على مراقبة إصدار العملات الرقمية المشفرة، وتنظيم التعامل بها، وتوفير الغطاء القانوني لها.

قائمة المراجع:

المراجع باللغة بالعربية:

أولا المراسيم والقوانين:

- القانون رقم 17 -11 مؤرخ في 09 ربيع الثاني 1439هـ المواق لـ 28 ديسمبر 2017م المتضمن قانون المالية 2018م، الصادر في الجريدة الرسمية للجمهورية الجزائرية، عدد 76.
- القانون رقم 194 منشور في الجريدة الرسمية لجمهورية مصر العربية، العدد 37 مكرر (و) بتاريخ 2020/9/15 والمعمول به من 9/16/ 2020م.

ثانيا الكتب:

- أيمن صالح، واقع العملات الرقمية، صندوق النقد العربي، الإمارات العربية المتحدة، 2021م

- خالد محمد نور عبد الحميد الطباخ، العملات الافتراضية ودور في تمويل الإرهاب وغسل الأموال، دار النهضة، مصر، ط2، 2022م.
- أحمد هشام قاسم النجار، العملات الافتراضية المشفرة دراسة اقتصادية شرعية محاسبية، دار النفائس للنشر والتوزيع، الأردن، 2019م.
- العملات المشفرة، البنك المركزي الأردني، 2020م.
- علي محمد الخوري، المدفوعات الإلكترونية والعملات الرقمية، مجلس الوحدة الاقتصادية العربية، القاهرة، 2021م.
- الفيروز آبادي، القاموس المحيط، مؤسسة الرسالة، بيروت، من دون سنة النشر.
- كولن ب كلارك وآخرون، السيناريوهات المالية المستقبلية للدولة الإسلامية في العراق والشام، مؤسسة راند، كاليفورنيا، 2017م.

ثالثا: المقالات المحكمة

- إبراهيم محمد جبريل، جريمة التعامل في العملات المشفرة أو النقود الرقمية، دراسة مقارنة، جامعة المنصورة، مجلة البحوث القانونية والاقتصادية، عدد 79، مارس، 2022م.
- رامي متولي القاضي، المواجهة الجنائية لجرائم العملات الرقمية المشفرة والذكاء الاصطناعي، دراسة تحليلية في التشريع المصري والمقارن، مجلة الشريعة والقانون، مجلد 89، عدد 06، 2020م.
- عبد اللطيف حاجي صادق، أثر سد الذرائع في التعامل بالعملات الافتراضية البتكوين نموذجا، مجلة الشريعة والدراسات الإسلامية، جامعة الكويت، عدد 16، 2019م.

قائمة المراجع الأجنبية:

- FATF Financial Action Task Force. (2014). Report Virtual Currencies Key Definitions and potential AML/CFT Risks.

- Vejacka, Martin, Basic concepts about virtual currencies, Journal of Economy, Business and finance, 2017.

- European Central Bank (2018)، Report on electronic money , Frankfurt, Germany

- IMF Staff Discussion Note, Virtual Currencies and Beyond: Initial Considerations, January 2016.

- Deutsch Bank, (2018), Bitcoin: Myths, misconceptions and misunderstandings, Frankfurt, 12

- J. (Everette) and others: Risks and vulnerabilities of virtual currency, cryptocurrency as a payment method: Public-privat Analytic Exchange Program , 2017,.

- MCKINNEY (Ralph E) / SHAO (Lawrence P) / SHAO (Dale H.) / ROSENLIEB (Duane C.)، The evolution of financial instruments and the legal protection against counterfeiting: a look at coin, paper, and virtual currencies, journal of Law Technology & Policy, Vol.2 , 2015.

- DYNTU (Valeriia)، Cryptocurrency as a means of money laundering, Entrepreneurship, Economy and Law , the all-Ukrainian scientific and practical economic and legal journal, Mai 2018.

- DUROS (Staci) , Cryptocurrency and Blockchain: Background and Regulatory Approaches, Wisconsin Policy Project, Wisconsin Legislative Reference Bureau, Volum1 Number 2, September 2018.

- Europol: Internet Organised Crime Threat Assessment (2016), Carlisle.

.

مداخلة بعنوان : التعليق على كيفية تجريم المشرع للجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

بن عربية شفاء

كلية الحقوق، جامعة الجزائر -1-

Ch.benarbia@univ-alger.dz

الملخص:

أحدث التطور التكنولوجي تغيرا جذريا في حياة الأفراد و المجتمعات و ترك تأثيراته على كل تفاصيلها، فلم يسلم أي مجال من مجالات الحياة من هذا التأثير سواء كان ذلك بطريقة إيجابية أو سلبية، و لكون الجريمة ظاهرة من الظواهر الاجتماعية الملازمة للمجتمعات فإنها لم تكن بمنأى عن هذا التأثير[1]، حيث استغل مجرمي الذكاء أو ما يسمون بمجرمي الياقة البيضاء هذا الوضع في تطوير الجريمة، سواء من حيث استحداث جرائم جديدة أو تطوير أساليب ارتكاب جرائم تقليدية

هذا الوضع اعتبر تحدي فرض على الهيئات التشريعية وجوب صياغة أحكام تجريمية في إطار قانوني يحقق التوازن بين متطلبات مبدأ الشرعية – الدقة و الوضوح – و تداعيات التكنولوجيا في مجال تطور الإجرام

الكلمات المفتاحية:

القانون الجنائي ، التطور التكنولوجي، أحكام التجريم، الجرائم المستحدثة، مبدأ الشرعية،

Abstract :

Technological development has brought about a radical change in the lives of individuals and societies and has left its effects on all its details. No area of life was spared from this influence, whether in a positive or negative way, and because crime is one of the social phenomena inherent in societies, it was not immune from this. Impact, as intelligence criminals or what are called white collar criminals took advantage of this situation to develop

---

[1] عبد القادر عميمر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة) ،أطروحة لنيل شهادة الدكتوراه في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2020، ص 2

crime, whether in terms of creating new crimes or developing methods of committing traditional crimes.

This situation was considered a challenge that imposed on legislative bodies the need to formulate criminal provisions within a legal framework that achieves a balance between the requirements of the principle of legality - accuracy and clarity - and the implications of technology in the development of crime

Keywords:

Criminal law, technological development, criminalization provisions, new crimes, the principle of legality

المقدمة:

إن الثورة المعلوماتية و نتيجة للتقنيات العالية التي تقوم عليها و التي تتمثل في استخدام الحواسيب و الشبكات المعلوماتية التي تربط بينها قد تركت أثارا ايجابية و شكلت قفزة حضارية نوعية في حياة الأفراد و الدول، حيث تعتمد القطاعات المختلفة في الوقت الحالي في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية نظرا لما تتميز به من عنصري السرعة و الدقة في تجميع المعلومات و تخزينها و معالجتها و من ثم نقلها و تبادلها بين الأفراد و الجهات و الشركات و المؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول، كما اصبحت هذه الأنظمة مستودعا لأسرار الأشخاص المتعلقة بحياتهم الشخصية أو بطبيعة أعمالهم المالية و الاقتصادية ، كذلك أمست مستودعا لأسرار الدول الحربية و الصناعية و الاقتصادية التي تعتبر على قدر من الأهمية و السرية[1]

و في مقابل تباين الذهنيات و المستويات العلمية لمستعملي شبكة الانترنت ظهرت ممارسات غير مشروعة، فأصبحت هذه الشبكة أداة لارتكابها او محلا لها حسب الحالة، مما أدى لظهور طائفة جديدة من الجرائم مختلفة عن باقي الجرائم التقليدية، و قد سميت بالجرائم المعلوماتية أو الاليكترونية أو جرائم الانترنت[2]

بسبب الطبيعة الخاصة لهذا النمط الإجرامي المستجد، كان لزاما على الأنظمة الجزائية[3] التحرك من أجل إيجاد سبل للحد من تفاقم تداعيات تكنولوجيا الإعلام و الاتصال على الظواهر الاجتماعية، فوجد المشرع الجزائري نفسه – و هو حال جل التشريعات –أمام عنصرين يتطلبان مراعاتهما بشدة في صياغة الأحكام الجزائية المقررة لهذه الآفة، و هما التطور اللامتناهي للجريمة بفضل تكنولوجيا الإعلام و الاتصال ،و وجوب احترام مبدأ الشرعية مع ما يفرضه من قيود في صياغة الأحكام الجزائية

و بالتالي و من أجل دراسة مدى تمكن المشرع الجزائري في تحقيق الموازنة بين العنصرين السابق ذكرهما حق لنا طرح الإشكال التالي _كيف أثر استخدام التكنولوجيا الحديثة على أحكام التجريم ؟

---

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 1، دار الثقافة للنشر و التوزيع، الاردن، 2010، ص13

[2] محمد بن أحمد علي المقصودي، الجرائم المعلوماتية: خصائصها و كيفية مواجهتها قانونيا، المجلة العربية للدراسات الامنية ، المجلد33، العدد 70، السعودية، 2016، ص 102

[3] أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه في القانون الخاص،كلية الحقوق، جامعة برج بوعريريج، الجزائر، 2021/2020، ص 1

إن تكنولوجيا الإعلام و الاتصال ألزمت المشرع في وظيفته التجريمية انتهاج خطة تتضن شقين:

1 استحداث جرائم المساس بأنظمة المعالجة الآلية للمعطيات

2 التوسع في تحديد مدلول الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

أولا : استحداث جرائم المساس بأنظمة المعالجة الآلية للمعطيات

ساهمت تكنولوجيا الإعلام و الاتصال في استحداث جرائم لم يتمكن المشرع من مجابهتها بالنصوص التقليدية سواء المتوفرة – النصوص التقليدية– في قانون العقوبات أو في قوانين خاصة و ذلك بسبب الطابع المعنوي و اللامادي لها ، و هنا بطبيعة الحال نتحدث عن الحالة التي تكون فيها المعلومة منفصلة عن الدعامة المادية لأنه في الحالة العكسية (أين تكون المعلومة على دعامة مادية) فإن إمكانية تطبيق النصوص التقليدية عليها متوفرة مع بعض التحفظات التي يفرضها مبدأ الشرعية و لكن هنا الحديث يكون بشكل أساسي عن الحالة التي تكون فيها المعلومة منفصلة عن الدعامة المادية و الإشكالات التي تخلقها مع ما يفرضه مبدأ الشرعية من وجوب التفسير الضيق لنصوص التجريم و في هذا الصدد نشير إلى بعض إجتهادات الفقه في محاولة تطبيق النصوص التقليدية لمواجهة هذه الجرائم المستحدثة و تتمثل هذه الاجتهادات فيما يلي

1. محاولة تطبيق نصوص جريمة السرقة (المادة 350 من قانون العقوبات): تصطدم هذه المادة بمبدأ الشرعية عند محاولة تطبيقها على الجرائم المستحدثة بتكنولوجيا الإعلام و الاتصال من حيث أن المعلومة هي ذات طبيعة معنوية فكيف يحدث الاختلاس الذي هو ذو طبيعة مادية[1] كما أن المعلومة تتعارض مع فكرة الاختلاس لأنها لا تخرج بل تبقى في حيازة صاحبها – أي لا تنتقل– بل فقط يفقد ميزة الاستئثار[2] بها بالإضافة إلى عدم تحقق السلوك المادي لكون الاختلاس

[1] أنظر نعمان عبد الكريم، الجرائم الإلكترونية و موقف المشرع الجزائري منها، رسالة ماجيستير في القانون الجنائي، كلية الحقوق ،جامعة الجزائر 1، الجزائر، 2017/2016، ص 183

[2]أنظر عفيفي كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون ، دراسة مقارنة، منشورات الحلبي الحقوقية، 2003، ص 146

كان بمجرد نشاط ذهني فقط أي الالتقاط الذهني عن طريق السمع و البصر و بالتالي لا يمكن تطبيق نصوص السرقة عليها[1]

2. جريمة النصب (المادة 372 من قانون العقوبات) : يستنتج من نص المادة 372 بأنه ليس كل شيء مادي ومنقول يصلح أن يكون محلا لجريمة النصب بل يجب أن يكون ضمن الأشياء التي عددتها المادة 372 على سبيل الحصر من جهة اخرى لم يقيد المشرع المنقول بأن يكون ماديا مما يسمح بتفسير هذا النص على نحو يسمح بدخول برامج الحاسب ضمن الأشياء التي تقع عليها جريمة النصب إلا أنه حتى وان أخذنا بهذا التفسير، نصطدم بعدم وجود نشاط مادي ملموس يحصل به التسليم والاستلام ،وحتى على فرض أن التسليم قد تم ،فإن المجني عليه لا يحرم من حيازة البرنامج والبيانات التي تبقى تحت سيطرته التامة[2] .

3. جريمة خيانة الأمانة (المادة 376 من قانون العقوبات) : إن قراءة المادة 376 يوضح أن محل الجريمة يتمثل في أي منقول مادي مملوك للغير يمكن إدراكه بالحواس و يتم تسليمه إلى الجاني بمقتضى أحد العقود الواردة على سبيل الحصر في ذات المادة و عليه لا تصلح البرامج و المعلومات لأن تكون موضوعا لجريمة خيانة الأمانة و ذلك لطبيعتها المعنوية[3]

4. جريمة الإتلاف (المادة 407 و 396 من قانون العقوبات) : حددت المادة 407 محل جريمة الإتلاف و الذي يتمثل في الأموال الثابتة و المنقولة و المحددة على سبيل الحصر في المادة 396 من قانون العقوبات[4] و بالتالي لا يمكن للبرامج و البيانات المنفصلة عن الدعامة المادية أن تكون محلا للجريمة نظرا لطابعها اللامادي[5]

---

[1] أنظر نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية و تطبيقية، الطبعة الاولى، منشورات حلبي القانونية، مصر، 2005، ص 151

[2] أنظر فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية المزمع عقده بأكاديمية الدراسات العليا بليبيا فى أكتوبر 2009، كلية الحقوق و العلوم السياسية، جامعة زيان عاشور الجلفة ، ص 6

[3] أنظر نعمان عبد الكريم، المرجع السابق، ص 185 و 186

[4] أنظر نعمان عبد الكريم، المرجع نفسه، 188

[5] أنظر رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية ، الطبعة الاولى، منشورات حلبي الحقوقية، لبنان، 2012، ص 114

بالإضافة إلى نصوص قانون العقوبات حاول الفقه مواجهة الجرائم المستحدثة بتكنولوجيا الإعلام و الاتصال ببعض النصوص الواردة في قوانين خاصة نذكر من بينها الأمر رقم 07/03 المتضمن براءة الإختراع غير أن هذا الأخير استبعد صراحة برامج الحاسوب من براءة الاختراع بموجب المادة 7 منه التي نصت " لا تعد من قبيل الاختراعات بمفهوم هذا الأمر ....برامج الحاسوب...." كما حاول الفقه مواجهة هذه الجرائم عن طريق الأمر 05/03 المتعلق بحقوق المؤلف و الحقوق المجاورة غير أنه رغم إعتراف هذا الأمر بموجب المادة 4 منه على برامج الحاسوب كمصنف أدبي أو فني محمي بموجبه إلا أن هذه الحماية تنصب على البرنامج أو مضمونه الإبتكاري فقط دون أن تغطي كل مضمون البرنامج[1]

إن هذا السبب – عدم قدرة النصوص التقليدية على مواجهة ما استحدثته تكنولوجيا الإعلام و الاتصال من جرائم –يضاف إليه كثرة التدخلات و النداءات حول تكاثر ظاهرة الجرائم الاليكترونية ألزم المشرع الجزائري بالتدخل عن طريق تعديل قانون العقوبات بموجب القانون رقم 15/04 لسنة 2004 و الذي استحدث به القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات ضمن الفصل الثالث المعنون بالجنايات و الجنح ضد الأموال – يكون بذلك قد حذا حذو المشرع الفرنسي – تضمن 8 مواد هي من 394 مكرر الى 394 مكرر 7 و هي :

- الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك (المادة 394 مكرر فقرة 1) و تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة (المادة 394 فقرة 2)
- الدخول أو البقاء المؤدي إلى تخريب نظام اشتغال المنظومة (المادة 394 فقرة 3)
- إدخال أو إزالة أو تعديل بطريق الغش المعطيات في نظام المعالجة الآلية (المادة 394 مكرر 1)
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر 2 فقرة 1)

[1]أنظر نعمان عبد الكريم، المرجع نفسه، ص 194 و 199

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان معطيات المتحصلة من إحدى الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر 2 فقرة 2)[1]

كما أضاف المشرع بموجب القانون رقم 06/16 المعدل لقانون العقوبات المادة 394 مكرر 8 التي جرمت بعض التصرفات المرتكبة من قبل مقدمي خدمات الانترنت و قبله كان المشرع قد تدخل أيضا سنة 2006 بقانون 23/06 اين قام بتشديد عقوبة الغرامة المرصودة لهذه الجرائم

ثانيا: التوسع في تحديد مدلول الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

قصد مواجهة فعالة لهذا النوع من الإجرام الذي يتميز بالخطورة و التطور الدائم، دعم المشرع القسم السابع مكرر بقانون خاص يحمل رقم 04/09 ،يتضمن 19 مادة موزعة على 6 فصول واجه فيها الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال بإطار قانوني يحمل نوع من الخصوصية لهذه الجريمة لا سيما من حيث التجريم، و هو النقطة الثانية المعالجة في هذه الدراسة

إن القانون الجزائي بمفهومه الواسع يتضمن ثلاثة أجزاء رئيسية، هي القانون الجزائي العام و القانون الجزائي الخاص و قانون الإجراءات الجزائية حيث ،جمع المشرع محتوى الأول و الثاني في قانون العقوبات في حين افردت الإجراءات الجزائية بقانون خاص[2]

يختص قانون الجزائي العام بدراسة الشروط العامة للتجريم و القواعد العامة لتحديد العقوبات، و التي يقصد بها مجموعة أحكام أساسية لا تتعلق بجريمة بعينها و إنما تسري على جميع أنواع الجرائم، جنايات جنح مخالفات و الجزاءات المقررة لها من عقوبات و تدابير أمن، سواء كانت هذه الجرائم محددة في قانون العقوبات أو في قوانين خاصة، و قد نظمها المشرع في المواد من 1 الى 60 مكرر 1 من قانون العقوبات[3]

إن جمع المبادئ العامة و جل الجرائم في تقنين واحد يعتبر مظهر راسخ من مظاهر قوة النص الجنائي، و معلم واضح من معالم الثبات الذي يحققه في المراكز القانونية المضمونة و الممنوحة للمخاطبين بذلك النص، فهو يمنح القوة لسلطة التشريع الجنائي من خلال عقلانية الشكلية المستمدة من الهيكلة و التنظيم، و كونه تعبيرا منظما عن القيم الأساسية المشتركة في المجتمع و رمزا لما هو صحيح و من ثمة عامل

[1] أنظر نعمان عبد الكريم، المرجع السابق، ص 204 و 205

[2] أنظر: أحسن بوسقيعة، الوجيز في القانون الجزائي العام ، الطبعة 16، دار الهومة، الجزائر، 2017، ص 13

[3] أنظر: عبد الله أوهايبية، شرح قانون العقوبات الجزائري، القسم العام، موفم للنشر، الجزائر، 2015، ص 12 و 13

تماسك اجتماعي تضفي هيبته فعالية على التشريع الجنائي، فينصاع الأفراد لقواعده لعلمهم بأنها جزء من مجموعة متماسكة و منطقية[1] ،فطابع الوحدة في التقنين هو الحارس و الضامن الأساس لمبدأ الأمن القانوني[2] و المقرر الأول لقاعدة الاستقرار في المراكز القانونية[3]

و لقد حرص المشرع الجزائري في مرحلة مبكرة من الاستقلال على إصدار تقنين العقوبات لطابعه السيادي المتميز إذ أنه أصدر سنة 1966 بموجب الأمر 156/66 ،و حرص منذ ذلك الحين على الحفاظ على مركزية مكانته في التشريع العقابي، ليصب فيه العديد من التعديلات التي فرضتها الالتزامات الدولية في المادة الجزائية[4] كما هو شأن مثلا في القانون رقم 15/04 المؤرخ 2004/11/10 المعدل و المتمم لقانون العقوبات و الذي استحدث في قانون العقوبات عدة جرائم من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات[5]

بالرغم مما يمكن التماسه من إرادة لدى المشرع في المحافظة على مركزية تقنين العقوبات كمصدر للقاعدة الجزائية الناشئة عن العولمة التشريعية، إلا أن مسعاه هذا خلق مواضع تصدع في التنظيم و الهيكلة الأساسية التي بني عليها التقنين، بسبب صعوبة الادراج المنطقي و العقلاني للجرائم المستحدثة داخل التقسيمات الأصلية لتقنين العقوبات، القائمة على أساس المصالح المعتدى عليها و هي مصالح قد قننت بتاريخ نشأة تقنين العقوبات، في حين أن تطور الجريمة أدى إلى بروز مصالح جديدة جديرة

---

[1] أنظر: علا كريمة، عادل بوزيدة، تحولات مبدأ الشرعية في ظل عولمة النصوص الجزائية، مقال غير منشور، الجزائر، دون سنة ، ص 4 و 5

[2] أنظر: علا كريمة، عادل بوزيدة، المرجع نفسه ، ص5 نقلا عن
G.Braubant, La problématique de la codification,1997, Rev.fr.d'adm.pub.165,168

[3] أنظر: علا كريمة، عادل بوزيدة، المرجع نفسه، ص 5

[4] أنظر: علا كريمة، عادل بوزيدة، المرجع نفسه، ص 6 . على سبيل المثال القانون رقم 01/09 المؤرخ في 2009/02/25 الذي أدرج في قانون العقوبات ثلاثة أقسام مكررة في الفصل المتعلق بالجنايات و الجنح ضد الأشخاص و هي القسم 5 مكرر بعنوان جرائم الإتجار بالأشخاص و القسم 5 مكرر 1 بعنوان الإتجار بالأعضاء و القسم 5 مكرر 2 بعنوان تهريب المهاجرين و ذلك مواءمة مع اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية و البروتوكولين المكملين لها . كذلك القانون رقم 01/14 المؤرخ في 2014/02/04 الذي استحدث بعض صور الجريمة الإرهابية و كذا جرائم التمييز و غيرها و ذلك تماشيا مع الاتفاقية الدولية الخاصة بإزالة جميع اشكال التمييز العنصري لسنة 1965 و اتفاقية العربية لمكافحة الإرهاب لسنة 1989 و اتفاقية منظمة الوحدة الإفريقية للوقاية و مكافحة الإرهاب لسنة 1999، أنظر: علا كريمة، عادل بوزيدة، المرجع السابق، ص 6

[5] أنظر: كريمة علا، عادل بوزيدة، المرجع نفسه، ص 5 و 6

بالحماية الجزائية يصعب أن تجد لها مكانا ضمن المصالح الأصلية[1] ،غير أنه بالنسبة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات قد استطاع المشرع بموجب تعديل 15/04 أن يدرجها في قانون العقوبات بإدراج القسم الخاص بها في الفصل الثالث بعنوان الجنايات و الجنح ضد الأموال – و هو نفس توجه المشرع الفرنسي – ،و بالتالي فإن توجه المشرع نحو ادراج هذه الجرائم في تقنين العقوبات نلمس منه رغبته أو سعيه في المحافظة على وحدوية التقنين – المشار إليها أعلاه –غير أن المشرع و في وقت لاحق، – بعد تعديل 2004– حاد عن مسعاه في المحافظة على وحدة التقنين و ذلك ما نلمسه في ادراج تجريم عام في القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و بالضبط في المادة 2 فقرة أ ،حيث عرفت هذه الأخيرة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال أنها، " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإليكترونية"

أن المتمعن في نص المادة يجد أن المشرع في هذا القانون الخاص قد أضاف تكنولوجيا الإعلام و الاتصال كعنصر في التجريم يلحق جميع الجرائم التي يقبل ركنها المادي هذه الوسيلة لإتمامه سواء كانت في قانون العقوبات أو في قوانين خاصة ،و قد أعطى لها المشرع حسب هذا القانون تسمية الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ،و التي يستنتج منها أن الواقعة التي يستعين ركنها المادي بتكنولوجيا الإعلام و الاتصال يصبح لها وصف آخر غير الوصف الأصلي لها ،و للتوضح أكثر نعطي المثال التالي : جريمة السب و القذف في قانون العقوبات مجرمة بموجب المواد 296 إلى 299 و لا نجد فيها السب و القذف باستعمال تكنولوجيا الإعلام و الاتصال لكن عندما نذهب لقانون 04/09 يصبح عندنا السب و القذف باستعمال تكنولوجيا الإعلام و الاتصال فيصبح للواقعة وصف ثاني غير المحدد في قانون العقوبات

إن استحداث المشرع لجرائم معينة – محددة على سبيل الحصر – و إدراجها في تقنين العقوبات بموجب قانون 15/04 ثم اللجوء الى قوانين خاصة لإدراج تجريم عام يوضح أن المشرع قد اعتمد خطة مزدوجة

[1] أنظر: كريمة علا عادل بوزيدة، المرجع نفسه، ص 7 . كتصنيف جرائم التمييز ضمن جرائم الاعتداء على الحريات الفردية لعدم وجود حماية جزائية لمبدأ المساواة داخل التقنين أو تصنيف تبييض الأموال ضمن الباب الخاص بالجرائم الواقعة ضد الأفراد بالرغم من اعتبارها جرائم مالية ...إلخ ،أنظر: كريمة علا عادل بوزيدة، المرجع نفسه، ص 7

في التجريم، و هذا الأسلوب أو هذه الخطة لا نقول أن فيها مساس بمبدأ الشرعية و لكنها تحدث اضطراب في تحديد الجريمة و وضوحها[1]

بالإضافة إلى ماذهب إليه المشرع بإدراج تجريم عام في قانون خاص – 04/09– فإنه يجدر بنا التذكير أن مبدأ شرعية و بالأخص شرعية التجريم يقتضي أن يكون النص القانوني واضحا و صريحا و محددا بدقة عناصر الفعل المجرم، غير أن الملاحظة الثانية التي يمكن رصدها من خلال المادة 2 الفقرة أ من القانون رقم 04/09 ،أن المشرع في هذه المادة لم يحدد ما هي الجرائم التي ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية أو نظام الاتصالات الإليكترونية ،و لا يمكن لنا حصر هذه الجرائم لأن المشرع ذكر الوسيلة التي يستعين بها الركن المادي – فقط– في الجريمة، سواء كانت هذه الأخيرة محددة في قانون العقوبات أو في قوانين خاصة ،ما يعني أن المشرع في صياغته لهذه الفقرة يتضح و كأنه يتجه في الاتجاه الذي ينادي بضرورة إضفاء بعض المرونة على مبدأ الشرعية حتى يستطيع النص القانوني مواكبة التطور الذي تعرفه هذه الجرائم خاصة و أنها تتم من قبل مجرمين يتمتعون بالذكاء أو ما يعرفون بأصحاب الياقة البيضاء

أما العنصر الثالث و الأخير الذي يمكن ملاحظته من خلال المادة 2 فقرة أ أن المشرع لم يحدد الجزاء الذي يطبق على الواقعة في حال اقترانها بتكنولوجيا الإعلام و الاتصال، حيث أن الفقرة أ اكتفت في التجريم بالركن المادي وهو اقتران السلوك بتكنولوجيا الإعلام و الاتصال دون إشارة للجزاء و دون الاشارة للركن المعنوي، و ذلك بخلاف القانون رقم 05/20 المتعلق بالوقاية من التمييز و خطاب الكراهية و مكافحتهما أين اعتبر المشرع في المادة 31 منه استعمال تكنولوجيا الإعلام و الاتصال كظرف مشدد يرفع العقوبة إلى الحبس من 2 سنة إلى 5 سنة و الغرامة من 100.000 الى 300.000 دج ،بعد أن كانت في المادة 30 من نفس القانون الحبس من 6 أشهر إلى 3 سنوات و غرامة من 60.000 إلى 300.000 دج ،أما بالنسبة للقانون 04/09 فالملاحظ أن خطة المشرع في التجريم دون ضبط الجزاء لم

[1] إن الملاحظة التي يمكن رصدها في هذا المجال أن المشرع رغم تعميمه للتجريم من خلال الفقرة (أ) المادة 2 من قانون 09-04 لكنه في مجال الجرائم الإرهابية و التخريبية لم يكتفي بالقانون الخاص و إنما قام بالنص على هذه الحالة – استعمال التكنولوجيا في الجرائم الإرهابية و التخريبية – في قانون العقوبات باستحداث المادة 87 مكرر 11 إثر قانون العقوبات بقانون رقم 16-02

توضح مكانة التكنولوجيا إن كانت كظرف تشديد، و إن كانت القراءة توحي أن المشرع قد أدرجها من باب غلق أي فراغ قانوني و الدليل على ذلك أن المشرع لم يضبطها بجزاء و لم يحدد إن كانت كظرف مشدد

الخاتمة:

بسبب خطورة الجريمة المعلوماتية، طابعها العالمي، سهولة ارتكابها، تحرك المشرع الجزائري لضبط هذه الجريمة سنة 2004 من خلال تعديل قانون العقوبات باستحداث القسم السابع مكرر ، تضمن 8 مواد ، رسمت أركان هذه الجريمة و حددت عقوبتها ، غير أنه في سنة 2009 تفطن المشرع للفراغ الذي آثره تعديل 2004 منه أن عبارة الافعال الماسة بأنظمة المعالجة الآلية للمعطيات تنصرف إلى المعلومات و النظام الذي يحتويها فقط ، فتدخل للمرة الثانية من خلال توسيع مدلول الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و أعطى لها تعريف عام و شامل يغلق جميع المنافذ التي قد يلجأ إليها مجرمي الذكاء من بينها ارتكاب جرائم معروفة – الجرائم الاقتصادية و الجرائم الإرهابية – باستعمال المنظومة المعلوماتية أو نظام الاتصالات الإليكترونية ، غير أنه و إن كان التوسع في التجريم باستعمال عبارات عامة و شاملة هو الاتجاه الذي سارت فيه جل التشريعات لمواجهة تداعيات التطور التكنولوجي على أمن المجتمع و استقراره ، غير أن التسرع في هذا الاتجاه يكون له تداعياته أيضا على متطلبات الدقة و الوضوح في مبدأ شرعية التجريم

لذلك و من أجل الموازنة بين المصلحتين نقترح استدراك النقطتين الاتيتين :

1. نقل مضمون المادة 2 فقرة (أ) من قانون 09-04 إلى قانون العقوبات لكون هذا الأخير هو الأصل و المرجع العام في ضبط القواعد العامة لجميع الجرائم و حتى يتحقق نوع من الوضوح الذي يتطلبه مبدأ الشرعية
2. تحديد مكانة تكنولوجيا الاعلام و الاتصال كظرف مشدد خاصة في الجرائم الإرهابية و الجرائم الإقتصادية

قائمة المراجع

الكتب:

- عبد الله أوهايبية، شرح قانون العقوبات الجزائري، القسم العام، موفم للنشر، الجزائر، 2015
- أحسن بوسقيعة، الوجيز في القانون الجزائي العام ، الطبعة 16، دار الهومة، الجزائر، 2017
- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 1، دار الثقافة للنشر و التوزيع، الاردن، 2010
- عفيفي كامل عفيفي، جرائم الكمبيوتر و حقوق المؤلف و المصنفات الفنية و دور الشرطة و القانون ، دراسة مقارنة، منشورات الحلبي الحقوقية، 2003
- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية و تطبيقية، الطبعة الاولى، منشورات حلبي القانونية، مصر، 2005
- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية ، الطبعة الاولى، منشورات حلبي الحقوقية، لبنان، 2012

مقالات:

- محمد بن أحمد علي المقصودي، الجرائم المعلوماتية: خصائصها و كيفية مواجهتها قانونيا، المجلة العربية للدراسات الامنية ، المجلد33، العدد 70، السعودية، 2016
- علا كريمة، عادل بوزيدة، تحولات مبدأ الشرعية في ظل عولمة النصوص الجزائية، مقال غير منشور، الجزائر، دون سنة

رسائل دكتوراه و ماجيستير:

- عبد القادر عميمر، آليات إثبات الجريمة المعلوماتية في التشريع الجزائري (دراسة مقارنة) ،أطروحة لنيل شهادة الدكتوراه في القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2020
- أومدور رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة دكتوراه في القانون الخاص،كلية الحقوق، جامعة برج بوعريريج، الجزائر، 2021/2020
- نعمان عبد الكريم، الجرائم الإلكترونية و موقف المشرع الجزائري منها، رسالة ماجيستير في القانون الجنائي، كلية الحقوق ،جامعة الجزائر 1، الجزائر، 2017/2016

ملتقيات دولية

- فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربى حول القانون والمعلوماتية المزمع عقده بأكاديمية الدراسات العليا بليبيا فى أكتوبر 2009، كلية الحقوق و العلوم السياسية، جامعة زيان عاشور الجلفة

المداخلة كاملة

اللقب: مالك

الاسم: نسيمة

الدرجة العلمية: أستاذة محاضرة أ

المؤسسة: كلية الحقوق جامعة الجزائر 1

العنوان الالكترونيnassimamelek@gmail.com:

لغة المداخلة: اللغة العربية

عنوان الملتقى: القانون الجنائي في ظل التطور التكنولوجي -إشكالات ومعالجات-

عنوان المحور: أثر استخدام التكنولوجيا الحديثة على أحكام التشريع

عنوان المداخلة: تأثير تكنولوجيات الإعلام والاتصال على حق المؤلف

مقدمة:

ان الفضاء الافتراضي أدى الى تزايد حدة التواصل بين الأشخاص وتقاسم المحتويات بمختلف أنواعها، تلك التي تتضمن منتجات فكرية محمية مثل المنتجات الأدبية المكتوبة والمنتجات الموسيقية والمنتجات السينماتوغرافية، خاصة بعد تطور وسائل إنتاجها من الصيغ التقليدية الى صيغ حديثة تقوم أساسا على التقنية المعلوماتية، فأصبحت في شكلها المعلوماتي قابلة للمعالجة والتراسل والعرض عبر الأنظمة المعلوماتية وهو ما يشكل اعتداءات تجرمها القوانين التي تحمي حقوق المؤلف.

من بين مظاهر الجرائم الماسة بحقوق الملكية الفكرية في الفضاء الافتراضي هناك عملية تقليد المصنفات الفنية والأدبية وترويجها حيث أصبحت شبكة الانترنت تشكل فضاء مثالي لإيجاد مصنفات فنية، خاصة الموسيقى والأفلام وهي أعمال فنية محمية بموجب قانون حقوق التأليف غير أن تكنولوجيات الاتصال منحت لمستعمليها سهولة نسخ هذه المصنفات دون مراعاة حقوق المؤلف فأنتشرت المواقع التي تعرض المصنفات الفنية التي فتحت المجال للتحميل والترويج لأغراض تجارية.

وحسب الاحصائيات الواردة من الديوان الوطني لحقوق المؤلف والحقوق المجاورة[1] وصل حجم الاعتداء على حقوق المؤلف الى مستوى كبير بسبب تطور وانتشار استعمال تكنولوجيات الإعلام والاتصال بالموازاة مع عدد المشتركين في خدمات الانترنت وهي ظاهرة إجرامية ظهرت مسبقا في الدول المتطورةمن حيث تكنولوجياالاتصالات، حيث تشير المعطيات المتداولة الى ما يقارب 45000 فيلم سينمائي يتم تحميله بطريقة غير مشروعة يوميا[2].

كما ظهرت منظمات إجرامية تقوم بنسخ الأفلام والبومات الموسيقى وإعادة بيعها، اما على أقراص مضغوطة واما من خلال مواقع تنشأ لهذا الغرض ويتم دفع مستحقاتها عن طريق الدفع الالكتروني[3]وهناك من يقومون بأفعال التحميل غير المشروع لأغراض شخصية واستعمال المصنفات[4] peer to peerبتقنية .

ان المظاهر الاجرامية الماسة بحقوق الملكية الفكرية يتم معالجتها من الناحية القانونية من عدة زوايا الا ان معالجتي للموضوع يقتضي التركيز على المسائل التي تستدعي تكييف التشريع الساري قبل ظهور الفضاء الافتراضي مع الواقع الذي خلفه دخول عنصر تكنولوجيات الاتصالات على الجرائم التقليدية.

في هذا السياق سوف أتناول مسألة تأثير تكنولوجيا الاتصالات على حقوق الملكية الفكرية بالنظر الى عنصرين أولهما ان هذه التكنولوجيات قد انتجت منتجات تكنولوجية لم تكن موجودة من قبل وأصبحت محل اعتداء على الحقوق المرتبطة بها وبالتالي وجب تصنيفها كمؤلفات فكرية بهدف حمايتها على أساس أنها أفكار، أما العنصر الاخر فيتمثل في كون تكنولوجيا الاتصالات منحت فرص لم تكن موجودة من قبل للاعتداء على المؤلفات الفكرية مما يستدعي النظر في مدى نجاعة تدابير الحماية الجزائية في شقها الموضوعي من الاعتداء على حقوق المؤلف في البيئة الرقمية التي خلقتها تكنولوجيات الاعلام والاتصال.

وعلى هذا الأساس يتم التطرق الى تصنيف المنتجات المتولدة من المعلوماتية كمؤلفات فكرية، وبعدها سوف أتطرق الى حماية المؤلفات الفكرية في البيئة الرقمية.

---

[1] onda

[2] المركز الوطني للسينماتوغرافيا الفرنسي، معلومات لدى .Myriam Quemener et JoelFrery-cybercriminalité ,2eme edition Economica,Paris,2009,p.194.

[3] Marcha Cadogan et KonstantiaKoutouki,evolution des cas relatifs à la proprietè intellectuelle en 2019 et implications pour l avenir des droits de proprietè intellectuelle dans le monde, revue les cahiers de propriètè intellectuelle , èdition Yvon Blais,Canada, volume32 n02, mai 2020

[4] P2Pالمقصود من جهاز الى جهاز للدلالة على نظام الاتصال بين الأجهزة المرتبطة عبر الانترنت لتقاسم الملفات للمزيد حول ظاهرة تقاسم المصنفات الفنية عبر هذه التقنية.
https://www.etudier.com/dissertations/Telechargement-illegal/45940824.html

المبحث الأول: تصنيف المنتجات المعلوماتية كمؤلفات فكرية

تعد المنتجات المعلوماتية كل المخرجات التي تتولد عن عملية المعالجة الآلية للمعطيات وهو مفهوم واسع، غير أن الاعتداء المعنوي عليها لا يتحقق الا باعتبارها من الأفكار وفي هذه الحالة يتوجب حمايتها بموجب قوانين الملكية الفكرية، لأجل ذلك فإن حماية المنتجات المعلوماتية من الاعتداءات المعنوية تقتضي تصنيفها ضمن المؤلفات الفكرية.

المطلب الأول: موقف التشريعات من تصنيف المنتجات المعلوماتية

اتجهت الأنظار في مسألة حماية المنتجات المعلوماتية في الفقه الى براءة الاختراع[5]كوسيلة من وسائل الحماية، خاصة بالنسبة لبرامج الحاسوب،غير أن هذا الطرح لم يستقم ولم يجد التجاوب اللازم في التشريعات المختلفة التي استبعدت برامج الحاسوب والمنتجات الشبيهة من هذا المجال لكون هذه الأخيرة لا تتوفر على شروط البراءة، اذ انها عبارة عن أفكار موجودة وشائعة الاستعمال يتم التعبير عنها بطريقة جديدة مع اتباع الأسس التي وضعها مخترع الحاسوب، فمن الصعب تطبيق عناصر براءة الاختراع على المكونات غير المادية للحاسوب أي عنصري الجدة والقابلية للاستغلال الصناعي فشرط الجدة يقتضي ان يعكس البرنامج تطبيق جديد للخوارزميات في حين ان الخوارزميات هي كالأفكار يحق للجميع استغلالها مع ابتعاد البرنامج عن المدلول المادي الذي يقتضيه شرط الاستغلال الصناعي. على هذا الأساس استبعد البرنامج في أغلب التشريعات من مجال براءة الاختراع.

في مقابل هذا الطرح أجمع الفقه على اعتبار حقوق المؤلف بأنها الوسيلة الأنسب لفرض حماية جزائية على المنتجات المعلوماتية، وهو ما سأتطرق اليه من خلال أحكام التشريع الوطني(الفرع الأول) ثم القانون المقارن(الفرع الثاني).

الفرع الأول: في التشريع الوطني

تناول المشرع الجزائري النظام القانوني لحقوق المؤلف من خلال الأمر 03-05 المؤرخ في 19-07-2003 المتعلق بحقوق المؤلف والحقوق المجاورة حيث ينص في المادة 04 ضمن الفصل الأول بعنوان المصنفات المحمية، على أن برامج الحاسوب تعتبر من المصنفات المحمية كما ينص في المادة 05

---

[5]عرف المشرع الوطني براءة الاختراع في المادة 2-2من الامر 03-07 المتعلق ببراءة الاختراع بأنها "وثيقة تسلم لحماية اختراع" فهي شهادة تمنحها الدولة للمخترع تثبت له حق احتكار استغلال اختراعه ماليا لمدة معينة وتنص المادة 03منه على ما يلي: يمكن ان تحمي بواسطة براءة الاختراع الاختراعات الجديدة والناتجة عن نشاط اختراعي والقابلة للتطبيق الصناعي". كما عرفت المحكمة الإدارية المصرية الاختراع الجدير بالحماية بأنه: " تقديم شيء جديد للمجتمع لم يكن موجودا من قبل وقوامه أو مميزه أن يكون ثمرة فكرة ابتكارية أو نشاط ابتكاري يتجاوز الفن الصناعي القائم أو التعديلات الجزئية غير الجوهرية التي لا تغيب عن رجل الصناعة المتخصص في حدود المعلومات الجارية والتي هي وليدة المهارة الحرفية وحدها حسب قرار المحكمة الإدارية المصرية العليا المؤرخ في 03-04-1965 منشور بمجموعة المبادئ القانونية التي قررتها المحكمة الإدارية العليا رقم 80-ص.11.

منه، بأنه تعتبر أيضا من المصنفات المحمية قواعد البيانات (دون ان يعطي تعريفا لبرنامج الحاسوب أو قواعد البيانات) فمن خلال إدراج برامج الحاسوب وقواعد البيانات صراحة ضمن قائمة المصنفات الأدبية أو الفنية المشمولة بالحماية، يكون التشريع الجزائري قد حسم مسألة تصنيف المنتجات المعلوماتية التي حصرها في برامج الحاسوب وقواعد البيانات وخصها بالحماية المقررة بموجب حقوق المؤلف.

الفرع الثاني: في القانون المقارن

اختلفت التشريعات الغربية حول مسألة حماية برامج الحاسوب مما دفع بالقضاء الى تقدير هذه الحماية على أساس القواعد العامة لذلك عرفت أحكام القضاء تذبذب بين إقرار الحماية لبرامج الحاسوب باعتبارها من المصنفات الأدبية وبين انكارها وهذا الى غاية مطلع التسعينات أين بدأت تتجلى فكرة الحماية المقررة لبرامج الحاسوب في القوانين. ففي أوروبا صدرت التوجيهية[6]

250/91 المؤرخة في 1991/05/14 عن مجلس اتحادات أوروبا المتضمنة إقرار الحماية القانونية لبرامج الحاسوب بموجب حقوق المؤلف وكذلك التوجيهية[7]

9/96 المؤرخة في 1996/03/11 عن البرلمان الأوروبي المتضمنة إقرار الحماية القانونية لقواعد البيانات بموجب حقوق المؤلف كذلك، فعملت الدول الأوروبية على إفراغ أحكام هذه التوجيهات في قوانينها الداخلية المعنية بحماية حقوق المؤلف.

تطبيق لتلك التوجيهات قام المشرع الفرنسي بتعديل قانون الملكية الفكرية حيث أدرج ضمن المصنفات المحمية برامج الحاسوب في المادة 2-112ل وقواعد البيانات في المادة 3-112 ل معتبرا إياها من الأعمال الفكرية.

كما سارعت الدول العربية في مصر، الامارات، الأردن، المغرب وتونس الى تعديل قوانينها لمسايرة التطورات التكنولوجية التي عرفها العالم وانعكاساتها على القانون، ففي مصر تم تعديل قانون الملكية الفكرية سنة 1994 بإدراج برامج الحاسوب وقواعد البيانات ضمن المصنفات الفكرية، أما في الامارات صدر القانون الاتحادي رقم 40 لسنة1992 المتعلق بالمصنفات الامريكية وحقوق المؤلف الذي أدرج برامج الحاسوب ضمن المصنفات المحمية.[8]

---

[6]Directive du conseil des communautèseuropèenes n 91/250 www.legifrance.gouv.fr le 25/11/2021

[7] Directive du parlement europèen et du conseil, n96/9www.legifrance.gouv.fr le 25/11/2021.

[8]بن لخضر محمد، حماية برامج الحاسوب وقواعد البيانات في القانون الجزائري والقانون المقارن، مجلة القانون، جامعة غليزان، مجلد 6عدد2، 2018، ص.86.

والمغرب هو الاخر أضاف قانونها المتعلق بحماية حقوق المؤلف الصادر في 18-05-2000، برامج الحاسوب الى قائمة المصنفات الفكرية المحمية بموجب المادة 3وقواعد البيانات في المادة 5 منه.

\اما على الصعيد الدولي، قد اهتمت المنظمة العالمية لحقوق المؤلف بموضوع حماية المنتجات المعلوماتية حيث وضعت اتفاق خاص ضمن اتفاقية برن لحماية المصنفات الأدبية والفنية، الا وهو معاهدة الويبو بشأن حقوق الملف التي صدرت سنة 1996 وبدأت سريانها في 06 مارس 2002، هذه المعاهدة اعتنت بحماية المصنفات وحقوق مؤلفيها في البيئة الرقمية، كما أضافت الى قائمة المصنفات المحمية، برامج الحاسوب وقواعد البيانات، إذ تنص في المادة 04 منها بأن برامج الحاسوب تتمتع بالحماية باعتبارها مصنفات أدبية بمفهوم المادة 02 من اتفاقية برن، في حين تنص المادة 05 على حماية قواعد البيانات.

المطلب الثاني: العناصر الجديرة بالحماية القانونية في المنتجات المعلوماتية

لقد تم تصنيف المنتجات المعلوماتية لأغراض هذا البحث الى منتجات معلوماتية تطبيقية وهي البرامج والتطبيقات ومنتجات معلوماتية غير تطبيقية وهي قواعد البيانات والمواقع الالكترونية، لتبيان العناصر الجديرة بالحماية القانونية في هذه المنتجات التطبيقية (الفرع الأول) ثم في المنتجات غير التطبيقية (الفرع الثاني).

الفرع الأول: المنتجات المعلوماتية التطبيقية

لم تعرف التشريعات أغلبها العمل الفكري ومنها التشريع الجزائري التي اكتفت بإعطاء قائمة الأعمال التي تندرج ضمن هذا الصنف ومنها المصنفات الأدبية ومصنفات المسرح والمصنفات الدرامية والمصنفات الموسيقية والسينمائية وبرامج الحاسوب ...وهذا بنص المادة 04 و05 من الامر 03-05 السابق الذكر والمتعلق بحقوق المؤلف والحقوق المجاورة، وقد نصت المادة 03 من نفس الأمر بأنه تمنح الحماية مهما يكن نوع المصنف ونمط تعبيره ودرجة استحقاقه ووجهته بمجرد ايداعه.

فكيف يتم حماية برامج الحاسوب، قبل ذلك ما هو مفهوم برنامج الحاسوب؟

لا يوجد مسمى خاص بالبرنامج المعلوماتي في اللغة العربية على عكس اللغة الإنجليزية التي تعبر عنه بمصطلح " software%

للدلالة على الكيان غير المادي للحاسوب وهو المصطلح الذي يقابله باللغة الفرنسية "logiciel"

فمن الناحية اللغوية نجد برنامج الحاسوب هو المصطلح الأكثر استعمالا للدلالة على المصطلح الإنجليزي " software"

حيث يعرف بأنه " مجموعة تعليمات مرتبة ترتيبا معينا ومكتوبة بلغة الحاسوب لحل مسألة أو مشكلة معينة[9]

تعرف المراجع التقنية برنامج الحاسوب بأنه: " سلسلة من التعليمات القابلة للتنفيذ المباشر من طرف الحاسوب[10]

كما ورد تعريفه أيضا ضمن قرار صادر بالجريدة الرسمية الفرنسية حول المصطلحات المرتبطة بمجال المعلوماتية بأنه " مجموعة البرامج والعمليات والقواعد والوثائق إن وجدت المتعلقة بمجموع معالجات المعلومات[11]

غير ان هذا التعريف و ان كان لا يطرح إشكال من الناحية التقنية فإنه بالنسبة للقانونيين لا يفي بالغرض الذي تتطلبه الدراسة القانونية، اذ لا بد من البحث عن التعريف الذي يأخذ بعين الاعتبار العناصر القانونية التي تجتمع في البرنامج المعلوماتي باعتباره منتوج فكري جدير بالحماية.

عرفت المنظمة العالمية للملكية الفكرية برنامج الحاسوب بأنه مجموعة من التعليمات المعبر عنها بكلمات أو برموز أو برسوم أو بأي طريقة أخرى، تمكن حينما تدمج في دعامة قابلة لفك رموزها بواسطة آلة أن تنجز أو تحقق مهمة محددة أو تحصل على نتيجة بواسطة حاسوب أو بأي طريقة الكترونية قادرة على معالجة معطيات[12]

من جهتها نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 2 منها المخصصة للمصطلحات أن : " البرنامج المعلوماتي هو مجموعة من التعليمات والأوامر قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما".

أما الفقه فقد تباين في تعريفه لبرامج الحاسوب إذ عرفه الأستاذ محي الدين بن عكاشة بأنه مجموعة التعليمات المعبر عنها بمفردات أو بدائل أو بمخططات أو بأي شكل آخر والتي تمكن من القيام بنشاط

---

[9] معجم مصطلحات الحاسبات، مجمع اللغة العربية بالقاهرة، 2012، ص.122.

[10] Alain Hollande et Xavier Linant de Bellefonds, pratique du droit de l informatique et de l internetK 6 edition Delmas, Dalloz, France,2008, p.256 parg 1001.

[11] قرار صادر في 1981/12/22 حول إثراء مصطلحات المعلوماتية الجريدة الرسمية الفرنسية، 1982/01/17.

[12] https ;//wipopearl.wipo.int/12/12/2021.

علمي أو نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم باندفاعات إلكترونية أو أي أسلوب الكتروني آخر أو ما يشبه ذلك بشرط أن يكون صالحا لمعالجة الاعلام[13]

كما عرفه جانب من الفقه بانه تعليمات مكتوبة بلغة ما موجهة الى جهاز تقني معقد يسمى الحاسب الالكتروني بغرض الوصول الى نتيجة معينة[14]

من خلال التعاريف على سبيل الاستدلال يتبين ان الإحاطة بمفهوم برنامج الحاسوب تثير إشكالية تعريف الحاسوب في حد ذاته، لكون الحاسوب هو الحيز الذي يسري فيه البرنامج، ومنه التساؤل ان كان الحاسوب المقصود لتحديد مفهوم البرنامج هو الحاسوب بالمفهوم الشائع أم ان الامر يتعلق بمفهوم أوسع ليشمل أجهزة أخرى، بعبارة أخرى هل البرنامج يتعلق بالحاسوب فقط ام انه يمتد الى أجهزة أخرى شبيهة

ان الحاسب الالي هو وسيلة تقنية تقوم بإنجاز العمليات الحسابية المعقدة تتكون من كيان مادي يضم وحدات ادخال ووحدات اخراج للمعطيات وكيان غير مادي يتكون من المعطيات والبرامج التي تقوم بوظيفة المعالجة ، كما أن التطور الذي عرفته التقنية المعلوماتية جعلت الحاسب الآلي يتطور من شكله التقليدي إلى أشكال أخرى مما دفع الى تحديث المفاهيم الكفيلة باستيعاب هذا التطور، لذلك شاع مصطلح نظام المعالجة الآلية للمعطيات كبديل لمصطلح الحاسب الالي ، فالحاسب الالي هو عبارة عن نظام يقوم بالمعالجة الآلية للمعطيات بواسطة برنامج

فالبرنامج هو جزء من الكيان غير المادي لأي نظام للمعالجة المعطيات بصفة آلية وهو عنصر أساسي فيه أي انه لا وجود لنظام المعالجة الآلية للمعطيات بدون برنامج والا أصبح مجرد كومة من المعدات المادية [15]وهو البرنامج الذي يرشد الحاسوب الى كيفية تأدية الوظائف المنوطة به[16]

لا بد من التنويه الى ان البرامج تختلف بحسب الغاية التي تحققها لذا نجدها تنقسم الى ثلاث فئات، هي:

برامج التشغيل وهي التي تحدد كيفية وطريقة عمل الحاسوب أو النظام المعلوماتي، فهي برامج تسمح بإقامة التواصل بين الانسان والآلة الحاسوب ومن الأمثلة برامج الحواسيب windows et Linuxلتشغيل أو لتشغيل الهواتف النقالة واللوحات الالكترونية Android

[13]محي الدين عكاشة، حقوق المؤلف على ضوء القانون الجزائري الجديد، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، 2005، ص.75.
[14]رشا عي الدين، النظام القانوني لحماية البرمجيات، دار الجديدة للنشر، الإسكندرية،2007، ص12.
[15]عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، الطبعة الثانية، بيروت، 2007، ص25.
[16] www.futura-sciences.com/tech/definitions/informatique-logiciel-16/11/2021.

البرامج التطبيقية وهي برامج تسمح بإنجاز وظائف تكميلية غير مدرجة في نظام التشغيل مثل وظيفة الارتباط بالأنترنت التي تحتاج تطبيقة تصفح أو متصفح أنترنت مثل internet explorer ou mozilafirfox.

هذه البرامج تحتاج لتشغيلها الى وجود برنامج التشغيل الذي يقبلها ((compatible

البرامج المهنية وهي برامج تطبيقية أيضا لكنها ليست مخصصة لتأدية وظائف عامة يحتاجprogiciels

عموم المستعملين وانما هي مخصصة لتأدية وظائف ذات طابع مهني في مجال محدد حيث يتم تصميم هذه النوع من البرامج بناء على طلب المستعمل ومن الأمثلة على ذلك برامج الرسم المعماري وبرامج تسيير المعطيات الطبية وغيرها.

الفرع الثاني: المنتجات المعلوماتية غير التطبيقية

تتضمن المنتجات المعلوماتية غير التطبيقية قواعد البيانات والمواقع الالكترونية

أولا: قواعد البيانات

ان العالم الافتراضي جعل التعامل بالبيانات امرا ضروريا مما أدى الى الاستثمار في انشاء وتطوير البيانات من طرف شركات متخصصة في المعلوماتية، فهذه الأخيرة أصبحت تعتمد على قواعد البيانات في نشاطاتها بما توفره للمستخدم من السرعة في الحصول على المعلومات.

ان قواعد البيانات توفر القدرة على تخزين كمية كبيرة من المعلومات أو البيانات دون الحاجة الى أماكن للتخزين بل يتم تخزينها في دعامة لا يتعدى حجمها بعض السنتيمترات مكعب ولا يزيد وزنها عشرات الغرامات، بالإضافة الى توفير عدة طرق لتصنيف المعلومات المخزنة فيسهل في البحث عن المعلومة، والأهم من ذلك هو إمكانية الولوج الى قاعدة المعطيات عن بعد من خلال الشبكات المعلوماتية فيضع المعلومات في تناول المستخدم أينما كان.

وأصبحت الحاجة الى قواعد البيانات أمرا حتميا فأدى الى التطور السريع في الاستثمار مما أدى بالشركات المستثمرة تطالب بحماية منتجاتها التي تعتبر منتجات فكرية جديرة بالحماية القانونية.

لقد أدرجت أغلب التشريعات قواعد البيانات من بين المصنفات المحمية بموجب حقوق المؤلف، وعليه نتطرق الى مفهوم قاعدة البيانات ثم شروط الاستفادة من الحماية القانونية.

1-مفهوم قواعد البيانات

تعد قاعدة البيانات كم من المعلومات المجمعة ضمن تنظيم معين يسمح باسترجاعها عند الحاجة وقد أصبحت في أيامنا قواعد البيانات منظمة كلها ضمن تشكيل معلوماتي.

لقد منحت التقنية المعلوماتية طرق مختلفة لهيكلة وتنظيم قواعد البيانات بشكل يسمح بتخزين كم هائل من المعلومات واسترجاعها عند الحاجة بسهولة.[17]

الا ان المشرع الجزائري لم يعرف قواعد البيانات في النص المشار اليه واكتفى بادراجها ضمن المصنفات المحمية، غير ان المادة 112-3 من قانون الملكية الفرنسي عرفتها بأنها مجموعة أعمال، معطيات، وعناصر مستقلة أخرى مشكلة بطريقة آلية أو منهجية ويمكن الولوج اليها فرديا عبر الوسائل الإلكترونية أو بأي وسيلة كانت[1918]

أما الاتفاق الافريقي المعدل لاتفاقية بانغاي فقد عرفها بأنها: " تجميع معطيات أو أحداث"

2- شروط الاستفادة من الحماية القانونية

أدرج المشرع الجزائري من خلال الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة في المادة 5 منه قواعد البيانات ضمن المصنفات المحمية على أساس انتقاء موادها أو ترتيبها، مع العلم ان القضاء الفرنسي قد أقر حماية قواعد البيانات كأعمال فكرية[20]

قبل إدراجها في التشريع الفرنسي بموجب القانون المؤرخ في 1998/07/01 المعدل لقانون الملكية الفكرية وفقا للمعيار الأوروبي.

كل قاعدة بيانات لكي تكون محل حماية يجب ان تتوفر فيها عنصري الانتقاء والترتيب الذي يعكس المجهود الإبداعي، حيث سبق في هذا الامر القضاء الفرنسي أن رفض الحماية القانونية لقاعدة بيانات تضم تجميع بسيط للبيانات[21]

---

[17] https://www.techno-science.net/glossaire-definition/Base-de-donnees.html le12/12/2021.

[18] Version originale : « On entend par base de données un recueil d œuvres,de données ou d autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessible par des moyens électroniques ou par tout autre moyen ».

[19] المادة 2 من الملحق 6 لاتفاق تعديل اتفاق بانغاي حول انشاء منظمة افريقية للملكية الفكرية في صيغته الأصلية باللغة الفرنسية
« une base de données est une compilation de données ou de faits ».

[20] Cassassplenière 30/10/1997 ;Courd appel Paris 4ème ch15/01/1997-jurisdata n 022369.

[21] TGI de compiègne 2/6/1989 droit et expertie du numérique, ibid, p.60.

سواء كان التنظيم الذي تتضمنه البيانات والذي يمثل عملية ابتكار أو المصنفات الفكرية لا بد ان يتوفر في قاعدة البيانات عنصر الابتكار لكي تحظى بالحماية والمتمثلة في بصمة مؤلف قاعدة البيانات والمتمثلة في مساهمته الإبداعية والفكرية التي تنعكس في اختيار وترتيب المواد التي تتضمنها قاعدة البيانات، في قرار لمحكمة الاستئناف بليل الفرنسية بحث القضاة في أصلية قاعدة البيانات المدعى حولها قبل الحكم في جريمة التقليد، مما دفعهم الى وضع العناصر التي يستخلص منها الابتكار وهي المخطط، التركيبة، الشكل، الهيكلة، اللغة، كما يشترط من المؤلف ان يترك مجهود شخصي يتجاوز مجرد التصميم الآلي.[22]

لقد تضمن المشرع الفرنسي حماية من طبيعة خاصة لمنتجي قواعد البيانات بموجب القانون الخاص بقواعد البيانات المنصوص عليه في المواد 1-341-1 و 2-341-1 من قانون الملكية الفكرية الذي يهدف الى حماية محتوى قاعدة البيانات باعتباره استثمار مالي ومادي وبشري وليس باعتباره عملا فكريا، يعلق الأمر بإضفاء حماية قانونية إضافية لقواعد البيانات تقوم على معيار الاستثمار المعتبر الذي باشره منتج قاعدة البيانات، بموجب هذا القانون يمكن لمنتج قاعدة البيانات الإعتراض على أخذ جزء أو كل المحتوى الذي تتضمنه قاعدة البيانات لتثبيته على دعامة أخرى، وكذا الاعتراض على إعادة استعمال عن طريق العرض على الجمهور لكل أو جزء هام من محتوى قاعدة البيانات[23]

ثانيا: المواقع الالكترونية

المواقع الالكترونية هي المكون الرئيسي لشبكة الانترنيت، يتكون أي موقع إلكتروني " السيت واب " من عدة صفحات ويب، فنجد صفحة رئيسية مرتبطة بصفحات أخرى تتضمن كل منها محتويات نصية، بيانية، سمعية، بصرية وغيرها من المحتويات ذات الشكل الرقمي.

لم ترد المواقع الالكترونية ضمن المصنفات المذكورة في المواد 4 و 5 من الأمر 03-05 المتعلق بحقوق المؤلف، فإدراجها ضمن المصنفات المحمية متوقف على اعتبارها عمل فني أو أدبي أصلي.

تنص المادة 4 من الأمر 03-05 على ما يلي: " تعتبر على الخصوص كمصنفات أدبية أو فنية....، مما يعني أن المصنفات المذكورة في هذه المادة ليست على سبيل الحصر وبالتالي تبقى القائمة مفتوحة إذ أن المعيار الذي يحدد هذه المصنفات هو ذلك الذي ورد في المادة 3 من نفس الأمر والتي تنص بأنه " يمنح كل صاحب إيداع أصلي لمصنف أدبي أو فني الحقوق المنصوص عليها في هذا الأمر"، وبالتالي

---

[22] قرار محكمة الاستئناف الفرنسية بليل المؤرخ في 2009/11/19.

[23] Hubert Bitan , droit et expertise du numérique, édit wolkerskluwer, Paris, 2015, p.93, n112.

فإن أي عمل فني أو أدبي يتميز بالأصالة يكون جديرا بالحماية التي يكفلها قانون حقوق المؤلف، فهل ينطبق هذا على المواقع الالكترونية؟

من خلال قرار محكمة النقض الفرنسية ان عنصر الابتكار يتم تقديره بصفة دقيقة، فعلى قضاة الموضوع البحث في مدى اعتبار الخيارات التي لجأ اليها المؤلف كمساهمة فكرية منه ومجهود شخصي وهي المعايير التي تمنح دون سواها صفة المصنف ذو الطابع الأصلي الجدير بالحماية، وهو نفس المبدأ الذي ينطبق على مواقع الانترنت.

ان ترتيب المحتويات المتضمنة في صفحات الويب وطريقة ربطها ببعضها البعض بطريقة مستوحاة من فكر مصمم الموقع يجعل من الموقع الالكتروني عمل ذهني مبتكر جذير بالحماية القانونية من منظور حقوق المؤلف[24]

فعلى قاضي الموضوع تقدير عنصر الابتكار في الموقع الالكتروني محل التقليد مما يستبعد فيه أوجه التشابه في ترتيب المحتوى حين تفرضه القيود العملية أو التقنية، كما ان الصفحات الرئيسية للمواقع تتقارب فيما بينها من حيث التصميم وطبيعة المحتويات التي تتضمنه لكونها تهدف الى تقديم المعلومات الأساسية لمتصفحي الموقع مثل التعريف بالموقع، توجيهات للمتصفح...الخ لذلك يخضع تصميم الصفحة الرئيسية الى هذه القيود مما يضيق من المجهود الشخصي والابداعي لمصمم الموقع.

ألغت محكمة النقض الفرنسية في قرار صادر في 2011/05/12 القرار الصادر عن محكمة الاستئناف القاضي بعدم قيام فعل تقليد موقع إلكتروني بسبب انعدام عنصر الابتكار في الموقع الالكتروني محل الدعوى وقد حيثت محكمة النقض قرارها بأن الحكم المستأنف لم يوضح كيف ان الخيارات التي لجأ اليها مصمم الموقع في جمع عناصر الموقع بشكل معين لا تعتبر ابتكارا[25]

وبعد إحالة نفس القضية من جديد أمام محكمة الاستئناف أقرت في قرارها الصادر في 2013/07/02 ان الموقع الالكتروني للشركة المدعية يتميز بالأصالة وان عنصر الابتكار فيه يتمثل في خيار دمج العناصر المكونة له بشكل معين لإبراز نوع من الجمالية دون أن يكون ذلك ناتج عن القيود التقنية، مما أعط للموقع مظهر خاص يميزه عن مواقع إلكترونية أخرى تتعلق بنفس مجال النشاط الشيء الذي يعكس جهدا ابداعيا.[26]

---

[24] Alain Hollande et Xavier Linant de Bellefonds, pratique du droit de l informatique et de l internet 6eme édition, Delmas, France, 2008,p.282n1075.

[25]Casscrim du 12/05/2011 n10-17852. www.legifrance.com

[26]Cour d appelVerssailles, 12eme ch-02/07/2013 www.legalis.net

المبحث الثاني: حماية حقوق المؤلف في البيئة الرقمية

أدت تكنولوجيا الاتصالات الى سهولة الحصول على المؤلفات الفكرية بكافة أنواعها، بسبب خاصية الاستنساخ التي لا تتطلب أي مجهود أو تكلفة مادية، حيث يمكن نسخ عدد غير متناهي من الملفات المكتوبة أو السمعية البصرية حين تكون في صيغة مرقمة، الأمر الذي يفسر رواج المؤلفات الفنية والأدبية عبر شبكة الانترنت التي تنشر دون موافقة مؤلفيها[27]، الأمر الذي يدعو الى ان نتساءل عن مدى كفاية التدابير الجزائية الموضوعية الخاصة بتجريم انتهاكات حقوق الملكية الفكرية، لردع هذه الأفعال في ظل الفضاء الافتراضي.

وقد اختلف الفقه حول طبيعة حقوق المؤلف مما أدى الى ظهور نظريات مختلفة، فبرز تيار فقهي يعتبر حقوق المؤلف من الحقوق الشخصية في حين اعتبرها تيار آخر حق ملكية، كما اعتبرها تيارا حق من طبيعة مختلطة بمفهوم ان حق المؤلف ليس حقا واحدا وانما ينقسم الى حدين احدهما مالي والأخر ادبي، حيث وافقت محكمة النقض الفرنسية هذا التوجه في قرارها المعروف بقرار "لوكوك" الذي جاء فيه أن حق المؤلف يتكون من عنصرين هما حق في الاستغلال المالي الذي يتقرر للمؤلف ولأسرته بعد وفاته والحق الأدبي الذي يتضمن الامتيازات ذات الطبيعة الشخصية والأدبية[28].

وبذلك فإن الحماية التي يكفلها قانون الملكية الفكرية للمؤلفين، تتضمن تجريم المساس بالحقوق المالية.

المطلب الأول: حماية الحقوق الأدبية لمؤلف المنتجات المعلوماتية

اعتبر الفقه اللاتيني الحقوق الأدبية على انها حقوق شخصية باعتبارها لصيقة بالحقوق الشخصية التي تهدف الى حماية الشخص في كيانه كحقه في الحياة وسلامته الجسدية أو حمايته معنويا كالحق في الاسم والحق في الصورة وحماية حرمته، محلها الشخص نفسه فهي تثبت للإنسان بمجرد اكتسابه الشخصية القانونية لذلك تنتفي الطبيعة المالية عن هذه الحقوق فلا يمكن ان تكون محلا للتداول ولا تسقط بالتقادم ولا تنتقل الى الورثة بوفاة صاحب الحقوق.

عرف بعض الفقهاء ان الحق الادبي هو:" تعبير عن العلاقة الوثيقة القائمة بين المصنف ومؤلفه " ومن ثم فإن هذا الحق يخول للمؤلف سلطات متعددة منها سلطة تقرير نشر المصنف أو رفضه في حياته

---

[27] عبد الكريم نعمان، الجرائم الالكترونية وموقف المشرع الجزائري منها، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر 1، 2017، ص.54.

[28] حسن جميعي، مدخل الى حقوق المؤلف والحقوق المجاورة، ورقة بحثية مقدمة في حلقة الويبو التمهيدية حول الملكية الفكرية، المنظمة العالمية للملكية الفكرية ويبو ووزارة التجارة المصرية، القاهرة، مصر، 2004/10/10، رقم الوثيقةCAI/IP/WIPO//04/1 ص4.

ونسبته اليه وإدخال تعديلات على مصنفه وسحبه من التداول ان لزم الأمر ومعارضة الاعتداء عليه أو انتحاله من قبل الغير حفاظا على سمعته أو شهرته الأدبية أو العلمية أو الفكرية[29].

ينص المشرع الجزائري بموجب الأمر 03-05 ان الحق المعنوي للمؤلف يتضمن حق الكشف، حق التوبة، حق احترام سلامة المؤلف وحق سلامة المؤلف وحق وضع الاسم.

وعلى هذا الأساس سيتم التساؤل عن مدى تطبيق هذه الحقوق على المصنفات في البيئة الرقمية.

الفرع الأول: حق السيطرة الأدبية

يشمل حق السيطرة الأدبية على قدرة المؤلف على التحكم في الكشف عن مؤلفه وإمكانية العدول والتعديل والذي يسمى حق التوبة.

أولا: حق الكشف

ان ظهور تكنولوجيات الاعلام والاتصال أدت الى ابتكار أنواع جديدة من المصنفات والتي تكون في شكل رقمي منذ نشأتها مثل المصنفات التقليدية التي يمكن تحويلها بعد انشاءها الى شكل رقمي ونشرها عبر الوسائط الرقمية.

ان الشكل الرقمي للمصنفات قد يحد من حق المؤلف في الكشف عن مصنفه حيث أعطت تكنولوجيات الاتصال والاعلام الفرصة لنشر المصنفات بشكل خارج عن السيطرة بالنظر الى إمكانية الحصول على نسخ رقمية من المصنف ونشرها عبر شبكة الانترنت دون قيد وبدون حاجة للحصول على موافقة المؤلف، بالإضافة الى ان المصنفات الرقمية بكل أشكالها هي بطبيعتها رقمية وحتى التي تم تحويلها من شكلها التقليدي الى شكل رقمي مما يلزم المؤلف الى الاعتماد على متعامل يتقن التعامل بتكنولوجيات الاعلام والاتصال من اجل القيام بالجانب التقني لإعطاء المصنف شكله الرقمي وجعله قابل للنشر على الوسائط التكنولوجية مما يجعل المؤلف خاضعا لشروط المفروضة من المتعامل التقني المتعلقة بطريقة وتوقيت نشر المؤلف بما يسمح له بتحقيق مردودية لاستثماراته التقنية وبالتالي سيقلص من الحق الادبي للمؤلف المتمثل في التحكم لوحده في تقرير وكيفية وتوقيت اتاحة المؤلف للجمهور[30]

ثانيا: حق التوبة

---

[29] عبد المجيد زعلاني، المدخل لدراسة القانون النظرية العامة للحق، دار هومة، الجزائر، 2010، ص*.34.

[30] رامي إبراهيم حسن الزواهرة، النشر الرقمي للمصنفات وأثره على الحقوق الأدبية والمالية للمؤلف، الطبعة الأولى، دار وائل للنشر والتوزيع، الأردن، 2013، ص.344.

يتمثل حق التوبة في حق المؤلف أن يقرر سحب المصنف من التداول أو تعديله حين يظهر له بعد مدة من نشر المؤلف ولأسباب أدبية أن أفكاره قد تغيرت ولم يعد مصنفه معبرا عن آرائه ومعتقداته وان استمراره قد يسيء لسمعته فيقوم بتعديله أو سحب المصنف من التداول، الا ان سحبه أو تعديله بعد نشره عبر الفضاء الافتراضي يصبح عائقا له مما يجعل النصوص القانونية التي تنص على هذا الحق غير قادرة على حل هذا العائق.

ان نشر المؤلف عبر تكنولوجيات الاعلام والاتصال يجعله المصنف متداول وتعديله وإعادة نشره قد لا يؤدي الغرض المرجو وهو تصحيح الأفكار التي تعكس شخصية المؤلف لان نشره معدل قد يعتبره القراء نفس المصنف السابق وبذلك لا يحقق الغرض المرجو، وبهذا أقر المشرع الفرنسي تفويض حق التوبة لمؤلف برنامج الحاسوب بالنظر الى خصائص هذا النوع من المصنفات وماتقتضيه متطلبات استغلاله مثلما نصت عليه المادة 7-121ل من قانون الملكية الفكرية الفرنسي.

الفرع الثاني: حق احترام سلامة المصنف

يقتضي حق احترام سلامة المصنف ان لا يتعرض المصنف الى أي تعديل دون موافقة صريحة من المؤلف، كما لا يوضع المصنف محل تغيير وهو حق مخول للمؤلف للدفاع عن حقه في دفع أي اعتداء عل مصنفه متمثلا في الاقتباس أو التحوير أو التحريف بما يجعل هذا الحق متصفا بالصبغة العلاجية وليس فقط الوقائية[31].

وبموجب هذا الحق اعتبر القضاء الفرنسي ان تسجيل موسيقى على قرص DVD بنوعية رديئة يعتبر إساءة لحق المؤلف في احترام مصنفه، كما اعتبر ان تسجيل أغنية في شكل رنة هاتف هو كذلك إساءة لحق المؤلف في احترام مصنفه، كما اعتبر ان تسجيل اغنية في شكل رنة هاتف هو كذلك إساءة لحق المؤلف في احترام سلامة مصنفه، مثلما قضت به محكمة باريس في حكم صادر في 2001/10/11في قضية[32].MC Solaar

أكدت محكمة الاستئناف الفرنسية على أنه في حالة الإساءة الى المصنف حتى ولو كانت غير مادية فهي انتهاك لحق المؤلف، مثل: كأن يتم نشر المصنف ضمن موقع الكتروني ذو بعد سياسي مخاف تماما لتوجه المؤلف أو بدون اذنه أو في موقع إباحي.

المطلب الثاني: حماية الحقوق المالية لمؤلف المنتجات المعلوماتية

[31]Papa Assane Toure, le traitement de la cybercriminalité devant le juge,éditl harmattan, PARIS, 2014, P250.
[32] Papa Assane Toure, ibid, p.251.

لقد عرف الفقه الحق المالي بأنه ذلك الحق الذي يعبر عن الاعتراف للمؤلف بإمكانية الحصول على نصيب معقول من العائد المالي المتحصل عليه من انتفاع الجمهور بمصنفه[33]، كما نص المشرع الجزائري من خلال الأمر 03-05، في المادة 27، أنه يحق للمؤلف استغلال مصنفه بأي شكل من أشكال الاستغلال والحصول على عائد مالي منه.

من هذا النص يمكن الجزم على أن المؤلف له الحق في استغلال مصنفه ماليا وبها فهو يتمتع باحتكار استئثاري على كافة متحصلات استغلال مصنفه بما نص عليه القانون، فيتسم هذا الحق بكونه من حقوق الملكية فيتميز بخصائص متعددة، من حيث عدم قابلية الحجز عليه وكونه حق مؤقت وإمكانية انتقاله الى الخلف العام وإمكانية التصرف فيه بكافة أنواع التصرفات القانونية.

أوردت مختلف التشريعات والاتفاقيات الدولية الحقوق المالية للمؤلف في صور مختلفة، منها حق نقل المصنف الى الجمهور بأي طريقة وحق النشر، وحق النسخ، وحق التتبع وغيرها[34]الا ان التساؤل المطروح هو مدى قابلية التشريع القائم للتطبيق على المصنفات المستحدثة بتكنولوجيات الاعلام والاتصال والاشكالات التي تعترض تطبيق هذا التشريع في الفضاء الافتراضي.

الفرع الأول: حق النسخ

ان التطورات التكنواوجية لعبت دورا هاما في التأثير على الحقوق المالية للمؤلف باعتبارها أحدثت تقنيات النسخ الرقمي للمصنفات وبه سمحت لمستخدمي الانترنت إمكانية تصفح المصنفات عبر العالم الافتراضي والاستفادة منها بإعادة نسخها واستغلالها دون موافقة مسبقة من المؤلف صاحب الحق.

أعطى القانون للمؤلف حق الاستئثار بمصنفه لأنه جهد لعمل فكري يقابله الاستفادة بمقابل مالي الناتج عن نسخ المصنف وإتاحته للجمهور، لذلك فإن النسخ دون إذن من المؤلف يعتبر اعتداء على حق المؤلف تترتب عليه جزاءات مدنية وجزائية.

نصت المادة 27 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة على حق المؤلف أن يقوم أو يسمح بمن يقوم باستنساخ المصنف بأي وسيلة كانت.

أما قانون الملكية الفكرية الفرنسي قد نص في المادة 3-122ل " بأن حق النسخ يتضمن التثبيت المادي للعمل الذهني بكل الوسائل التي تسمح بإيصاله للجمهور بصورة غير مباشرة".

---

[33] عبد الرشيد مأمون ومحمد سامي عبد الصادق، حقوق المؤلف المجاورة في ضوء قانون حماية حقوق الملكية الفكرية الجديدة، دار النهضة العربية، القاهرة، 2008، ص369.

[34] رامي إبراهيم حسن الزواهرة، المرجع السابق، ص.70.

من هذا النص يتبين ان اغلب التشريعات تركت المجال مفتوحا أمام كل الوسائل وبذلك لم تحصر طرق النسخ، وحتى بعض التشريعات القديمة التي صدرت قبل تطور تكنولوجيات الرقمنة استعملت عبارة" كل الوسائل" مما سمح لنصوصها من استيعاب التطور الذي حصل بعد صدورها في مجال طرق النسخ، الا ان تشريعات أخرى لجأت الى تعديل أحكامها بإدراج الاشكال المستحدثة في طرق النسخ التي أفرزتها التكنولوجيات الحديثة وظهور الوسائط الالكترونية.

ومن هذا المنطلق سوف يتم التطرق الى تأثير تكنولوجيات الاعلام والاتصال على حق النسخ ثم التطرق الى استثناء النسخة الخاصة.

أولا: تأثير تكنولوجيات الاعلام والاتصال على حق النسخ

أثرت تكنولوجيات الاعلام والاتصال على طرق النسخ بشكل مباشر، حيث منحت تقنيات الاعلام الآلي إمكانية تحويل المصنفات الى شكل رقمي حتى يتم وضعها في متناول القراء عبر الوسائط الإلكترونية وتخزينه في الدعائم الرقمية، فباستثناء المصنفات التي تنشأ في البيئة الرقمية كبرامج الحاسوب أو المواقع الالكترونية، تقتضي رقمنة المصنفات الأخرى تحويلها من شكلها الأصلي كتسجيلات سمعية بصرية أو مثبتة على دعائم مغناطيسية أو ملفات أدبية مكتوبة على الورق أو صور، الى ملفات رقمية.

تتم عملية الرقمنة بعدة طرق حسب طبيعة المصنف الأصلي، فإذا كان عبارة عن تسجيل صوتي على شريط ممغنط، فيتم استعمال تجهيزات لتحويل الإشارة التناظرية الى إشارة رقمية قابلة للمعالجة بواسطة الأنظمة المعلوماتية التي تستعمل البرامج المعلوماتية[35]، أما إذا كان موضوع الرقمنة هو صورة أو كتابة مثبتة على دعامة مادية صلبة(ورق مثلا)فيتم التقاط المحتوى بواسطة تجهيزات رقمية مثل الات التصوير الرقمية أو أجهزة السكانير التي تقوم بتحويل الصورة الملتقطة الى سلسلة من الأرقام التي تعبر عن مضمون المحتوى تكون قابلية للمعالجة من خلال الأنظمة المعلوماتية التي تمنحها شكل رقمي ذو امتدادات مختلفة يتم قراءتها بواسطة برامج مناسبة.

تزايدت حالات نشر المصنفات المحمية عبر شبكة الانترنت في ظل تكنولوجيات الاعلام والاتصال حيث يقتضي وضع المصنف على شبكة الانترنت بفعلين

1- رقمنة المصنف بتحويله من شكله الأصلي إلى الشكل الرقمي:

[35] الموسوعة الحرة ويكيبيديا www.wikipedia.org/wiki/numerisation/ متصفح في 2021/02/02.

صدرت محكمة باريس الابتدائية في 1997/05/05" ان رقمنة المصنف يشكل تقنية يتم بمقتضاها ترجمة المصنف الى لغة رقمية يرمز اليها بلارقام صفر وواحد وتختلف تلك اللغة بحسب نوع المصنف فيما إذا كانت نص أو صور ثابتة أو متحركة أو أصوات، كما ورد في نفس القرار " إنه يمكن عن طريق جهاز السكانير المتصل بجهاز الحاسب الآلي عرض صفحات من كتاب على شاشة الكومبيوتر ، كذلك يمكن عرض مصنف فني ثلاثي الأبعاد بواسطة التصوير أو التصوير السينمائي ومثل هذه العملية ، رقمنة صفحات الكتاب أو الفيلم تشكل فعل نسخ يقع في نطاق حقوق المؤلف وأن هذه العملية تشكل نقل للمواد المثبتة من وسط الى آخر فهذا يعني ان مجرد رقمنةالمسح الضوئي عبر جهاز السكانير في هذه القضية مصنف محمي وتنزيله عبر شبكة الانترنت أي جعله متاح للجمهور يكون من فعل النسخ ويحتاج إذن مسبق من صاحب المصنف[36].

2-فعل التخزين:

ان عملية الرقمنة تتم بعد تثبيت الملف الذي نتج عن عملية الرقمنة في الذاكرة الحية لجهاز الحاسوب، وقضى القضاء الفرنسي في قضية" ساردو" أن تثبيت مصنف على القرص الصلب لجهاز الحاسوب يشكل فعل تثبيت مادي للمصنف المنصوص عليه في قانون حماية الملكية الفكرية حيث ورد أن "كل نسخ عن طريق رقمنة مصنف موسيقي محمي بموجب حقوق المؤلف من شأنه إتاحته لأشخاص مرتبطين بشبكة الانترنت يجب أن يحظى بموافقة أصحاب الحقوق[37]

وفي حكم صادر عن محكمة بونتواز، اعتبر القضاة أن كل ملف بتضمن مصنف في شكل رقمي يتم تثبيته في القرص الصلب لمتصفح الانترنت المستقبل يعتبر نسخ[38].

اما المسألة التي يمكن إثارتها فهي موقف القانون من نسخ مصنف سبق إتاحته للجمهور بطريقة قانونية وإعادة إتاحته للجمهور عبر شبكة الانترنت، وتعرضت محكمة نانتير الفرنسية أن تعرضت لهذه المسألة فيما يعرف بقضية Edirom حيث اعتبرت أن المدعي عليه قام باعتداء على حقوق التأليف بقيامه بنسخ جزء من المصنف وجعله متاحا للجمهور على شبكة الانترنت[39]

[36]TGI de Paris, 05/05/1997 aff Queneau
[37] TGI de Paris, 14/08/1996.
[38]TGI de Pantoise,02/02/2005, www.juriscom.net
[39]TCN, 27/01/1998.

الا ان هذا الحكم تم نقده من الفقه، فيجب تطبيق قاعدة استنفاذ الحقوق عبر الانترنت على أساس أن قيام المؤلف بمنح موافقته الأولى لوضع مصنفه وإتاحته عبر شبكة الانترنت يؤدي الى فقدانه السيطرة على استغلال مصنفه بسبب ما توفره التقنية المعلوماتية للمستخدمين من إمكانية نسخ ونقل المصنف من موقع الى آخر عبر الشبكة، فلا يمكنه بعد ذلك الادعاء بأن هناك اعتداء على حقه.

وقضت محكمة بروكسل في حكم صادر في 1996/09/16، بأن نشر مقالات صحفية في جرائد يومية وأسبوعية لا يتضمن ترخيص ضمني بإعادة نشر نفس المقالات عبر شبكة الانترنت باعتبار ان النشر عبر الانترنت يقتضي رقمنة المقالات الصحفية المنشورة في الجرائد الورقية وهو ما يعتبر نسخ بمفهوم قانون حقوق المؤلف[40]

ثانيا: استثناء النسخة الخاصة

أقرت أغلب قوانين حقوق المؤلف استثناء على حق النسخ وهو استثناء النسخة الخاصة، وقد ورد هذا الاستثناء في التشريع الجزائري في المادة 124 من الامر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة يقتضي هذا المبدأ أن المؤلف لا يمكنه الاعتراض على نسخ مصنفه لأجل الاستعمال الشخصي في إطار خاص.

في هذا الاطار يرى جانب من الفقه يرى أنه لابد من وضع قيود على استثناء النسخة الخاصة حين تتم عبر الرقمنة في بيئة الانترنت للحد من حرية المستخدم في النسخ عن طريق الوسائل التقنية كالتشفير للحد من النسخ الواسع واللامتناهي للمصنفات في حين يرى جانب اخر انه لابد من الإبقاء على استثناء النسخة الخاصة في بيئة الانترنت حتى لا يتقيد حق المجتمع في بلوغ العلو والمعرفة.

الا انه بالرجوع الى قضية "ساردو" نرى أن القضاء غلب حق المؤلف حين اعتبر نسخ مصنف ووضعه في موقع الكتروني هو بمثابة نسخ غير قانوني يستوجب إذن المؤلف.

ان ارسال نسخة من مصنف عبر البريد الالكتروني الخاص لعدة أشخاص يثير إشكالات ، فهل يعتبر هذا الفعل من قبيل النسخة الخاصةأم انه خارج على اطار النسخة الخاصة؟

هناك من يرى ان الفعل يقع تحت طائلة الحظر لكونه مساس بحقوق المؤلف ولا يدخل ضمن استثناء النسخة الخاصة الموجهة للاستعمال الشخصي في حين يرى رأي اخر ان المؤلف قد تنازل عن حقه ضمنيا.

---

[40] رامي إبراهيم حسن الزواهرة، المرجع السابق، ص.508.

ثار جدل واسع بين الفقه حول تأثير تكنولوجيات الاعلام والاتصال على تطبيق استثناء استثناء النسخة الخاصة، أما القضاء اتجه في فرنسا نحو اشتراط شرعية المصدر للاستفادة من استثناء النسخة الخاصة على غرار ما أقرته محكمة الاستئناف في باريس في 2005/03/20 في قضية نسخ برامج حاسوب والعاب الكترونية حيث رفضت قيد النسخة الخاصة الذي تحجج به المدعي عليهم بداعي ان عدم شرعية المصدر يفسد كل الاستعمالات اللاحقة وهو الاتجاه الذي أيدته محكمة النقض في قرارين مبدئيين مؤرخين في 2006/05/30 و 2006/06/07.

الفرع الثاني: حق اعلام الجمهور

يتضمن حق اعلام الجمهور في حق المؤلف الترخيص بأداء مصنفه علنيا وايصاله الى الجمهور وكذا حقه في تأجير المصنف وتوزيعه فحق الأداء العلني ويسمى أيضا حق التمثيل هو تنفيذ العمل الأدبي عن طريق العرض أو العزف أو الالقاء أو السرد أو التمثيل[41]حيث ان طرق الأداء المدني تختلف حيب طبيعة المصنف إذ ان كل نوع من الاعمال الفنية والأدبية يتطلب طرق أداء معينة تتناسب معه، في حين يمكن أن يكون الأداء مباشر كأن يتم عرض الأداء على جمهور يكون مجتمع في قاعة عرض أو غير مباشر يتطلب وضع وسيلة اتصال تكون بمثابة ناقل للعرض الى جمهور غير مجتمع في مكان العرض ولا في وقت العرض، وعليه سوف اتناول حق الأداء العلني وحق التأجيروأثر تكنواوجيات الاتصال والاعلام عليهما.

أولا: اثر التكنولوجيات الاعلام والاتصال على الأداء العلني

يمكن التساؤل حول تحقق ركن العلانية في حال ما اذا تم ارسال مصنف عبر البريد الخاص الى مجموعة محددة من الأشخاص، حيث أن الاستثناء الواجب تطبيقه على هذه الحالة هي إرادة المرسل وقدرته على تحديد عدد المرسل اليهم، فاذا قام بارسال مصنف الى عدد محدد من المرسل اليهم وجب تطبيق الاستثناء ، أما اذا كان البريد الالكتروني موجه الى مجموعة من المستخدمين دون ان يتمكن من تحديد عددهم أو التحكم في تزايد هذا العدد فيما بعد ينعدم الاستثناء ويقوم حق المؤلف في الترخيص للأداء العلني.

ان التشريع الجزائري اعتبر طرق شبكة الانترنت كوسيلة من وسائل النشر من خلال نصه في المادة 27 على ابلاغ المصنف الى الجمهور " بأية منظومة معالجة معلوماتية" مما يسمح باستيعاب الحالات

[41]رامي إبراهيم حسن الزواهرة، المرجع السابق، ص.536.

المتمثلة في الأداء العلني عبر هذه الشبكة ليحسم الجدل المتعلق بانعدام البث المتزامن ومسألة العلانية التي تتحقق بموجب هذه النصوص عبر شبكة الانترنت.

أما الارسال الى مجموعة محددة من مستخدمي الانترنت يجب ان يخضع لتقدير القضاء من حيث هو نشر موجه الى الجمهور فيتحقق بموجبه الأداء العلني أو نشر خاص لا يحقق الأداء العلني.

ثانيا: أثر تكنولوجيات الاتصال والاعلام على الحق في التأجير

يقتضي حق الاجير استفادة المؤلف من عائدات تأجير مصنفه بهدف الانتفاع به لمدة معينة ثم اعادته الى المؤجر، حيث نص المشرع الجزائري على هذا الحق في المادة 27 –2 من الأمر 03–05 .

ان اتفاقيةتريبس كرست حق تأجير المصنف فيما يتعلق ببرنامج الحاسوب والمصنفات السينمائية، أما المصنفات الأخرى فلم تقرر أي التزام على الدول الأعضاء في الاتفاقية ملزمة بتقرير حق المؤلف في الاستئثار بمؤلفه والحصول على موافقته وتأدية مقابل مالي له عند تأجير مصنفه إذا تعلق الأمر ببرنامج حاسوب أو عمل سينمائي.

ان السبب في تخصيص التأجير لبرامج الحاسوب والمصنفات السينمائية يعود الى كون برامج الحاسوب هي من المصنفات التي يمكن نسخها بشكل غير محدود دون التأثير على خصائصها التقنية، كما أن الاعفاء من تقرير حق تأجير البرنامج عندما لا يكون هو الموضوع الأساسي للتأجير مفاده أنه يمكن تأجير معدات تتضمن برنامج حاسوب مثل مركبة تحتوي على برنامج حاسوب ، إذ ان موضوع تأجير هو المركبة لغرض التنقل فلا يمكن ان ا يكون البرنامج الذي يحتوي عليه محلا لحقوق المؤلف في التأجير، أما إذا كان محلا للتأجير الذي هو جهاز الكتروني يعمل بواسطة البرنامج فانه يصبح الموضوع الأساسي للتأجير وتضمن اتفاقية الوايبو نفس التدابير في المادة 07 فقرة 1–29.

لقد انقسم الفقه بين من يرى لنه من الصعب تطبيق حق التأجير في البيئة الرقمية اين يصعب السيطرة على تداول المصنفات وبين من يرى ان البيئة الرقمية لا تشكل عائقا لتجسيد هذا الحق حيث يمكن وضع ترتيبات تقنية تسمح بمراقبة تأجير المصنفات عبر شبكة الانترنت كما هو الحال بالنسبة للأفلام السينمائية التي تخضع ادفع ثمن مقابل مشاهدتها عبر القنوات.

الخاتمة

ان التشريع الوطني قد ساير التطور الذي عرفه القانون عبر دول العالم الأكثر تطورا من خلال ادراج تدابير جديدة في القانون المتعلق بحقوق المؤلف الصادر بموجب الامر03-05 المؤرخ في 2003/07/19 ، حيث أهتم بالتدابير التي صدرت في معاهدة الويبو فيما يخص حق المؤلف الصادرة في سنة1996 كما أخذ بعين الاعتبار التدابير المستحدثة في التشريع الفرنسي المتعلق بالملكية الفكرية والنص صراحة على اعتبار برامج الحاسوب وقواعد البياناتمن المصنفات المحمية وكذلك اهتم بأثر النسخ بالطرق المعلوماتية على هذين المصنفين مما أدى الى استثنائهما من قيد النسخة الخاصة(المادة 41).

الا انه يبقى بعض الغموض يعرقل تطبيق القانون فيما يخص برامج الحاسوب من حيث تحديد العناصر الجديرة بالحماية بالنظر الى الطابع المعقد لتصميم البرنامج وصعوبة تناوله من طرف رجل القانون ، مع العلم ان المشرع الفرنسي أضاف عبارة "عتاد التصميم التحضيري" الى البرنامج المعلوماتي لرفع اللبس عن أجزاء البرنامج المعنية بالحماية وإضفاء وضوح على النص، كما أضاف التشريع الفرنسي حماية من طبيعة خاصة لمنتجي قواعد البيانات بموجب ما يعرف بالقانون الخاص بقواعد البيانات المنصوص عليه في المواد 1-341 L و2-341 L من قانون الملكية الفكرية.

تبقى مسألة النشر عبر الوسائل التي تتيحها تكنولوجيات الإعلام والاتصال تثير إشكال من حيث اعتبارها وسيلة يتحقق بواسطتها نشر المصنفات التي تفرض رخصة المؤلف أم عدم اعتبارها كذلك بسبب انعدام البث المتزامن ، يضاف اليها مسألة النشر عن طريق البريد الخاص ان كان يحقق مفهوم الجمهور أم لا، وهي مسائل تعرض لها القضاء الفرنسي وأصدر عدة اجتهادات بشأنها.

الاقتراحات

لحماية المنتجات المعلوماتية بموجب قانون حقوق المؤلف، يستحسن إضافة عبارات توضيحية على ذات القانون بشكل يسمح برفع اللبس عن المنتجات المعلوماتية المحمية، لاسيما برامج الحاسوب التي تستدعي توضيح الأجزاء المحمية، وهذا لتفادي إثقال كاهل القضاء بالدعاوي الغير مجدية التي تهدف الى حماية عناصر غير قابلة للحماية في هذه المنتجات، كما سيبقى على القضاء إثراء الاجتهاد فيما يخص طرق نشر المصنفات الفكرية عبر وسائل الاتصال الرقمية التي يتحقق بها النشر الموجب لرخصة المؤلف.

قائمة المصادر

الاتفاقيات الدولية

الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المصادق عليها بموجب المرسوم الرئاس14-252، المؤرخ في 08سبتمبر 2002.

النصوص التشريعية

الأمر رقم 66-155 المؤرخ في 8 يونيو1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم

الأمر رقم 03-05 المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة

قائمة المراجع

عبد المجيد زعلاني، المدخل لدراسة القانون ، النظرية العامة للحق، دار هومة للطباعة والنشر، الجزائر ،2007.

رامي إبراهيم حسن الزواهرة، النشر الرقمي للمصنفات وأثره على الحقوق الأدبية والمالية للمؤلف ، دار وائل، الطبعة الأولى، عمان ، الأردن.

رشا علي الدين، النظام القانوني لحماية البرمجيات، دار الجديدة للنشر، الإسكندرية، 2007.

عفيفي كامل عفيفي، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، منشورات زين الحقوقية، الطبعة الأولى، لبنلن، 2007.

عبد الرشيد مأمون ومحمد سامي عبد الصادق، حقوق المؤلف المجاورة في ضوء قانون حماية حقوق الملكية الفكرية الجديدة، رقم 82 لسنة 2002، دار النهضة العربية، القاهرة،2008.

مذكرات الماجستير

عبد الكريم نعمان، الجرائم الالكترونية وموقف المشرع الجزائري منها، مذكرة ماجستير، كلية الحقوق، جامعة الجزائر1 ، 2017.

فتيحة رصاع، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة تلمسان، 2012.

المقالات

حسن جميعي، مدخل الى حقوق المؤلف والحقوق المجاورة، ورقة بحثية مقدمة في حلقة الويبو التمهيدية حول الملكية الفكرية، المنظمة العالمية للملكية الفكرية ويبو، وزارة التجارة المصرية، القاهرة، 2004/10/10، رقم الوثيقة CAI/ IP/WIPO /04/01 ص4.

OUVRAGES

Alain Hollande et Xavier Linant de Bellefonds, pratique du droit de l informatique et de l interne, 6eme édition, Delmas, France,2008.

Papa Assane Toure, le traitement de la cybercriminalité devant le juge, édit L Harmattan, Paris,2014.

الاسم : أمال **الاسم : علي**

اللقب : بيدي **اللقب : عثماني**

الرتبة العلمية : أستاذة محاضرة أ **الرتبة العلمية : أستاذ محاضر أ**

التخصص : حقوق(قانون دولي وعلاقات دولية) **التخصص : حقوق**

المؤسسة : جامعة زيان عاشور – الجلفة – **المؤسسة :المركز الجامعي أفلو الأغواط**

رقم الهاتف :0675713915

البريد الالكتروني : bidiamal18@gmail.com

عنوان المداخلة: حدود التقنيات الحديثة في مجال تنفيذ العقوبة الجنائية بين الرؤية الفقهية و الأنظمة الجنائية .

The Limit of modern techniques in the field of criminal punishment execution between the jurisprudential vision and criminal systems.

المحور : الثالث

الملخص :

إن العقوبة مقترنة بالجريمة ، وذلك من أجل استتباب الأمن والسلام في المجتمع ، غير أن الجرائم لم تعد بشكلها البسيط ولا بوسائلها التقليدية ، ومزامنة مع تطور التكنولوجيا الذي رافقها تقنيات حديثة في اكتشاف الجريمة وتنفيذ العقوبة ، ولتبيين مدى نجاعة هذه التقنيات في تنفيذ العقوبة الجنائية ، فمثلا أصبحت وسائل حديثة في تنفيذ حكم الإعدام مثلا الحقنة المميتة ، الكرسي الكهربائي ...إلخ .

ومنه جاءت دراستنا تهدف إلى توضيح رؤية الفقه الإسلامي حول هذه التقنيات ومدى فائدتها في الأنظمة الجنائية ، وبناء عليه نتوصل إلى مجموعة النتائج ولعل أهمها حتمية تطبيق هذه التقنيات لما لها من أهمية في احترام الكرامة الإنسانية حتى أثناء تنفيذ العقوبة.

الكلمات المفتاحية :

العقوبة ، التقنيات الحديثة ، الفقه الإسلامي ، الأنظمة الجنائية .

Summary

Punishment is associated with crime, in order to establish security and peace in society, but crimes are no longer in their simple form or by their traditional means, and synchronized with the development of technology, which was accompanied by modern techniques in the discovery of crime and the implementation of punishment, and to show the effectiveness of these techniques in the implementation of criminal punishment, for example. Modern methods of executing the death sentence have become, for example, lethal injection, electric chair...etc.

Hence, our study aims to clarify the vision of Islamic jurisprudence about these techniques and their usefulness in criminal systems, and accordingly we reach a set of results, perhaps the most important of which is the imperative to apply these techniques because of their importance in respecting human dignity even during the execution of punishment.

Keywords : Punishment, modern technologies, Islamic jurisprudence, criminal systems.

مقدمـــة:

لقد ارتبطت الجريمة كظاهرة اجتماعية ارتباطا وثيقا بالمجتمعات وعاداتهم وتقاليدهم والمتغيرات الاقتصادية والسياسية التي يمر بها المجتمع، فالجريمة إذن تتطور وفقا للظروف المتغيرة ولكن بسرعة قد تتجاوز أحيانا سرعة حركة المجتمع لاسيما في عالم اليوم الذي رفعت فيه المجتمعات الحواجز والحدود القانونية التقليدية، وأدى إلى ترابط عضوي بين الأمم والشعوب الذي فرضته سنة التطور وتدعمه تقنية وسائل النقل والاتصال الحديثة.

إن لتجدد الحوادث الاجتماعية الناتجة عن التطورات العلمية والتكنولوجية تأثير عظيم في كثير من المسائل الفقهية، مما يستوجب النظر فيها، والاجتهاد في حكمها من جديد، وفق التقنيات والتطورات العلمية المعاصرة في شتى المجالات. وليس من الصواب بحث دراسة المسائل الفقهية الاجتهادية بمعزلٍ عن الواقع والمستجدات المعاصرة، وذلك لأن التقنيات الحديثة قد أثرت تأثيراً بالغاً في الكثير من المسائل الفقهية التي ذكرها الفقهاء.

الإشكالية :

كيف يرى الفقه الإسلامي إلى التقنيات الحديثة التي أفرزتها التكنولوجيا في تنفيذ العقوبة الجنائية و هل كانت كافية في تحقيق أهدافها أم أنها عجزت على ذلك ؟

منهج الدراسة :

نظرا لطبيعة الورقة البحثية في خضوعها للوصف والتحليل ، فإننا وظفنا المنهج الوصفي التحليلي ، بوصف للوضعية القانونية للموظف الدولي ، ثم تعرضنا للآثار بوصف وتحليل لها

المبحث الأول: مدخل لمصطلحات الدراسة

لقد غزت التكنولوجيا حياة الأفراد في كل المجالات ولعل المجال الجريمة والعقوبة من أكثرها ، ذلك أن قطاع الأمن من أهم القطاعات وأكثرها حساسية التي تفرض استخدام هذه التقنيات الحديثة التي تتطور باستمرار .

ومنه في هذا المبحث سنقوم أولا بتقديم عرض موجز حول مفهوم أهم المصطلحات التي ستتناولهم الدراسة.

المطلب الأول: ماهية التقنية الحديثة

الفرع الأول: التعريف القانوني للتقنية الحديثة:

التقنية هي استخدام التكنولوجيا الاستخدام الأمثل في مختلف مجالات العلم والمعرفة من خلال معرفتها وتطبيقها وتطويعها لخدمة الانسان ورفاهيته، فهي استخدام كل ما يتوصل إليه التقدم العلمي في مختلف المجالات، وعلة كافة الجوانب التي ترتبط بتنظيم وإدارة وتشغيل العملية الإنتاجية[1].

التقنيات الحديثة هي الاكتشافات العلمية التي أفادت مجال الخبرة الجنائية سواء تمثل ذلك في أجهزة أو علم تطبيقي أو نظم فتح آفاق جديدة في مجال الاثبات الجنائي[2].

الفرع الثاني: التعريف الفقهي للتقنية الحديثة:

[1] سلام محمد علي، أثر التقنيات الحديثة في الأدلة الجنائية دراسة مقارنة بين الشريعة والقانون، مجلة مداد الآداب، كلية القانون، الجامعة العراقية، العدد 11، ص 460.

[2] سالم بن حامد بن علي البلوي، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة مقدمة لاستكمال نيل شهادة الماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2009، ص 09.

لا يختلف المعني اللغوي عن المعني الاصطلاحي، فالحديث: عكس القديم، وإنما قيدت التقنية بالحديثة احترازا من التقنيات القديمة التي كانت موجودة في الزمن القديم وأدركها أسالفنا، فعلى سبيل المثال: البوصلة، وهي ما يعبر عنها الفقهاء قديما ببيت الإبرة، كانت موجودة في العصور المتقدمة وهي بلا شك تقنية تفيد في معرفة الاتجاهات، وكذلك العدسة المكبرة أو المنظار المكبر كانت موجودة في السابق بصورة بدائية لا على ما هي عليه الآن، فإن تكبيرها للأشياء فاق ملايين المرات، فالتقنية مصطلح شامل يعني استخدام كل ما يتوصل إليه التقدم العلمي في مختلف المجالات، وعلى كافة الجوانب التي ترتبط بتنظيم وإدارة وتشغيل العملية الإنتاجية أو الخدمية ككل متكامل في أي من القطاعات الاقتصادية أو الخدمة في مجتمع ما. فالتقنية أداة تساعدنا على إنجاز العمل بشكل أسرع وأكثر كفاءة، وتشمل التقنية الحديثة استخدام الأدوات، الآلات، والمواد، والأساليب، ومصادر الطاقة، لكي تجعل العمل ميسوراً، وأكثر إنتاجية، وتستخدم كلمة التقنية أحيانا لوصف استخدام معين كالتقنية الطبية، والتقنية الصناعية، والتقنية العسكرية، تهدف كل واحدة من التقنيات المتخصصة إلى أهداف محددة وتطبيقات بعينها، كما أن لها أدوات ووسائل لتحقيق هذه الأهداف[1].

هذا التعريف الذي ركز على الغرض والهدف من التقنية الحديثة في الفقه الإسلامي يجد قبولا إذ أن هذا المصطلح غير معروف فقها لأنه مصطلح مرتبط بعلوم أخرى يمكن أن يجد تعريفاً في العلوم الأخرى ولكن الفقه الإسلامي لا يمانع من استخدام التقنيات الحديثة في شتى المجالات طالما كان الغرض مشروعا، وبالتالي فإن المفهوم لهذا المصطلح طالما كان موافقاً للغرض فيمكن الأخذ به في نطاق الفقه الإسلامي[2].

[1] سلطان مرزوق فايز الحربي، أثر استخدام التقنيات الحديثة في مجال تنفيذ العقوبات الجنائية في تحقيق الزجر والردع، المجلة الالكترونية الشاملة، الجامعة السعودية الالكترونية، العدد 08، 2018، ص 12.

[2] سلطان مرزوق فايز الحربي، مرجع سبق ذكره، ص 13.

المطلب الثاني: ماهية القانون الجنائي

الفرع الأول: التعريف القانوني للقانون الجنائي:

يقصد بالقانون الجنائي مجموعة القواعد القانونية التي تبين الأفعال المحظورة قانونا، وما تقرر لها من جزاءات مقابلة سواء كانت عقوبات أو تدابير أمن، وهذا تماشيًا مع ما استقر عليه الفقه والتشريعات الحديثة، من وجوب خضوع التجريم والعقاب لمبدأ الشرعية الذي نادت به المدرسة التقليدية الأولى، حيث عرفه عبد القادر عدو بأنه: "مجموعة القواعد القانونية التي تبين أنواع السلوك المعتبر جرائم وتحدد الجزاءات المقررة لها، سواء كانت عقوبات أو تدابير أمنية"[1].

يعرف القانون الجنائي بأنه: "مجموعة القواعد التي تختص بدراسة الشروط العامة للتجريم والقواعد العامة لتحديد العقوبات فيصنف الجرائم حسب خطورتها ويحدد أركان الجريمة وأحكام المسؤولية الجنائية وأسباب انعدامها وكذلك أسباب الإباحة"[2].

الفرع الثاني: التعريف الفقهي للقانون الجنائي:

الجناية تعرف بأنها: "اسم لفعل محرم حل بمال أو نفس أو غير ذلك"، كالجناية على المال بالنصب والسرقة، والجناية على النفس والأطراف بالقتل والجرح، وهي مرادفة للفظ الجريمة، التي عرفها الفقه بأنها محضورات شرعية زجر الله عنها بحد أو تعزير أو قصاص"[3].

---

[1] محمد العايب، مذكرة التشريع الجنائي المقارن، محاضرات لطلبة السنة الثالثة تخصص شريعة وقانون، كلية العلوم الإسلامية، جامعة باتنة، 2020، ص 02.

[2] نسمة حسين، دروس في القانون الجنائي العام الجريمة والجزاء المقرر لها، محاضرات مقدمة للسنة الثانية تخصص القانون الخاص، د.س.ن، ص 02.

[3] فريد روابح، محاضرات في القانون الجنائي العام، مطبوعة الدروس لطلبة السنة الثانية ليسانس، كلية الحقوق والعلوم السياسية، جامعة سطيف، 2018، ص 04.

القانون الجنائي هو قانون الجرائم يهتمُّ بالجريمة ومُعاقبة مُرتكبيها. ولذلك يعُرّفه الفقه بأنهّ "مجموع القواعد القانونية التي تحُدّد الجرائم، والعقوبات وتدابير الأمن التي توُقع على مُرتكبيها"[1].

المبحث الثاني: أهم وسائل التقنيات الحديثة المستخدمة في المجال الجنائي

لقد تطورت وسائل التقنيات الحديثة المستخدمة في المجال الجنائي ، وذلك للتطور المتسارع للتكنولوجيا وكان من المحتم التطور فيها في المجال القانوني والجنائي بالخصوص، وسنقوم بعرض أهمها في هذا المبحث ، حيث لا يمكن حصرها لأنها في تطور متزايد ومستمر وهذا مايثبت أن العلم في تطور دائم ،ولابد الاستفادة منه في كل المجالات.

المطلب الأول: البصمة الوراثية

من المسائل العلمية التي ظهرت حديثا بصمات الأصابع، حيث ثبت علميا أن شكل بصمة أي إصبع من أصابع الإنسان لا يتغير رسمها على الإطلاق مدى الحياة، وأنه لا يوجد بين ملايين البشر شخصان تتماثل بصمات أصابعهما وهذا ما يضفي على البصمات أهمية ويكسبها قيمتها في تحقيق الشخصية في العصر الحديث كدليل قاطع لا يرقى إليه الشك[2].

البصمة الوراثية هي الصفات الوراثية التي تنتقل من الأصول إلى الفروع، والتي من شأنها تحديد شخصية كل فرد عن طريق تحليل جزء من حامض ال DNA الذي يحتوي عليه خلايا جسده، والمتمركز في نواة أي خلية من خلايا جسمه[3]. [1]

---

[1] ماهية القانون الجنائي، على الموقع: https://www.elmizaine.com/2021/05/blog-post_48.html، تم الاطلاع في: 2022/08/23، الساعة 19:13.

[2] دنيا زاد ثابت، مشروعية إجراءات التحقيق الجنائي، مذكرة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، د.س.ن، ص 155.

[3] آمال عبد الرحمان يوسف حسن، الأدلة العلمية الحديثة ودورها في الإثبات الجنائي، رسالة مقدمة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2011، ص 64.

أثبتت البصمة الوراثية مع الزمن دورها في الميدان الجنائي بفضل خصائصها المتميزة فقد سلمت معظم المحاكم في مختلف الدول بقيمة البصمة الوراثية مع زمن بعيد ما يجب الإشارة إليه هو أن اهتمام الباحثين بالبصمة الوراثية كدليل الإثبات كان على يد العالمين "جيمس واطسون" و"فرانس كريك" سنة 1953 ثم جاء الدكتور "إريك" ليفصل فيها أكثر من خلال أبحاثه[2].

من المعلوم أن المشرع الجزائري لم ينص سابقا بشكل صريح إلى مفهوم البصمة الوراثية أو استعمالها، وإنما لمح إلى ذلك تلميحا من خلال عدة نصوص قانونية نورد منها الفقرة الأخيرة من المادة 68 من قانون الإجراءات الجزائية الجزائري حيث تنص على ما يلي (... يجوز لقاضي التحقيق أن يأمر بإجراء الفحص الطبي كما له أن يعهد إلى طبيب بإجراء فحص نفسي أو يأمر باتخاذ أي إجراء يراه مفيدا، وإذا كانت تلك الفحوص الطبية قد طلبها المتهم أو محاميه فليس لقاضي التحقيق أن يرفضها إلا بقرار مسبب)، وكذلك من خلال الفقرة الأخيرة من المادة 40 من قانون الأسرة الجزائري التي تنص على ما يلي (...يجوز للقاضي اللجوء إلى الطرق العلمية لإثبات النسب)، تاركا الأمر في ذلك إلى السلطة التقديرية للقاضي في الاحتكام إلى البصمة الوراثية من عدمه، وأعتبرها دليلا مساعدا يلجأ إليه حسب قناعته الشخصية[3].

المطلب الثاني: العينات من الدم واللعاب والعرق والبول والمني والشعر

استفاد علم الإثبات من الاكتشافات العلمية لتصنيف فئات الدم وفصائله حيث تعتبر البقع الدموية المعثور عليها من أهم الأدلة خاصة إذا أثبت التحليل البيولوجي ارتباط هذه الدماء بموضوع الجريمة، إذ

1

[2] عائشة مغاوي، مدى حجية الدليل المستمد من التسرب في الاثبات الجنائي دراسة مقارنة، مذكرة لنيل شهادة الماستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة مستغانم، 2020، ص 40.

[3] محمد السعيد زناتي، أحمد بنيني، أثر أدلة الاثبات الجنائي الحديثة على الاقتناع الشخصي للقاضي الجزائي في التشريع الجزائري، مجلة الواحات للبحوث والدراسات، المجلد 14، العدد 01، 2021، ص 872.

يترتب على حدوث أي جرح أو خدش نزيف دموي، ما يجعل منه أثرا ماديا يستفاد منه. أما المني فهو سائل هلامي لزج القوام، لونه أبيض مصفر، ذو رائحة مميزة، يصبح قوامه سائلا بعد نصف ساعة من تعرضه للهواء بسبب فعل الخمائر الموجودة فيه، ويتكون المني من جزئين هما جزء سائل ويفرز من غدد في الجسم، أهمها غدة البروستات وافرازات القناة الناقلة والحويصلات المنوية والثاني جزء خلوي ويتكون من الحيوانات المنوية التي تتكون في الخصيتين، ويشكل هذا النوع من الافرازات إحدى أهم الأدلة الجنائية[1].

يعتبر الشعر أحد الأدلة الجنائية كذلك إذ يتمتع بخصائص ومكونات تختلف عند الإنسان منه عند الحيوان، والشعر كدليل أو كأثر مادي يتخلف في جرائم العنف مثل: الاغتصاب فنجد الشعر تحت أظافر الجاني، أو عالقا بملابسه أو على جسمه في مواقع تتفق مع طبيعة الجريمة، أو يكون الشعر عالقا بالآلة المستخدمة في ارتكاب الجريمة[2].

المطلب الثالث: التسجيل الصوتي

التسجيلات الصوتية هي عملية ترجمة للتغيرات المؤقتة لموجات الصوت الخاصة بالكلام أو الموسيقى إلى نوع آخر من الموجات أو التغيرات الدائمة ويتم التسجيل بواسطة أجهزة الكترونية متعددة ومتخصصة بتسجيل الصوت ويتم تخزينها داخل أشرطة أو داخل قرص مضغوط، وأنه يتم تخزينها على ذاكرة متنقلة أو يتم تخزينها على برامج بواسطة الانترنت مما يسهل اعادة سماع هذه التسجيلات في أي وقت، وأنه يتم تسجيل الأصوات بواسطة الهواتف النقالة الذكية، والتسجيلات الصوتية إما أن تكون بالصورة المباشرة والتي يتم تسجيل الأحاديث التي تدور بين الأشخاص بواسطة أجهزة التقاط صغيرة، وإما

[1] علاء الدين سلماني، دور الشرطة العلمية في إثبات الجريمة، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة بسكرة، 2013، ص 75-83.

[2] علاء الدين سلماني، مرجع سبق ذكره، ص 86.

أن تكون بصورة غير مباشرة والتي يتم فيها تسجيل الأحاديث عن طريق التنصت على المكالمات الهاتفية أو تسجيل الأحاديث الهاتفية ويكون هذا النوع من التسجيل خلسة أو بالسر في أغلب الأحوال[1].

يتم التسجيل الصوتي بطرق أهمها[2]:

- التسجيل الآلي: ويكون عادة بواسطة آلة خاصة تترجم موجات الصوت إلى اهتزازات خاصة عن طريق إبرة تعمل في سطح من الشمع أعد خصيصا لذلك. وتتفق هذه الاهتزازات مع الأصوات التي تحدثها بالضبط، ولكي يمكن إعادة الصوت، يكفي قلب العملية بحيث تؤثر العلامات على سطح الشمع في الإبرة التي تترجم ذلك آليا، أو كهربائيا، إلى أصوات متشابهة مع الأصوات الأولى التي تم تسجيلها.
- التسجيل المغناطيسي: تعد هذه الطريقة متطورة بالنظر إلى الطريقة السابقة، ويتم التسجيل وفق هذه الطريقة على شريط من البلاستيك، ويتم تمرير الشريط في رأس مسجل مغناطيسي يتصل به ميكرفون، ويحول الميكروفون الأصوات إلى ذبذبات كهربائية مطابقة تطبع على الشريط. وعند القيام بالتسجيل على شريط تماثلي، فإن الشريط يلامس أولا رأس المسح، ويقوم رأس المسح، الذي يتم تنشيطه تلقائيا أثناء التسجيل، بإنتاج مجال مغناطيسي قوي يزيل أية تسجيلات سابقة على الشريط، ويتحرك الشريط الخالي بعدئذ أمام رأس التسجيل.

المبحث الثالث: مدى مشروعية التقنيات الحديثة في المجال الجنائي

الأكيد أن العقوبة مهمة في ردع المجرم والحفاظ على حياة الفرد ، لكن عند توقيع العقوبة لابد من مراعاة حرمة الانسان وعدم التمثيل به أو تشويه أو العبث بجسمه سواء كان حيا أو ميتا ، ومنه سنقوم في هذا

[1] نوف حسين متروك العجارمة، حجية المستخرجات الصوتية والمرئية في الإثبات الجزائي دراسة مقارنة، رسالة مقدمة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2019، ص 34.

[2] جابر إسماعيل الحجاحجة، حجية التسجيل الصوتي في الإثبات الجنائي في ضوء الفقه الإسلامي، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 08، العدد 01، 2011، ص 22.

المبحث من تقديم مدى مشروعية هذه التقنيات الحديثة في مجال تنفيذ العقوبة الجنائية ، والتي تفرض دوما مراعاة الشرع وعدم تجاوز حدوده.

المطلب الأول: مشروعية البصمة الوراثية:

إن البصمة الوراثية تدل على هوية كل انسان بعينه، وإنها وسيلة حديثة للتعرف على الشخصية، والاستدلال من خلالها على مرتكبي الجرائم نتيجة أخذ العينات في مسرح الجريمة، ثم اجراء التحليلات اللازمة ومطابقتها على البصمات الوراثية للمتهمين بعد اجراء الفحوصات على بصماتهم الوراثية. إن استخدام البصمة الوراثية، والاستدلال بها كقرينة من القرائن الدالة على اكتشاف المجرمين واقاع العقوبة عليهم في غير الحدود والقصاص، أمر ظاهر الصحة والجواز لدلالة الأدلة الشرعية الخاصة بالأخذ بالقرائن والحكم بموجبها، ومشروعية استعمال الوسائل المتنوعة لاستخراج الحق ومعرفته. والمستند الشرعي لجواز الأخذ بالبصمة الوراثية في المجال الجنائي، أنها وسيلة لغاية مشروعة، وللوسائل حكم الغايات، ولما في الأخذ بها من تحقيق لمصالح كثيرة ودرء لمفاسد ظاهرة[21].

والقول بجواز الأخذ بالبصمة الوراثية في المجال الجنائي في غير الحدود والقصاص هو ما ذهب إليه الفقهاء في المجامع الفقهية، حيث أن مجلس المجمع الفقهي الاسلامي لرابطة العالم الاسلامي في دورته 15 المنعقد في مكة المكرمة في 1998/10/31م، ودورته 16 المنعقدة بمكة المكرمة في المدة من 05-2002/01/10م، نظر في موضوع البصمة الوراثية ومجالات الاستفادة منها وقرر أن البصمة الوراثية بمثابة دليل يمكن الاعتماد عليها في إثبات الجرائم التي لا يترتب عليها حد شرعي[3].

المطلب الثاني: مشروعية العينات من الدم واللعاب والعرق والبول والمني والشعر

1

[2] سلام محمد علي، مرجع سبق ذكره، ص 487-488.

[3] نفس المرجع، ص 488.

جاءت الشريعة الإسلامية الغراء بما يدل على جواز الأخذ بآثار العينات كما يلي[1]:

- ما روى عن عبد الرحمان بن عوف أن ابني عفراء تداعيا قتل أبي جهل يوم غزوة بدر، فقال رسول الله صلى الله عليه وسلم (هل مسحتما سيفكما؟) قالا: لا، فنظر إلى السيفين فقال: كلاكما قتله، وقضي بسلبه لمعاذ بن عمرو بن الجموح، واستدل الرسول بوجود الدم على سيفهم بأنهم اشتركا في قتله، ولكنه قضي لأحدهما دون الآخر بالسلب لأنه كان الأعمق ضربا بالسيف وذلك بأثر الدم على النصل، وهذا دليل أن صاحب السيف هو القاتل.
- ما ورد عن عمر بن الخطاب رضي الله عنه "أنه أتي إليه بامرأة تعلقت بشاب من الأنصار وكانت تهواه واحتالت عليه وأخذت بيضة وألقت صفارها وصبت البياض على ثوبها وبين فخذيها، ثم جاءت إلى عمر صارخة، فقالت: هذا الرجل غلبني في نفسي وفضحني في أهلي، وهذا أثر فعاله، فسأل عمر النساء، فقلن: إن ببدنها وثوبها أثر المني، فهم بعقوبة الشاب، فجعل يستغيث ويقول: يا أمير المؤمنين تثبت في امرئ، فو الله ما أتيت فاحشة وما هممت بها، فقد راودتني عن نفسي فاعتصمت، فقال عمر: يا أبا الحسن ما تري في أمرهم؟ فنظر رضي الله عنه إلى ما على الثوب، ثم دعا بماء حار شديد الغليان، فصب على الثوب فتجمد ذلك البياض، ثم أخذه واشتمه وذاقه فعرف طعم البيض، وزجر المرأة فاعترفت.
- ما ورد عن علي بن أبي طالب رضي الله عنه حيث قضي بأن المضروب إذا ادعى أنه أخرس يؤمر بإخراج لسانه ونخسه بإبرة فإن خرج الدم أحمر فهو صحيح اللسان، وإن خرج الدم أسود فهو أخرس.
- ما ورد عن الامام أحمد رحمه الله من أن امرأة ادعت أن زوجها عنين، وأنكر الزوج هذا –وهي ثيب– فإنه يخلى معها ويقال له أخرج ماءك على شيء فإن ادعت إنه ليس بمني جعل على

[1] سالم بن حامد بن علي البلوي، مرجع سبق ذكره، ص 122-123.

النار فإن ذاب فهو مني وبطل قولها ولو كان بياض لتجمد وتيبس، وإن قال إني أعجز عن إخراج مائي صح قولها.

ومن كل هذه الأدلة السابق سردها تؤكد على جواز الأخذ بالعينات واعتبارها دلائل تدل على ثبوت التهمة أو نفيها.

المطلب الثالث: مشروعية التسجيل الصوتي

إن الدليل المستمد من التسجيل الصوتي يعد قرينة ضعيفة ودلالته ظنية لا يدان المتهم بموجبها، ولكن يمكن الاستعانة بها لتقوية التهمة لا سيما إذا انضمت مع قرائن أخرى، وذلك للأسباب التالية[1]:

- أن الأصوات تتشابه، والمقصود بالتشابه هنا التشابه الظاهر للناس، وإلا فالأصوات تختلف من شخص لآخر، يدل على ذلك قوله تعالى: {ومن آياته خلق السماوات والأرض واختلاف ألسنتكم وألوانكم إن في ذلك لآيات للعالمين}[2].
- أنه من الممكن فنيا إدخال تبديل وإحداث تغيير واجراء عمليات حذف ونقل لعبارات من موضع إلى موضع آخر على شريط التسجيل وهو ما يطلق عليه عملية "المونتاج"، وبذلك أصبح من السهل تغيير مضمون التسجيل.
- عملية التشخيص الصوتي ما زالت تدور في حيز الظنون، والدراسات والتجارب التي لم تسفر عن أمر ولم تثبت على حال فلا يعتد بها الشرع حجة في تعيين شخصية الفاعل، لأن أحكام الشرع تناط بأمور ثابتة، ولا تناط بأمور مازالت لم تتبلور بشكل نهائي.

[1] حبيب تجاني طاهر، الاثبات الجنائي بالطرق الحديثة في الفقه الإسلامي والقانون النيجيري (دراسة فقهية مقارنة)، أطروحة لنيل درجة الدكتوراه في الفقه الإسلامي، كلية الدراسات العليا، جامعة السودان، 2019، ص 121-123.

[2] سورة الروم، الآية رقم 22.

لم يعرف التسجيل الصوتي إلا في وقتنا الحاضر، ولهذا لا يوجد له ذكر في كتب المؤرخين من الفقهاء فضلا عن المتقدمين منهم. ولكن نظرا لتطور أجهزة التسجيل حتى أصبحت سهلة الحمل وسهلة الاستعمال، وسهلة الاخفاء الذي يمكن أن يفاد منها في الإثبات، أو النفي يبرز سؤال عن مدى موقف الشريعة الإسلامية من حكم استخدام التسجيل الصوتي وسيلة إثبات، أما عن استخدامه لمعرفة أسرار الناس واكتشاف أحوالهم، فهذا حرام لقول الباري جل شأنه: "ولا تجسسوا ولا يغتب بعضكم بعضا أيحب أحدكم أن يأكل لحم أخيه ميتا فكرهتموه". والتجسس عام سواء أكان بجهاز التسجيل المعروف، أو بمراقبة المحادثات الهاتفية أو غيرها[1]

الخاتمــة:

يعد المجال الجنائي وجمع الاستدلالات من الأنشطة الأمنية التي تأتي في مقدمة محاولات مواجهة الجرائم المستحدثة وذلك عن طريق استحداث الأساليب والارتقاء بالمحققين وتزويدهم بالعلوم والتقنيات الحديثة، ولهذا حظيت التقنية في العقود الأخيرة باهتمام متزايد من قبل جميع الأمم، وقد برز هذا الاهتمام نتيجة الدور الذي لعبه التقدم العلمي والتقني في تطور الدول بصفة عامة والمجال الجنائي بصفة خاصة.

النتائج :

01*تعتبر العقوبة إحدى أهم الضمانات التي تهدف إلى حماية حياة الفرد وماله وعرضه ، وآلية ردع إلى كل من تسول له نفسه المساس بغيره .

02*رغم أن الشريعة كانت صارمة في تنفيذ العقوبة خاصة عند تطبيق القصاص ، إلا أنها راعت النفس البشرية وحرصت على عدم التعذيب والتمثيل بالمجني عليه، وهذا ما يؤكد على عظمة الإسلام واحترامه لآدمية الانسان حتى عند العقاب.

[1] حبيب تجاني طاهر، مرجع سبق ذكره، ص 119-120.

03*تطبيق التقنيات الحديثة في تنفيذ العقوبة في المجال الجنائي من شأنه يسهل توقيعها ، لكن لابد من مراعاة الشق الشرعي وعدم إهماله لأي سبب من الأسباب .

04*التقنيات الحديثة في تنفيذ العقوبة في المجال الجنائي لها أهمية كبيرة خاصة مع تطور أسلوب الجريمة وصورها ، والتي أحيانا يصعب التحقق من وقوعها ، لذلك الحداثة في وقوع الجريمة يصحبه الحداثة في أسلوب تنفيذ العقوبة مع ما تستوجبه الشريعة الاسلامية التي جاءت للحفاظ على الانسان وكل ما يتعلق به.

التوصيات :

01* ضرورة مراعاة الشق الشرعي دوما في تنفيذ العقوبة ، وذلك للموازنة بين الجريمة والعقوبة .

02*ضرورة التمكن من استخدام التقنيات الحديثة في تنفيذ العقوبة في المجال الجنائي ، وذلك لن يتأتى إلا بعد التمكن من هذه التقنيات .

03*ضرورة تدريب الأطقم الأمنية على هذه التقنيات وذلك من خلال الاستفادة من تجارب الدول الرائدة في مجال التقنيات والتكنولوجيا ، مع الاستمرار في مواكبتها وتطوير قطاع الأمن .

04*العمل على ضرورة تنفيذ العقوبة في المجال الجنائي بما تسمح به التقنيات الحديثة وذلك مع ما تراه الشريعة الاسلامية دون المساس بحق الانسان حتى عند توقيع العقوبة .

05*ضرورة جعل ضوابط وحدود في استخدام هذه التقنيات الحديثة ، وذلك حتى لا يكون هناك تعسف في استخدامها.

قائمة المراجع :

أ/ المذكرات و الاطروحات العلمية :

1. آمال عبد الرحمان يوسف حسن، الأدلة العلمية الحديثة ودورها في الإثبات الجنائي، رسالة مقدمة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2011.
2. حبيب تجاني طاهر، الاثبات الجنائي بالطرق الحديثة في الفقه الإسلامي والقانون النيجيري (دراسة فقهية مقارنة)، أطروحة لنيل درجة الدكتوراه في الفقه الإسلامي، كلية الدراسات العليا، جامعة السودان، 2019.
3. دنيا زاد ثابت، مشروعية إجراءات التحقيق الجنائي، مذكرة لنيل شهادة الماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر، دون سنة نشر.
4. سالم بن حامد بن علي البلوي، التقنيات الحديثة في التحقيق الجنائي ودورها في ضبط الجريمة، رسالة مقدمة لاستكمال نيل شهادة الماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف للعلوم الأمنية، الرياض، 2009.
5. عائشة مغاوي، مدى حجية الدليل المستمد من التسرب في الاثبات الجنائي دراسة مقارنة، مذكرة لنيل شهادة الماستر في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة مستغانم، 2020.
6. علاء الدين سلماني، دور الشرطة العلمية في إثبات الجريمة، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة بسكرة، 2013.
7. نوف حسين متروك العجارمة، حجية المستخرجات الصوتية والمرئية في الإثبات الجزائي دراسة مقارنة، رسالة مقدمة لنيل شهادة الماجستير في القانون العام، كلية الحقوق، جامعة الشرق الأوسط، 2019.

ب/ المقالات العلمية المحكمة:

8. جابر إسماعيل الحجاحجة، حجية التسجيل الصوتي في الإثبات الجنائي في ضوء الفقه الإسلامي، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، المجلد 08، العدد 01، 2011.
9. سلام محمد علي، أثر التقنيات الحديثة في الأدلة الجنائية دراسة مقارنة بين الشريعة والقانون، مجلة مداد الآداب، كلية القانون، الجامعة العراقية، العدد 11.
10. ..سلطان مرزوق فايز الحربي، أثر استخدام التقنيات الحديثة في مجال تنفيذ العقوبات الجنائية في تحقيق الزجر والردع، المجلة الالكترونية الشاملة، الجامعة السعودية الالكترونية، العدد 08، 2018.
10. محمد السعيد زناتي، أحمد بنيني، أثر أدلة الاثبات الجنائي الحديثة على الاقتناع الشخصي للقاضي الجزائي في التشريع الجزائري، مجلة الواحات للبحوث والدراسات، المجلد 14، العدد 01، 2021.

ج/ المحاضرات :

11. فريد روابح، محاضرات في القانون الجنائي العام، مطبوعة الدروس لطلبة السنة الثانية ليسانس، كلية الحقوق والعلوم السياسية، جامعة سطيف، 2018.
12. محمد العايب، مذكرة التشريع الجنائي المقارن، محاضرات لطلبة السنة الثالثة تخصص شريعة وقانون، كلية العلوم الإسلامية، جامعة باتنة، 2020.
13. نسمة حسين، دروس في القانون الجنائي العام الجريمة والجزاء المقرر لها، محاضرات مقدمة للسنة الثانية تخصص القانون الخاص، دون سنة نشر.

د/المواقع الالكترونية :

14 https://www.elmizaine.com/2021/05/blog-post_48.html

دور التكنولوجية الحديثة في مواجهة مخاطر تطبيق العقوبات السالبة للحرية قصيرة المدة " نظام الوضع تحت المراقبة الالكترونية نموذجا"

The role of modern technology in addressing the risks of applying penalties for the deprivation of liberty of short duration "Eletronic-surveillance system as a model"

تحانوت ناية

أستاذة محاضرة قسم أ

جامعة الجزائر 1 كلية الحقوق

nadiatahanout@gmail.com

الملخص:

استطاعت السياسة العقابية أن تساير وتوظف التطور التكنولوجي الحديث في مجال التنفيذ العقابي من خلال تبنيها لنظام الوضع تحت المراقبة الالكترونية لما حققته هذه التقنية من نجاح في الدول المتقدمة كآلية بديلة لمواجهة وتفادي مخاطر العقوبات السالبة للحرية القصيرة المدة والحد من مساوئها. وترتكز هذه الدراسة على الجوانب القانونية والتقنية لهذا النظام، التي تشمل مفهوم وأهمية هذه التقنية وشروط وطرق تطبيقها، ولا نكتفي ببيان فعاليتها ودورها أثناء تطبيقها بل سنبحث أيضا في مدى تأثيرها على حقوق الانسان.

الكلمات المفتاحية: المراقبة الالكترونية، التكنولوجية الحديثة، العقوبات السالبة للحرية، السوار الالكتروني

Abstract: The punitive policy was able to keep pace and employ modern technological developments in the field of punitive execution by adopting the system of electronic surveillance of the success of this technology in the developed countries as an alternative mechanism to counter and avoid the risks of sanctions against short-term liberty and reduce its disadvantages. This study is based on the legal and technical aspects of this system, which encompass the concept and relevance of this technique and the conditions and methods of its application, and not only demonstrate its effectiveness and role during its application, but also examine its impact on human rights

Keywords: electronic surveillance, modern technology, penalties for deprivation of liberty, electronic bracelet.

مقدمة

أمام سرعة وتيرة التطور التكنولوجي واجتياحه لمختلف المجالات، وجد مجال القانون نفسه متأثرا بهذه التطورات التي أصبحت ضرورة يجب مواكبتها ومسايرتها، وهو وما جعله عرضة للتعديل والتحديث، بصياغة نصوص تنظم الاستفادة من هذا التقدم التكنولوجي وضبطها حتى لا تحيد عن إطارها القانوني. ولقد تطلعت الأنظمة العقابية بدورها إلى ابتكار تقنيات حديثة من أجل تعزيز وتجسيد الأغراض التي ترمي إليها السياسة العقابية الحديثة، والمتمثلة في الإصلاح وإعادة التأهيل الاجتماعي للمحكوم عليه في مرحلة التنفيذ العقابي، لا سيما إذا تعلق الأمر بالعقوبات السالبة للحرية باعتبارها العقوبات الوحيدة التي يمكن أن تحقق فكرة الردع الخاص الذي يدخل فيه التأهيل.

وتجنبا لمساوئ العقوبات السالبة للحرية القصيرة المدة وآثارها السيئة على المحبوس، التي لم تعد تؤدي الأغراض المرجوة منها في الإصلاح والتأهيل، تمّ ابتكار نظام الوضع تحت المراقبة الإلكترونية كنظام يحل مشكلات هذا النوع من العقوبات، تحل فيه التكنولوجية الحديثة محل المراقب والحارس على تحركات وتنقلات المحكوم عليه الذي يتم اخضاعه لهذه التقنية.

وعليه، أصبح نظام الوضع تحت المراقبة الإلكترونية باعتباره نظام لتكييف العقوبة آلية بواسطتها يتم توظيف التكنولوجية الحديثة في مجال إعادة ادماج المحكوم عليه في المجتمع بمنحه فرصة ثانية، بتمكينه من قضاء كل العقوبة السالبة للحرية القصيرة المدة خارج المؤسسة العقابية عن طريق حمله للسوار الإلكتروني، الذي يعد نمطا حديثا من العقوبات الأكثر مرونة التي تسعى السياسة العقابية من خلالها إلى أنسنة وتفريد مرحلة التنفيذ العقابي خارج أسوار السجون. فهذه التقنية الحديثة تأتي إذن من أجل حل العديد من المشكلات التي تطرحها العقوبات السالبة للحرية قصيرة المدة ، وللتخلي قدر الإمكان عن الأنظمة التقليدية التي اثبتت فشلها من خلال حالات العود للجريمة وللمؤسسات العقابية.

وباعتبار الوضع تحت المراقبة الإلكترونية من الآليات الحديثة التي أفرزها التطور التكنولوجي في مجال تطبيق العقوبات السالبة للحرية، فإن الاشكالية التي تثار في هذا الصدد تتمثل في: **ما مدى فعالية تطبيق نظام الوضع تحت المراقبة الإلكترونية كتقنية مستحدثة في حل مشكلة العقوبات السالبة للحرية القصيرة المدة ؟**

وللإجابة على هذه الإشكالية، تم تقسيم الورقة البحثية إلى محورين إثنيين:

المحور الأول/ يتعلق بالإطار المفاهيمي لنظام الوضع تحت المراقبة الإلكترونية : تناولت فيه مفهوم نظام الوضع تحت المراقبة الإلكترونية، ثم تحديد خصائص هذا النظام، وأهميته كتقنية مستحدثة في السياسة العقابية.

المحور الثاني/ يخص الاطار التكنولوجي لنظام الوضع تحت المراقبة الالكترونية: وفيه تعرضت إلى شروط توظيف التكنولوجية الحديثة لتطبيق هذا النظام، ثم الطرق التقنية لتنفيذه، وصولا إلى الآثار المترتبة عن تطبيقه خاصة من جانب الآثار التي تمس بحقوق الانسان عن طريق استعمال التكنولوجية الحديثة. ثم نخلص بخاتمة تشمل أهم النتائج والتوصيات المتوصل إليها.

المحور الأول/ الإطار المفاهيمي لنظام الوضع تحت المراقبة الإلكترونية

توصّل الفكر العقابي الحديث إلى ضرورة استغلال نتائج التكنولوجيا الحديثة للحدّ من مساوئ العقوبة السّالبة للحرية القصيرة المدة باستحداث تقنيات جديدة بدلا من اللجوء إليها، حيث تشكل المراقبة الإلكترونية مرحلة جديدة وهامّة من مراحل تطور التنفيذ العقابي.

أولا/ مفهوم نظام الوضع تحت المراقبة الإلكترونية

قبل التطرق إلى تعريف نظام المراقبة الإلكترونية، نشير إلى أن الفقه الجنائي المقارن استخدم عدة مصطلحات تعبر عن مفهوم واحد لها، كالوضع قيد المراقبة الإلكترونية أو السوار الإلكتروني أو الإقامة الجبرية مع المراقبة الإلكترونية[1].

1- تعريف نظام الوضع تحت المراقبة الالكترونية

عرفت المادّة 150 مكرر الفقرة الثانية من قانون تنظيم السجون وإعادة الادماج الاجتماعي للمحبوسين المتمم بالقانون رقم 18-01، كما يلي " يتمثل الوضع تحت المراقبة الإلكترونية في حمل الشخص المحكوم عليه، طيلة المدّة المذكورة في المادة 150 مكرّر1 لسوار إلكتروني يسمح بمعرفة

[1]- رامي متولي القاضي، نظام المراقبة الإلكترونية في القانون الفرنسي والمقارن، مجلة الشريعة والقانون جامعة الإمارات العربية المتّحدة، ، العدد الثالث والسّتون، يوليو 2015، السنة التاسعة والعشرون، ص 284.

تواجده في مكان تحديد الإقامة المبيّن في مقرر الوضع الصّادر عن قاضي تطبيق العقوبات"،[1] فالمراقبة الإلكترونية هي طريقة حديثة لتنفيذ العقوبات السالبة للحرية بهدف درء الآثار السلبية لهذه العقوبات متى كانت قصيرة المدة[2]. فهذا الجهاز ليس كما يعتبره البعض أنّه يراقب كافة تحركات الشخص في كل زمان ومكان وكل صغيرة أو كبيرة في حياة المحكوم عليه، إذ أنّه يعلن فقط عن ابتعاد الشخص عن محل الإقامة المحدّدة له في محيطه المكاني[3]. وعلى هذا الأساس عرّف على أنه نظام يمكن من خلاله استخدام تقنيات التكنولوجية الحديثة من قبل أجهزة إنفاذ القانون خارج السجن في أماكن وأوقات محددة سلفا ومن خلال إخضاعه لمجموعة من الالتزامات والشروط، ويترتب على مخالفتها معاقبته بعقوبة سالبة للحرية[4]. ومما سبق يمكن استخلاص أهم الخصائص التي يتميز بها هذا النظام فيما يلي:

2- خصائص نظام الوضع تحت المراقبة الالكترونية

يعتبر الوضع تحت المراقبة الالكترونية نموذجا عقابيا مبتكرا ذو خصوصية واضحة يسعى إلى تقييد الحريّة لا إلى سلبها، وتعد الجزائر أول دولة عربية تستخدم السوار الالكتروني، وثاني دولة افريقية بعد دولة جنوب افرقيا، مما يدل على المجهودات التي تبذلها الجزائر من أجل مواكبة مختلف التطورات[5]، ولقد أخذت عدة تشريعات بهذا النظام بأشكال وصور مختلفة كآلية للحد من اكتظاظ السجون ومساوئه[6]، وذلك نظرا لمجموعة الخصائص التي يتميز بها النظام والمتمثلة في:

---

[1]-_ استحدث المشرع فصلا رابعا في الباب السادس الخاص بتكييف العقوبة تحت عنوان الوضع تحت المراقبة الإلكترونية ابتداء من المادة 150 مكرر إلى 150 مكرر 16 ، وذلك بموجب القانون رقم 18-01 المؤرخ في 30 يناير 2018 المتمم للقانون رقم 05-04 المتضمن قانون تنظيم السجون ، الجريدة الرسمية عدد 06 صادر في 30 يناير 2018.

[2]- أحمد سعود، المراقبة الإلكترونية كبديل للعقوبة السالبة للحرية قصيرة المدة، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 09، العدد03 ، السنة 2018، ص 680.

[3]- فريد بلعيدي، تنفيذ العقوبة السّالبة للحرية، مذكرة لنيل شهادة ماجيستير في علم الإجرام والعلوم الجنائية، جامعة أبي بكر بلقايد، تلمسان، كلية الحقوق، ص 54-55.

[4]-رامي متولي القاضي ، نظام المراقبة الإلكترونية في القانون الفرنسي والمقارن، المرجع السابق، ص 285.

[5]- سامية بوروبة، الجزائر أول دولة عربية تستخدم السوار الالكتروني: توسيع العقوبة البديلة عن السجن، المفكرة القانونية، يوم الاطلاع : 2 مارس 2018، الموقع: https://legal-agenda.com

[6] - يعرف التشريع الفرنسي ثلاثة أنواع من المراقبة الالكترونية ، فإلى جانب الوضع تحت المراقبة الالكترونية (PSE) ، تحديد الإقامة تحت المراقبة الالكترونية (ARSE) ، الوضع تحت المراقبة الالكترونية المتحركة(PSEM). للمزيد أنظر :

-Tony Ferri , La surveillance électronique pénale (son statut, son sens, ses effets) , Editions Bréal 2017, p / 27.

أ- الطابع التكنولوجي للمراقبة الالكترونية

يتميز نظام الوضع تحت المراقبة الالكترونية بالطابع التقني والفني، حيث يتطلب الوضع تحت هذا النظام وجود أجهزة تقنية تتمثل في جهاز استقبال موضوع في مكان الإقامة ويرتبط بخط تيليفوني، وجهاز إرسال يتم وضعه في يد الخاضع للرقابة، وجهاز كومبيوتر مركزي يسمح بتعقب المحكوم عليه عن بعد[1].

ب- الطابع المقيد للحرية للمراقبة الالكترونية

يظهر الطابع المقيد للحرية للمراقبة الالكترونية من خلال إلزام الشخص الخاضع لها بأحد التدابير المقيدة للحرية سواء من حيث المكان أو الزمان، ويمكن إجمال هذه القيود في:

القيود أو الالتزامات الواردة في المادة 150 مكرر 5 من قانون تنظيم السجون وتتمثل في :

- عدم مغادرة المحكوم عليه منزله أو المكان الذي يعيّنه قاضي تطبيق العقوبات خارج الفترات المحدّدة في مقرر الوضع، وتؤخذ بعين الاعتبار الأوقات والأماكن التي يمارس فيها مهنة أو لمتابعة دراسة أو تكوين أو تربص أو شغله لوظيفة أو لمتابعة علاج[2].

- يجب على الشخص الموضوع تحت المراقبة الإلكترونية أن يضع السوار الإلكتروني على مدار اليوم أي 24 ساعة.

أما القيود أو الالتزامات الواردة في المادة 150 مكرر 6 من قانون تنظيم السجون فهي:

-عدم ارتياد بعض الأماكن،

-ممارسة نشاط مهني أو متابعة تعليم أو تكوين مهني،

-عدم الاجتماع ببعض المحكوم عليهم، بما في ذلك الفاعلين الأصليين والشركاء في الجريمة،

-عدم الاجتماع ببعض الأشخاص لاسيما الضحايا والقصر،

-الالتزام بشروط التكفل الصحي أو الاجتماعي أو النفسي، والتي تهدف إلى إعادة ادماجه اجتماعيًا.

- كما يتضمن أيضًا مقرر الوضع تحت المراقبة الإلكترونية إلزام المحكوم عليه بالاستجابة إلى استدعاءات قاضي تطبيق العقوبات أو السلطة العمومية التي يعيّنها له هذا الأخير[3].

---

[1]- عبد الرحمان خلفي ، بدائل العقوبة دراسة فقهية تحليلية تأصيلية مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2015، ص 246.

[2]- أحمد سعود، المراقبة الإلكترونية، المرجع السابق، ص 689.

[3]- محمد أمين بكوش، نبيلة هبة هروال، المراقبة الإلكترونية في التشريع الجزائري، مجلة الدراسات الحقوقية، جامعة الدكتور طاهر مولاي سعيدة ، العدد 1 ، الجزء 06 ، السنة 2019، ص 136 -137

ج– الطابع الرضائي للوضع تحت المراقبة الالكترونية

تعتبر المراقبة الالكترونية بديلا رضائيا صريحا، يتجلى ذلك من خلال اشتراط قبول الشخص الذي سيخضع لها، ولا يمكن الحديث على نجاح هذا النظام ما لم يكن المعني به متقبلا ومتعاونا في تنفيذه، والحكمة من اشتراط الرضا بتطبيق المراقبة الالكترونية كون هذه الأخيرة تقيد حرية المحكوم عليه في التنقل وقد تمس بخصوصيته، فالرضا يجعله يتنازل عن بعض حقوقه التي تصبح بمثابة إلتزامات يتقيد بها [1]. ولقد نصت المادة 150 مكرر 2 على الرضا واعتبرته شرطا أساسيا، حيث لا يمكن تطبيق هذا النظام إلاّ بموافقة المحكوم عليه أو ممثله القانوني إذا كان قاصرا.

د– الطابع القضائي للوضع نحت المراقبة الالكترونية

تتسم المراقبة الالكترونية بالطابع القضائي، على أساس أن القضاء هو الحامي والحارس الطبيعي على حقوق وحرّيات الأفراد، ولضمان ذلك أسند المشرّع صلاحية تقرير هذا النظام إلى قاضي تطبيق العقوبات تلقائيا، أو بناءً على طلب المحكوم عليه أو محاميه أو ممثله القانوني في حالة ما إذا كان المحكوم عليه حدثًا وهو ما يستخلص من نصّ المادة 150 مكرر 1 من قانون تنظيم السجون ، حيث يتم تقديم طلب الاستفادة من هذا النظام إلى قاضي تطبيق العقوبات لمكان إقامة المحكوم عليه أو المكان الذي يوجد به مقر المؤسسة العقابية للمحبوس بها المعني، ويفصل قاضي تطبيق العقوبات في طلب الاستفادة في أجل قدره 10 أيام من إخطاره ويكون الفصل بمقرّر غير قابل لأيّ طعن ، ويمكن للمحكوم عليه الذي رفض طلبه أن يقدّم طلبا جديدا بعد مضي 6 أشهر من تاريخ رفض طلبه عملا بالمادة 150 مكرر 4. وبالإضافة إلى مهمة إصدار قرار وضع المحكوم عليه تحت المراقبة الالكترونية، فقد أناط المشرع بقاضي تطبيق العقوبات دون غيره مهمة الإشراف والمراقبة، وإن أشار في بعض النصوص إلى ضرورة أخذ رأي النيابة العامة ولجنة تطبيق العقوبات في ذلك[2]. ويتعين في حالة وجود أي خرق لمواقيت أو لالتزام من التزامات الوضع اخطار قاضي تطبيق العقوبات فورا مع ارسال تقارير دورية له.

---

[1] _ عبد اللطيف بوسري ، العقوبة الرضائية وأثرها في ترشيد السياسة العقابية ، أطروحة دكتوراه في العلوم الجنائية ، جامعة باتنة –1– كلية الحقوق والعلوم السياسية ، 2018/2017 ، ص 213.

[2] – جمال قتال ،الوضع تحت المراقبة الالكترونية وفق مقتضيات قانون رقم 18–01 المتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين ،مجلة معالم الدراسات القانونية والسياسية ،المجلد 04 ،العدد 01 ،السنة 2020 ،ص 337.

هـ- الطابع المؤقت للوضع تحت المراقبة الالكترونية

يتميز الوضع تحت المراقبة الالكترونية بأنه إجراء مؤقت وغير مستمر، أي محدد المدة والتوقيت، ينتهي بمجرد انتهاء مدة العقوبة المحكوم بها، والتي يتعين أن لا تتجاوز ثلاث (3) سنوات، ولقد أجاز القانون لقاضي تطبيق العقوبات إلغاء هذا النظام ووضع حد له، وذلك في حالة عدم احترام المعني لالتزاماته دون مبررات مشروعة، أو في حالة الإدانة الجديدة، أو إذا طلب المعني ذلك[1]، على أن ينفذ هذا الأخير بقية العقوبة المحكوم بها داخل المؤسسة العقابية بعد اقتطاع مدة وضعه تحت هذا النظام.

ثانيا- أهمية نظام الوضع تحت المراقبة كتقنية مستحدثة في السياسة العقابية

تبنى المشرع الجزائري هذا النظام لتحقيق الاستفادة من التكنولوجية الحديثة في مجال السياسة العقابية باعتبارها أحد الوسائل المستحدثة لحل مشكلة تطبيق العقوبات السالبة للحرية قصيرة المدة داخل المؤسسات العقابية، التي لم تعد تؤدي هدفها التربوي أو الإصلاحي للمحبوس، كما أنها تؤدي لنتائج أخرى ضارة كاكتظاظ السجون، حتى قيل أنه دواء أسوء من الداء[2]، وتكمن أهمية هذه التقنية في:

أولا : الوضع تحت المراقبة الالكترونية كتقنية للتخفيف من اكتظاظ السجون

يعد اكتظاظ السجون ظاهرة لا يكاد يخلو سجن أو مؤسسة إصلاحية منه اليوم، وهي واحدة من أصعب المشاكل التي تعاني منها نظم العدالة الجنائية في جميع إنحاء العالم، واللجوء إلى نظام الوضع تحت المراقبة الالكترونية من شأنه التخفيف من الاكتظاظ التي تشكو منه السجون، خاصة تلك التي يقيم بها المحبوسين المبتدئين ممن ارتكبوا أفعالا جنحية[3]. فبتزايد الأخذ بالعقوبات السالبة للحرية القصيرة المدة كرد فعل عقابي وردعي المعتمد من التشريعات لمواجهة الجريمة، تفاقم الوضع وشكل ضغطا كبيرا على السجون وطاقتها الاستعابية، وهو ما أدى إلى عرقلة دور الإصلاح أو تهذيب المحبوسين المحكوم عليهم

---

[1] _المادة 150 مكرر 10 من قانون 18-01 المتمم لقانون تنظيم السجون.

[2]-نيلة صدراتي ،الوضع تحت المراقبة الاليكترونية كنظام جديد لتكييف العقوبة (دراسة في ضوء القانون رقم 18-01 المتمم لقانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين) ،مجلة الدراسات والبحوث القانونية ،المجلد 3، العدد 02 ،جوان 2018 ،ص 162.

[3]- أيمن عبد العزيز الملك، بدائل العقوبات السالبة للحرية كنموذج لإصلاح في نظام العدالة الجنائية، أطروحة دكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا قسم العلوم الاجتماعية، المملكة العربية السعودية 2010، ص 29.

لما يخلفه من آثار وتداعيات وخيمة على نفسيتهم. ولما كان اكتظاظ السجون من بين مسببات زيادة الخطورة الإجرامية لدى المحكوم عليهم، فإن الوضع تحت المراقبة الالكترونية يعد أداة مفيدة واقتراح بديل عن الحبس القصير المدة تطبيقه يحل ويحد من مشكلة الاكتظاظ، ويحول دون تعرض الأشخاص غير الخطيرين إلى العزلة الاجتماعية[1].

ثانيا : الوضع تحت المراقبة الالكترونية كتقنية للتخفيض من معدلات العود للجريمة

يعد العود إلى الجريمة أحد أبرز المشاكل التي تعاني منها السياسات العقابية التي حاولت إيجاد حلول لها، ومن بينها تطبيق نظام الوضع تحت المراقبة الالكترونية باستعمال السوار الالكتروني باعتبارها تقنية تنفذ خارج المؤسسة العقابية، إذ يمنع اختلاط المحكوم عليه بالمجرمين المحترفين الذي من خلاله أثبتت الدراسات والبحوث أن خريجي السجون يميلون للعودة للجريمة بسبب اندماجهم مع مجرمين أكثر خطورة منهم عن طريق الاحتكاك بهم خاصة مروجي المخدرات والتهريب، فالعزل عن المجتمع أمر يفقد روح المبادرة ويولد الشعور بالحقد والكراهية وذلك بسبب ضعف برنامج التأهيل داخل هذه المؤسسات وعدم الاهتمام اللاحق بخريجي هذه المؤسسات العقابية[2] .

ثالثا : الوضع تحت المراقبة الالكترونية كتقنية للتخفيض من النفقات المالية

إن تنفيذ عقوبة الحبس السالبة للحرية ترهق ميزانية الدولة نتيجة ما تنفقه من مبالغ مالية طائلة لتشييد السجون، وتوفير الوسائل المالية والبشرية لحسن تسييرها من خدمات لازمة للمحكوم عليه من اطعام وإيواء وعلاج وحراسة، بالإضافة إلى مصاريف التي تنفقها الدولة في تصنيف المجرمين داخل المؤسسات العقابية مراعاة لاعتبارات التأهيل، إذ أن الإفراط المستمر في اللجوء إلى العقوبات السالبة للحرية قصيرة المدة يرهق ميزانية الدولة، حيث تقدر نفقات نظام المراقبة الالكترونية في اليوم الواحد أقل بأربع مرات من يوم في السجن[3]، فتطبيق هذا النظام سيمكن من اقتصاد مبالغ وميزانية مالية كبيرة توجه سنويا إلى إدارة

---

[1]– نادية تحانوت، مصير أنسنة السجون بعد جائحة كورونا، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 58، العدد 02، السنة 2021، ص 450.

[2]–عامر جوهر وعباسة الطاهر، السوار الالكتروني إجراء بديل للعقوبة السالبة للحرية في التشريع الجزائري، مجلة الاجتهاد القضائي، العدد 16، السنة مارس 2018 ، ص 186 .

[3]–رامي متولي القاضي، توظيف التقنيات الحديثة في مجال السياسة العقابية(السوار الالكتروني نموذجا)، مجلة الفكر الشرطي، مجلد 26، العدد 103،السنة اكتوبر 2017،ص 294.

السجون[1]، بفعل تقليل عدد المحبوسين ومن الاكتظاظ داخل المؤسسة العقابية. دون أن ننسى أن تطبيق نظام الوضع تحت المراقبة الالكترونية بالسوار الالكتروني يمكن الشخص الحامل له من ممارسة أي نشاط مهني أو أي وظيفة معهودة له، بالإضافة إلى مزاولة دراسته أو التكوين بشكل طبيعي[2].

المحور الثاني/ الإطار التكنولوجي لنظام الوضع تحت المراقبة الإلكترونية

تكمن أهمية نظام الوضع تحت المراقبة الالكترونية في تعزيز أوجه الاستفادة من التطور التكنولوجي وتكريسه في خدمة العدالة الجنائية، عن طريق إدخال تقنيات حديثة في مجال تطبيق العقوبات السالبة للحرية لا سيما القصيرة المدة لتجنب مساوئها وآثارها السلبية أثناء التنفيذ العقابي، وخصص هذا المحور لتناول شروط توظيف التكنولوجية الحديثة في مجال هذا النظام، وكذا الطرق التقنية التي يتم بواسطها تنفيذه، وأثره على حقوق الانسان.

أولا : شروط توظيف التكنولوجية الحديثة لتطبيق آلية المراقبة الالكترونية

يتطلب تطبيق إجراء المراقبة الالكترونية على أرض الواقع مجموعة من الشروط التقنية عبارة عن أجهزة مرتبطة فيما بينها تعمل على تسهيل عملية المراقبة، كما يتطلب هذا الاجراء بعض الشروط المادية تتعلق بمحيط الشخص المراد إخضاعه لها.

1- الشروط التقنية لتطبيق آلية المراقبة الالكترونية

تجدر الإشارة أنه في أحكام القانون 18 /01 لم يتطرق المشرع الجزائري إلى الشروط التقنية وما يتطلبه الوضع تحت المراقبة الالكترونية من مستلزمات سوى نصه على وضع السوار الالكتروني. وعلى العموم فإن الشروط التقنية تنحصر في 3 عناصر سنذكرها كالآتي :

أ- السوار الالكتروني : وهو عبارة عن جهاز إلكتروني يشبه ساعة اليد كبيرة الحجم ومستطيلة الشكل ذات لون أسود على غرار ساعات الغطس، ويتم وضعه إما في معصم اليد أو في كاحل القدم للشخص الذي يحمله من خلال رباط مطاطي، ويبلغ وزنه حوالي 100غ إلى 142غ ويقوم هذا الجهاز بإرسال إشارات كهرومغناطيسية خلال فترة زمنية محددّة (كل 30 ثانية) في محيط مسافة محددّة أن لا

---

[1]-عامر جوهر ،عباسة الطاهر ،المرجع السابق ،ص 191و 192.

[2]-أنظر المادة 150 مكرر 6/الفقرة الأولى من قانون 18-01 المعدل والمتمم لقانون تنظيم السجون

تزيد عن خمسين مترًا[1]، يتم التقاطها عن طريق جهاز الاستقبال بالشكل الذي يمكن مركز المراقبة من التأكد من تواجد الشخص في المدى الجغرافي المحدّد قضائيًا في قرار الوضع تحت المراقبة الإلكترونية[2].

يتميز السوار الالكتروني بمجموعة من الخصائص التقنية التي تدخل في تكوينه، فهو جهاز مقاوم للماء والحرارة والرطوبة والغبار والأشعة فوق البنفسجية ويتحمل قوة الضغط والاهتزازات والذبذبات والصدمات وقابل للشحن، كما أنه ضد الحساسية لكونه يحتوي على عازل مصنوع من قماش حتى لا يؤثر على بشرة حامله، ويتميز بكونه غير قابل للتمزق أو القطع، وفي محاولة العبث بهذا الجهاز عن طريق الكسر أو الإتلاف يقوم بإرسال إشارات تحذيرية لضُباط المراقبة[3].

ومن الناحية الفنية فإن السوار الإلكتروني المعمول به في الجزائر يتمثل في قطعة معدنية تحيط بكاحل المحكوم عليه، وتتكون من جزأين الأول به شريحة الهاتف النقّال وأنظمة لتحديد المواقع، والثاني بطّارية لشحن السّوار، ويرفق السّوار لوحة تحكم منقولة يحملها المتهم معه، تتضمن تطبيقًا يسهل عمل مصالح المراقبة في تحديد المواقع المسموحة والممنوعة عليه[4].

ب- وحدة الاستقبال : هو عبارة عن جهاز إلكتروني مستقبل، يتم تثبيته في محل إقامة الشخص الخاضع للإجراء، يتم ربطه بخط تيليفوني ثابت بالدائرة الكهربائية لهذا المكان وربطه بجهاز الكمبيوتر المركزي الخاص بالمراقبة، حيث يقوم هذا الأخير برصد الإشارات الواردة من جهاز الارسال –السوار الالكتروني – ثم يقوم بفك شيفرتها وإعادة ارسالها عبر الخط التليفوني الى جهاز آلي مركزي، كما تقوم وحدة الارسال تلقائيا بإرسال رسائل تحذيرية إلى الحاسب الآلي في حالة خروج الخاضع للمراقبة عن الاطار الجغرافي المحدد له[5] .

---

[1] – سعاد خلوط ، عبد المجيد لخذاري، الوضع تحت المراقبة الالكترونية كآلية مستحدثة للتفريد العقابي في التشريع الجزائري وفقا لقانون 18-01، مجلة البحوث والدراسات، مجلد 15، عدد 2، السنة 2018 ، ص 248.

[2]– عبد اللطيف بوسري، المرجع السابق، ص 215.

[3] فيصل بدري، الوضع تحت المراقبة الالكترونية –السوار الالكتروني كبديل للعقوبة السالبة للحرية قصيرة المدة–، مجلة الباحث للدراسات القانونية والسياسية، مجلد 2، العدد 10، السنة جوان 2018، ص 805.

[4]– فوزية هوشات، العقوبات البديلة في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوة منتوري، قسنطينة ، المجلد 30، عدد 2، السنة ديسمبر 2019، ص294.

[5]–رامي متولي القاضي ، نظام المراقبة الإلكترونية في القانون الفرنسي والمقارن، المرجع السابق، ص 288.

ج – مراكز المراقبة : جهاز كومبيوتر مركزي بالإضافة إلى أجهزة ومعدات إلكترونية أخرى ثانوية يتم ربطها به، عادة ما يكون منصبا في الإدارة العقابية، ويشرف على استعماله أعوان مؤهلين فنيا، ولا بد أن يكون هذا الكمبيوتر مزود ببرامج وتقنيات تسمح له بالتواصل مع السوار الالكتروني، والتقاط الإشارات المرسلة منه كتقنية GPS للبحث وتحديد الأماكن عبر الأقمار الصناعية، كما يقوم بمهمة تحديد طبيعة الإنذارات المرسلة، ومعرفة ما إذا كانت تلك الإنذارات سببها عدم التزام الخاضع للمراقبة الالكترونية بواجبات المراقبة أو عبثه بجهاز المراقبة، أم أنها مجرد عطل فني، ففي هذه الحالة الأخيرة يتعين إخطار قاضي تطبيق العقوبات بذلك، ليبادر بإرسال التقنيين القائمين على وضع وتركيب أجهزة المراقبة الإلكترونية إلى محل إقامة الموضوع تحت المراقبة لمعاينة الأجهزة والتأكد من أسباب الخلل[1].

2 / الشروط المادية لتطبيق آلية المراقبة الالكترونية

نص المشرع الجزائري على الشروط المادية في المادة 150 مكرر 3، وأكد أن جميع الوسائل التقنية عند اتخاذها يجب مراعاة مجموعة من الشروط التي تتمثل في :

أ– أن يكون للمحكوم عليه مقر سكن أو محل إقامة ثابت: يقوم قاضي تطبيق العقوبات بتحديد محل الإقامة سواء كان خاصا بالمحكوم عليه أو غيره، وفي هذه الحالة يجب الحصول على موافقة مالك العقار أو مؤجره لإتباع إجراءات المراقبة الالكترونية[2]. وبهذا الصدد نلاحظ أن المشرع الجزائري لم يحدد هل يكون محل الإقامة ملكا للمحكوم عليه أو ملكا للغير، وما هو الحكم في الحالة الأخيرة، عكس المشرع الفرنسي الذي أوجب الحصول على موافقة مالك العقار أو مؤجره في حالة ما إذا كان محل إقامة المحكوم عليه ملكا للغير[3].

ب– الشروط الخاصة بحامل السوار الالكتروني: لقد أولى التشريع الجزائري عناية خاصة بالمحكوم عليه خاصة فيما يتعلق برضائه على حمل السوار الالكتروني وألا يمس بصحته[4]، إذ لا يجوز وضع السوار الالكتروني إلا اذا ثبت أنه لا يضر بصحة المعني حسب ما تقرره المادة 150 مكرر 3، ويثبت

---

[1]– شعيب ضريف، المراقبة الإلكترونية للمحكوم عليهم في السياسة العقابية الجزائرية، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة احمد دراية، المجلد 03، العدد1، السنة جوان 2019 ، ص 180.

[2]– سعاد خلوط ، عبد المجيد لخذاري ، المرجع السابق، ص 247 .

[3]– رامي متولي القاضي، توظيف التقنيات الحديثة في مجال السياسة العقابية(السوار الالكتروني نموذجا)،ص 281.

[4]– الزهرة كوميشي، اساليب المعاملة العقابية داخل السجون، الطبعة الاولى، دار الباحث 2019، ص 167.

ذلك بشهادة طبية تؤكد أن الحالة الصحية للشخص تتوافق مع وضع السوار الالكتروني، فإذا أثبت من التقرير الطبي أن الوسائل التقنية قد ألحقت ضررا بصحة الخاضع لها أو بسلامته الجسدية، فإنه يتعين في هذه الحالة إلغاء مقرر الوضع تحت المراقبة الالكترونية[1].

ومن جهة ثانية، تؤخذ بعين الاعتبار الوضعية العائلية للمعني أو متابعته لعلاج طبي أو نشاط مهني أو دراسي أو تكويني، أو إذا أظهر ضمانات جدية للاستقامة عن الوضع تحت المراقبة الالكترونية[2]، والهدف من ذلك هو ضمان توافق قرار الوضع تحت المراقبة الالكترونية مع الحالة الفردية والشخصية لكل محكوم عليه، فتحدد أوقات الحضور حسب المعطيات المهنية والعائلية له.

وبالمقابل لا يتم وضع المحكوم عليه تحت المراقبة الالكترونية إلا بعد أن يسدد مبالغ الغرامات والمصاريف القضائية المحكوم بها عليه، غير أن أغفل المشرع الجزائري في المادة 150 مكرر 3 ولم ينص على سداد مبلغ التعويضات المحكوم بها كشرط للاستفادة من هذا الإجراء، بالرغم من أنها مبالغ مقررة لصالح الضحايا من شأنها أن تجبر تلك الأضرار وتساعد المحكوم عليه على ادماجه اجتماعيا.

ج- أن يكون محل الإقامة مزودا بخط هاتفي: يكفي أن يكون جهاز التيليفون مهيئا لاستقبال الاتصالات الهاتفية التي تأتي من طرف الهيئة المكلّفة بالسّهر على المراقبة الإلكترونية، لتؤكد من مدى تواجد المحكوم عليه في محل إقامته أو المكان المخصص لأداء وظيفته أو ممارسة تعليمه أو أثناء قيامه بأي نشاط محدد بموجب مقرر الوضع تحت المراقبة الإلكترونية، حيث يقوم جهاز الإرسال الذي يحمله المحكوم عليه في معصمه أو كاحله بإرسال معلومات متتالية طيلة المدة التي يكون فيها المحكوم عليه غائبًا عن محل إقامته إلى جهاز الاستقبال الموصول بخط تيليفوني ثابت، ولا يشترط أن يكون الخط الهاتفي هذا متصلاً بخدمة الانترنت، كما لا يوجد مانع أن يستخدمه المحكوم عليه في إرسال واستقبال مكالمات شخصية[3].

---

[1]- اليازية سلطان الظاهري، الوضع تحت المراقبة الالكترونية في التشريع الاماراتي، مذكرة ماجستير في القانون العام، جامعة الامارات العربية المتحدة، كلية الحقوق قسم القانون العام، نوفمبر 2020، ص 58.

[2]-نلاحظ ان المشرع الجزائري لم يحدد مختلف الضمانات الجدية للاستقامة خاصة أن هذه الفئة لم يتم وضعها مسبقا في المؤسسة العقابية، وعليه تعد مبادرة المعني بالوضع تحت المراقبة الالكترونية إلى إصلاح الاضرار التي خلفتها الجريمة أو تعويض الضحايا من الضمانات الجدية التي تدل على استقامته. - نبيلة صدراتي ، المرجع السابق، ص 166

[3]- شعيب ضريف، آليات تنفيذ العقوبة السالبة للحرية في التشريع الجزائري، اطروحة لنيل شهادة دكتوراه ل م د في القانون العام تخصص قانون جنائي وعل.م الاجرام، جامعة الجزائر 1 كلية الحقوق، جانفي 2019، ص 93.

ثانيا: الطرق التقنية لتنفيذ الوضع تحت المراقبة الالكترونية

مع انتشار نظام الوضع تحت المراقبة الالكترونية في أغلب التشريعات الحديثة تنوعت آلية تنفيذها إلى ثلاث طرق تتمثل في:

1- المراقبة الالكترونية بطريقة التحقق من الصوت

تتم هذه الطريقة بحبس الشخص الموضوع تحت المراقبة الالكترونية في المنزل عن طريق الاتصالات الهاتفية، بعد أخذ بصمة الصوت له التي يتم تخزينها بطريقة إلكترونية، حيث يقوم النظام الالكتروني بالرقابة والتوثيق المستمر عن وجود المعني في البيت من عدمه من خلال مكالمة هاتفية بواسطة حاسوب مركزي، ويتوجب على الشخص الخاضع لهذا النظام أن يستجيب للمكالمة ويكرر الكلمات التي سيتوجب قولها، وبعدها يقوم الحاسوب بمقارنة هذه الكلمات مع النموذج الآلي لصوته[1].

وفي حالة عدم مطابقة بصمة صوت المتصل لبصمة الصوت الأصلية المسجلة على الكمبيوتر المركزي الخاضع لهذا النظام أو قيامه باستخدام تليفون آخر في الاتصال في الأوقات المحددة له فيها بالبقاء في المنزل وفي المكان المحدد لتنفيذ الحبس المنزلي ، يقوم الكمبيوتر المركزي بإثبات مخالفته لقواعد تطبيق النظام، ومن الدول التي تستخدم هذه الوسيلة الولايات المتحدة الأمريكية، بلغاريا، إنجلترا[2].

2- المراقبة الإلكترونية عن طريق البث المتواصل

تتم من خلال جهاز يسمح بمتابعة المحكوم عليه للتأكد من وجوده في المكان المخصص له ، ذلك بوضع سوار إلكتروني في معصم الخاضع للمراقبة أو أسفل قدمه، يقوم كل 15 ثانية بإرسال إشارات محددة إلى الجهة المشرفة على المراقبة التي تتعرف من خلال هذه الإشارات على وجود الخاضع للمراقبة في النطاق الجغرافي المحدد له، وهذه التقنية أخذ بها المشرع الفرنسي[3]، وهي نفس التقنية التي أخذ بها التشريع الجزائري، حيث يستخلص من نص المادة 150 مكرر "يتمثل الوضع تحت المراقبة الالكترونية في حمل الشخص المحكوم عليه طيلة المدة المذكورة في المادة 150 مكرر 1 السوار الالكتروني يسمح

---

[1] -محمد صالح معزي، الاتجاهات الحديثة في العقوبات البديلة، الطبعة 1، دار غيداء للنشر عمان، 2016، ص 46.

[2]- سعاد خلوط ، عبد المجيد لخذاري ، المرجع السابق ، ص 248-249 .

[3]- محمد بن حميد المزمومي، المراقبة الالكترونية كبديل للعقوبة السالبة للحرية دراسة في ضوء النظام السعودي والأنظمة المقارنة، مجلة صوت القانون، مجلد 7، عدد 2، السنة نوفمبر 2020، ص 874

بمعرفة تواجده في مكان تحديد الإقامة المبين في مقرر الوضع الصادر عن قاضي تطبيق العقوبات". وقد أدت التجارب الأولية باستخدام سوارين الكترونيين على مستوى محكمة تيبازة قصد التأكد من نجاعة هذه التقنية ليتسنى تعميمها على باقي الجهات القضائية، كما حقق اجراء تجارب التقنية في حيز الخدمة مع متعاملي الهاتف النقال نتائج مرضية.

3- المراقبة الالكترونية عن طريق الاقمار الاصطناعية

تقوم تقريبا على نفس المتطلبات الفنية، بحيث يقوم السوار الالكتروني بإرسال موجات مؤمنة ومشفرة حسب هوية كل شخص تحت المراقبة، إلا أنها طويلة بالقدر الذي تلتقطه الأقمار الاصطناعية، وقد كانت فرنسا تستعمل في بداية هذا الإجراء جهازا مستقلا يدعم قوة الموجات الصادرة عن السوار، ويثبت على حزام الخاضع للمراقبة، أين يتم معالجتها وإعادة إرسالها بموجات طويلة ومشفرة إلى الكمبيوتر المركزي بالمركز المكلف بالمتابعة والمراقبة، لتحديد المكان ومواقيت تواجد الخاضع لهذا الإجراء. وتختلف هذه التقنية عن سابقتها في كونها مراقبة مستمرة تتبع باستمرار موقع الشخص الخاضع للمراقبة باستعمال نظام عالي الدقة يسمى " GPS" ، إلا أن تكلفتها باهظة، بالإضافة إلى وجود معوقات كثيرة ومتعددة تحول دون نجاعتها، أهمها عدم استقبال الأقمار الاصطناعية للموجات التي يرسلها السوار الالكتروني نتيجة بعض المكونات الجزيئية الموجودة في الغلاف الجوي، أو لوجود مباني شاهقة أو عازلة للموجات وغيرها، وأخذت بهذه التقنية الولايات المتحدة الأمريكية، وهي البلد الوحيد إلى حد الآن الذي يعمل بهذه التقنية[1].

ثالثا: أثر تقنية الوضع تحت المراقبة الالكترونية على حقوق الانسان

لا يخلو استعمال التكنولوجية الحديثة من مخاطر على حقوق الانسان، فبالرغم من مزايا استخدام تقنية المراقبة الالكترونية في السياسة العقابية التي تساهم في اصلاح وتأهيل المحكوم عليه بإنقاذه من الوسط الاجرامي ومن العود إلى الجريمة، وبالتخفيف من الاكتظاظ من السجون، إلا أن تطبيقها يثير بعض المشاكل التي تمس بكرامة الانسان وسلامته الجسدية وخصوصته [2].

---

[1]- محمد بن حميد المزمومي، المرجع نفسه، ص 873.

[2] - تنص الفقرة 2 من المادة 150 مكرر 2 من القانون رقم 18-01 المعدل والمتمم لقانون تنظيم السجون على "يجب احترام كرامة الشخص المعني وسلامته وحياته الخاصة عند تنفيذ الوضع تحت المراقبة الالكترونية".

1- أثر تقنية الوضع تحت المراقبة الالكترونية على كرامة الانسان

قد يعرض استخدام السوار الالكتروني الشخص الذي يحمله إلى نظرات مريبة من بعض أفراد المجتمع، حيث ينظر إليه على أنه انسان خطير وخارج عن القانون، حيث أصبح حمله يشكل وصمة عار تلاحق حامله مما يجبره على العزلة والانطواء، كما يترك في نفسيته نوعا من الإيلام والمعاناة نظرا لشعوره بأنه مراقب في كل وقت وفي أي مكان يرتاده[1]، بالإضافة إلى كونه ليس حرا في تحركاته وأن عليه العودة إلى البيت قبل الوقت المحدد، وفي حال غيابه تنطلق صفارة الانذار، دون أن ننسى الزيارات الفجائية للمشرفين والمراقبين[2].

في الحقيقة لا يمكن الاحتجاج بما سبق طالما كان المعني بالوضع تحت نظام المراقبة الالكترونية على علم مسبق بهذا النظام وما يفرضه عليه من إلتزامات فيها مساس بكرامته، خاصة وأن المشرع لم يغفل المبدأ الدستوري الذي يضمن كرامة الانسان عند ادراج التكنولوجيات الحديثة في مجال التنفيذ العقابي[3]، فلا يتم وضعه تحت هذا النظام إلا بعد موافقته التي تدل على تجاوبه مع الجهات المسؤولة على تنفيذه والتقيد بإلتزاماته، ومن جهة أخرى أجاز القانون للمعني طلب إلغاء هذه التقنية. كما يبقى السوار الالكتروني جهازا ليس من الضخامة بمكان، حجمه بسيط يمكن حجبه وستره بملابس حامله، أما عن الايلام النفسي الذي قد يشعر به حامله على نحو يشينه يعد ضئيلا مقارنة بالإيلام الذي يسببه له السجن حينما يكون محصورا بين جدرانه وسط مجموعة من المجرمين.

2- أثر تقنية الوضع تحت المراقبة الالكترونية على حرمة جسد الانسان

يعتبر الحق في حرمة الجسد وسلامته من الحقوق اللصيقة بكرامة الإنسان في كيانه المادي والمعنوي، ولقد أولاه المشرع حماية خاصة من خلال تجريم كل أشكال الاعتداء عليه، وقد شكل حمل السوار الالكتروني في معصم أو كاحل المحكوم عليه اعتداء على حرمة جسده، خاصة وأن من

---

[1] – محمد بن حميد المزمومي، المرجع السابق، ص 887.

[2] – حنان زعيمش، السياسة الجنائية لبدائل العقوبات السالبة للحرية، اطروحة لنيل شهادة الدكتوراه في العلوم، جامعة جيلالي ليابس، كلية الحقوق والعلوم السياسية، 2017/2016، ص 194.

[3] – ينص الدستور على أن الدولة تضمن عدم انتهاك حرمة الانسان، ويحظر أي عنف بدني أو معنوي أو أي مساس بالكرامة. المادة 39 الفقرتان 1، 2 من التعديل الدستوري الصادر بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 2020/12/30، الجريدة الرسمية عدد 82، صادر في 2020/12/30.

مستلزمات المراقبة الالكترونية تفرض حمله طيلة مدة الوضع تحت نظامها، بل يشكل انتزاعه جريمة يعاقب عليها القانون، وهو ما يترتب عليه حسب منتقدي هذه التقنية أضرارا صحية بعيدة المدى بحامله.

وسعيا منه لحماية المحكوم عليه من أن يؤثر هذا الجهاز على صحته، فقد نص المشرع في المادة 150 مكرر 7 الفقرة 1 منه على أنه يجب على قاضي تطبيق العقوبات، قبل وضع المحكوم عليه تحت المراقبة الالكترونية، أو في أي وقت أثناء تنفيذ هذا الإجراء، التحقق تلقائيا أو بناء على طلب المعني من أن السوار الالكتروني لا يمس بصحة المعني.

3 – أثر تقنية الوضع تحت المراقبة الالكترونية على حرمة الحياة الخاصة للانسان

يثير تطبيق نظام الوضع تحت المراقبة الاكترونية العديد من المشاكل التي تمس بالحياة الخاصة للشخص الخاضع لها، وذلك من خلال تحول منزله لمكان تنفيذ العقوبة، وما يترتب على ذلك من إمكانية دخول التابعين لمصالح خارجية تابعة لإدارة السجون المكلفين بالزيارات الميدانية في أي وقت يشاؤون، ومن ثم تحول المكان الخاص إلى مكان عام باسم المراقبة الالكترونية[1].

كما تطبيق هذا النظام يثير هذه المسألة بالنسبة للمقيمين مع المحكوم عليه في نفس المسكن من أفراد عائلته أو أشخاص آخرين، ليمتد ويمس بحقهم في حياتهم الخاصة وحرمة منزلهم، غير أنه لا مجال للحديث عن انتهاك هذه الحرمات طالما أن هذه المراقبة لا تتم بواسطة كاميرا مراقبة، بل المراقبة تقتصر على مدى إلتزام المحكوم عليه بعدم مغادرة المكان في أوقات معينة[2].

ويمكن الرد أيضا على ذلك، بأن مشروعية الاعتداء على حرمة المسكن ناتج من رضا المحكوم عليه وقبوله الخضوع له، على أساس أن حصانة وحرمة المسكن تبقى قائمة طالما لم يرض المعني بهذه المراقبة. ومع ذلك فقد أغفل المشرع الجزائري أن يحيط تطبيق هذا النظام بضمانات أخرى مهمة، منها عدم زيارة المحكوم عليه أثناء الليل، وعدم الدخول إلا بعد إذن صاحب الشأن، وعدم جواز استعمال المراقبة عن طريق التصوير لأنه اعتداء صارخ على الحق في السرية والعيش في حياة اسرية عادية[3].

---

[1]– أحمد كيلان عبد الله، بلال عبد الرحمن محمد خلف، سياسة استبدال الصفة الجنائية للعقوبة –دراسة مقارنة–، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة 2020، ص 255.

[2]– شعيب ضريف، آليات تنفيذ العقوبة السالبة للحرية في التشريع الجزائري، المرجع السابق، ص 85.

[3]–أحمد كيلان عبد الله، بلال عبد الرحمن محمد خلف، نفس المرجع ، نفس الصفحة .

الخاتمة

يقوم نظام الوضع تحت المراقبة الالكترونية على إيجاد نوع من التوازن بين حماية المجتمع من خطورة الجاني وإعادة ادماجه فيه، وذلك بتوظيف التطور التكنلوجي في التنفيذ العقابي، من خلال اتباع هذه التقنية الجديدة دون اللجوء إلى تطبيق العقوبة السالبة للحرية قصيرة المدة تفاديا لمساوئها وأضرارها، ففي الوقت الذي تقيد حرية المحكوم عليه بالتزامات، يسمح له بالاحتفاظ بدفء حياته العائلة وعلاقاته الاجتماعية والمهنية. ومن خلال هذه الورقة البحثية توصلت إلى النتائج التالية:

-أن التطور العلمي والتكنولوجي الذي وصلت إليه الدول المتقدمة وتأثر به القانون، يفرض على المشرع مواكبته وتوظيفه في مجال السياسة العقابية، ويعد الوضع تحت المراقبة الالكترونية من التقنيات المستحدثة كآلية بديلة للعقوبات السالبة للحرية قصيرة المدة.

-أن نظام المراقبة الالكترونية لما له من أهمية وخصائص يتميز بها أثبت نجاعته في حل مخاطر اكتظاظ السجون والتخفيف من حالات العود والنفقات التي تتكبدها العقوبات السالبة للحرية، غير أن ذلك لا يتحقق إلا بتوافر شروط قانونية وتقنية، مع ضرورة موافقة وتجاوب الخاضع لها بالتقيد بكل الالتزامات التي تقع على عاتقه، مما يجعله نظاما معتدلا لا يتعارض مع حقوق وكرامة الانسان وسلامته الجسدية ولا يمس بحياته الخاصة بشكل كبير.

وبناء على تلك النتائج، أقترح التوصيات التالية:

-ضرورة إعادة تفعيل وتطوير نظام المراقبة الالكترونية وتوسيعه بما يضمن تعميم اللجوء إليه بدلا من الجوء إلى العقوبات السالبة للحرية قصيرة المدة.

-ضرورة الاستفادة من تجارب الدول المتقدمة في المجال السياسة العقابية باعتبارها السباقة في تطوير نظام المراقبة الالكترونية باستغلال المزايا وتجنب المساوئ التي قد تنجم عنها.

-ضرورة إجراء فحص لشخصية المحكوم عليه للتأكد من مدى خطورته، وعدم الجدوى من اللجوء إلى هذا النظام في هذه حالة خطورة المحكوم عليه، مع ضرورة اسناد سلطة تقديرها للقاضي المختص.

- ضرورة التقليص من مدة الوضع تحت المراقبة الالكترونية لمدة سنة كما تقتضيه العقوبة السالبة للحرية قصيرة المدة، حيث تشكل مدة ثلاث سنوات مدة طويلة نوعا ما لحمل السوار الالكتروني التي تكون لها انعكاسات سلبية على صحة المحكوم وعلى نفسيته.

قائمة المراجع

أولا / الكتب

1-أحمد كيلان عبد الله، بلال عبد الرحمن محمد خلف، سياسة استبدال الصفة الجنائية للعقوبة -دراسة مقارنة-، الطبعة الأولى، المركز العربي للنشر والتوزيع، القاهرة 2020.

2-الزهرة كوميشي، اساليب المعاملة العقابية داخل السجون، الطبعة الاولى، دار الباحث 2019.

3-عبد الرحمان خلفي ، بدائل العقوبة دراسة فقهية تحليلية تأصيلية مقارنة، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2015.

4-محمد صالح معزي، الاتجاهات الحديثة في العقوبات البديلة، الطبعة 1، دار غيداء للنشر، عمان، 2016.

5-Tony Ferri, La surveillance électronique pénale (son statut, son sens, ses effets) , Editions Bréal 2017.

ثانيا/ الرسائل الجامعية

1-أيمن عبد العزيز الملك، بدائل العقوبات السالبة للحرية كنموذج لإصلاح في نظام العدالة الجنائية، أطروحة دكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا قسم العلوم الاجتماعية، المملكة العربية السعودية 2010.

2-حنان زعيمش، السياسة الجنائية لبدائل العقوبات السالبة للحرية، اطروحة لنيل شهادة الدكتوراه في العلوم، جامعة جيلالي ليابس، كلية الحقوق والعلوم السياسية، 2017/2016.

3-شعيب ضريف، آليات تنفيذ العقوبة السالبة للحرية في التشريع الجزائري، اطروحة لنيل شهادة دكتوراه ل م د في القانون العام تخصص قانون جنائي وعل.م الاجرام، جامعة الجزائر 1 كلية الحقوق، جانفي 2019.

4-عبد اللطيف بوسري ، العقوبة الرضائية وأثرها في ترشيد السياسة العقابية ، أطروحة دكتوراه في العلوم الجنائية ، جامعة باتنة -1- كلية الحقوق والعلوم السياسية ، 2018/2017.

5-اليازية سلطان الظاهري، الوضع تحت المراقبة الالكترونية في التشريع الاماراتي، مذكرة ماجستير في القانون العام، جامعة الامارات العربية المتحدة، كلية الحقوق قسم القانون العام، نوفمبر 2020.

6-فريد بلعيدي، تنفيذ العقوبة السّالبة للحرية، مذكرة لنيل شهادة ماجيستير في علم الإجرام والعلوم الجنائية، جامعة أبي بكر بلقايد، تلمسان، كلية الحقوق.

ثالثا/المقالات

1- أحمد سعود، المراقبة الإلكترونية كبديل للعقوبة السالبة للحرية قصيرة المدة، مجلة العلوم القانونية والسياسية، جامعة الوادي، المجلد 09، العدد03 ، السنة 2018.

2-جمال قتال ،الوضع تحت المراقبة الالكترونية وفق مقتضيات قانون رقم 01/18 المتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين ،مجلة معالم الدراسات القانونية والسياسية ،المجلد 04 ،العدد 01، السنة 2020.

3-رامي متولي القاضي، توظيف التقنيات الحديثة في مجال السياسة العقابية(السوار الالكتروني نموذجا)، مجلة الفكر الشرطي، مجلد 26، العدد 103،السنة اكتوبر 2017.

4-رامي متولي القاضي، نظام المراقبة الإلكترونية في القانون الفرنسي والمقارن، مجلة الشريعة والقانون جامعة الإمارات العربية المتّحدة، ، العدد الثالث والسّتون، يوليو 2015، السنة التاسعة والعشرون.

5-سعاد خلوط ، عبد المجيد لخذاري، الوضع تحت المراقبة الالكترونية كآلية مستحدثة للتفريد العقابي في التشريع الجزائري وفقا لقانون 18-01، مجلة البحوث والدراسات، مجلد 15، عدد 2، السنة 2018.

6-شعيب ضريف، المراقبة الإلكترونية للمحكوم عليهم في السياسية العقابية الجزائرية، المجلة الإفريقية للدراسات القانونية والسياسية، جامعة احمد دراية، المجلد 03، العدد1، السنة جوان 2019.

7-عامر جوهر وعباسة الطاهر، السوار الالكتروني إجراء بديل للعقوبة السالبة للحرية في التشريع الجزائري، مجلة الاجتهاد القضائي، العدد 16، السنة مارس 2018.

8-فوزية هوشات، العقوبات البديلة في التشريع الجزائري، مجلة العلوم الإنسانية، جامعة الإخوة منتوري، قسنطينة ، المجلد 30، عدد 2، السنة ديسمبر 2019.

9-فيصل بدري، الوضع تحت المراقبة الالكترونية -السوار الالكتروني كبديل للعقوبة السالبة للحرية قصيرة المدة-، مجلة الباحث للدراسات القانونية والسياسية، مجلد 2، العدد 10، السنة جوان 2018.

10-محمد أمين بكوش، نبيلة هبة هروال، المراقبة الإلكترونية في التشريع الجزائري، مجلة الدراسات الحقوقية، جامعة الدكتور طاهر مولاي سعيدة ، العدد 1 ، الجزء 06 ، السنة 2019.

11-محمد بن حميد المزمومي، المراقبة الالكترونية كبديل للعقوبة السالبة للحرية دراسة في ضوء النظام السعودي والأنظمة المقارنة، مجلة صوت القانون، مجلد 7، عدد 2، السنة نوفمبر 2020 .

12-نادية تحانوت، مصير أنسنة السجون بعد جائحة كورونا، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 58، العدد 02، السنة 2021.

13-نيلة صدراتي ،الوضع تحت المراقبة الاليكترونية كنظام جديد لتكييف العقوبة (دراسة في ضوء القانون رقم 18-01 المتمم لقانون تنظيم السجون و إعادة الإدماج الاجتماعي للمحبوسين) ،مجلة الدراسات والبحوث القانونية، المجلد 3،العدد 2 ، جوان 2018.

رابعا/ مواقع الانترنت

1- سامية بوروبة، الجزائر أول دولة عربية تستخدم السوار الالكتروني: توسيع العقوبة البديلة عن السجن، المفكرة القانونية، يوم الاطلاع : 2 مارس 2018، الموقع: https://legal-agenda.com

الملتقى الدولي الافتراضي الموسوم بـ

" القانون الجنائي في ظل التطور التكنولوجي – إشكالات ومعالجات–

مداخلة في المحور الثاني الموسومة بـ

" حماية المنتوجات الرقمية من الجرائم الإلكترونية"

من إعداد: د. قزوت لامية

دكتورة في القانون الخاص تخصص حماية المستهلك والمنافسة

وأستاذة مؤقتة

البريد الإلكتروني: guezoutlamiaepchikhaoui@gmail.com

كلية الحقوق – جامعة الجزائر 1

ملخص

تعتبر المنتوجات الرقمية في الوقت الحالي سلعة يمكن التعامل فيها وتسويقها نظراللتقنيات الحديثة التي ساهمتفي سرعة انتشارها، إلا أنها جديرة بالحماية كونها تتطلب نشاطا وجهدا فكريا ولو في حده الأدنى، إذ ما يميز هذه السلعة عن باقي السلع أنها تعتبر سلعة غير ملموسة أي تكون عبارة عن مجرد تصور أو فكرة في ذهن صاحب المنتوج ، هذا ما يجعله عرضة لمخاطر القرصنة و السرقة التي تشكل جريمة وفقا لمفاهيم القانون الجنائي، كما يمكن أن تكون تلك المنتوجات الرقمية نفسها مخالفة للقانون بحيث تكون ماسة بالنظام العام والآداب العامة في المجتمع أو تسببأضرار مادية ومعنوية لدى فئة الأطفال والمراهقين.

وباعتبار أن المنتوج الرقمي ينطبق عليه مفهوم المنتوج الوارد في قانون حماية المستهلك وقمع الغش، فلابد أن يكون هذا المنتوج آمن عند الاستعمال المشروع المنتظر منه، كما لا يجب أن يلحق أضرار بمستهلكه وبالجمهور المعروض عليه ، ومن أجل ذلك، كان لابد من اللجوء إلى اتخاذ تدابير وقائية وأخرى ردعية للحد من انتشار الجرائم الإلكترونية الناجمة عن استعمال مختلف المنتوجات الرقمية.

الكلمات الافتتاحية:

جريمة إلكترونية، منتوج رقمي، حماية قانونية، وسائل تكنولوجية حديثة.

Abstract

Digital products are currently considered a commodity that can be dealt with and marketed due to modern technologies that have contributed to the rapid spread of them. However, they are worthy of protection as they require intellectual activity and effort, even at a minimum. What distinguishes this commodity from other commodities is that it is considered an intangible commodity, i.e. a phrase Just a perception or idea in the mind of the product owner, this is what makes him vulnerable to the risks of piracy and theft, which constitute a crime according to the concepts of criminal law, and these digital products themselves can be in violation of the law so that they affect public order and public morals in society or cause material and moral damage I have children and teens category.

Considering that the digital product applies to the concept of the product contained in the Consumer Protection and Fraud Suppression Law, this product must be safe when the expected legitimate use of it, and it should not cause harm to its consumer and the public offered to it, and for that, it was necessary to resort to taking measures Preventive and deterrent to limit the spread of cybercrime resulting from the use of various digital products.

Opening words:

Electronic crime, digital product, legal protection, modern technological means.

مقدمـــــــــــة

إن التدفق الحر والغزير للمعلومات لما توفره التكنولوجيا الحديثة من إمكانيات متطورة خاصة تكنولوجيات الاتصال كالأنترنيت والأقمار الصناعية التي تعتبر نتيجة حتمية للعولمة المفروضة، أدى إلى التزايد المستمر للمنتوجات الرقمية في الآونة الأخيرة نظرا للاستخدام الكبير لشبكات الأنترنيت ووسائل التواصل الاجتماعي بحيث أضحى الكبير والصغير يقبل عليها ويستعملها في حياته اليومية.

وبالتالي أصبحت البيئة الرقمية بيئة خصبة لنمو مختلف المحتويات و المنتوجات الرقمية و ازدهارها بحيث أزالت الحواجز الجغرافية وسمحت بانتقال المعلومات والبرامج بكل حرية وذلك بالاعتماد بالدرجة الأولى على الحاسبالآلي بعدما أصبحت شبكة الأنترنيت ضرورة ملحة لا يمكن لأحد الاستغناء عنها.

فبات فضاء الأنترنيت مجالا رحبا لعرض مختلف السلع والخدمات، سواء العلمية منها أو التجارية، بحيث يكون عرضها سهلا على المستهلك، فمن الطبيعي أن يساء استخدامها كالاستيلاء على منتوجات ومجهودات شخص آخر، أو عرض سلع وخدمات وهمية، أو المساهمة في مشاريع استثمارية لا وجود لها، أو سرقة معلومات أو بطاقات الائتمان واستخدامها دون أي وجه حق، وكذا ممارسة أشكال التنمر وراء شاشات الحاسوب سواء على السلع المعروضة أو على أصحابها .

وهذا جاء تماشيا مع الطفرة الإعلامية التي ظهرت مؤخرا عقب الثورة التكنولوجية وتطور وسائل الإعلام، بحيث أصبحت هناك مرونة في التعامل مع حرية التعبير إذ توسع نطاق هذه الأخيرة وبات في بعض الأحيان يهدد حرمة وقدسية الحياة الشخصية التي يكرسها الدستور ويحميها..

وما يميز الجرائم الإلكترونية المرتكبة ضد المنتوجات الرقمية هو السرعة و عدم القدرة على إقامة الحجة على مرتكبيها بسهولة، لذا فإن التكنولوجيا الحديثة بقدر ماهي مسؤولة عن إنتاج المزيد من المنتوجات والمحتويات الحديثة ، فهي مسؤولة أيضا عن توفير المزيد من الحماية لها أيضا، و بالتالي لابد من مسايرة التشريعات والقوانين الحديثة لتطور البيئة الرقمية وتوفير الحماية اللازمة لها خاصة من القرصنة والمتاجرة غير المشروعة بها والأهم من ذلك من ظاهرة الاستيلاء على مجهودات الغير دون وجه حق.

من هنا نصل لطرح الإشكالية التالية: **كيف يتم مواجهة الجريمة الإلكترونية والحد منها في ظل انتشار المنتوجات الرقمية؟**

للإجابة عن هذه الإشكالية ستقسم المداخلة إلى شقين رئيسيين: سيتم التعرض في المبحث الأول إلى **خصوصية الجريمة الإلكترونية المتركبة في البيئة الرقمية**أين سيتم التطرق أولا**للمنتوجات الرقمية الأكثر عرضة للجريمة الإلكترونية** في المطلب الأول ثم إلى **أنواع الجرائم التي ترد على المنتوجات الرقمية** في المطلب الثاني.

أما المبحث الثاني من المداخلة فسوف يخصص**للتدابير المتخذةلمواجهة الجريمة الإلكترونية في البيئة الرقمية** والتي تنقسم بدورها إلى**التدابير الوقائية التكنولوجية الحديثة**التيتعيق الوصوللمنتوج الرقمي والاستفادة منه إلا لمن يحمل ترخيصاً بذلك والتي سيتم التطرق إليها في المطلب الأول،**والتدابير الردعيةالمتخذة ضد الجريمة الإلكترونية** التي سيتم التطرق إليها في المطلب الثاني.

وباعتبار موضوع بحثنا هذا من مواضيع الساعة وذو أهمية بالغة في المجتمع و القانون، فسنتبع للإلمام بكل جوانبه والتعمق في تفاصليه كل من المنهج الوصفي والتحليلي في نفس الوقت، مستندين على أدوات النثر والبلاغة اللازمة لذلك.

المبحثالأول: خصوصية الجريمة الإلكترونية المتركبة في البيئة الرقمية

تعتبر الوسائط الإلكترونية في الوقت الحالي سلعة يمكن التعامل فيها وتسويقها لما ساهمت في ذلك التقنيات الحديثة من سرعة في انتشارها، إلا أنها جديرة بالحماية كونها تتطلب نشاطا وجهدا فكريا ولو في حده الأدنى[1]، إذ ما يميز هذه السلعة عن باقي السلع أنها تعتبر سلعة غير ملموسة أي تكون عبارة عن مجرد تصور أو فكرة في ذهن صاحب المنتوج ، هذا ما يجعله عرضة لمخاطر القرصنة و السرقة التي تعتبر شكل من أشكال الجريمة الإلكترونية ، كما يمكن أن تكون تلك المنتوجات الرقمية نفسها مخالفة للقانون بحيث تكون ماسة بالنظام العام والآداب العامة في المجتمع أو من شأنها الإضرار بصحة الإنسان والبيئة على حد سواء.[2]

وباعتبار أن المنتوج الرقمي ينطبق عليه مفهوم المنتوج الوارد في قانون حماية المستهلك وقمع الغش[3]، فلابد أن يكون هذا المنتوج آمن عند الاستعمال المشروع المنتظر منه، كما لا يجب أن يلحق أضرار بمستهلكه وبالجمهور المعروض عليه وعلى كل منتج لهذا النوع من المنتوجات احترام إلزامية الأمن خصوصا عندما يتعلق الأمر بفئات المستهلكين الأكثر عرضة للخطر كالأطفال والمراهقين الذي يواجهون أخطار الأضرار النفسية وحتى المادية التي تصيبهم إثر استخدام هذه المنتوجات الرقمية.[4]

---

[1] – يسرية عبد الجليل، حقوق حاملي براءات الاختراع ونماذج المنفعة، دارالنشر منشأة المعارف بالإسكندرية – مصر– 2005، ص 19.

[2] – إياس بن سمير الهاجري، أمن المعلومات على شبكة الأنترنيت، ، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية ، الرياض – السعودية –2004، ص 140.

[3] – انظر المادة 3 الفقرة العاشرة من القانون رقم09 –03 المتعلق بحماية المستهلك وقمع الغش و المؤرخ في25 فبراير2009 الصادر في الجريدة الرسمية بتاريخ 08مارس2009 العدد15، والتي تنص أن المنتوج هو:" كل سلعة أو خدمة يمكن أن يكون موضوع تنازل بمقابل أو مجانا.

[4] – انظر المادتين 09 و10 من نفس القانون.

المطلب الأول: المنتوجات الرقمية الأكثر عرضة للجريمة الإلكترونية

هناك أنواع متعددة من المنتوجات الرقمية التي لاتعد ولا تحصى، إلا أن الخبراء القانونيون والاقتصاديين أجمعوا على أن هناك منتوجات محددة تعد الأكثر انتشارا و شيوعا، فلإضفاء الحماية القانونية على أي منتوج رقمي لابد أن يتوفر فيه شرط الإبداع والابتكار بحيث يكون ذلك المنتوج لم يكن يسبق عرضه ولم يكن معروفا من قبل[1]، فرغم أن هناك من يرى أن هذه المنتوجات ذات طبيعة تقنية بحتة تفتقد للمسة ابتكارية، إلا أن الحقيقة عكس ذلك تماما فالمزج الرقمي بين عناصر متعددة كالصوت والصورة و الألوان يسفر عن منتوج ذو إبداع وأصالة لامثيل لها، كما أنه ناتج عن جهد فكري وذهني غير مباشر[2].

وتمتاز المنتوجات الرقمية بالاستمرارية كونها تهدف لتحقيق المصلحة العامة[3]وكذا بسهولة الحصول عليها من عامة الناس ودون تكلفة، فبالرغم من الأخطار الكبيرة التي تشكلها المنتوجات الرقمية والجرائم الناتجة عنها، إلا أن هذا لم يقلل من الإقبال الكبير عليها وهذا راجع لأمرين أساسيين:[4]

– الأمر الأول يتمثل في ازدياد أهمية المنتوجات الرقمية في حياتنا اليومية، فالاعتماد عليها يسهل للناس حياتهم ويلبي احتياجاتهم بأقصى سرعة وبأقل تكلفة ، كما تحقق لهم هذه المنتوجات أسباب المتعة والرفاهية.

– الأمر الثاني هو الدور الفعال الذي تلعبه وسائل الدعاية والإعلان بحيث أصبح المستهلك يلجأ للمنتوجات الرقمية حتى في تلقي الدروس والدورات التكوينية والتدريبية.

وسنذكر أهم خمسة فئات أساسية للمنتوجات الرقمية والتي تندرج تحتها جميع المنتوجات الرقمية الأخرى بمختلف أنواعها[5]:

1- إنشاء محتوى متميز

---

[1] – عبد الفتاح بيومي حجازي، مقدمة في حقوق الملكية الفكرية وحماية المستهلك في عقود التجارة الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، الاسكندرية – مصر –2005، ص 9.

[2] – انظر مدونة التجارة الإلكترونية العربية.

[3] – محمد محمد أحمد أبو سيد أحمد، حماية المستهلك في الفقه الاسلامي، منشورات محمد علي بيضون، دار الكتب العلمية، الطبعة الأولى، بيروت – لبنان2004، ص80 .

[4] - علي فتاك، تأثير المنافسة على الالتزام بضمان سلامة المنتوج، دار الفكر الجامعي، الاسكندرية، مصر2007، ص20.

[5] – رامي ابراهيم حسن زواهرة و محمد خليل أبو بكر، " الابتكار كشرط لحماية حقوق المؤلف الفكرية وأثر تكنولوجيا المعلومات عليه" دراسة مقارنة، مركز الأبحاث بجامعة الزيتونة ، عمان – الأردن – 2017، ص65.

وهي عبارة عن المواقع و المدونات التي يمكن الولوج إليها مجانا ويكون المحتوى المتميز في كل شيء دون استثناء : نصوص، مقالات ، كتيبات، صوتيات، فيديوهات، صور ، تصاميم، لذا قد يكون فضاء ملائما لممارسة كل أشكال الجرائم الإلكترونية من قرصنة وسرقة علمية وغيرها من الجرائم الإلكترونية.

2 – الكتب الرقمية (الإلكترونية)

تعرف هذه الكتب على أنها" نشر إلكتروني فيه نصوص و صور، تنتج وتنشر وتقرأ على الحواسب أو أية أجهزة إلكترونية أخرى" .

وتعتبر الكتب الرقمية المنتوجات الأكثر شيوعا وأولها التي تبادر في الذهن عند سماع " منتوج رقمي أو إلكتروني" ، وهو كذلك أسهل المنتوجات الرقمية عند الإنتاج لأنه يعتمد على الفكر والعقل فقط، ولا يتطلب خدمات ما بعد البيع مقارنة بالمنتوجات الأخرى.

وتدخل تحت هذه الفئة جميع المنتوجات الفكرية الكتابية منها : الكتيبات ، الدوريات، المجلات ، المدونات، المنشورات و كل ما يتعلق بالكتابة.

غير أن، وبالرغم من الفائدة العارمة التي تعود بها هذه المنشورات الإلكترونية على مستخدميها، إلا أنها هي أيضا عرضة للجريمة الإلكترونية سواء عن طريق تشويه سمعة صاحبها أو الاستهزاء به أو حتى الاستيلاء عليها ونسبها لشخص آخر وابتزازه بذلك.

3 – الدورات التدريبية:

وهي تلك الدورات التي تقدم دروس عبر شبكة الأنترنيت دون حاجة للحضور إلى الأقسام الدراسية، ولا تكون مرتبطة أيضا بوجود مدرس أو مدرب، وتكون هذه الدورات في شكل كتيبات أو مقاطع فيديو للشرح والتوضيح، كما تعتبر هذه الدورات ثاني أكثر منتوج رقمي انتشارا وهذا لسهولة التعلم من خلاله .

4 – البرمجيات

تعتبر البرمجيات أهم المنتوجات الرقمية على الإطلاق بحيث تشمل كل برامج الإعلام الآلي دون استثناء بمختلف أنواعها ولغاتها وأهدافها ، فكلما كان البرنامج قوي ومتكامل كلما زاد انتشاره خاصة إذا واكب التطورات التكنولوجية الحديثة.فيعتبر البرنامج المحرك الأساسي الذي يشتغل به الحاسوب وبدونه يصبح جسم بلا فائدة[1]، وهناك نوعين من البرمجيات: برامج التشغيل وبرامج التطبيق، فيسمح الأول بتشغيل الحاسوب و استغلاله والثاني بتنفيذ عمل محدد وحل مشكلة معينة[2].

---

[1] – بن عبو نسيمة ، "البرمجيات بين حقوق المؤلف وبراءات الاختراع"، مجلة بحوث – جامعة الجزائر 1 – العدد08–2015 ، ص 10.

[2] – نفس المرجع ، ص 11 .

غير أن هذه المنتوجات الرقمية تحتاج إلى الكثير من الكفاءة والخبرة ، بالإضافة إلى دعم وفير وخدمة للعملاء بصفة مستمرة، بخلاف المنتوجات الرقمية الأخرى كالكتب الإلكترونية.

3- التصاميم المختلفة

تشمل هذه الفئة الكثير من المنتوجات مثل الرسوم المختلفة ، القوالب الجاهزة، الصور والإنتاجالإعلامي وتطوير المواقع و أي منتوج يدخل ضمن المنتوجات الرقمية[1]، ولكن هذه المنتوجات مثلها مثل البرمجيات تحتاج إلى كفاءة و موهبة معينة حتى يكون الإبداع و الإنتاج في أفضل مستوياته وتلقى قبولوطلب لدى العملاء ، كما تحتاج أيضا للدعم الفني والخدمة ما بعد البيع التي ترافق مثل هذه المنتوجات بشكل عام، هذا ما يعرض أصاحبها لكل أساليب التهديد والابتزاز ومحاولة الاستيلاء عليها دون وجه حق.

ولتحقيق أمن وسلامةالمنتوج الرقمي، لابد من اتخاذ إجراءات ضرورية لحماية أجهزة الحاسوب والإعلام الآلي عموما وكذا شبكات الأنترنيت و ذلك لبلوغ ثلاثة أهداف[2] وهي:

أ- تأمين سرية المعلومات: من خلال ضمان الحفظ الجيد للمعلومات المخزنة في أجهزة الحاسوب وعدم الاطلاع عليها إلا منقبل الأشخاص المخولين لذلك، وكذلك ضمان سرية انتقال المنتوجات الرقمية عبر الشبكة العنكبوتية أو الأنترنيت، وهذا حفاظا على حرمة الحياة الشخصية للأفراد وأيضا على سرية المعلومات المتعلقة بأمن الدولة.

ب- تأمين سلامة المعلومات: وذلك من خلال الإبقاء على المنتوجات الرقمية والمعلومات التي تحتويها على حالها في أجهزة الإعلام الآلي وضمان عدم إحداث أي تغيير عليها إلا من قبل الأشخاص الذين لديهم الحق في ذلك، وذلك ضمانا بقاء المعلومات المخزنة في الحواسيب على حالها ودون تعرضها لأي تحريف أو إنقاص يؤثر على قيمتها.

ج- تأمين وجود المعلومات: وهو عدم تعرضها للحذف والإتلاف إلا في حدود ما يسمح به القانون، كون ذاكرة الحاسوب ومختلف الأجهزة الإلكترونية الأخرى تعد مرجع مهم في كل المؤسسات وحتى لدى الأشخاص العادية، لهذا يجب الحفاظ عليها قدر الإمكان لمنع التسريب غير القانوني للمعلومات أو حذف معلومات مهمة عمدا بغرض تشويه سمعة شخص ما التي هي من قبيل الجريمة الإلكترونية كما سيتم توضيحه لاحقا.

هذا لأن أجهزة حفظ المنتوجات الرقمية كأجهزة الحاسوب و الأقراص المضغوطة وشبكات الأنترنت تواجه عدة مخاطر يمكن تصنيفها في صنفين: مخاطر داخلية ومخاطر خارجية.

---

[1] - محمد رحايلي ، حقوق المؤلف و الحقوق المجاورة في البيئة الرقمية : الحالة الجزائرية، أطروحة مقدمة ضمن متطلبات نيل شهادة الدكتوراه في القانون الخاص، جامعة الأمير عبد القادر – قسنطينة- السنة الجامعية 2014-2015 ، ص 10.

[2] - رامي ابراهيم حسن زواهرة ومحمد خليل أبو بكر، مرجع سابق، ص 66.

المخاطر الداخلية التي تتمثل في عمليات التخريب التي يقوم بها أشخاص يعملون داخل المؤسسة التي تتواجد بها الأجهزة التي تحتوي على المنتوجات الرقمية، والتي قد تكون في بعض الأحيان عبارة عن أخطاء عفوية نتيجة الاستخدام الخاطئ لتلك الأجهزة ولكنها تفتح باب لقرصنة أي منتوج أو محتوى رقمي.

أما المخاطر الخارجية فهي التي تصدر عن أشخاص أو جهات خارجية، سواء من خارج المؤسسة التي يتواجد بها المنتوج الرقمي أو حتى من خارج الوطن بأكمله، والتي قد تستعمل عدة وسائل تجسس أو تخريب من أجل الظفر بالمنتوج الرقمي والاستيلاء عليه.

ويكون ذلك نتيجة عدة دوافع: البعض منها سياسية يكون الغرض منها التجسس والحصول على معلومات مفيدة حول سياسة واقتصاد دولة ما.

وقد تكون الدوافع ذات طابع تجارية تهدف إلى السيطرة على السوق والهيمنة عليها من خلال استعمال أساليب المنافسة غير المشروعة غرضها سرقة منتوجات منافس آخر أو تخريبها وتشويهها.

وغالبا ما يقوم بهذه الأعمال أشخاص محترفين و متمرسين سواء بتحريض من جهة معينة مقابل مبلغ من المال أو لمجرد حب التطفل والشهرة، وكذا إثبات القدرات العلمية والتكنولوجية[1]، من أجل ذلك يتعين إيجاد وسائل قانونية تحول دون تحقق هذه المخاطر التي تهدد المنتوجاتالرقمية وكذا المخاطر التي يمكن أنتشكلها هذه الأخيرة.[2]

المطلب الثاني – أنواع الجرائم التي ترد على المنتوجات الرقمية

إن حساسية المنتوج الرقمي وسهولة الاستيلاء عليه وقرصنته أدى إلى كثرة الجرائم الماسة به، فمنها ما هو مادي يتجلى في استعمال أساليب تكنولوجيا حديثة للاستيلاء على أموال الغير وابتزازهم وتهديدهم بتسريب أمور شخصية مقابل الحصول على مبلغ من المال، ومنها ما هو ثقافي الذي يرمي لسرقة مجهودات الغير الفكرية والأدبية والثقافية ونسبها لغير صاحبها الأصلي أو تحريفها لتشويه سمعته والتنكيل بشخصه، كما نجد نوع جديد من الجرائم وهي الجريمة المعلوماتية والتي يهدف من وراءها الوصول إلى معلومات مهمة مخزنة بحكمة في دعائم تكنولوجية حديثة لاستعمالها فيما يسيئ لسمعة الشخص وشرفه ونزاهة عمله، لذا سنتناول كل واحدة من هذه الجرائم على حدى.

أولا– الجريمة المادية

[1] – فرحات حمو ، التنظيم التشريعي لحقوق الملكية الصناعية ودوره في التنمية ، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق– جامعة وهران– السنة الجامعية 2011–2012 ، ص 40.

[2]– إياس بن سمير الهاجري، مرجع سابق، ص 141.

وهي تلك الجريمة التي تسبب أضرارا مالية للغير هدفها النصب والاستيلاء على الأموال والابتزاز بالتهديد والتي تتخذ ثلاث أشكال:[1]

أ- السرقة الإلكترونية: كالاستيلاء على مكنات الصرف الآلية للبنوك عن طريق القيام بنسخ البيانات الإلكترونية لبطاقة الصراف الآلي، وكذا الاستيلاء على حسابات مواقع التواصل الاجتماعي ونشر الإشاعات والأخبار الكاذبة للحصول على الأموال من الشركات الوصية.

ب- القيام بإنشاء صفحة أنترنيت مطابقة لموقع أحد المؤسسات المالية الكبرى أو أحد رجال الأعمال وأصحاب العلامات التجارية العالمية لابتزازهم والاستيلاء على زبائنهم .

ج- رسائل البريد الإلكتروني المجهولة المصدر والتي توهم الجمهور بإمكانية الفوز بجوائز أو الحصول على مبالغ مالية معتبرة مقابل إرسال رقم الحساب المصرفي بغرض الاستيلاء عليه، أو الرسائل التي تضمن طلب مبلغ من المال خلال مدة معينة تحت طائلة التهديد بنشر وفيديوهات تمس بشرف وسمعة صاحب البريد الإلكتروني.

ثانيا - الجريمة الثقافية

وهي قيام شخص بالاستيلاء على حقوق الملكية الفكرية سواء لصحفي أو أي شخص آخر ونسبها لنفسه دون وجه حق ودون علم صاحبها[2]ومن بعض أشكالها:

أ- القيام بقرصنة البرمجيات[3]والقيام بنسخها على أسطوانات أو تقليدها و إعادة بيعها بأسعار أقل للإطاحة بصاحب العمل والتقليل من شأنه .

ب- القيام بنسخ المؤلفات العلمية والأدبية بالطرق الإلكترونية الحديثة مع تحريفها بغرض تشويه سمعة صاحبها.

ج- التمكن من الدخول للقنوات الفضائية المشفرة وفتحها للجمهور عبر مواقع الأنترنيت للنشر الفساد والرذيلة.

ثالثا – الجريمة المعلوماتية

وهي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات

---

[1] - بن دريس حليمة، حماية حقوق الملكية الفكرية في التشريع الجزائري، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبي بكر بلقايد – تلمسان- السنة الجامعية 2013- 2014، ص 50.

[2] - عميمر عبد القادر، "الحماية القانونية للصحفي في إطار قانون حق المؤلف"، مجلة بحوث – جامعة الجزائر 1 – العدد08-، ص 255 .

[3] - بن عبو نسيمة، مرجع سابق ، ص 11.

الإلكترونية، سواء بواسطة نظام إلكتروني منفصل أو بواسطة عرض وقائع أو معلومات أو مفاهيم في شكل جاهز للمعالجة بما في ذلك البرامج الآلية والإلكترونية[1].

كل هذه الجرائم تعتبر جرائم إلكترونية، فرغم خصوصيتها إلا أنها تكتسي الطابع الإجرامي المنصوص عليه في قانون العقوبات إذ تعتبر جرائم مكتملة الأركان وتطبق عليها العقوبات المنصوص عليها قانونا.

المبحث الثاني: التدابير المتخذة لمواجهة الجريمة الإلكترونية في البيئة الرقمية

إن الهدف من ارتكاب الجرائم المتعلقة بالأنترنيت والإعلام الآلي والتكنولوجيا عموما هو الحصول على المنتوج الرقمي بالطرق غير المشروعة أو التشهير به وتشويه سمعة صاحبه والتي تشترك من حيث طبيعتها مع جرائم التخريب والسرقة التقليدية وكذا جرائم القذف والسب والشتم، كما قد تستعمل وسائل إجرامية حديثة مرتبطة بالتكنولوجيا المعلوماتية كنشر الفيروسات الرامية إلى تدمير المنتوج الرقمي وتحريف محتواه والمعلومات المخزنة به.[2]

إلا أن المشرع الجزائري لم يحدد المدة القانونية اللازمة لحماية المنتوجات الرقمية ومصنفات الحاسب الآلي عموما، وبالتالي سنقيس مدة حماية هذه المنتوجات على الحماية الأصلية لمصنفات الملكية الفكرية المنصوص عليها قانونا وهي طيلة مدة حياة المؤلف و 50 سنة بعد وفاته.[3]

لأجل ذلك، أوجد المشرع الجزائري عدة تدابير، البعض منها ذو طابع تقني بحت يعتمد على التقنيات التكنولوجية الحديثة مسايرة لطبيعة وكيفية استعمال واستغلال المنتوجات الرقمية، والبعض الآخر ذو طابع ردعي

تطبق عندما يشكل الاستيلاء على منتوج رقمي أو تشهير به أو بصاحبه جريمة يعاقب عليها القانون ، فتعرف الجريمة فقها على أنها" كل فعل غير مشروع يعاقب عليه القانون، صادر عن قصد وإرادة بنية الحاق الضرر بالغير".[4]

المطلب الأول: التدابير الوقائية التكنولوجية الحديثة

---

[1] – انظر المادة الثانية من القانون رقم 09– 04 المؤرخ في 05 أوت2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، جريدة رسمية عدد47 الصادرة في 16 أوت 2009.

[2] – إياس بن سمير الهاجري، مرجع سابق، ص 142.

[3] – يحيى يحياوي ، أوراق في التكنولوجيا و الاعلام و الديموقراطية، دار الطبع بيروت، الطبعة الأولى، لبنان يناير 2004، ص 68 .

[4] – هذا التعريف أجمع عليه جمهور فقهاء علم الاجرام و القانون الجنائي.

وهي تهدف إلى إعاقة الحصول على المنتوج الرقمي والاستفادة منه إلا لمن يحمل ترخيصاً من صاحب الحق نفسه[1] التي هي متعددة ، نذكر منها على سبيل المثال لا الحصر ثلاث تدابير تكنولوجية حديثة وهي: النظام الإلكتروني لإدارة حقوق المؤلف، التوقيع الرقمي وتشفير البيانات[2].

أولا– النظام الإلكتروني لإدارة حقوق المؤلف

عبارة عن نظام يستخدم لمراقبة طلبات الوصول إلى الوثيقة الإلكترونية، فهو يتحكم في السماح للوصول إلى مصنف معين من عدمه، ويعمل على إعداد تقارير بما قام بتسجيله، وتساعد تلك التقارير الناشرين والمنتجين على معرفة محاولات الدخول غير المصرح بها للمصنف، وتعمل هذه النظم على تقييد ما يمكن للمستخدم عمله للملف الإلكتروني، كما يمكن من خلالها أيضاً تحديد عدد مرات استرجاع العمل نفسه، أو نسخه، أو فتحه، أو طباعته.

ثانيا– التوقيع الرقمي

وهو يستخدم للتأكد من أن الرسالة التي جاءت من مصدرها لم تتعرض لأي تغيير أثناء نقلها، ويستخدم المرسل مفتاح خاص لتوقيع المنتوج الرقمي إلكترونيا، أما الطرف الآخر وهو المستقبل فيتم التحقق من صحة التوقيع من خلال استخدام المفتاح العام المناسب، وباستخدام التوقيع الرقمي يتم تأمين سلامة الرسالة والتحقق من صحتها.

وهناك نوعان من التوقيع متوفران حاليا:

1 – التوقيع المفتاحي

وهويقوم بتزويد المنتوج الرقمي بتوقيع مشفر مميز يحدد خلاله الشخص الذي قام بتوقيع الوثيقة والوقت الذي قام فيه بالتوقيع ومعلومات عن صاحب التوقيع، يتم تسجيل التوقيع الرقمي بشكل رسمي عند جهات تعرف باسم طرف محايد مهمته التأكد من صحة ملكية التوقيع الرقمي للأشخاص الذين يقومون بتوقيع الوثائق الإلكترونية لتسجيل التوقيع المفتاحي عنده، وتقوم بعدها بجمع معلومات من حامل التوقيع الإلكتروني المراد تسجيله، بعد ذلك تصدر لهذا الشخص شهادة تمكنه من التوقيع الإلكتروني على المنتوجات الرقمية، ويزود هذا الشخص بكلمة سر خاصة تمكنه من استخدام التوقيع الإلكتروني.

---

[1] – محمد رحايلي، مرجع سابق، ص 15.

[2] – أحمد عبد الله مصطفى ، "حقوق الملكية الفكرية والتأليف في بيئة الأنترنت"، مجلة أبحاث، العدد 03، الصادر في 21 ديسمبر 2009، ص 17.

2-التوقيع البيومترى

عبارة عن تحديد نمط خاص تحرك به يد الشخص الموقع خلال التوقيع، من خلال توصيل قلم إلكتروني بجهاز الكمبيوتر ويقوم الشخص بالتوقيع باستخدام هذا القلم الذي يسجل حركة اليد حيث لكل شخص سمة توقيع خاصة به تميز سمات شخصيته، ويتم تسجيل التوقيع البيومتري كما هو الحال في التوقيع المفتاحي.

3- تشفير البيانات

عبارة عن إدخال تعديلات على المعلومات عند إرسالها إلى جهة معينة، أو تحويلها إلى رموز بدون معنى، بحيث عندما تصل إلى أشخاص آخرين لا يستطيعون فهمها أو الاستفادة منها، لذا فهي عبارة عن تشفير وتحويل للنصوص العادية الواضحة إلى نصوص مشفرة وغير مفهومة، فتحتاج كل معلومة لفكها وإعادتها إلى الوضع الأصلي.[1]

المطلب الثاني: التدابير الردعية

تتعدد العقوبات المسلطة على الجرائم الإلكترونية نظرا لخطورتها ومساسها بالحقوق الأدبية والمالية في نفس الوقت، إلا أنه لا نجد قانونا خاصا بهذه العقوبات وإنما نجدها متفرقة في العديد من القوانين التي لها علاقة وطيدة بالمنتوج الرقمي فنجد بطبيعة الحال عقوبات واردة في قانون العقوبات إلى جانب تلك الواردة في قانون حقوق المؤلف والحقوق المجاورة، إضافة إلى العقوبات الواردة في قانون خاص بجرائم التكنولوجيا الحديثة وهو قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها.

أولا- العقوبات المنصوصعليها في قانون حقوق المؤلف والحقوق المجاورة

لم يتم النص صراحة على المنتوجات الرقمية ضمن قانون حقوق المؤلف والحقوق المجاورة وإنما تمت الإشارة إليها فقط في بعض المواد مثل في المادة 05 التي تنص " تعتبر مصنفات محمية قواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى".

كما نصت المادة 52 من نفس القانون على " وجوب استعمال برامج الحاسوب للغرض الذي اكتسب من أجله ووفقا للشروط التي كانت قائمة عند اكتسابه.[2]

يفهم من هذه المادة أن كل استغلال غير شرعي لبرامج الحاسوب، وقياسا عليها كل المنتوجات الرقمية المذكورة آنفا، يعرض صاحبه للعقوبات المنصوص عليها في قانون حقوق المؤلف والحقوق المجاورة ، فتنص المادة

---

[1] - المرجع السابق ، ص 20.

[2] - انظر المواد 05 و 52 من الأمر رقم 03- 05 المؤرخ في 19 جويلية 2003و المتعلق بحقوق المؤلف والحقوق المجاورة، جريدة رسمية عدد 44 الصادرة في 23 جويلية 2003.

152 منه" يعد مرتكبا لجريمة التقليد كل من ينتهك الحقوق المحمية بموجب هذا الأمر"، فنفهم من ذلك على أنه يعاقب كل من يقلد منتوج رقمي مهما كان نوعه.

ثانيا– العقوبات المنصوص عليها في قانون العقوبات

لقد جاء تعديل قانون العقوبات لسنة 2015 بمواد جديدة لم تكن موجودة في القانون القديم بحيث تجرم الأعمال الناتجة عن المساس بالمنتوجات الرقمية الحديثة والتي من شأنها الحاق الضرر بالغير بحيث خصص القسم السابع مكرر3 " للمساس بأنظمة المعالجة الآلية للمعطيات".[1]

فجاءت المادة 394 مكرر بقفزة نوعية في مجال التجريم والعقاب في إطار الجرائم الرقمية، بحيث أنها تعاقب " بالحبس من ثلاثة أشهر إلى سنة و بغرامة مالية من 000 50 دج إلى 000 100 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"

أما المادة 394 مكرر1 فتضاعف العقوبة لكل من " أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

وهذا إن دل على شيء فيدل على صرامة المشرع الجزائري في حالة المساس بالمنتوجات الرقمية، كما صدر قانون يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها وهو القانون رقم 09– 04 المؤرخ في 5 أوت 2009.

3 – العقوبات المنصوص عليها في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام ومكافحتها

عندما تكتشف السلطات المكلفة بمراقبة وسائل تكنولوجيات الإعلام والاتصال خلال قيامها بتفتيش منظومة معلوماتية معلومات مفيدة للكشف عن الجرائم أو مرتكبيها، تقوم بنسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

أما في حالة استحالة الحجز على المعطيات، تقوم السلطة المعنية باستعمال التقنيات المناسبة لمنع الوصول إلى تلك المعطيات، كما تتخذ الإجراءات اللازمة لمنع الاطلاع عليها بأي شكل من الأشكال.

ويمكن أن تأمر نفس السلطات مقدمو الخدمات(شركات الاتصال كجيزي و أوريدو) بحفظ كل المعطيات التي تسهل التعرف والوصول إلى مرتكبي الجرائم، لاسيما المعطيات التي تسمح بالتعرف على المرسل إليهم وكذا عناوين المواقع المطلع عليها، كما يتعين على مقدمي الخدمات السحب الفوري لأي معطيات مخالفة للقانون أو مشكلة لجريمة ما مع اتخاذ جميع التقنيات اللازمة لمنع الوصول إليها.

[1]– انظر المواد من 394 مكرر 1 إلى 394 مكرر 7 من قانون العقوبات المعدل والمتمم.

لذلك تم إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها للقيام بعمليات تفتيش المنظومات المعلوماتية ومباشرة الإجراءات المشار إليها أعلاه[1].

كون أن تفادي الجرائم الإلكترونية لا يكون بمنع المستهلكين من الوصول إلى المنتوجات الرقمية لأن هذا يعد شبه مستحيل في وقتنا الحالي، وإنما الحل يكمن في تعزيز وسائل الحماية عليها، فتحقيق الحماية للمنتوج الرقمي، باعتباره حق أدبي ومالي هام ويعتمد أساسا على وسائل التكنولوجيا الحديثة ، سيساهم بشكل فعال في حماية الاقتصاد الوطني وتطويره.[2]

خاتـــــــــمة

وفي الختام يمكن القول أن مثل هذه الجرائم الإلكترونية من الصعب تحديد معالمها و أركانها رغم التطورات التكنولوجية السارية في هذا المجال، ولذلك فإن الجزائر، على غرار الدول النامية، في حاجة ماسة إلى استحداث تدابير أكثر فعالية وسن إجراءات قانونية مواكبة للتدفق التكنولوجي الغزير وتغيراته المتسارعة، وبهذا لابد أن تكون الحماية القانونية من الجرائم الإلكترونية مسايرة لتطور التكنولوجي الحديث.

ولذلك فإن تفادي الجرائم الإلكترونية لا يكون بمنع المستهلكين من استخدام الشبكة العنكبوتية ووسائل التواصل الاجتماعي لأن هذا يعد شبه مستحيل في وقتنا الحالي، وإنما الحل يكمن في تعزيز وسائل الحماية عليها، كون أن التوصل إلى التحكم في تفشي الجرائم الإلكترونية سيساهم بشكل فعال في حماية المجتمع وتطويره وتحقيق الاستقرار والأمن الذي تسعى إليه كل دولة.

فالمشرع الجزائري أولى اهتماما كبيرا، ولو بصفة متأخرة بعض الشيء، بحماية البيئة الرقمية مواكبة للوسائل الإلكترونية الحديثة على غرار سائر دول العالم وذلك في إطار العولمة المفروضة وضرورة الاندماج فيها.

فقد أصبحت الأنترنيت ووسائل التواصل الاجتماعي بشتى أنواعها جزء لا يتجزأ من حياتنا اليومية بحيث لا يمكن الاستغناء عنها، بل أصبحت في تزايد مستمر و بات من السهل على أي شخص امتلاك حساب إلكتروني وهذا للأسباب التالية :

. سهولة الولوج إلى العالم الافتراضي.

---

[1]– لمزيد من المعلومات انظر المواد 06،07 ،08 ،09 ،10 ،11 ،12 و13 من القانون 09– 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[2]– جمال محمود الكردي، حق المؤلف في العلاقات الخاصة الدولية والنظرة العربية والاسلامية للحقوق الذهنية في منظومة الاقتصاد العالمي الجديد، دار الجامعة الجديدة، الاسكندرية– مصر– 2003، ص179.

. بساطة إمكانيات الإنتاج بالنسبة للمنتوجات الرقمية.

. سرعة وسهولة انتشارها وتوزيعها.

غير أن هذا لا يمنع من التحذير من مخاطر هذا النوع من المنتوجات خاصة على المراهقين مما قد تحتويه من معلومات هدامة وإباحية وفي بعض الأحيان تشجع على العنف والانحراف وفساد المجتمع.

فيمكن القول في الأخير أن المنتوجات الرقمية سلاح ذو حدين: فمن جهة تشجع على التطور التكنولوجي وتواكب العولمة كما تساعد في فك العزلة عن الفرد والمجتمع، ومن جهة أخرى قد تكون أداة لنشر الفساد والآفات الاجتماعية هذا ما يبرر ضرورة إحاطتها بحماية قانونية.

نصل في الأخير إلى إعطاء بعض التوصيات التي عسى ولعل أن تفيد الباحثين في نفس الموضوع مستقبلا وكذا القائمين على مكافحة الجريمة الإلكترونية بكل أنواعها:

– تطبيق قواعد قانونية شاملة لحماية المنتوجات الرقمية من الجريمة الإلكترونيةفي المجال الرقمي والمعلوماتي.

– وضع إجراءات جديدة لمكافحة الجريمة الإلكترونية وجزاءات رادعة في قانون العقوبات وقانون الإجراءات الجزائية وكذا في القوانين الخاصة بحماية المؤلف والجرائم التكنولوجية.

–إيجاد آليات فعالة لضمان التطبيق العملي للقواعد والجزاءات المستحدثة مع تعميم تطبيقها على كافة المستويات.

– تأهيل أشخاص و فرق أمنية متخصصة ومدربة على الأجهزة التكنولوجية الحديثة و كيفية الكشف عن سرقة وقرصنة المنتوجات الرقمية.

قائمة المصادر والمـــــراجع

أولا / قائمة المصادر

–النصوص القانونية

1– الأمر رقم 03– 05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، جريدة رسمية عدد44 الصادرة في 23 جويلية 2003.

2- قانون العقوبات المعدل والمتمم.
3 - القانون رقم09 -03 المتعلق بحماية المستهلك وقمع الغش والمؤرخ في25 فبراير2009 الصادر في الجريدة الرسمية بتاريخ 08مارس2009 العدد15.
4- القانونرقم 09-04 المؤرخفي 05 أوت 2009 المتضمنالقواعدالخاصةللوقايةمنالجرائمالمتصلةبتكنولوجياتالاعلاموالاتصالومكافحتها،جريدةرسميةعدد47 الصادرةفي16 أوت 2009.

ثانيا/ قائمة المراجع

أ – الكتب

1- إياس بن سمير الهاجري، أمن المعلومات على شبكة الأنترنيت، ، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية ، الرياض – السعودية –2004.
2- جمال محمود الكردي، حق المؤلف في العلاقات الخاصة الدولية والنظرة العربية والاسلامية للحقوق الذهنية في منظومة الاقتصاد العالمي الجديد، دار الجامعة الجديدة، الاسكندرية- مصر- 2003.
3- عبد الفتاح بيومي حجازي، مقدمة في حقوق الملكية الفكرية وحماية المستهلك في عقود التجارة الإلكترونية، دار الفكر الجامعي، الطبعة الأولى، الاسكندرية - مصر –2005.
4- علي فتاك، تأثير المنافسة على الالتزام بضمان سلامة المنتوج، دار الفكر الجامعي، الاسكندرية، مصر2007
5 – محمد محمد أحمد أبو سيد أحمد، حماية المستهلك في الفقه الاسلامي، منشورات محمد علي بيضون، دار الكتب العلمية، الطبعة الأولى، بيروت – لبنان2004.
6-مدونة التجارة الإلكترونية العربية.
7-يحيى يحياوي ، أوراق في التكنولوجيا و الاعلام و الديموقراطية، دار الطبع بيروت ،الطبعة الأولى، لبنان يناير 2004.
8-يسرية عبد الجليل، حقوق حاملي براءات الاختراع ونماذج المنفعة، دارالنشر منشأة المعارف بالإسكندرية – مصر- 2005.

ب - الرسائل الجامعية

1- بن دريس حليمة، حماية حقوق الملكية الفكرية في التشريع الجزائري، أطروحة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبي بكر بلقايد – تلمسان- السنة الجامعية 2013- 2014.
2- فرحات حمو ، التنظيم التشريعي لحقوق الملكية الصناعية ودوره في التنمية ، أطروحة مقدمة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق -جامعة وهران- السنة الجامعية 2011- 2012.

3- محمد رحايلي، حقوق المؤلف و الحقوق المجاورة في البيئة الرقمية: الحالة الجزائرية، أطروحة مقدمة ضمن متطلبات نيل شهادة الدكتوراه في القانون الخاص، جامعة الأمير عبد القادر – قسنطينة- السنة الجامعية 2014- 2015.

ج- المقالات

1- أحمد عبد الله مصطفى، "حقوق الملكية الفكرية والتأليف في بيئة الإنترنت"، مجلة أبحاث، العدد 03، الصادر في 21ديسمبر 2009.

2- بن عبو نسيمة ، "البرمجيات بين حقوق المؤلف وبراءات الاختراع"، مجلة بحوث – جامعة الجزائر 1 – العدد08-2015.

3- رامي ابراهيم حسن زواهرة ومحمد خليل أبو بكر، " الابتكار كشرط لحماية حقوق المؤلف الفكرية وأثر تكنولوجيا المعلومات عليه" دراسة مقارنة، مركز الأبحاث بجامعة الزيتونة ، عمان – الأردن –2017..

4- عميمر عبد القادر،" الحماية القانونية للصحفي في إطار قانون حق المؤلف"، مجلة بحوث – جامعة الجزائر 1 – العدد 08- 2015.

جامعة الجزائر 1 بن يوسف بن خدة.

كلية الحقوق.

الملتقى الدولي الافتراضي الموسوم ب:

((القانون الجنائي في ظل التطور التكنولوجي"إشكالات ومعالجات"))

يومي 28 و29 سبتمبر 2022.

مداخلة للمشاركة في فعاليات الملتقى ضمن المحور الثاني منه المعنون ب: أثر استخدام التكنولوجية الحديثة على أحكام التجريم.

عنوان المداخلة:

مقتضيات تجريم التمييز وخطاب الكراهية عبر الوسائط الالكترونية على ضوء قانون05/20. تجريم وقائي أم علاجي؟

من تقديم: الدكتورة بلغيث سمية. أستاذ محاضر –ب– جامعة العربي بن مهيدي –أم البواقي–.البريد الالكتروني: belghit.soumia@yahoo.fr

الملخص:

لقد تدعمت المنظومة القانونية في الجزائر بصدور قانون 20–05 الذي عني بتجريم أفعال التمييز وخطاب الكراهية عبر مختلف الوسائل التقليدية، الاعلام أو المواقع والحسابات الالكترونية، وذلك حرصاً من المشرع على حماية الكرامة الانسانية والسلامة الجسدية للأفراد، وضمان الأمن وحماية المجتمع من الفتن والضغينة التي تحاول بعض الجهات الداخلية أو الخارجية زرعها مساساً بالوحدة الترابية والسيادة الوطنية، لذلك فإننا نتساءل هل

وفق المشرع في تجريم التمييز وخطاب الكراهية عبر الوسائط الالكترونية؟ وما هي السياسة التي اتبعها في هذا التجريم؟.

الكلمات المفتاحية: التمييز، خطاب الكراهية، مواقع الكترونية، تجريم وقائي، تجريم علاجي.

Abstract:

The legal system in Algeria was supported by the issuance of Law 20-05, which was concerned with the criminalization of acts of discrimination and hate speech through various traditional means, the media or websites and electronic accounts, in the interest of the legislator to protect human dignity and physical integrity of individuals, and to ensure security and protect society from sedition and resentment that is trying to Some internal or external parties planted it in violation of the territorial integrity and national sovereignty. Therefore, we wonder whether the legislator has approved the criminalization of discrimination and hate speech through electronic media? What is the policy followed by this criminalization?

Keywords: Discrimination , hate speech, Social Media, preventive incrimination, Therapeutic criminalization.

مقدمة.

لقد عانت الجزائر في الآونة الأخيرة من تفشي ظاهرة التميّيز وانتشار خطاب الكراهية عبر مختلف المواقع الالكترونية، ومنصات التواصل الاجتماعي، خاصة مع نجاح الحراك الشعبي السلمي للثاني والعشرين من شهر فيفري على الصعيدين الوطني والدولي، وظهور جهات معادية تصطاد في المياه العكرة، وتغوص في مواضع الضعف عند البعض، لزرع الفتنة والتفرقة بين أفراد الوطن الواحد، حيث سعت بعض الجهات لنشر خطابات الكراهية

والتميّيز والتطرف ضد جماعات معينة بهدف التفرقة بين العرب والقبائل عبر مواقع التواصل الاجتماعي كالفيسبوك والتويتر...الخ. لزرع نار الفتنة التي زادت حدتها مع انتشار فيروس كورونا (كوفيد)19، وما شهدته البلاد من أزمات أنذاك. الأمر الذي دفع بالمشرع الجزائري إلى الإسراع في احتواء المسألة، ومجابهتها قبل أن تشتد أوزارها، من خلال تجريم أفعال التميّيز وخطاب الكراهية بمقتضى القانون رقم 05/20 المتعلق بالوقاية من التميّيز وخطاب الكراهية ومكافحتهما.

ولئن كانت منصات التواصل الاجتماعي واحدة من أهم المواقع الالكترونية التي جادت بها التطورات التكنولوجية الحديثة، تتيح للأفراد فرص التعبير عن ما يجول بخاطرهم من مشاعر، وأفكار، وأراء بكل حرية، تعزيزاً للحق في حريتي الرأي والتعبير المعترف بهما دولياً ودستورياً، لدى مختلف دول العالم، بما فيها الجزائر، إلاّ أن هذه الحرية في التعبير عن الرأي لم تقرّر على إطلاقها، بل وجب ضبطها بقيود تكبح جماحها ضد التعسف، والإساءة لحقوق وحريات الآخرين، لذلك فإنّنا نتساءل: هل وفق المشرع في ضبط حرية التعبير عن الرأي المقررة دولياً ودستورياً لجميع الأفراد، والمعبر عنها عبر مختلف الوسائط الالكترونية، متى ترتب عليها نشر التفرقة والتميّيز بين أفراد المجتمع، وزرع الكراهية والدعوة إلى العنف، قصد المساس بحقوق الإنسان وحرياته الأساسية، وتهديد الوحدة الوطنية للدولة من خلال قانون التميّيز وخطاب الكراهية 20-05 أم لا؟. أو بمعنى آخر هل وفق المشرع في تجريم التمييز وخطاب الكراهية عبر الوسائط الالكترونية؟ وما هي السياسة التي اتبعها في هذا التجريم؟.

للإجابة على هذه الإشكالية اعتمدنا على المنهجين الوصفي والتحليلي: الوصفي نوضفه عن الوقوف على تعريف وتوضيح بعض المفاهيم المرتبطة بموضوع البحث، أمّا المنهج التحليلي فتناول من خلاله تحليل بعض النصوص القانونية ومناقشتها بغيرها للوقوف

على الأحكام التي يمكن استنباطها من خلالها لمعرفة السياسة التي اتبعها المشرع من خلال هذا التجريم.

كما اعتمدنا التقسيم الثنائي؛ حيث نقسم هذه الورقة البحثية إلى مبحثين: نتناول في المبحث الأول دور مواقع التواصل الاجتماعي في نشر خطاب التمييز والكراهية، ونخصص المبحث الثاني لدراسة جريمة التمييز وخطاب الكراهية عبر المواقع والحسابات الالكترونية على ضوء قانون 20-05 فيما يلي.

المبحث الأول: دور مواقع التواصل الاجتماعي في نشر خطاب التميّيز والكراهية.

لقد لعبت مواقع التواصل الالكتروني دوراً مهماً في نشر ثقافة التمييز والعنف وخطاب الكراهية في الكثير من المجتمعات عبر العالم، على غرار الجزائر، كغيرها من الوسائل التقليدية للنشر كالصحف والمجلات ووسائل الاعلام، لذلك فإننا سنتولى دراسة تعريف التمييز وخطاب الكراهية (المطلب الأول)، فالتعريف بهذه المواقع (المطلب الثاني) ثم دراسة تأثير مواقع التواصل الاجتماعي على نشر التمييز وخطاب الكراهية (المطلب الثالث).

المطلب الأول: تعريف التمييز وخطاب الكراهية.

أولاً: تعريف التمييز: يعرّف التميّيز في اللغة: ماز الشيء أي عزله وفرزه، ويقال امتاز القوم إذا تميّز بعضهم على بعض، ويقال أيضاً ماز الشيء عن الطريق أي أزاله، كما ترادف لفظ التميّيز لغوياً مع التفرقة وهو فعل مبني على أساس فصل الأشياء عن النوع الذي تنتمي إليه لجعلها في فئات خاصة. أمّا من الناحية الاصطلاحية فيقصد بالتميّيز كل تفرقة أو استثناء أو تقيّيد أو تفضيل يقوم على أساس الجنس أو العرف أو اللون أو النسب أو الأصل

القومي، أو الأثني أو اللغوي أو الانتماء الجغرافي أو الإعاقة أو الحالة الصحية، حيث ينتج عنه تعطيل أو عرقلة الاعتراف بحقوق الإنسان والحريات الأساسية أو التمتع بها أو ممارستها على قدم المساواة في المجال السياسي أو الاقتصادي أو الاجتماعي أو الثقافي أو في أي مجال آخر من مجالات الحياة.[1] وعرّف أيضاً بأنّه " شكل من أشكال الممارسات العنصرية ويعدّ من أخف هاته الممارسات وطأة، إذ يصل بعضها أحيانا إلى التناحر والإبادة، ومن أبرز أشكال التميّيز الحرمان من الحصول على الفرص المجتمعية واستخدام لغة الازدراء التي تكاد تكون عدوانية، كما يعرف التميّيز العنصري بأنّه تفرقة بين الناس في حقوقهم وواجباتهم لاختلاف أجناسهم وألوانهم."[2] والتميّيز العنصري كما يراه علماء المسلمين هو التفرقة بين جنس وجنس، أو عرق وعرق، أو لون ولون بين الناس، وعليه فالاهتمام بالإنسان وتقرير حقوقه يلازم الإنسان، ولا يرتبط بشعب دون آخر ولا بأرض خاصة ولا بعصر معيّن، لكنه يتجاوز حدود الإقليم والأرض والجنس واللون والزمان والمكان. وقد قرّر ذلك قول رسول الله صلى الله عليه وسلّم :يا أيّها الناس ألا إنّ ربكم واحد وإنّ أباكم واحد ألا لا فضل لعربي على أعجمي ولا لعجمي على عربي، ولا لأحمر على أسود، ولا لأسود على أحمر إلاّ بالتقوى. أبلّغت. قالوا: بلّغ رسول الله صلى الله عليه وسلم.[3] [4]

أمّا من الناحية القانونية فقد عرّف المشرع الجزائري التميّيز في الفقرة الثانية من المادة الثانية من القانون رقم 20- 05[5]بقوله(("التمييز": كل تفرقة أو استثناء أو تقييد أو تفضيل

---

[1]سمير قاسمي: **((التميّيز وخطاب الكراهية بين القانون 05/20 والإتفاقيات الدولية))**، مقال منشور في مجلة العلوم الإنسانية والإجتماعية ، العدد الخامس، جامعة الجيلالي بونعامة، خميس مليانة، الجزائر، مارس 2021، ص ص151،150.

[2]خالد ضو: **((الأحكام الجزائية لجرائم التميّيز وخطاب الكراهية في التشريع الجزائري ضمن القانون 20-05))**، مقال منشور في مجلة التمكين الاجتماعي، المجلد الثالث، العدد الرابع، جامعة عمار ثليجي، الأغواط، الجزائر، ديسمبر 2021، ص112.

[3]أخرجه الإمام أحمد في مسند المكيين برقم 15322، وفي مسند الأنصار برقم:22399.

[4]محمد صبحي سعيد: **((جرائم التميّيز والحض على الكراهية والعنف، دراسة مقارنة))**، أطروحة دكتوراه في القانون الجنائي، كليّة الحقوق جامعة القاهرة، مصر، د س، ص ص 8-9.

[5]**القانون رقم 20-05** المؤرخ في 05 رمضان عام 1441هـ الموافق 28 أبريل سنة 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الصادر في ج ر ج ج بتاريخ 6 رمضان عام 1441هـ الموافق 29 أبريل سنة 2020م، العدد 25، ص 4.

يقوم على أساس الجنس أو العرق أو اللون أو النسب أو الأصل القومي أو الاثني أو اللغة أو الانتماء الجغرافي أو الإعاقة أو الحالة الصحية، يستهدف أو يستتبع تعطيل أو عرقلة الاعتراف بحقوق الإنسان والحريات الأساسية أو التمتع بها أو ممارستها على قدم المساواة في المجال السياسي أو الاقتصادي أو الاجتماعي أو الثقافي أو في أي مجال آخر من مجالات الحياة العامة.)) وقد جاء هذا التعريف مطابقاً حرفياً للتعريف الذي تناولته المادة 295 مكرر1 من قانون العقوبات التي تمّ إلغاؤها وتعويضها بهذا القانون وفقاً لأحكامه النهائية (م46)، مع إضافة ثلاثة أسس جوهرية جديدة للتمييّز هي: "اللغة"، "الانتماء الجغرافي"، و"الحالة الصحية"، مع حذف الفقرة الأخيرة من المادة 295 مكرر المقررة للعقوبات المطبقة على مرتكبي الفعل المجرم واستبدالها بمواد جزائية تفصيلية ضمن هذا القانون، الأمر الذي يوحي بأنّ توجه المشرع الجزائري إلى معالجة مسألة التمييز العنصري لم يكن وليد قانون 20-05 وإنّما سبقه تعديل قانون العقوبات لسنة 2014 بموجب القانون رقم 14-01 في ذلك.

وقد جاء هذا التعديل كتأكيد من المشرع بضرورة مسايرة النصوص التشريعية الوطنية لمختلف الإعلانات والاتفاقيات الدولية ذات الصلة؛ على غرار المادة الثانية من الإعلان العالمي لحقوق الإنسان[1] التي جاء فيها ((لكل إنسان حق التمتع بجميع الحقوق والحريات المذكورة في هذا الإعلان دونما تمييّز من أي نوع، ولاسيما التمييّز بسبب العنصر، أو اللون، أو الجنس، أو اللغة، أو الدين، أو الرأي السياسي وغير السياسي، أو الأصل الوطني أو الاجتماعي، أو الثروة، أو المولد، أو أي وضع آخر...))، والفقرة الثانية من المادة الثانية من العهد الدولي للحقوق الاجتماعية والاقتصادية[2] التي تنص على أنّه ((تتعهد الدول الأطراف بأن تضمن جعل ممارسة الحقوق المنصوص عليها في هذا العهد بريئة من أي

[1] الإعلان العالمي لحقوق الإنسان المصادق عليه في الجمعية العامة بموجب القرار رقم 217أ(3) في 10 ديسمبر 1948.

[2] العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية اعتمد وعرض للتوقيع والتصديق والإنضمام بموجب قرار الجمعية العامة للأمم المتحدة 2200ألف (د21-) المؤرخ في 16 ديسمبر 1966، دخل حيّز النفاذ في 3 يناير 1976 وفقاً لأحكام المادة 27 من العهد.

تميّيز بسبب العرق، أو اللون، أو الجنس، أو اللغة، أو الدين، أو الرأي سياسياً أو غير سياسي، أو الأصل القومي أو الاجتماعي أو الثروة أو النسب أو غير ذلك من الأسباب...))، وكذا المادة الخامسة من الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري[1] التي ورد فيها: ((تتعهد الدول الأطراف بحظر التمييز العنصري والقضاء عليه بكافة أشكاله، وبضمان حق كل إنسان دون تميّيز بسبب العرق، أو اللون، أو الأصل القومي أو الاثني، في المساواة أمام القانون.))، في حين تولت الفقرة الأولى من المادة الأولى من الاتفاقية الخاصة بمكافحة التمييز في مجال التعليم لسنة 1960[2] تعريف مصطلح التميّيز بقولها: ((لأغراض هذه الاتفاقية تعني كلمة "التميّيز" أي ميز أو استبعاد، أو قصر، أو تفضيل على أساس العنصر أو اللون أو الجنس أو اللغة أو الدين أو الرأي سياسياً وغير سياسي، أو الأصل الوطني أو الاجتماعي، أو الحالة الاقتصادية أو المولد، يقصد منه أو ينشأ عنه إلغاء المساواة في المعاملة في مجال التعليم أو الإخلال بها))، وما نلاحظه بالنسبة للتعريف الذي أورده المشرع الجزائري أنّه أسقط الدين كأساس للتميّيز مقارنة بباقي التعاريف الدولية الأخرى، ويبرر ذلك حسب اعتقادنا بأنّ الإسلام هو دين الدولة الجزائرية والديانة الوحيدة بها فلا مجال للتمييز بين مواطنيها على هذا الأساس، وإن وجدت قلة قليلة من الأجانب غير المسلمين فإنّ كرامتهم مصانة بما يتمتعون به من حقوق وامتيازات في إطار التشجيع على السياحة والاستثمار ببلادنا، ومسألة خضوعهم للتميّيز مستبعدة جداً.

ثانياً: تعريف خطاب الكراهية: مفهوم خطاب الكراهية مفهوم مركب يتكون من لفظين: الخطاب والكراهية؛ والخطاب في اللغة يعني "مراجعة الكلام، وقد خاطبه بالكلام مخاطبة

---

[1] الاتفاقية الدولية للقضاء على جميع أشكال التميّيز العنصري، اعتمدت وعرضت للتوقيع والتصديق والإنضمام بموجب قرار الجمعية العامة للأمم المتحدة (2106) ألف (د-20) المؤرخ في 21 كانون الأول/ديسمبر 1965، دخلت حيّز النفاذ في 4 كانون الثاني/ يناير 1969 وفقاً للمادة 19.

[2] الاتفاقية الخاصة بمكافحة التميّيز في مجال التعليم، اعتمدها المؤتمر العام لمنظمة الأمم المتحدة للتربية والعلم والثقافة في 14 كانون الأول/ديسمبر 1960، في دورته الحادية عشر، ودخلت حيّز النفاذ في 22 آيار/مايو 1962، وفقاً لأحكام المادة 14.

وخطاباً وهما يتخاطبان، والمخاطبة مفاعلة من الخطاب والمشاورة، أراد: أنت من الذين يخطبون الناس ويحثونهم على الخروج والاجتماع للفتن."[1] أمّا الكراهية فهي مشتقة من كره الشيء كرهاً وكراهة، وكراهيّة خلاف أحبه، فهو كريه وكروه، فالكاف والراء والهاء أصل صحيح واحد، يدل على خلاف الرضا والمحبة، يقال كرهت الشيء أكرهه كرهاً، ويقال : الكره والكراهية، والكريهة الشدة في الحرب.[2] ويعرف البعض خطاب الكراهية بشكل عام بأنّه بث الكراهية والتحريض على النزاعات والصراعات الطائفية والإقليمية الضيقة، والتحريض على إنكار وجود الآخر وإنسانيته وتهميشه ونشر الفتنة واستخدام أساليب طائفة دينية أو عرقية والحض على العنف واتهام الطرف الآخر بالخيانة والفساد، ... وإن كانت الكراهية هي الحقد والغضب والشعور بالضغينة تجاه شخص ما، فإنّ الأفعال القولية التي تصدر عن دولة أو جماعة أو أفراد وتدعو صراحة إلى الكراهية يطلق عليها "خطاب الكراهية"، في حين أنّ كافة الجرائم التي تحركها الكراهية وتدفع مرتكبيها لفعل جرمي بسبب الكراهية أياً كانت، تسمى "جرائم الكراهية" هذه الجرائم قد ترتكب ضد أفراد أو جماعات لأسباب الكراهية المتعلقة بالدين أو العرق أو اللغة، أو الجنس أو الإعاقة العقلية أو البدنية.[3] وينعت البعض خطاب الكراهية بكونه نوع من أنواع العنف وهو العنف اللفظي بالقول بأنّه "خطاب مبني على العنف اللفظي، يهدف إلى القتل المعنوي للآخر وإقصائه من خلال الشتم والسب والقذف والإهانة والتعصب الفكري والاستعلاء، وصولاً إلى العنف المادي والقتل، ويشكل خطاب الكراهية أداة مهمة لتحفيز المشاعر وإثارتها وتوجيهها في اتجاه معين، بما ينشأ عنه

---

[1] ابن منظور، محمد بن مكرم بن علي،**((لسان العرب))**، دار صادر، بيروت، لبنان، 2010، ص 361.

[2] أبو الحسين، أحمد بن فارس زكريا: **((معجم مقاييس اللغة))**، دار الفكر للطباعة والنشر، الجزء الخامس، 2007، ص 172.

[3] بن عودة نبيل ونوار محمد: **((الصلاحيات الحديثة للضبطية القضائية للكشف وملاحقة مرتكبي الجرائم المتعلقة بالتمييز وخطاب الكراهية، "التسرب الالكتروني نموذجاً"** ، مقال منشور في مجلة الأكاديمية للبحوث في العلوم الإجتماعية، المجلد الأول، العدد الثاني، المركز الجامعي لإيليزي، سبتمبر 2020، ص323.

من سلوك وثقافة مبنية على العنصرية ضد من وجه الخطاب ضدهم، ومن هنا تكمن خطورة هذا الخطاب، خاصة إذا توافرت منصات إعلامية مهيأة لهذا النوع.[1]

وقد تولى المشرع الجزائري تعريف خطاب الكراهية في الفقرة الأولى من المادة الأولى من قانون 20-05 بالقول: ((خطاب الكراهية": جميع أشكال التعبير التي تنشر أو تشجع أو تبرر التمييز، وكذا تلك التي تتضمن أسلوب الازدراء أو الإهانة أو العداء أو البغض أو العنف الموجهة إلى شخص أو مجموعة أشخاص على أساس الجنس أو العرق أو اللون أو النسب أو الأصل القومي أو الاثني أو اللغة أو الانتماء الجغرافي أو الإعاقة أو الحالة الصحية.))،

وعلى المستوى الدولي افتقرت الإعلانات والاتفاقيات الدولية ذات الصلة للنص على تعريف واضح ودقيق للكراهية أو خطاب الكراهية حيث ربطت أغلبها هذا الأخير بأفعال التعصب والعنصرية الدافعة للكراهية والعنف على غرار مبادئ كامدن التي وضعتها منظمة المادة 19 بالتعاون مع مجموعة من الخبراء القانونيين والإعلاميين التي اعتبرت الكراهية "حالة ذهنية تتسم بانفعالات حادة وغير عقلانية من العداء والمقت والاحتقار تجاه المجموعة أو الشخص المحرض ضده"[2] ويرى البعض "أن المشرع الجزائري تناول خطاب الكراهية من زوايا تتفق تارة، وتختلف تارة أخرى عن تناول هذا الخطاب من طرف الاتفاقيات الدولية ، ذلك أنّ المشرع الجزائري ربط خطاب الكراهية بالتمييز القائم على أساس الجنس أو العرق أو اللون أو النسب أو الأصل القومي أو الاثني وجمع بين المفهومين في قانون واحد بهدف التصدي لهما معاً، بينما توجه القانون الدولي إلى اعتبار خطاب الكراهية سبباً في ارتكاب جرائم الإبادة الجماعية، وقد عبّر القانون الدولي عن خطاب الكراهية بالدعاية للحرب أو

---

[1] لبنى رحموني: **((الإعلام الديني الإسلامي في مواجهة خطاب الكراهية والتنميط الغربي))**، مقال منشور في مجلة المعيار المجلد الرابع والعشرون، العدد الثاني والخمسون، مجلة المعيار، جامعة العلوم الإسلامية الأمير عبد القادر، قسنطينة، الجزائر، سبتمبر 2020، ص221.

[2] شيماء الهواري: **((مفهوم الكراهية في الشرعية الدولية))**، مقال منشور في مجلة المركز الديمقراطي العربي للدراسات الإستراتيجية، الإقتصادية والسياسة، متاح عبر الموقع الإلكتروني https://democraticac.de أطلع عليه بتاريخ 2022/07/16، على الساعة 13:28.

دعوة إلى الكراهية القومية أو الدينية، مع تطرق بعض الاتفاقيات الدولية للتمييّز العنصري الذي يعتبر أرضاً خصبة لتفشي خطاب الكراهية."[1]

وفي إطار البحث حول موضوع التمييز وخطاب الكراهية عبر الوسائط الالكترونية يعرف البعض خطاب الكراهية على أنّه "أي محتوى على وسائل التواصل الاجتماعي يشمل التعدي على أشخاص بناء على عرقهم ودينهم وجنسهم وانتمائهم الوطني أو بناء على إعاقتهم ومرضهم."[2] كما تولى كل من فايسبوك وتويتر تعريف خطاب الكراهية حسب وجهة نظرهم؛ حيث يعرف فايسبوك خطاب الكراهية ويؤكد أنّه (لا يسمح بالمحتوى الذي يهاجم الأشخاص على أساس عرقهم الفعلي أو المتصور أو الاثنية أو الأصل القومي أو الديانة أو الجنس أو النوع الاجتماعي أو الهوية الجنسية أو التوجه الجنسي أو الإعاقة أو المرض) كما يؤكد الموقع على ما يلي: (ولكننا في الوقت ذاته نسمح بالتعبيرات التي تنشر على سبيل الدعابة أو السخرية والتي قد يعتبرها البعض تهديداً أو هجوماً، ويتضمن هذا المحتوى الذي قد يعتبره العديد من الأشخاص مفتقداً إلى الذوق(مثال: النكات أو الأعمال الكوميدية القصيرة أو كلمات الأغاني الشعبية وما إلى ذلك)، وفي المقابل يعبر يوتيوب أن (الكلام الذي يحض على الكراهية هو كل محتوى يروج للعنف أو يهدف أساساً إلى التحريض على الكراهية ضد أفراد أو مجموعات على أساس سمات معينة، على سبيل المثال العرق أو الجذور العرقية أو الدين أو الاعاقة أو الجنس أو العمر أو حالة الخدمة في السلك العسكري أو الميول الجنسية/الهوية الجنسية)[3]

---

[1] وريدة جندلي بنت مبارك: **((التصدي لخطاب الكراهية في القانون الدولي والتشريع الجزائري: التكريس القانوني وسبل الوقاية.))**، مقال منشور فيي المجلة العربية للدراسات الأمنية، العدد السابع والثلاثين، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2021، ص118.

[2] صخر أحمد الخصاونة وسهل علي العتوم: **((دور وسائل التواصل الاجتماعي في نشر خطاب الكراهية من وجهة نظر الصحفيين الأردنيين- دراسة ميدانية-))**، مقال منشور في مجلة الجامعة الإسلامية للدراسات الشرعية والقانونية، المجلد التاسع والعشرون، العدد الأول، الجامعة الإسلامية، غزة، ص 304.

[3] إبراهيم صابر: **((كيف يتفادى الصحافي خطاب الكراهية والتحريض على العنف))**، مقال منشور عبر موقع www.aljazeera.net بتاريخ 26 أغسطس 2020، وأطلع عليه بتاريخ 2022/08/20، على الساعة 13:25.

المطلب الثاني: التعريف بمواقع التواصل الاجتماعي.

شبكات التواصل الاجتماعي أو الشبكات الاجتماعية مصطلح يطلق على مجموعة من المواقع على شبكة الانترنيت ظهرت مع الجيل الثاني للويب، أو ما يعرف باسم ويب 2.0، تتيح التواصل بين الأفراد في بيئة مجتمع افتراضي يجمعهم حسب مجموعات اهتمام أو شبكات انتماء (بلد، جامعة، مدرسة، شركة ...الخ)، كل هذا يتم عن طريق خدمات التواصل المباشر مثل إرسال الرسائل أو الإطلاع على الملفات الشخصية للآخرين، ومعرفة أخبارهم ومعلوماتهم التي يتيحونها للعرض[1]. وتعبر هذه الشبكات وسيلة فعالة للتواصل الاجتماعي في وقتنا الحالي بما تقدمه من خدمات وامتيازات تسمح بالتعرف على أصدقاء جدد عبر العالم وإبرام علاقات معهم، وكذا خاصية إرسال الصور والفيديوهات أو إنشاء ألبومات عبر الصفحات الشخصية، واقتناء منتجات تعرضها الإعلانات التجارية عبر بعض الصفحات كالفيسبوك. وتعرّف وسائل التواصل الاجتماعي على أنّها "مجموعة هويات اجتماعية ينشئها أفراد أو منظمات لديهم روابط نتيجة التفاعل الاجتماعي، ويمثلها هيكل أو شكل ديناميكي لجماعة اجتماعية، وهي تنشأ من أجل توسيع وتفعيل العلاقات المهنية أو علاقات الصداقة، وتتضمن الفيس بوك وتويتر واليوتيوب والمدونات والمنتديات."[2] وتعرّف أيضاً بأنها "شبكات اجتماعية تفاعلية تتيح التواصل لمستخدميها في أي وقت يشاءون، وفي أي مكان من العالم، وعبر شبكة الانترنيت من التواصل المرئي والصوتي وتبادل الصور وغيرها من الإمكانات التي توطد العلاقة الاجتماعية بينهم"[3]

المطلب الثالث: تأثير مواقع التواصل الاجتماعي على نشر التميّز وخطاب الكراهية.

---

[1] محمد أمزيان برغل: **((اتجاهات أساتذة علوم الإعلام والاتصال في الجزائر نحو تقنية النشر الالكتروني، دراسة وصفية تحليلية 2011))**، مذكرة مقدمة لنيل شهادة الماجستير في علوم الإعلام والاتصال، تخصص دراسات الجمهور، جامعة الجزائر 3، الجزائر، 2012،2011، ص88.

[2] صخر أحمد الخصاونة وسهل علي العتوم، (المرجع السابق) ،ص304.

[3] ناصر الرحامنة: **((خطاب الكراهية في شبكة الفيس بوك في الأردن، دراسة مسحية))**، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في الإعلام، قسم الصحافة والإعلام، كلية الإعلام، جامعة الشرق الأوسط ، عمان، الأردن، نيسان 2018، ص 8.

لقد لعبت مواقع التواصل الاجتماعي دوراً كبيراً في نشر الأخبار والمعلومات، وتقريب المسافات، وتوطيد العلاقات بين الأفراد لعقد طويل من الزمن، غير أنّها سرعان ما فتأت تساهم في زرع الفتن وتوسيع فجوة الخلافات لاسيما عند النزاعات والأزمات من خلال ما ينشره البعض من خطاب الكراهية والتمييز والدعوة للعنف عبر العديد من دول العالم. مما دفع بالكثيرين إلى القول "بأن تأثير شبكات التواصل الاجتماعي ومن أهمها فيس بوك وتويتر واليوتيوب ليس محصوراً على التغيير الإيجابي في الجانب الاجتماعي والاقتصادي والسياسي بل بدأ يظهر تأثيرها السلبي شيئاً فشيئاً لاسيما في نشر الثقافات المنحرفة، وبث الكراهية، والطائفية والنزاعات القبلية، وتكفير الناس، وسب الدين وغيرها من الأمور السلبية، ولعلّ أكثر مثال معبّر في هذه النقطة النزاع السني_الشيعي الذي غالباً ما يؤدي لأعمال عنيفة على الواقع"[1]

ذلك أنّ كثافة انتشار واستخدام وسائل التواصل الاجتماعي ساعدت على اكتساب معاني ومعتقدات وتصورات جديدة حول العالم الذي تقدمه، قد تكون مختلفة عن العالم الواقعي، حيث أتاحت وسائل التواصل الاجتماعي تلاقي أصحاب الفكر المتعصب والمتطرفين عبر المسافات وبأسماء وهمية، وسهلت عملية التواصل فيما بينهم وبمبالغ زهيدة، وذلك بهدف الحشد والتجنيد لبث الكراهية تجاه فئات ومجموعات معينة.[2]

لقد أصبحت مواقع التواصل الاجتماعي وسيلة مهمة وفعالة في زرع الفتن عبر خطابات الكراهية والدعوة إلى العنف تفوق في تأثيرها وسرعة انتشارها ذلك الدور الذي لعبته وسائل الإعلام التقليدية منذ سنوات خلت، ذلك أن استحداث وسائط إعلام عبر الانترنيت، وفتح صفحات خاصة بها عبر الفيسبوك سمح بالدعوة إلى الكراهية بصورة أسرع وأكثر انتشاراً، حيث يرى بعض الباحثين أنّ "وسائط الإعلام على الانترنيت تسمح لمن يدعو إلى

[1] خديجة بريك وآية حيدوسي: **((خطاب الكراهية عبر مواقع التواصل الاجتماعي وانعكاساته على الشباب الجزائري_دراسة ميدانية_))**، مقال منشور في مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد السابع، العدد الثاني، أفريل 2022، ص240.

[2] صخر أحمد الخصاونة وسهل علي العتوم، (المرجع السابق) ،ص304.

خطاب الكراهية أو التعبير عن الكراهية عبر شبكات الانترنيت بالوصول السهل إلى جمهور عريض، تخضع إلى تنظيم أقل من وسائط الإعلام التقليدية، وتتيح إخفاء الهوية لمن يريد استغلالها، مع توفير مجالات جديدة لمشاركة الأقليات في النقاش...فالخوف الكامن وعدم اليقين والأمل واليأس يفسر انتشار الغضب عبر الانترنيت أكثر من انتشار الفرح مما يفسر ازدياد خطاب الكراهية والخطابات المضادة في الوسائط الرقمية أكثر من وسائل الإعلام التقليدية التي هي أكثر مهنية وتخضع لمختلف القوانين."[1]

المبحث الثاني: جريمة التمييز وخطاب الكراهية عبر المواقع والحسابات الالكترونية.

لقد تولى المشرع الجزائري تجريم أفعال التمييز وخطاب الكراهية عبر المواقع أو الحسابات الالكترونية (المطلب الأول)، وقرر عقوبات أصلية وأخرى تكميلية تطبق على مرتكبي هذه الجرائم (المطلب الثاني) وقاية منه وحماية للمجتمع من الأضرار التي تلحق به جراء هذا النوع من الجرائم (المطلب الثالث).

المطلب الأول: أركان جريمة التمييز وخطاب الكراهية عبر المواقع والحسابات الالكترونية.

تعتبر جريمة التمييز وخطاب الكراهية عبر المواقع والحسابات الالكترونية جريمة كغيرها من جرائم القانون العام يشترط لقيامها توافر ركن شرعي، مادي ومعنوي على النحو التالي:

أولاً: الركن الشرعي: جرّم المشرع الجزائري أفعال التمييز ونشر خطاب الكراهية ضمن المادة 34 من قانون 20-05 التي تنص على أنّه ((دون الإخلال بالعقوبات الأشد، يعاقب بالحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 5.000.000 دج إلى 10.000.000 دج كل من ينشئ أو يدير أو يشرف على موقع إلكتروني أو حساب

[1] نصر الدين بويحي: **((خطر خطاب الكراهية عبر وسائل الإعلام))**، مقال منشور في مجلة الشرطة، المديرية العامة للأمن الوطني، العدد 149، أكتوبر 2021، ص31.

إلكتروني يخصص لنشر معلومات للترويج لأي برنامج أو أفكار أو أخبار أو رسوم أو صور من شأنها إثارة التمييز والكراهية في المجتمع.)) فيكون بذلك المشرع قد خص أفعال التمييز وخطاب الكراهية عبر الوسائط الالكترونية بنص خاص يجرمه إلى جانب العديد من النصوص الواردة في هذا القانون التي تجرم هذه الأفعال في ظروف وأحوال مختلفة؛ كالتمييز وخطاب الكراهية باستعمال تكنولوجيات الإعلام والاتصال (م31)، والتمييز وخطاب الكراهية عبر الجمعيات والتنظيمات المحلية والوطنية، كواحدة من أشكال وصورة من صور التمييز ونشر خطاب الكراهية وحسناً فعل المشرع، ذلك أن الاكتفاء بنص المادة 30 التي تضمنت المعاقبة على التمييز وخطاب الكراهية بشكل عام قد يؤدي إلى استفحال الظاهرة أكثر فأكثر وإفلات المجرمين من العقاب. كما تعززت سياسة التخصيص بالتشديد؛ حيث شدد في العقوبة المقرر للجريمة في صورتها العادية وعقوبتها الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 60.000 دج إلى 300.000 دج إلى الحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة من 5.000.000 دج إلى 10.000.000 دج، فتغيّر بذلك الوصف القانوني للفعل من جنحة بسيطة إلى جنحة مشددة طالما المشرع رفع في حدي العقوبة الأدنى والأقصى وحافظ على لفظ (الحبس) المقررة للجنح.

ثانياً: الركن المادي. يتمثل الركن المادي لجريمة التمييز وخطاب الكراهية عبر المواقع والحسابات الالكترونية في سلوك إجرامي ونتيجة وعلاقة سببية بين السلوك والنتيجة؛ ويتجسد السلوك الإجرامي حسب المادة 34 أعلاه في:

- أن يقوم الجاني بإنشاء أو إدارة أو الإشراف على موقع أو حساب إلكتروني.
- أن يخصص هذا الموقع أو الحساب الالكتروني لنشر معلومات للترويج لأي برنامج أو أفكار أو أخبار أو رسوم أو صور تثير التمييز والكراهية في المجتمع.

ويشترط لاكتمال البناء القانوني لهذا السلوك تحقق نتيجة معينة بذاتها حددتها المادة 34 وهي إثارة التمييز والكراهية في المجتمع، ذلك أن مجرد إنشاء حساب الكتروني ينشر أخبار أو أفكار أو معلومات عن ثقافة وتقاليد منطقة معينة بغرض الترويج للسياحة أو لنشر سلع تجارية بهدف بيعها لا يشكل سلوكا إجرامياً لهذه الجريمة لانتفاء النتيجة الإجرامية المطلوبة للتجريم وهي إثارة التمييز والكراهية في المجتمع.

ثالثاً: الركن المعنوي: جريمة إنشاء حساب أو موقع الكتروني أو إدارته أو الإشراف عليه بغرض نشر أفكار أو أخبار أو رسومات أو صور لإثارة التمييز والكراهية في المجتمع جريمة عمدية لا يتصور ارتكابها عن طريق الخطأ، لأنّه يصعب إثبات خطأ الجاني بالإهمال أو الرعونة أو عدم الانتباه طالما اشترط المشرع في المادة 34 أن يكون من شأن هذه الصور أو الرسوم المنشورة إثارة التمييز والكراهية في المجتمع، وهو غرض لا يتحقق إلاّ عن طريق القصد.

وبناء عليه يتابع كل من ينشئ عمداً صفحة على موقع فيسبوك بغرض نشر معلومات للترويج لأفكار تعزز الطائفية أو العروشية بغرض إثارة الفتنة وبث الكراهية والدعوة إلى التمييز والتفرقة بين أفراد الوطن الواحد بارتكابه لجريمة التمييز وخطاب الكراهية عبر الوسائط الالكترونية طبقاً للمادة 34 أعلاه. ويستوي في ذلك أن يكون الجاني شخصاً طبيعياً أو مجموعة أشخاص طبيعيين أو شخصاً معنوياً لكون المادة 38 من قانون 20-05 تنص على معاقبة الشخص المعنوي في ارتكاب الجنح المنصوص عليها في هذا القانون.

ويستوي في ذلك أن يكون الجاني قد أكمل تنفيذ السلوك الإجرامي وتحققت النتيجة أو شرع في ذلك؛ بأن يكتشف أمره بصدد التحقيق معه لارتكابه جريمة أخرى. وذلك طبقاً للمادة 39 التي تنص على أنّه (يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القانون بالعقوبات المقررة للجريمة ذاتها.).

المطلب الثاني: العقوبات المقررة لمرتكبي الجريمة.

قرّر المشرع الجزائري عقوبات أصلية تطبق على مرتكب جريمة التمييز وخطاب الكراهية عبر المواقع أو الحسابات الالكترونية ضمن المادة 34 من قانون 20-05، وتولى تحديد عقوبات تكميلية أخرى في نصوص موالية لها، في حين تولت المادة 40 من نفس القانون تحديد الأعذار المعفية والمخففة للعقوبة على النحو التالي:

أولاً: العقوبات الأصلية: قرّرت المادة 34 من قانون 20-05 الواردة أعلاه عقوبة أصلية تطبق على مرتكب جريمة التمييز وخطاب الكراهية عبر الوسائط الالكترونية وهي الحبس من خمس (5) سنوات إلى عشر (10) سنوات وبغرامة مالية من 5.000.000دج إلى 10.000.000 دج، فيكون بذلك المشرع قد جمع بين عقوبتي الحبس والغرامة معاً فلا يجوز للقاضي أن يحكم بإحداهما دون الأخرى، ورفع في حدي العقوبة وأبقى على لفظ العقوبة الحبس للمحافظة على وصف الجنحة كما أشرنا سابقاً، وما يشير الانتباه هو أن المشرع بدأ المادة 34 بعبارة (دون الإخلال بالعقوبات الأشد) بمعنى أنّه في حالة خطاب الكراهية المتضمن الدعوة إلى العنف تطبق عقوبة الحبس إلى سبع (7) سنوات الواردة في المادة 32 من نفس القانون.[1]

ثانياً: العقوبات التكميلية: بالرجوع إلى المادة 37 من قانون 20-05 نجد المشرع الجزائري حدد العقوبات التكميلية المقررة لمرتكبي هذه الجريمة بقوله ((مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة أو أكثر من الجرائم المنصوص عليها في هذا القانون والأموال المتحصلة منها، وإغلاق الموقع الالكتروني أو الحساب الإلكتروني الذي ارتكبت بواسطته الجريمة أو جعل الدخول إليه غير ممكن وإغلاق محل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكه.)) وبناء

[1] تنص المادة 32 من قانون 20-05 على أنّه ((يعاقب على خطاب الكراهية بالحبس من ثلاث (3) سنوات إلى سبع (7) سنوات وبغرامة من 300.000 دج إلى 700.000 دج إذا تضمن الدعوة إلى العنف.))

عليه يمكن لقاضي الموضوع أن يحكم على مرتكب هذه الجريمة، إلى جانب العقوبات الأصلية بعقوبة أو أكثر من العقوبات التكميلية التالية:

1-مصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب الجريمة والأموال المتحصلة منها، كأن يكون الجاني يعمل لحساب أيادي خارجية أو منظمة إرهابية لزرع التفرقة والفتنة في المجتمع والمساس السيادة الوطنية بمقابل مالي.

2-إغلاق الموقع أو الحساب الالكتروني الذي ارتكبت بواسطته الجريمة أو جعل الدخول إليه غير ممكن.

3-إغلاق المحل أو المكان المستغل كمحلات مقدمي خدمات الأنترنيت متى ارتكبت الجريمة فيه بعلم مالكه.

وفي جميع الحالات لابد من الاحتفاظ بحقوق الغير حسن النية؛ بمعنى لا تصادر الأجهزة أو البرامج أو المستخدمة في ارتكاب الجريمة، ولا تغلق المواقع أو الحسابات لا المحلات متى كانت مملوكة لغير الجاني وكان هذا الغير حسن النية لا يعلم بالجريمة المرتكبة ولا صلة له بها، وإن تمّ مصادرة هذه الأجهزة كأدلة إثبات أثناء إجراء التحقيقات وجب على القاضي المختص إرجاعها لأصحابها ضمن إجراءات استرداد الأشياء المحجوزة المعمول بها في قانون الإجراءات الجزائية.

أضف إلى ذلك منح المشرع القاضي الجزائي سلطة الحكم بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات بموجب المادة 41 من قانون 20-05 التي تنص على أنّه (يمكن الجهة القضائية المختصة الحكم على مرتكبي الجرائم المنصوص عليها في هذا القانون بعقوبة أو أكثر من العقوبات التكميلية المنصوص عليها في قانون العقوبات)، حيث يتضمن هذا النص إحالة صريحة إلى المادة 09 وما يليها من قانون العقوبات، ويتعلق الأمر ب: الحجر القانوني، الحرمان من ممارسة الحقوق الوطنية

والمدنية والعائلية، تحديد الإقامة، المنع من الإقامة، المنع المؤقت من ممارسة مهنة أو نشاط، الإقصاء من الصفقات العمومية، الحظر من إصدار الشيكات و/أو استعمال بطاقات الدفع، تعليق أو سحب رخصة السياقة أو إلغاؤها مع المنع من استصدار رخصة جديدة، سحب جواز السفر، نشر أو تعليق حكم أو قرار الإدانة. وطبعاً إلى جانب عقوبتي المصادرة وإغلاق المؤسسة أو المحل المقررتين بموجب المادة 37 أعلاه. وتبقى مسألة تقرير أي من هذه العقوبات للسلطة التقديرية لقاضي الموضوع حسب ملابسات كل قضية على حدى وحسب حالة كل محكوم عليه.

ثالثاً: الأعذار المعفية والمخففة للعقوبة: قررت المادة 40 من قانون 20-05 نوعين من الأعذار القانونية؛ أعذار معفية وأخرى مخففة للعقوبة بقولها (يستفيد من الأعذار المعفية من العقوبة المنصوص عليها في قانون العقوبات، كل من ارتكب أو شارك في جريمة أو أكثر من الجرائم المنصوص عليها في هذا القانون، وقام قبل مباشرة إجراءات المتابعة بإبلاغ السلطات الإدارية أو القضائية عن الجريمة وساعد على معرفة مرتكبيها و/أو القبض عليهم...)

وتضيف الفقرة الثانية من المادة 40 من قانون 20-05 (... تخفض العقوبة إلى النصف بالنسبة لكل شخص ارتكب أو شارك في إحدى الجرائم المنصوص عليها في هذا القانون والذي بعد مباشرة إجراءات المتابعة ساعد في القبض على شخص أو أكثر من الأشخاص الضالعين في ارتكابها و/أو كشف هوية من ساهم في ارتكابها.)

المطلب الثالث: مبررات التجريم.

يعتبر قانون 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية قفزة نوعية عززت المنظومة القانونية في بلادنا، من خلال ما تضمنه من تدابير وقائية وإجراءات عقابية للوقاية من أفعال التمييز وخطاب الكراهية، لذلك فإن قراءة أولية لنصوص هذا القانون توحي

بالطبيعة الوقائية له، في حين أن التعمق في محتواه يعزز التجريم العلاجي له. على النحو التالي:

أولاً: التجريم الوقائي: لقد جرّم المشرع الجزائري أفعال التمييز وخطاب الكراهية عبر المواقع والحسابات الإلكترونية لحماية الكرامة الإنسانية للأفراد، وصون كيان المجتمع ووجوده، وحماية سيادة الدولة وسلطتها على مختلف مؤسساتها الدستورية من الأضرار التي تلحق بها جراء نشر الفتن والدعوة للعنف من خلال شتى صور التمييز وأنواعه، ونشر خطاب الكراهية لاسيما عبر مواقع التواصل الاجتماعي، وقد فسر بعض الباحثين هذا التجريم بالقول أنّ "تصاعد موجة التطرف الإيديولوجي والراديكالية الفكرية ممثلة في انتشار خطاب الكراهية والتحريض على العنف والتمييز عبر شبكات التواصل الاجتماعي في الفترة الأخيرة هو ما شجع الدولة عل إصدار قوانين تجرم هذا. مما يعدّ خطوة إيجابية لردع المخالفين ومرضى النفوس الذين انغرست فيهم ثقافة الحقد والكراهية والانتقام من الآخر، خاصة ان الجزائر خرجت من تجربة مريرة بعد عشرية سوداء أتت على الأخضر واليابس، وكانت ثمرة لخطاب اليمين المتطرف بكل تياراته الايديولوجية، ووجود القابلية لاحتضان هذا الخطاب في عقلية من يدعي ملكية الحقيقة المطلقة"[1]، وقد جاء هذا التجريم على سبيل الوقاية وهذا ما يستشف من عبارة ((يتعلق بالوقاية من التمييز وخطاب الكراهية)) الواردة في تسمية القانون، وكذا مختلف الإجراءات التي تضعها الدولة حسب ما ورد في المادة الخامسة وما يليها من القانون نفسه التي تلزم الدولة وضع إستراتيجية وطنية للوقاية من التمييز وخطاب الكراهية قصد أخلقة الحياة العامة، ونشر ثقافة التسامح والحوار ونبذ العنف من المجتمع. لاسيما الإعلام والتحسيس حول مخاطر التمييز وخطاب الكراهية، وآثار استعمال وسائل تكنولوجيات الإعلام والاتصال في نشرها على غرار موقع التواصل الاجتماعي،

[1] أيوب حيرش: **((الجمهورية الجديدة ودسترة حظر خطاب الكراهية والتمييز))**، مقال منشور في مجلة الحوار بتاريخ 12 ماي 2020، أطلع عليه عبر موقع www.elhiwar.dz بتاريخ 2022/08/20، على الساعة 18:53.

خاصة مع تأزم الوضع الأمني في الجزائر عشية مقتل الشاب جمال بن اسماعيل، هذه الجريمة التي "أعادت خطاب الكراهية إلى الواجهة، ليتصدر بذلك مشهد وسائل التواصل الاجتماعي ويتحول إلى وسيلة خطيرة في أيدي أشخاص يسعون من خلالها إلى ترويج خطاب الكراهية والتفرقة بين أبناء الشعب الواحد رغم صراحة القانون... حيث انتشرت الفيديوهات والمناشير التحريضية على الكراهية والتفرقة عبر مختلف وسائل التواصل الاجتماعي، هذه الأخيرة تحولت إلى ساحة لتبادل السب والشتم والتحريض على الفرقة والكراهية ضد جهة معينة أو أشخاص معينين تحت ذريعة حرية إبداء الرأي، متناسين أن حرية الأشخاص تنتهي عندما تبدأ حرية الآخرين"[1].

إنّ سياسة الوقاية تعتبر واحدة من السياسات الحديثة التي اتبعها المشرع الجزائري مؤخراً، ذلك "أن العقوبات الجزائية وحدها ستكون عاجزة عن التصدي لجميع أشكال التمييز وخطاب الكراهية لذا ينبغي البدء بتدابير استباقية التي ستوفر إطار أكثر شمولية لمحاربة التمييز وخطاب الكراهية، وهو ما أقدم عليه المشرع الجزائري من خلال أحكام القانون رقم 20-05"[2]

ثانياً: التجريم العلاجي: "يقصد بالحماية العلاجية تلك الإجراءات التي من شأنها جبر الضرر عن فعل مجرم، وهي إجراءات لاحقة على ارتكاب سلوك المجرم على عكس الحماية الوقائية التي تكون سابقة له."[3] وبالرجوع إلى قانون 20-05 نجد المشرع الجزائري لم يكتف

---

[1] أسامة سبع: **((جريمة قتل جمال تعيد خطاب الكراهية إلى الواجهة ووعي الجزائريين جنب الفتنة))**، مقال منشور في جريدة المحور اليومس بتاريخ 16 أغسطس 2021، متاح عبر موقع : www.elmihwar.dz أطلع عليه بتاريخ 2022/08/20، على الساعة 19:04.

[2] حويذق عثمان وسلخ محمد لمين والذهبي خليفة: **((الأثر الوقائي لتجريم التمييز وخطاب الكراهية في التشريع الجزائري))**، مقال منشور في مداخلة مقدمة للمشاركة في الملتقى الدولي الخامس عشر بعنوان جرائم التمييز ... وخطاب الكراهية _الواقع والتحديات_ المنعقد يومي 29 و30 نوفمبر 2021 بكلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، الجزائر، ص 65.

[3] لعشيبي مراد وكعلة نجاح وعينة قيس: **((الآليات القانونية للحماية من جرائم التمييز وخطاب الكراهية))**، مداخلة مقدمة للمشاركة في الملتقى الدولي الخامس عشر بعنوان جرائم التمييز ... وخطاب الكراهية _الواقع والتحديات_ المنعقد يومي 29 و30 نوفمبر 2021 بكلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، الجزائر، ص 318.

بتجريم أفعال التمييز وخطاب الكراهية عبر المواقع والحسابات الالكترونية فحسب، بل راح يقرر حماية خاصة بضحايا التمييز وخطاب الكراهية على سبيل الحماية العلاجية لما يلحق هؤلاء من أضرار جراء هذه الأفعال، تتمثل في إجراءات التكفل الصحي والنفسي والاجتماعي بما يكفل أمن الضحايا وسلامتهم وحرمتهم الجسدية والنفسية وكرامتهم[1]، تسيير لجوئهم إلى القضاء[2]، استفادتهم من المساعدة القضائية بقوة القانون[3]، استفادتهم من الإجراءات الخاصة بحماية الضحايا والشهود المقررة في قانون الإجراءات الجزائية[4]، وكذا اللجوء إلى القضاء ألاستعجالي لتقرير تدبير تحفظي لوضع حد لتعدي[5].

وفي نفس الإطار وفي المجال الإجرائي تسعى الدولة جاهدة للكشف عن المجرمين ومتابعتهم جزائياً لما تملكه النيابة العامة من سلطة تحريك الدعوى العمومية ومباشرتها من تلقاء نفسها، "وفي نفس السياق تواصل المصالح المختصة للأمن الوطني بالتنسيق مع المصالح العملياتية في الضرب بيد من حديد لمواجهة ارتفاع خطاب الكراهية وحملات التحريض عبر منصات التواصل الاجتماعي، من خلال رصد وإيقاف أصحاب المناشير والفيديوهات التحريضية التي تمجد لخطاب الكراهية والعنف والعداوة، وتهدف إلى زرع الفتن والضغينة؛ حيث تمّ إفشال العديد من المخططات والمؤامرات المنفذة عبر الفضاء السيبراني لصالح أجندات خارجية تستهدف إثارة الفوضى والإخلال بالنظام العام والتشكيك في الثوابت الوطنية." [6]

خاتمة.

---

[1] المادة 16 من قانون 20-05.

[2] المادة 17 من قانون 20-05.

[3] المادة 18 من قانون 20-05.

[4] المادة 19 من قانون 20-05.

[5] المادة 20 من قانون 20-05.

[6] كريمة نعمان: **((الأمن السيبراني يضرب بيد من حديد المؤامرات الخبيثة للشبكات الإجرامية والتحريضية))**، مقال منشور في مجلة الشرطة، المديرية العامة للأمن الوطني، العدد 149، أكتوبر 2021، ص34.

لقد شكل قانون تجريم التمييز وخطاب الكراهية عبر المواقع والحسابات الالكترونية بموجب قانون 20-05 قفزة نوعية عززت المنظومة القانونية في الجزائر، وساهمت في حماية الكرامة الإنسانية للأفراد، وإطفاء نار الفتنة والضغينة التي سعى البعض من ضعاف النفوس إلى نشرها في الفترة الحساسة التي مرت بها بلادنا مؤخراً. لاسيما لو تدعمت هذه النصوص القانونية بالتطبيق الفعلي لها واقعياً، ومع ذلك لتعزيز هذه المبادرة لابد من تضافر الجهود بين مختلف الجهات والمؤسسات الدولية والجمعيات والمجتمع المدني، لذلك نقترح بعض التوصيات التالية:

- تفعيل دور المؤسسات التربوية والمساجد ومختلف الجهات الوصية في بث رسائل السلم والتعايش وروح التعاون والتسامح بين أفراد المجتمع.
- عقد ندوات وملتقيات وطنية ودولية لمناقشة مواضيع التمييز وخطاب الكراهية لاسيما عبر المواقع الالكترونية وإيجاد مواطن الفصل والتمييز بين ما يعتبر حرية تعبير وبين ما يعتبر خطاب كراهية.
- ضرورة تشديد الرقابة على مواقع التواصل الاجتماعي وما تحمله من أفكار هدامة تمس بالسلم و الأمن الوطني من خلال نشر خطابات الكراهية والتمييز بأسلوب هزلي ساخر.

استمارة المشاركة

الاسم واللقب: حطاب كمال

الرتبة العلمية: أستاذ محاضر ب

الهيئة المستخدمة: كلية الحقوق والعلوم السياسية، 19 مارس 1962، جامعة جيلالي ليابس سيدي بلعباس.

رقم الهاتف:92 89 61 94 07

البريد الالكتروني: kamalhat5@gmail.com

محور المداخلة: المحور الثاني: أثر استخدام التكنولوجيا الحديثة على أحكام التجريم

2/ المواجهة التشريعية للجرائم المستحدثة بالتطور التكنولوجي

عنوان المداخلة: الحماية الجزائية للمعطيات ذات الطابع الشخصي على ضوء القانون 07/18

ملخص:

يولي العالم اليوم أهمية بالغة لموضوع الحق في الخصوصية، لذلك تحمي التشريعات المختلفة هذا الحق المكرس دستوريا في معظم الدول، وتعاقب بعقوبات رادعة كل من ينتهك حرمة هذا الحق بأي شكل من الأشكال.

وزادت أهمية هذا الموضوع مع التطور الهائل للمعلوماتية، وما صاحب ذلك من تهديد الجرائم الإلكترونية لحرمة الحياة الخاصة، وخاصة المعطيات ذات الطابع الشخصي، فمن الطبيعي أن يتم أثناء إجراء المعاملات الإلكترونية تبادل هذه المعطيات، كالمعطيات المتعلقة بالموظفين والقائمين على الإدارة، ومستعملي الانترنت، وهذا الأمر يستوجب توفير حماية قانونية لازمة وكافية لهم خصوصا عند القيام بالتعاقد الالكتروني، ومن أهمها حماية المتعامل من الاطلاع على معطياته الشخصية التي يدلي بها بصورة مباشرة أو غير مباشرة قبل أو أثناء عملية إبرام العقد، أو عن طريق تتبع استخدامه للأنترنت.

الكلمات المفتاحية: المعطيات الشخصية، المعاملات الإلكترونية، الحماية الجزائية، المبادئ الأساسية السبعة لحماية المعطيات ذات الطابع الشخصي (مبدأ الشفافية، مبدأ الأمان والسرية، مبدأ التناسب...).

Penal protection of personal data in the light of Law 18/07

Abstract

The world today attaches great importance to the subject of the right to privacy, so various legislations protect this right, which is constitutionally enshrined in most countries, and punish with deterrent penalties anyone who violates the sanctity of this right in any way.

The importance of this subject has increased with the tremendous development of informatics, and the concomitant threat of cybercrime to the inviolability of private life, especially data of a personal nature.

It is normal that during the conduct of electronic transactions these data are exchanged, such as data related to employees, administrators and Internet users, and this requires the provision of necessary and adequate legal protection for them, especially when carrying out electronic contracting, the most important of which is to protect the customer from access to his personal data that he gives directly or indirectly before or During the process of concluding a contract, or by tracking his use of the Internet.

Keywords: Personal data, electronic transactions, penal protection, the seven basic principles for the protection of data of a personal nature (the principle of transparency, the principle of security and confidentiality, the principle of proportionality...).

مقدمة

من المواضيع الأكثر إثارة للجدل موضوع الحق في الخصوصية، الذي اعترفت به الدساتير والقوانين الوطنية بالإضافة إلى المواثيق الدولية، وهو ما يعرف أيضا بحرمة الحياة الخاصة، وهي فكرة عصرية، ظهرت حديثا وانتقلت من الجانب الأخلاقي إلى الجانب القانوني الذي عمل على صونها وحمايتها، ولقد تصدى الكثير من الفقهاء لتعريفها ووضع أطرها، إلا أنهم لم يتفقوا على تعريف جامع مانع لها، وإن اتفقوا حول عناصرها، وأنها مرتبطة بالشخص، وكل ماله صلة وثيقة بشخصه كمحل إقامته أو اسمه أو عائلته، وكذا بروتوكول الانترنت الخاص به (IP) وما إلى ذلك.[1]

هذه الخصوصية قد تتعرض للاعتداء خاصة فيما يتعلق بالمعطيات عند التعامل في المعاملات الإلكترونية المختلفة، لأن طبيعة هذه المعاملات تقتضي أن يدلي مستخدم الانترنت ببعض المعلومات الشخصية لإتمام المعاملة؛ وتقوم هنا أيضا مسؤولية مقدمي الخدمة الوسيطة عبر الانترنت في عدم التعدي على الحق في الخصوصية، بل وحمايتها من اعتداء الغير عليها.

كما أن التطور التكنولوجي من شأنه أن يعرض الحياة الخاصة بما فيها المعطيات الشخصية للخطر، خاصة عند استعمال الكعك المحلى"cookies" أو الرسائل المزعجة "spams" أو عند القيام بعملية تسويق المعطيات"commercialisation des données". [2]

بناء على ما تقدم يتم معالجة هذا الموضوع من خلال محاولة الإجابة عن التساؤلات التالية: ما المقصود بالمعطيات ذات الطابع الشخصي؟ ما هي أهم المبادئ الأساسية التي وضعها التشريع ونادى بها الفقه وكرسها القضاء حماية لهذه المعطيات وصونا لها؟ كيف عالج المشرع الجزائري موضوع حماية المعطيات الشخصية في القانون 07/18؟ وإلى أي مدى وفق في تحقيق الحماية الجزائية للمعطيات ذات الطابع الشخصي؟

يحاول البحث الإجابة عن هذه التساؤلات وغيرها عن طريق تحليل نصوص القانون 07/18، وتم تقسيم البحث إلى أربعة محاور، كالتالي:

- المحور الأول: مفهوم ومصادر حماية المعطيات ذات الطابع الشخصي.

- المحور الثاني: المبادئ والحقوق الأساسية المتعلقة بحماية المعطيات ذات الطابع الشخصي.

– المحور الثالث: الجرائم الواقعة على المعطيات ذات الطابع الشخصي.

– المحور الرابع: العقوبات المقررة لقمع الجرائم الواقعة على المعطيات ذات الطابع الشخصي.

المحور الأول: مفهوم ومصادر حماية المعطيات ذات الطابع الشخصي:

يعنى هذا المحور بمحاولة إعطاء مفهوم لمصطلح المعطيات ذات الطابع الشخصي، ثم ذكر أهم المصادر القانونية التي حمت هذه المعطيات قبل إصدار القانون 07/18.[3]

أولا: مفهوم المعطيات ذات الطابع الشخصي:

المعطيات ذات الطابع الشخصي هي حسب بعض الفقه الفرنسي، تلك المعطيات المتعلقة بالحياة الخاصة بالفرد كتلك المتعلقة بحالته الصحية والمالية والمهنية والوظيفية والعائلية، والعاطفية، وهي تلك المعطيات التي يحميها المشرع بمقتضى المادة التاسعة من القانون المدني الفرنسي، أي تلك المتصلة بحرمة الحياة الخاصة، ويذهب البعض أبعد من ذلك في تحديد مفهوم المعطيات ذات الطابع الشخصي بأنها أيضا كل ما يسمح برسم صورة لاتجاهات الشخص وميولاته السياسية والدينية وتعاملاته المالية والبنكية، وجنسيته وهواياته.[4]

فيما يتعلق بالأنترنت، وخاصة مواقع التواصل الاجتماعي، تبدو الأمور معقدة بعض الشيء، غير أن هنالك مبدأين ينبغي احترامهما: الحق في الهوية الرقمية (le droit à l'identité numérique)، والحق في النسيان الرقمي (le droit à l'oubli numérique)؛[5] فالمبدأ الأول يعني مجموعة المعطيات التي يضعها مستعمل الانترنت، على مواقع الانترنت، ويسمح له هذا الحق، بتسيير هذه المعطيات وضمان سريتها إذا رغب في ذلك، ويثور السؤال هنا: هل يعتبر غصب الهوية الرقمية جريمة يعاقب عليها القانون؟ لم يكن يعتبر هذا الفعل جريمة في حد ذاتها، بل "جنحة تحضيرية" لارتكاب جنح أخرى، بمعنى أن غصب الهوية الرقمية لم يكن معاقبا عليه إلا إذا ارتكب المغتصب جرائم أخرى، بيد أن الفقه الفرنسي نادى بأن يكون فعل الغصب جنحة مستقلة، كما هو الأمر بالنسبة لمجرد الولوج غير المشروع.[6] وهذا ما تم فعلا بفضل قانون مارس 2011 المسمى قانون التوجيه والبرمجة من أجل تحسين الأمن الداخلي (LOPPSI)[7]والذي أضاف نص م226-4-1 إلى قانون العقوبات الفرنسي. [8]

أما المبدأ الثاني فيرمي إلى محو المعطيات المتعلقة بالشخص والموجودة على مواقع الانترنت إذا رغب في ذلك، وأيضا ضرورة قيام مسيري مواقع الانترنت بمحو هذه المعطيات بعد مرور مدة زمنية معينة، وهما يشكلان الحق في محو الآثار، لذا وضعت مؤسسة (Google) في الفاتح أبريل 2012 قواعد جديدة للسرية لفائدة مستعمليها، تتعهد باحترامها، كما تعهدت بالتعاون مع السلطات المحلية المكلفة بإدارة المعطيات، وهو ما يعني بوضوح بأنها لا تنوي الارتباط بقوانين الدول التي تبث فيها المعطيات، ولكن فقط بقانون الو م أ.[9]

عموما إن موضوع الحياة الخاصة في علاقته بالانترنت يدور حول ستة محاور رئيسة هي: المعلومة، الرضا، التعديل أو التغيير، التبرير، الاحتفاظ ونقل المعطيات.[10]

ومن الفقه من صنف هذه الجرائم إلى أربع فئات، وهي الجرائم الماسة بالحق في الحياة الشخصية من الناحية الموضوعية، الجرائم التي تشكل خرقا للقواعد الإجرائية المتعلقة بتنظيم المعالجة الآلية للمعطيات ذات الطابع الشخصي، الجرائم الماسة بحق الشخص في الإحاطة علما بالمعطيات المتعلقة به، وأخيرا إهمال الإجراءات الأمنية، أو التقاعس عن اتخاذ التدابير الفنية اللازمة والكفيلة بتحقيق أمن المعطيات ذات الطابع الشخصي، كما أورد الفقيه (Ulrich Siber) صور انتهاك الخصوصية المتصلة بالمعالجة الآلية للمعطيات ذات الطابع الشخصي اعتمادا على نوعية الأساليب الإجرامية المستخدمة.[11]

وقد ساهم القضاء الفرنسي في تحديد مفهوم المعطيات ذات الطابع الشخصي التي يوفر لها القانون الحماية ومن ذلك رقم الهاتف، والمعلومات الخاصة بجنسية سكان عقار من العقارات والمعطيات الخاصة بالأفكار الفلسفية للمشتركين ببعض الدوريات، ولقد أدين أحد الأشخاص لقيامه بوضع صور عارية لخليلته السابقة على موقعه للأنترنت.[12]

يتطلب القانون الفرنسي لسنة 1978 المسمى "المعلوماتية والحرية" عند معالجة أي معطيات شخصية من قبل أشخاص القانون الخاص إخطار اللجنة القومية للمعلوماتية والحريات، ويتطلب الحصول على تصريح مسبق إذا كان من يقوم بجمع المعلومات أحد أشخاص القانون العام أو أحد أشخاص القانون الخاص العاملين لحساب الدولة.[13]

وإذا رغب القائمون على موقع من مواقع الانترنت التعامل مع المعطيات الشخصية تعين عليهم إخطار اللجنة الوطنية للمعلوماتية والحريات(CNIL)[14] مسبقا، وإخطار المواطنين بالمخاطر المترتبة عن وضع معطياتهم الشخصية بمواقع الانترنت، وحقهم في الاعتراض في أي وقت على نشر هذه المعطيات، وحقهم أيضا في الاعتراض والتصحيح ومحو المعطيات لأسباب مشروعة.

ويتعين أيضا عند الرغبة في استخدام نظام "الكعك المحلى cookies" إخطار اللجنة، لأنه يمكن عن طريق هذا النظام معرفة معلومات عن المستهلك تتعلق بالمواقع التي تصفحها والأشياء التي بحث عنها والوقت المفضل لديه للإبحار في الانترنت، وميولاته الشخصية، وبالتالي يمكن معالجة هذه المعلومات ووضعها على قاعدة للبيانات لاستخدامها.

كما اعتبر كذلك من قبيل معالجة المعطيات الشخصية عملية تتبع الأثر التي يقوم بها مزود الخدمة، والتي يتعرف من خلالها على المواقع التي تصفحها العميل ووقت وتاريخ التصفح، ويقوم بتخزين هذه المعطيات لمدة من الزمن وتحديد شخصية العميل، ونظرت اللجنة موضوع "الكعك المحلى" الذي يوضع على الاسطوانة الصلبة لجهاز الكمبيوتر الخاص بالعميل دون علمه، فيسمح بمعرفة شخصيته وهواياته، وأوجبت ضرورة إخطار المستخدمين بوضع "الكعك المحلى" على أجهزتهم بما يسمح لهم بالاعتراض على ذلك.[15]

عرف المشرع الجزائري في الفقرة الأولى من نص م3 من القانون 07/18 سالف الذكر المعطيات ذات الطابع الشخصي بأنها: "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه، والمشار إليه في هذا القانون بالشخص المعني، بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".

ما يلاحظ على هذا التعريف أنه جاء واسعا، فمن جهة ربط تعريف المعطيات بالمعلومة مهما كانت دعامتها سواء ورقية أو إلكترونية أو غير ذلك، ومن جهة ثانية ربطها أيضا بالشخص الطبيعي سواء أكان معرفا أم قابلا للتعرف عليه، ومن جهة ثالثة استعمل لفظ لا سيما ليفهم أن العناصر الخاصة بالمعلومة محل المعالجة واردة على سبيل المثال وليس على سبيل الحصر.

التعريف الوارد في نص م1/3 من القانون 07/18 يكاد يتطابق مع التعريف الذي أورده المشرع الفرنسي في م2 من 78-17 لسنة 1978 سالف الذكر.

ثانيا: مصادر الحماية الجزائية للمعطيات ذات الطابع الشخصي:

قبل صدور القانون 07/18 ثار جدل فقهي حول القواعد القانونية الواجبة التطبيق، على الاعتداءات الواقعة على المعطيات ذات الطابع الشخصي، ومما لا شك فيه أنه يجوز إعمال نصوص القسم السابع مكرر من ق ع المتعلق بحماية نظم المعالجة الآلية للمعطيات، وهذه القواعد القانونية وخاصة المواد 394 مكرر، و394 مكرر1، و394 مكرر2 توفر حماية غير مباشرة للمعطيات ذات الطابع الشخصي، ولكنها لا تغطي جميع الحالات التي يمكن تصورها.

ورأى البعض أنه يجوز إعمال نص م301 من ق ع، لتوفير حماية جزائية للمعطيات الشخصية، إلا أن جانبا من الفقه رأى أن محل الجريمتين مختلف، فجريمة إفشاء الأسرار تتطلب أن تكون المعلومات سرية، كما أن هنالك اختلافات أخرى بين الجريمتين. غير أن هذا لا يمنع من إعمال نص هذه المادة لتغطية بعض الحالات.

أضاف المشرع الجزائري بموجب القانون رقم 06-23 المؤرخ في 2006/12/20،[16] إلى قانون العقوبات المواد 303 مكرر إلى 303 مكرر3، لحماية الحياة الخاصة للأفراد،[17] بحيث جرمت م303 مكرر وعاقبت على أفعال المساس بحرمة الحياة الخاصة، بأي فعل من الأفعال التي ذكرتها المادة، وهي التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، أو صورة شخص ، في مكان خاص بغير إذن صاحبها أو رضاه، وبأية تقنية كانت، فلا تهم الوسيلة المستعملة في ارتكاب النشاط الإجرامي لهذه الجريمة.

كما أن م303 مكرر1، عاقبت وجرمت على التعامل بالأشياء المتحصل عليها من الجرائم المذكورة في المادة السابقة بالعقوبة ذاتها المقررة في م303 مكرر.

السؤال الذي أثير: هل يجوز إعمال نص هاتين المادتين لحماية المعطيات الشخصية في مجال المعلوماتية؟

إن هاتين المادتين لم توضعا أصلا لحماية المعطيات الشخصية في سواء من قبل المشرع الفرنسي أو الجزائري، ولذلك يتبادر في الذهن للوهلة الأولى أنه من غير المتصور إعمالهما، ولكن رغم ذلك هما توفران حماية غير مباشرة للحياة الشخصية لمستعمل الانترنت في الفرض الذي يتتبع أحدهم هذا المستعمل عبر الانترنت ويقوم بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، أو صورة الشخص عن بعد (الانترنت) عند اتصاله بالتاجر عبر هذه الوسيلة.

أمام التطورات السريعة في المجال التكنولوجي، أصدر المشرع الجزائري سنة 2018 القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وقد حوى هذا القانون 76 مادة قانونية، وقد بين المشرع في نص المادة 3 من هذا القانون المقصود من بعض المفاهيم الأساسية وهي: المعطيات ذات الطابع الشخصي، الشخص المعني، معالجة المعطيات ذات الطابع الشخصي، موافقة الشخص المعني، المعالجة الآلية، المعطيات الحساسة، المعطيات الجينية، المعطيات في مجال الصحة، الملف، الاتصال الالكتروني، المسؤول عن المعالجة، المعالج من الباطن، الغير، المرسل إليه، التنازل أو الإيصال، الربط البيني للمعطيات، السلطة الوطنية، مقدم الخدمات، الاستكشاف المباشر، وغلق المعطيات.

تناول المشرع الفرنسي في "قانون المعلوماتية والحرية" موضوع الحماية الجزائية للمعطيات ذات الطابع الشخصي، والذي أدرجت مواده في قانون العقوبات، وقد قصر المشرع الفرنسي نطاق حماية المعطيات على الأشخاص الطبيعية دون المعنوية،[18] ولا يشاطره في ذلك تشريعات أوربية أخرى كالنرويج والنمسا وايرلندا ولوكسمبورغ والدانمرك.[19]

أكدت CNIL على أن القواعد الواردة بقانون 1978 تنطبق على الانترنت.[20]

في مصر اقتبس المشرع المصري لفظا ومضمونا أحكام النصوص التي تكفل حماية حرمة الحياة الخاصة من قانون العقوبات الفرنسي القديم (المواد 368-372، التي تم تضمينها قانون العقوبات الفرنسي بمقتضى القانون الصادر في 17 جويلية 1970)، من خلال م309 مكرر وم309 مكرراً بمقتضى القانون رقم 37 لسنة 1972، إلا أن هذه النصوص توفر الحماية الجزائية لبعض صور الحياة الخاصة فقط (الأحاديث والصور) من أفعال معينة كالتسجيل والنشر والتصوير والتعرض لها، ولكنها لا توفر الحماية لقواعد البيانات من النسخ والاستخدام والاستغلال.[21]

وأضاف المشرع المصري مادتين جديدتين هما م21 وم22 في القانون رقم 96 لسنة 1996 المتعلق بتنظيم سلطة الصحافة، وهما تحميان الحياة الخاصة للمواطنين من تجاوزات الصحفيين.

كما أن قانون الإحصاء رقم 28 لسنة 1982 يحمي قواعد البيانات الخاصة بالتعداد والإحصاء.

قام المشرع المصري حديثا بإصدار القانون رقم 151 لسنة 2020 المتعلق بحماية البيانات الشخصية[22] وقد حوى 49 مادة، وهذا القانون قريب من القانون 18-07 فيما يخص الحماية الجزائية المقررة، ولكن الملاحظ أن المشرع المصري قد غلظ من عقوبة الغرامة، فهي لا تقل في معظم الجرائم عن 200.000 جنيه (ما يعادل 2.000.000 دج) وقد تصل في حدها الأقصى إلى 5 ملايين جنيه أي حوالي 50 مليون دج، من ذلك ما جاء في نص م45 من هذا القانون التي تعاقب بالغرامة التي لا تقل عن نصف مليون جنيه ولا تزيد عن 5 ملايين جنيه من يخالف أحكام التصاريح والتراخيص والاعتمادات المنصوص عليها قانونا.

الملاحظ أيضا أن هذا القانون أعطى إمكانية إجراء الصلح مع المجني عليه في أي مرحلة كانت عليها الدعوى العمومية، ولكن قبل صيرورة الحكم باتا، كما يجوز إجراء التصالح مع المركز إذا تعلق الأمر ببعض الجنح. ويترتب على ذلك انقضاء الدعوى العمومية (م49).

المحور الثاني: المبادئ والحقوق الأساسية المتعلقة بحماية المعطيات ذات الطابع الشخصي:

يتم التطرق أولا إلى أهم المبادئ الأساسية المتعلقة بالمعطيات ذات الطابع الشخصي ثم إلى أهم الحقوق المرتبطة بهذه المعطيات.

أولا: المبادئ الأساسية المتعلقة بحماية المعطيات ذات الطابع الشخصي:

اجتهد الفقه والقضاء في وضع بعض المبادئ الأساسية الكفيلة بصون وحماية المعطيات ذات الطابع الشخصي خاصة إذا تعلق الأمر بمجال المعلوماتية، كما أن المنظمات الدولية والإقليمية كالأمم المتحدة[23] والاتحاد الأوربي، ومنظمة التعاون الاقتصادي والتنمية ساهمت بشكل كبير في بلورة هذه المبادئ، ولقد تبنت الكثير من التشريعات هذه المبادئ، وكرستها كنصوص قانونية ضمن منظومتها التشريعية، وأهم هذه المبادئ ما يلي:[24]

1- مبدأ الغاية: (Principe de finalité)

إن المعطيات ذات الطابع الشخصي لا يجوز استقبالها ومعالجتها إلا من أجل استعمالات محددة سلفا ومشروعة، تتعلق بمهام الجهة المخولة قانونا بذلك، وأي استعمال لغاية أخرى غير المنصوص عليها قانونا يعرض صاحبه للمساءلة القانونية والعقاب الجزائي.

يجب أن تكون الغاية محددة، شرعية وصريحة، ومتوافقة مع نشاط الشخص المهني أو الاجتماعي، كما ينبغي أن تكون واضحة ومفهومة.

يتيح هذا المبدأ تحديد فترة الاحتفاظ بالمعطيات في الملف على ضوء الأهداف المرجوة، وعلى سبيل المثال عندما يغادر عضو ما جمعية ما ينبغي حذف معطياته.[25]

2- مبدأ التناسب (Principe de proportionnalité)

يقضي هذا المبدأ بأنه فقط المعلومات الضرورية والهامة هي الوحيدة التي يجوز تسجيلها وحفظها لاستعمالها من أجل الغاية التي شرعها القانون.

3-مبدأ الصلة (Principe de pertinence des données)

المعلومات المخزنة والمعالجة ينبغي أن تكون بالقدر اللازم فقط الذي يتطلبه القانون، فلا يجوز التوسع في معلومات إضافية، كما يجب أن تكون المعلومات ذات علاقة وثيقة بالموضوع.

4- مبدأ تحديد مدة الاحتفاظ بالبيانات(Principe de durée limitée de conservation des données)

هذا المبدأ يعرف أيضا بمبدأ الحق بالدخول في طي النسيان، ومؤداه أن المعطيات ذات الطابع الشخصي لا يجوز تخزينها لمدة غير محددة، بل يجب تحديد المدة اللازمة لتخزين هذه البيانات، حسب موضوع المعطيات، فإذا انقضت المدة القانونية وجب وضع هده المعطيات على دعامة مميزة وإيداعها بمركز الأرشيف.

5- مبدأ الأمان والسرية (Le principe de sécurité et de confidentialité)

المسؤول على معالجة المعطيات ذات الطابع الشخصي يقع عليه واجب توفير الأمان والسرية لها، إذ يجب عليه أخذ التدابير الضرورية لتوفير الأمن والتأكد من سرية المعطيات وعدم نشرها أو تسريبها للغير، وعلى هذا الأساس فإن المعطيات المعالجة والمخزنة في ملفات رقمية لا يجوز الدخول إليها، ومن باب أولى لا يجوز الاطلاع عليها إلا من قبل الأشخاص المؤهلين قانونا لذلك بسبب وظائفهم، كما يتوجب على المسؤول على معالجة المعطيات أخذ جميع التدابير اللازمة لمنع حدوث أي تغيير أو حذف أو تشويه للمعطيات المخزنة، وكذلك لمنع الدخول غير المشروع للغير إلى نظام المعالجة الآلية للمعطيات ذات الطابع الشخصي، وإذا تعامل مع مزود خدمة خارجي توجب عليه أخذ جميع الضمانات العقدية الكفيلة بحماية المعطيات المعالجة آليا، وعلى المسؤول أيضا تكييف التدابير التقنية الحمائية مع طبيعة المعطيات المعالجة وكذلك مختلف الأخطار المحدقة بها.

6-مبدأ الشفافية (Le principe de transparence)

مؤدى هذا المبدأ أن يمنح القانون للأشخاص الذين تم معالجة وتخزين بعض المعطيات الشخصية المتعلقة بهم المعلومات الأساسية حول هذه المعطيات، ويضمن لهم إمكانية المراقبة الشخصية لها، ويتوجب على المسؤول على معالجة المعطيات الشخصية تنبيه الأشخاص بأن معطياتهم قد خزنت، وفي حالة نقل بعض هذه المعطيات للغير وجب عليه إخبارهم بذلك كي يكونوا على بينة من أمرهم.

7- مبدأ احترام حقوق الأشخاص (le Principe du respect du droit des personnes)

ينبغي احترام حقوق الأشخاص الذين تكون معطياتهم الشخصية محلا للمعالجة الآلية والتخزين، ويتجلى ذلك عن طريق إعلامهم بأن معطياتهم محل تخزين، والغاية من وراء ذلك، وبالطابع الجوازي أو الإلزامي لعملية التخزين، بمسار هذه المعطيات، وبالحقوق التي يخولها القانون لهم في مثل هذه الحالات.

كما يجوز للأشخاص أن يدخلوا إلى المعطيات التي تخصهم ويقوموا بتصحيح الأخطاء أو حذف المعلومات غير الصحيحة، وهو ما يعرف ب:"حق الدخول" و"حق التصحيح"، كما يجوز لأي شخص الاعتراض على أن تكون معطياته الشخصية محل تخزين، إلا إذا كان هذا التخزين إلزاميا، وهو ما يعرف ب:"حق الاعتراض".

ثانيا: الحقوق المرتبطة بالمعطيات ذات الطابع الشخصي:

تطرق المشرع الجزائري في الباب الرابع من القانون 18-07 السالف ذكره إلى حقوق الشخص المعني، وقد حوى هذا الباب خمسة فصول، تناول كل فصل حقا من الحقوق، فالحق في الإعلام تناوله المشرع تحت الفصل الأول، وتطرقت إليه المادتان 32 و33، أما الفصل الثاني فتناول موضوع الحق في الولوج (م34)، والفصل الثالث موضوعه الحق في التصحيح (م35)، والفصل الرابع موضوعه الحق في الاعتراض (م36) أما الفصل الخامس والأخير فتناول منع الاستكشاف المباشر (م37).

1 -الحق في الإعلام:

يعتبر الحق في الإعلام من أهم الحقوق التي ينبغي أن يتمتع بها الشخص المعني، لأنه يعتبر قرينة عن الرضا، كما أن الشخص لا يمكنه ممارسة حقوقه في الاعتراض والتصحيح إذا لم يكن على علم مسبق بأن معطياته محل معالجة.

ويجب أن يتم إعلام الشخص المعني في الوقت المناسب وبالطرق الملائمة، عن طريق البريد الالكتروني أو الرسائل الالكترونية القصيرة وغيرها، وحسب م32 من القانون 07/18 فإن المسؤول عن المعالجة ينبغي عليه الاتصال بكل شخص يراد تجميع معطياته الشخصية، وإعلامه المسبق والصريح وبشكل لا لبس فيه بهوية المسؤول عن المعالجة وأغراضها، وكل المعلومات المفيدة خصوصا المرسل إليه ومدى إلزامية الرد والآثار المترتبة عن ذلك وغيرها، كما يجب على المسؤول قبل تسجيل المعطيات أو إرسالها للغير تزويده بالمعلومات المشار إليها آنفا إذا لم يكن على علم مسبق بها، والأمر ذاته إذا تعلق الأمر بجمع المعلومات في شبكات مفتوحة.

المادة 33 من القانون 07/18 سالف الذكر نصت على الحالات التي لا يجب فيها على المسؤول على المعالجة إعلام الشخص المعني.[26]

2 -الحق في الولوج:

تطرقت إلى هذا الحق م34 من القانون 07/18 سالف الذكر، ويقتصر هذا الحق في مكنة الشخص المعني في الوصول إلى معطياته، ولا يخول له الحق في الاطلاع على معطيات غيره، وتمكن هذه المادة الشخص من التعرف على مسار معطياته الشخصية وكل المعلومات المرتبطة بها حول مصدرها والأشخاص المرسل إليهم هذه المعطيات وغير ذلك.

كما تمكن هذه المادة الغير من إرسال طلباتهم للولوج إلى المعطيات المتعلقة بالشخص، ويقع على عاتق المسؤول عن المعالجة تقدير ما إن كانت طلباتهم مشروعة أم تعسفية، بحيث يجوز له تبعا لذلك رفضها أو قبولها، ويقع على عاتقه في حالة الرفض إثبات كونها تعسفية.

3 –الحق في التصحيح:

تناولت م35 من القانون 07/18 سالف الذكر موضوع الحق في التصحيح، ويدخل ضمن هذا الحق أيضا التعديل أو المحو أو الإضافة أو التحيين، وهذا الحق مجاني ويستفيد منه الشخص المعني أو ورثته، وفق الشروط المذكورة في المادة أعلاه.

يجب تبليغ الغير الذي وصلت إليه المعطيات الشخصية بكل تحيين أو تصحيح أو مسح أو إغلاق لهذه المعطيات.

4 –الحق في الاعتراض:

تناولت م36 من القانون 07/18 سالف الذكر موضوع الحق في الاعتراض، أي حق الشخص المعني في الاعتراض عن معالجة معطياته الشخصية إذا كانت له أسباب مشروعة كأن تتعارض المعالجة مع حقوقه وحرياته الأساسية، وحقه أيضا في الاعتراض عن استعمال المعطيات المتعلقة به أو نتائجها لأغراض دعائية، لاسيما التجارية منها، من قبل المسؤول الحالي عن المعالجة أو مسؤول عن معالجة لاحقة، ما لم تكن المعالجة ناتجة عن التزام قانوني أو تطبيقا لإجراء صريح في المحرر يرخص بها.

5 –الحق في منع الاستكشاف المباشر:

تطرقت إلى موضوع الحق في منع الاستكشاف المباشر م37 من القانون 07/18 سالف الذكر، وهو الحق الذي بمقتضاه يمنع استعمال معطيات شخص طبيعي بأي شكل من الأشكال بواسطة أي وسيلة تكنولوجية كجهاز الاستنساخ البعدي أو البريد الالكتروني، طالما لم يعبر الشخص عن موافقته المسبقة على ذلك، ما عدا الاستثناءات المذكورة في بقية فقرات المادة 37.

المحور الثالث: الجرائم الواقعة على المعطيات ذات الطابع الشخصي:

عالج المشرع الجزائري موضوع الجرائم الواقعة على المعطيات ذات الطابع الشخصي في الفصل الثالث من القانون 07/18 سالف الذكر، في المواد 54 وما بعدها، ويتم تناول هذا الموضوع من خلال التطرق إلى الأحكام المشتركة حول الجرائم الواقعة على المعطيات ذات الطابع الشخصي

أولا: الأحكام المشتركة حول الجرائم الواقعة على المعطيات ذات الطابع الشخصي:

جاء القانون 18-07 ببعض الأحكام المشتركة التي تنطبق على جميع الجرائم الواردة في هذا القانون، وهذه الأحكام هي:

1 -اعتماد المشرع سياسة التجنيح:

باستقراء نصوص المواد 54 وما بعدها من القانون 18-07، وكذا ما نصت عليه المادة 5 من ق ع، نلحظ من خلال العقوبات الأصلية التي أوردها المشرع في القانون 18-07 أن الجرائم الواردة عبارة عن جنح غير مغلظة، وهذا ما ذكرته أيضا صراحة م73 من هذا القانون "يعاقب على ... إحدى **الجنح** المنصوص عليها في هذا القانون...".

2 -العقاب على المحاولة:

بما أن الجرائم الواردة في هذا القانون عبارة عن جنح فإنه لا يجوز العقاب على المحاولة فيها (الشروع) إلا بناء على نص صريح، لذلك ذكرت م73 بأن محاولة ارتكاب جنحة من الجنح المذكورة في هذا القانون يعاقب عليها بالعقوبات نفسها المقررة للجريمة التامة، وهذا حسب القواعد العامة.

3 -إقرار المسؤولية الجزائية للشخص المعنوي:

حسب القواعد العامة لا يجوز مساءلة إلا الأشخاص المعنوية الخاصة، كما لا يجوز مساءلة الشخص المعنوي إلا بناء على نص خاص، لذلك جاء القانون 18-07 بنص م70 التي تجيز بأن يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته مساهما أصليا أو تبعيا، كما يسأل عن الجريمة التامة أو عن مجرد الشروع فيها،[27] كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي، بواسطة أحد أعضائه أو ممثليه الشرعيين، ولا تستبعد مسؤولية الشخص المعنوي الجزائية المسؤولية الجزائية للأشخاص الطبيعية، وهذا حسب نص م51 مكرر من ق ا ج.

4 –الركن المعنوي للجنح الواردة في القانون 18-07:

حسب القواعد العامة، فإنه لا بد من أن يتوافر لدى المجرم قدر من الإثم أو الخطأ يصطلح عليه الفقه الركن المعنوي، فلا يتصور قيام جريمة دون خطأ مهما كانت النتيجة المتمخضة عنها،[28] وللركن المعنوي صورتان يتفق الفقه الجنائي حولهما وهما القصد الجنائي والخطأ غير العمدي.[29]

من قراءة المواد 54 وما بعدها من القانون 07/18 نلاحظ أن المشرع الجزائري استعمل في نص م59 عبارة صريحة تدل على القصد الجنائي: "بطريقة تدليسية أو غير نزيهة أو غير مشروعة"، كما استخدم في نص المادة 69 عبارة "ولو عن إهمال" وهي تدل على الخطأ غير العمدي، وفي الوقت ذاته تدل على القصد الجنائي لأن عبارة "لو" تعطي الاحتمال في أن يقوم الركن المعنوي لهذه الجريمة إما على القصد الجنائي أو الخطأ غير العمدي.

هل يعني هذا أن بقية الجرائم الواردة في القانون 07/18 هي جرائم مادية؟

بما أن الجرائم الواردة في هذا القانون عبارة عن جنح، فإنه وحسب قانون العقوبات الفرنسي يجب لقيامها توافر الركن المعنوي المتمثل في القصد الجنائي بعنصريه العلم والإرادة، والراجح هنا أنه يكفي القصد العام دون القصد الخاص، إذ لم يتطلب المشرع نية خاصة، أو حصول نتيجة معينة، ولكن القصد الجنائي مفترض، بمعنى أن الجانح يفترض فيه سوء النية، وعليه لدحض التهمة عنه إثبات حسن نيته.

ثانيا: الجرائم المتعلقة بالقواعد الموضوعية للمعالجة:

ذكر القانون 18-07 مجموعة من هذه الجرائم، أهمها:

أ – الجرائم المتعلقة بتسيير المعطيات الشخصية:

تشمل نوعين من الجرائم هما: جنحة المعالجة غير المشروعة، وجنحة الاستعمال غير المشروع للمعطيات.[30]

1 -جنحة المعالجة غير المشروعة للمعطيات ذات الطابع الشخصي:

نصت على هذه الجنحة م02، وم59، وكذا م2/65 من القانون 18-07.

يتحقق السلوك الإجرامي المكون للركن المادي لهذه الجنحة بتوافر أحد الأفعال المنصوص عليها في المواد سالفة الذكر، وهي:

- معالجة المعطيات ذات الطابع الشخصي دون احترام للكرامة الإنسانية، والحياة الخاصة، والحريات العامة، أو المساس بحقوق الأشخاص وشرفهم وسمعتهم (م02).

تبدو العبارات الواردة في هذه المادة فضفاضة وغير دقيقة، من ذلك استعمال مصطلح الكرامة الإنسانية، فإذا كانت بعض الأفعال تدخل دون صعوبة في دائرة انتهاك الكرامة الإنسانية، فإن أفعالا أخرى قد يكون من العسير اعتبارها أم لا ماسة بالكرامة.

على كل، يبقى هذا الأمر من اختصاص قاضي الموضوع وفق ظروف وملابسات كل قضية على حدة.

في حالة التعدد المعنوي للجرائم فإن هذه المادة تحيلنا إلى تطبيق القواعد العامة، بمعنى تطبيق العقوبة الأشد.

- جمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة، أو غير مشروعة (م59).

وحسب القضاء الفرنسي، لا تقوم هذه الجريمة إلا إذا تم تسجيل المعطيات بعد جمعها، والاحتفاظ بها في "فيش" أو معالجتها بالحاسب الآلي.[31]

- الاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة القانونية (م2/65).

لا يجيز القانون أن يحتفظ المسؤول عن المعالجة بالمعطيات ذات الطابع الشخصي لمدة تفوق المدة المنصوص عليها في التشريع الساري المفعول أو الواردة في التصريح أو الترخيص، لأن ذلك يتعارض مع مبدأ الحق في النسيان.

2 –جنحة الاستعمال غير المشروع للمعطيات ذات الطابع الشخصي:

يقوم السلوك الإجرامي لهذه الجنحة إذا توافر أحد الأفعال التالية:

– ارتكاب الجنحة من قبل أشخاص معينين: المسؤول عن المعالجة أو المعالج من الباطن، سمحوا لأشخاص غير مؤهلين بالولوج لمعطيات ذات طابع شخصي (م60).

– الأشخاص المذكورون في م23 (أعضاء السلطة الوطنية)، وم27 (الأمين التنفيذي للسلطة الوطنية ومساعدوه) ملزمون بالحفاظ على السر المهني تحت طائلة العقوبات الواردة في قانون العقوبات (م301 ق ع)، دون الإخلال بأحكام جزائية أخرى حسب طبيعة المعلومات المعنية (م62).

– نقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية (م67) خرقا لأحكام نص م44، أي دون الحصول على ترخيص من السلطة الوطنية، ودون التأكد من أن هذه الدولة تضمن مستوى حماية كاف للحياة الخاصة والحريات والحقوق الأساسية للأشخاص، وكذلك عندما يؤدي نقل هذه المعطيات إلى المساس بالأمن القومي أو المصالح الحيوية للدولة.

– الولوج إلى السجل الوطني لحماية المعطيات ذات الطابع الشخصي دون أن يكون الشخص مؤهلا لذلك (م63)، وهذه المادة وقائية تعاقب على مجرد الولوج غير المسموح به إلى هذا السجل المذكور في نص م28 حتى وإن لم يترتب على هذا الولوج نتائج ضارة.

– التسبب أو التسهيل ولو عن إهمال، في الاستعمال التعسفي أو التدليسي للمعطيات المعالجة، أو إيصالها إلى غير المؤهلين لذلك (م69).

هذه الصورة الأخيرة لجنحة الاستعمال غير المشروع للمعطيات ذات الطابع الشخصي يكفي مجرد الإهمال لقيام ركنها المعنوي، كما يتصور أن تقوم على القصد الجنائي أيضا.

ب – الجرائم المتعلقة بحقوق الشخص المعني:

يشكل الاعتداء على أي حق من الحقوق الواردة في القانون 07/18 جريمة يعاقب عليها القانون.

1-جنحة الرفض غير المبرر لحقوق المعني:

إن المسؤول عن المعالجة يجب عليه احترام حقوق الشخص المعني (م64)، وأي رفض منه دون سبب مشروع حقوق الإعلام أو الولوج أو التصحيح أو الاعتراض وفق ما جاء في نصوص المواد 32، 34، 35، 36 يشكل جريمة تستوجب العقاب.

2-جنحة المعالجة دون رضا الشخص المعني أو رغم اعتراضه:

هذه الجنحة منصوص عليها في م55، وهي تجرم في فقرتها الأولى كل من يقوم بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام م07 التي تشترط الموافقة الصريحة للشخص المعني للقيام بالمعالجة، كما أنه يجوز للمعني التراجع عن الموافقة التي يكون قد أعطاها سلفا، وفي هذه الحالة تشكل المعالجة بعد التراجع عن الموافقة جريمة معاقبا عليها. كما أن م07 لا تجيز إطلاع الغير على المعطيات إلا من أجل غايات محددة قانونا وبعد الموافقة الصريحة والمسبقة للمعني.

غير أن هذه الجنحة لا تقوم ولو تمت المعالجة دون موافقة الشخص المعني إذا كانت المعالجة ضرورية لحماية حياة الشخص المعني، أو لتنفيذ عقد يكون الشخص المعني طرفا فيه، أو للحفاظ على مصالحه الحيوية، أو لتحقيق مصلحة مشروعة، أو مهمة من مهام الصالح العام (م5/7).

أما الفقرة الثانية من م55 فتجرم على معالجة المعطيات ذات الطابع الشخصي رغم اعتراض الشخص المعني، خاصة عندما تستهدف الإشهار التجاري، أو عندما يكون الاعتراض مبنيا على أسباب شرعية.

ثالثا: الجرائم المتعلقة بالقواعد الإجرائية للمعالجة:

إن إخلال المسؤول عن المعالجة ببعض الإجراءات قبل إجراء المعالجة يعتبر جريمة معاقبا عليها، كما أن إخلاله بالقيام ببعض الشكليات التي تضمن أمن المعطيات وسريتها جريمة معاقب عليها أيضا.

1-الجرائم المتعلقة بالإجراءات السابقة عن المعالجة:

لا يجوز القيام بمعالجة المعطيات ذات الطابع الشخصي قبل القيام بالتصريح أو الحصول على ترخيص حسب الحالة، من قبل السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، وفق ما جاء في نص م12، تحت طائلة المساءلة الجزائية، كما هو منصوص عليه في نص م56.

تطرق القانون 17-08 سالف الذكر إلى التصريح في المواد: 13، 14، 15، 16، وإلى الترخيص في المواد 17، 18، 19، 20، 21.

كما أنه لا يجوز تحت طائلة العقاب تقديم تصريحات كاذبة أو مواصلة نشاط المعالجة رغم سحب وصل التصريح أو الترخيص الممنوح (م2/56).

لا يجوز أيضا القيام بمعالجة المعطيات الحساسة دون الموافقة الصريحة للمعني أو دون الحصول على ترخيص من السلطة الوطنية في الحالات المذكورة في م18.

كما لا يجوز وضع أو حفظ في الذاكرة الآلية المعطيات ذات الطابع الشخصي بخصوص جرائم أو إدانات أو تدابير أمن (م68).

2 – جنحة عدم اتخاذ إجراءات حماية المعطيات:

إن المسؤول عن معالجة المعطيات ملزم تحت طائلة العقاب باتخاذ مجموعة من الإجراءات بغية حماية المعطيات الشخصية.

نص المشرع في م1/65 على جنحة عدم اتخاذ إجراءات حماية المعطيات، وهي تتعلق بالإخلال بالالتزامات الواردة في نص المادتين 38 و39، بقراءة هاتين المادتين نجد أن م38 تلزم المسؤول عن المعالجة بوضع التدابير التقنية والتنظيمية اللازمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف، أو التلف، أو النشر والولوج غير المرخصين، وهي تضمن مستوى ملائما من السلامة (الأمن) بالنظر إلى

المخاطر التي تمثلها المعالجة، وطبيعة المعطيات الواجب حمايتها، أما م39 فتطرقت إلى ضرورة حسن اختيار معالج من الباطن يقدم ضمانات السلامة التقنية الكافية ويسهر على احترامها.

3 – جنحة عرقلة عمل السلطة الوطنية:

نصت على هذه الجنحة م61 التي جرمت وعاقبت على عرقلة عمل السلطة الوطنية، سواء بالاعتراض على إجراء عملية التحقيق في عين المكان، أو عن طريق الامتناع عن تزويدها بالمعلومات والوثائق الضرورية للقيام بمهامها، أو إخفاء بعض أو كل المعلومات والوثائق عنها، أو تزويدها بمعلومات مغلوطة أو ناقصة أو خاطئة، أو عدم تقديمها بشكل مباشر وواضح.

المحور الرابع: العقوبات المقررة لقمع الجرائم الواقعة على المعطيات ذات الطابع الشخصي:

حسب القواعد العامة، هناك نوعان من العقوبات: عقوبات أصلية وعقوبات تكميلية.

أولا: العقوبات الأصلية:

العقوبات الأصلية هي التي يجوز الحكم بها بصفة أصلية وأساسية كجزاء عن الجريمة، ولا يتعلق الحكم بها على عقوبة أخرى.[32]

العقوبات الأصلية في مادة الجنح عبارة عن الحبس والغرامة حسب نص م5 من ق ع، وتختلف مدة الحبس بالنسبة للجرائم الواقعة على المعطيات ذات الطابع الشخصي حسب طبيعة كل جريمة ودرجة خطورتها، ولكن مدة الحبس القصوى هي خمس (5) سنوات حسب القانون 07/18 سالف الذكر (المواد: 54، 56، 57، 60، 67، 69)، أما مدته الدنيا فهي شهران (م64)، أما مقدار الغرامة فيختلف أيضا حسب الجرائم الواردة في القانون، ولكنه يتراوح من 20.000 د ج (م64) إلى 1.000.000 د ج (م67).

الملاحظ أن المشرع الجزائري في هذا القانون قد جمع بين عقوبتي الحبس والغرامة لبعض الجرائم (المنصوص عليها في المواد: 54، 55، 56، 57، 58، 59، 60، 67، 68، 69)، وخير بين العقوبتين بالنسبة لجرائم أخرى (المواد: 61، 63، 64، 66)، وعاقب بالغرامة فقط على الجريمة المنصوص عليها في م65.

أما الشخص المعنوي فعقوبته الأصلية تكون حسب القواعد العامة المنصوص عليها في ق ع (م70)، أي الغرامة التي تصل حتى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي (م18 مكرر ق ع).

الملاحظ هنا أن أقصى عقوبة يمكن أن يتعرض لها الشخص المعنوي بالنسبة للجرائم الواردة في القانون 07/18 هي خمسة ملايين دينار (م67 من القانون 07/18)، أما أدنى عقوبة فهي 500.000 دج (م58).

هذه الغرامات سواء المفروضة على الشخص الطبيعي أو المعنوي غرامات بسيطة نسبيا، إذا ما قورنت بالغرامات المتعلقة بالموضوع ذاته في تشريعات مقارنة ومنها التشريع الفرنسي وكذا التشريع المصري.

بخصوص الظروف المشددة ذكرت م74 ظرفا مشددا واحدا هو العود، وهو ظرف شخصي لتشديد العقوبة، بين المشرع الجزائري شروطه وأنواعه في م54مكرر وما بعدها من ق ع.

ذكرت م74 من القانون 07/18 أن العقوبات تضاعف في حالة العود، ولا ينتج عن ذلك أن يتغير وصف الجريمة من جنحة إلى جناية، بل تحتفظ بوصفها القانوني (جنحة) حسب القواعد العامة (م28 ق ع).

ثانيا: العقوبات التكميلية:

العقوبات التكميلية والتي يطلق عليها أيضا العقوبات الإضافية، هي تلك العقوبات المكملة للعقوبات الأصلية،[33] وهي نوعان وجوبية أو جوازية حسب ما ينص عليه القانون، فإذا كانت وجوبية تعين على القاضي النطق بها، أما إن كانت جوازية فلا يجب عليه ذلك، ويكون حكمه صحيحا غير معيب.[34]

العقوبات التكميلية في القانون 07/18 جوازية، حسب نص م71 "يمكن أن..." وأحالتنا هذه المادة إلى العقوبات التكميلية المنصوص عليها في قانون العقوبات (م9 ق ع، م18 مكرر/2 ق ع).

أجازت م2/71 من القانون 18-07 سالف الذكر مسح كل المعطيات محل المعالجة أو جزء منها، إذا كان قد نتج عنها ارتكاب الجريمة، ويكون هذا المسح تحت إشراف أعضاء ومستخدمي السلطة الوطنية الذين يعاينون المسح.

كما أن م72 من القانون نفسه تطرقت إلى مصادرة محل الجريمة بغرض إعادة التخصيص أو التدمير، ويتحمل مصاريف ذلك المحكوم عليه.

خاتمة

إن التطور التقني الهائل في مجال المعلوماتية، زاد من خطر استعمال الوسائل الحديثة في عالم الجريمة، وتكتسي البيانات الشخصية أهمية كبرى في حياة الأشخاص لأنها تعكس شخصيتهم وتعبر عن توجهاتهم وميولاتهم، وهي مرتبطة ارتباطا وثيقا بحرمة الحياة الخاصة، لذا وجب توفير الحماية القانونية الضرورية والكافية لها، وخاصة عن طريق وسيلة القانون الجزائي، باعتباره الأقدر على تحقيق الردع العام والخاص معا، ويحمي بشكل واضح البيانات ضد كل من تسول له نفسه أن يتعرض لها سواء بمجرد الاطلاع عليها، أو حتى تخزينها واستعمالها طالما أنه غير مرخص له قانونا بذلك.

لقد دأبت التشريعات المقارنة المختلفة على توفير النصوص القانونية الملائمة لحماية البيانات الشخصية، هادفة في معظمها إلى الموازنة بين صون حرمة الحياة الخاصة، وضرورات الكشف والاطلاع والتخزين للبيانات عندما تقتضي الأمور ذلك، ولا يتأتى هذا التوازن إلا إذا احترمت التشريعات المختلفة مجموعة من المبادئ أبرزها مبدأ الغاية، ومبدأ الشفافية، والحق في الهوية الرقمية والحق في الدخول في طي النسيان.

لقد حاول المشرع الجزائري مواكبة الركب من خلال إصداره لمجموعة من النصوص القانونية، كتلك المتعلقة بحرمة الحياة الخاصة، ثم القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، وقد حاول المشرع من خلال هذا القانون إضفاء مزيد من الحماية القانونية للمعطيات الشخصية، وقد وفق إلى حد كبير، ورغم ذلك هنالك بعض الملاحظات منها:

- ضرورة إقرار الحماية القانونية للمعطيات الشخصية بالنسبة للشخص المعنوي على غرار كثير من التشريعات الأوربية.

- تغليظ عقوبة الغرامة باعتبارها العقوبة الأنسب لقمع مثل هذه الجرائم، والعمل على مراجعتها دوريا، بما يتناسب مع سعر الدينار في السوق.

- إقرار نظام المصالحة والوساطة الجزائية، سواء مع المجني عليهم أو السلطة الوطنية، وفق شروط، ينتج عنها انقضاء الدعوى العمومية، كما فعل المشرع المصري في م49 من القانون 151 لسنة 2020.

- تكثيف التعاون القضائي مع مختلف الدول التي تضمن حدا مقبولا لحماية الخصوصية.

- إفادة القائمين على المعالجة الآلية للمعطيات من دورات تكوينية وتدريبية لتحسين المستوى.

الهوامش:

[1] Roseline Letteron, libertés publiques, Dalloz, Paris 2012, pp368-369.

[2]Luc Grynbaum et autres, Droit des activités numériques, Dalloz, Paris, France 2014, p748, n0 1031.

[3] قانون 07/18 مؤرخ في 10 يونيو 2018 متعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. ج ر العدد 34 المؤرخ في 10 يونيو 2018، ص ص 11-23.

[4] عماد حمدي حجازي، الحق في الخصوصية ومسؤولية الصحفي، دار الفكر الجامعي، الاسكندرية، مصر2008، ص141 وما بعدها.

[5] Roseline Letteron, op cit, p385.

[6] Mathieu Prud'homme, l'usurpation d'identité numérique: bientôt un nouveau délit, Gazette du palais 2, Mars Avril 2010, p777.

[7] Loi d'orientation et de programmation pour la performance de la sécurité intérieure.

[8] Romain v.Gola, droit du commerce électronique, Galino éditeur, Lextenso édition, Paris 2013, p236.

[9] Roseline Letteron, op cit, p387.

[10] Mme kheira Dari Bekara, protection des données personnelles coté utilisateur dans le e-commerce, thèse de doctorat conjoint Télécom Sud Paris et l'université Pierre et Marie Curie, Paris 2012, pp42-45.

[11] د. بولين أنطنيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، منشورات الحلبي الحقوقية، عمان الأردن (دون ذكر سنة النشر)، ص388.

[12] عبد الحليم رمضان، الحماية الجنائية للتجارة الالكترونية، دار النهضة العربية، القاهرة مصر 2012، ص86.

[13] المرجع نفسه، ص85.

[14] Commission nationale de l'informatique et des libertés.

[15] عبد الحليم رمضان، المرجع السابق، ص88.

[16] ج ر 84، ص23.

[17] Tayeb Belloula, droit pénal des affaires et des sociétés commerciales, Berti éditions, Alger 2011, p157.

[18] محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، عمان، الأردن 2004، ص84.

[19] غنام محمد غنام، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، المنصورة، مصر 2013 ص100.

[20] الشوابكة، المرجع السابق، ص85.

[21] مدحت عبد الحليم رمضان، المرجع السابق، ص110.

[22] الجريدة الرسمية لجمهورية مصر العربية، العدد 28 مكرر (هـ) الصادر في 15 يوليو 2020.

[23] أصدرت الأمم المتحدة في 20 من فبراير 1990 ما يعرف بالمبادئ التوجيهية لتنظيم استخدام ملفات البيانات الشخصية المجهزة إلكترونيا، وهي مبادئ تسترشد بها التشريعات الداخلية عند إعداد قوانينها، ونصت على تسعة مبادئ هي: مبدأ المشروعية والنزاهة، مبدأ الصحة (صحة البيانات)، مبدأ الغاية، مبدأ وصول الأشخاص المعنيين إلى الملفات، مبدأ عدم التمييز، إمكانية الاستثناء من المبادئ السابقة في حالات خاصة، مبدأ الأمن، الرقابة والعقوبات، تدفق البيانات عبر الحدود. اعتمدت هذه المبادئ ونشرت على الملأ بموجب قرار الجمعية العامة للأمم المتحدة رقم 45/95 المؤرخ في 1990/12/14. ينظر الموقع الالكتروني أدناه، تاريخ الولوج 2022/8/12 على الساعة 14.

http://hrlibrary.umn.edu/arab/b072.html

[24] ينظر الموقع الالكتروني أدناه، تاريخ الولوج: 2022/08/13 على الساعة 21 و25 د.

https://www.cnil.fr/cnil-direct/question/quels-sont-les-grands-principes-des-regles-de-protection-des-donnees?visiteur=part

[25] ينظر الموقع الالكتروني أدناه، تاريخ الولوج 2022/8/13 على الساعة 21 و35 د.

https://www.cnil.fr/cnil-direct/question/la-finalite-dun-fichier-cest-quoi?visiteur=part

[26] وهذه الحالات هي:

- إذا تعذر إعلام الشخص المعني، لا سيما في حالة معالجة المعطيات لأغراض إحصائية أو تاريخية أو علمية، ولكن يلزم المسؤول بإشعار السلطة الوطنية باستحالة إعلام الشخص، مع تقديم الأسباب.

- إذا تمت المعالجة تطبيقا للقانون.

- إذا تمت المعالجة بشكل حصري لأغراض صحفية أو فنية أو أدبية.

[27] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الأزاريطة، الإسكندرية، مصر 2010، ص115.

[28] سليمان عبد المنعم، النظرية العامة لقانون العقوبات، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان 2003، ص508، ر362.

[29] المرجع نفسه، ص536، ر386.

[30] عائشة بن قارة مصطفى، آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون 07/18، مجلة العلوم القانونية والسياسية، المجلد 10، العدد 01، أفريل 2019، جامعة الوادي، الجزائر، ص753.

[31] غنام محمد غنام، المرجع السابق، ص120.

[32] أحمد فتحي سرور، الوسيط في قانون العقوبات، القسم العام، ط6، دار النهضة العربية، القاهرة، مصر 2015، ص948، رقم548.

[33] المرجع نفسه، ص950، رقم 550.

[34] محمود نجيب حسني، شرح قانون العقوبات اللبناني، القسم العام، الجزء الثاني، ط3، منشورات الحلبي الحقوقية، بيروت، لبنان 1998، ص964، رقم 685.

الاسم واللقب: بعجي عبد النور.

الجامعة: كلية الحقوق سعيد حمدين، جامعة الجزائر 1.

رقم الهاتف: 05.51.10.06.41.

البريد الالكتروني : Abdennour.bdj@gmail.com

موضوع المداخلة:التهديد الناشئ للإرهاب السيبراني.

-The emerging threat of cyber terrorism-

محور المداخلة: في المحور الثاني، تحت عنوان "أثر استخدام التكنولوجيا الحديثة على أحكام التجريم".

لغة المداخلة: الإنجليزية.

THE TITLE; The emerging threat ofCyber terrorism

Abstract:

With the continuous flow of fighters to the organizations of "ISIS", Al-Qaeda, and their associated groups, Security Council Resolution 2322 (2016) binded all the states to criminalize the use of information and communication technologies "ICT", especially the Internet in facilitating terrorist acts and inciting the commission or the recruitment of criminal acts. The objective of this paper is to analyse and review the effectiveness of the current national response to cyber terrorism.

the general question is: how the Algerian legislator criminalize the use of ICT in terrorism?

Keywords; ICT- cyberterrorism- terrorist acts- penal law- foreign fighters

ملخص بالعربية:

مع تدفق المقاتلين الى الجماعات الإرهابية "داعش" والقاعدة وباقي التنظيمات المرتبطة بهم، صدر قرار مجلس الأمن 2322 (2016) الذي يلزم الدول بتجريم استخدام تكنولوجيات الاعلام والاتصال، خصوصا الانترنت في تسهيل الأعمال الإرهابية والتحريض على ارتكابها أو تجنيد الإرهابيين، ان الهدف من هذه الورقة هو تحليل واستعراض فعالية الاستجابة الوطنية الحالية للإرهاب السيبراني.

Introduction:

Modern terrorism has rapidly evolved, becoming increasingly nonphysical, with vulnerable "home grown" citizens being recruited, radicalized, trained and tasked online in the virtual and ungoverned domain of cyber space.

Security Council Resolution 2178 (2014) was passed, which marks a "turning point in efforts undertaken at the global level to reduce the threat of foreign terrorist fighters", it was adopted unanimously, therefore obliged all countries to enact laws criminalizing travel or attempting to travel for terrorist purposes, and requiring countries to suppress and prevent the organization, recruitment, transfer and equipping of foreign terrorist fighters, also to financing their activities, we can define the cyberterrorism is a convergence of cyberspace and terrorism, It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.

Finally, the national security machinery of governments has no choice only to find a way for combatting these threats, if they are to flourish in an increasingly competitive and globalized world. *so, the general question is: how the Algerian domestic law act with the phenomenon of use the ICT in terrorism?*

THE FIRST TOPIC: cyberterrorism a complex concept

Modern terrorism depends on information and communication technology, given the opportunities it provides that do not exist in the real world, as follows;

FIRST REQUIREMENT: Definition of ICT and cyberterrorism

we try to determine the definition of ICT as well as cyber terrorism, for purpose to know the nature of concepts.

Firstly:ICT is a technical or legal concept?

Societies rely on technologies to organise and administer themselves, offer services to citizens, educate and communicate, economic globalization is enhanced by new technologies, which provide opportunities in international markets.

Multinational enterprises, and also small and medium companies, are carrying out their businesses more easily, without spatial barriers. Technologies allow them to invest in new activities or enter new markets and free them to invent new ways of presenting themselves and offering their services/goods. A boundless, unlimited flow of information, together with the possibility to establish international networks, facilitates the reduction of economic costs, and direct and indirect risks, this is no different from what ICT allows criminals to do. They use new technologies to communicate, to organise themselves better, to widen the spectrum of their businesses, to update their modus operandi and techniques, and to avoid law enforcement risk[i].

The ICT revolution can be defined as a veritable 'Pandora's box' of criminal offences and challenges, it have been known by several names, it described as the new information and communication technologies NTIC, Then the word "new" was deleted from the label to become information and communication technology ICT, then with the beginning of the use of the Internet in the nineties, it was shortened to the name TI**,**in addition ICT is sometimes used synonymously with IT (for information technology); however, it is generally used to represent a broader, more comprehensive list of all components related to computer and digital technologies than IT.

ICT is also used to refer to the convergence of audiovisual and telephone networks with computer networks through a single cabling or link system. There are large economic incentives to merge the telephone network with the computer network system using a single

unified system of cabling, signal distribution, and management. it is an umbrella term that includes any communication device, encompassing radio, television, cell phones, computer and network hardware, satellite systems and so on, as well as the various services and appliances with them such as video conferencing and distance learning, it also includes analog technology, such as paper communication, and any mode that transmits communication[ii].

it posed a great danger to international peace and security, in this regard the Security Council had the resolution 2161 (2014)[iii], that express the increased use, in a globalized society, by terrorists and their supporters, of new information and communications technologies, in particular the Internet, to facilitate terrorist acts, as well as their use to incite, recruit, fund or plan terrorist acts.

In the law n° 09-04 related to "Special rules for the prevention and control of crimes related to ICT"[iv] the first item of Article 02, select the means by which these crimes are committed is the information system or a wired communication system, It concluded that the narrow concept of the term "information and communication technologies" is limited to two basic points or concepts, this is what the same article determine that: " B. Information system: any separate system or group of systems connected to each other or linked, one or more of which automatically processes data in implementation of a specific program," and that: "F. Electronic Communications: Any correspondence, transmission, or reception of various signs, signals, writings, images, sounds or information by any electronic means."

Consequently, the legislator hadn't a specific or clear definition of this term because it's considered among the technical terms.

Secondly: Cyber terrorism a complex concept

The term "cyberterrorism" appeared in the mid-eighties, which is consisted of "the Internet" and "terrorism" through a study by the researcher "BARRY COLLIN", he found a difficulty to define the terrorism phenomenon, and the computer role in the terrorist act, then it has been used widely, as it combines two of the century's greatest fears: cyberspace and terrorism[v].

In the year 1980, the term was used to refer to the cyber-attacks that affect the economy of the United States of America by the computer, these risks were demonstrated through studies, perhaps the most prominent of which is the report of the American National Academy of Sciences on computer security, which stated that the United States of America is in danger, due to the increasing used on computers, it's found in the management of power delivery, communications, aviation, financial services, and storing vital information, therefore it can be to a cyber-attack biggest than a bomb[vi].

In the early 2000s, Cyberterrorism has been a highly fashionable topic, therefore the events of September 11, 2001 had the effect of increasing interest of it, many scientific books and articles deal with this theme, for example, a search on engines for scientific articles reveals a thousand articles written on the subject since 2001, and it reported in the media.

In fact, according to the majority of specialists dealing with the subject cyberterrorism is one of the threats that are often considered as emerging. However, its ill-defined and still relatively obscure, even an opaque character, makes cyberterrorism a threat that is much more floating than tangible.[vii]

sooner or eventually, according to many specialists, terrorists will turn to information technology to launch cyberattacks against corporations, another motivation for attacks on computer networks is to further a political, religious or ideological cause Such attacks have the potential to cause considerable harm, possibly disrupting essential services such as water, power, hospitals, financial systems, emergency services, air/shipping control and the like[viii].

Given differing views on the meaning of 'terrorism', it is not surprising that the term 'cyberterrorism' is ill-defined, it may be divided into two categories. The first, simply

describes those situations where technology is used to facilitate the activities of terrorists, secondly Technology may also be utilised in raising finance.

SECOND REQUIREMENT: impact of technology in terrorist activities

Online organized crime and cyber terrorism are becoming more important[ix], I find a several type of terrorist activities through ICT, I review in what is actually cyberterrorism.

First: Traditional use of the Internet

The internet is a means of accessing to a dangerous source for terrorists it seems that some harmless sites provide valuable and substantial information to them where they can uncontrolled, for example, individual contacts between members of terrorist groups via the cyberspace, therefore is different from mobile communications wherever the content is sent without encode, so that local government agencies keep up instantly hear if the hidden parties are at present under "wiretapping" surveillance, However, the private Internet conversation is encrypted and easy. From this, e-mail typically allows them to communicate efficiently, for example, the principal offenders of the September 11 attacks acted by this effective way, they opened multiple accounts on largely anonymous email services like Hotmail[x].

Secondly: means of cyberterrorism

1-Cyberattack: it constitutes what's called the “cybercrime” and their offenders are cybercriminals[xi]**,** the most of them are motivated to defeat the information system and experience all problems related the security, they are curious about technology, This does not prevent the existence of groups has a highly competence that use the cyber-attacks as their financial income.

Online fraudsters can take the victim's data through ransom programs, the personal information of owner is encrypted and its unread, in order to claim money for a password that gives him access to his data, this techniques used to hide identity and provides the payment in virtual currency such as bitcoin[xii], the "reasonable ransom" was carefully chosen[xiii], it led to an explosion of the data extortion, so we can be said that cyber-attacks constitute a huge income for the terrorist to actually finance his terrorist networks.

On the other side, Cyber-attacks constitute a threat to the critical infrastructure, is generally represented in water treatment plants, oil refineries, power systems, gas pipelines, etc. which uses the "SCADA" systems to collect the data and control these systems, because it is difficult for humans to perform these services in the industrial plants and facilities, there may be a production lines or nuclear plant control.

2- Dissemination of terrorist content: Technology has influenced the means of online attack to become more developed, At the same time, Internet has created the possibility of disseminating information to all without any cost, or censorship of content, terrorists are not just using the Internet, Hence, terrorists use the internet not only to launch attacks, but also to spread the "war of ideas", and their beliefs, they exploits the information infrastructure and finance the extremism[xiv], so the terrorist groups exploit the Internet through websites , to spread extremism and display their criminal operations by recording their attacks for the best results

Participants in the Riyadh conference on the use of the Internet to fight the call of extremist violence recommended a need to disseminate counter-narratives through all relevant media channels, including social media, to counter the appeal of extremist messages.

THE SECOND TOPIC: criminalizing the use of ICT in terrorism

There is a several United Nations resolutions warn the potential danger of internet use by terrorists, especially after 11 September 2001 attacks in USA, according to the Article 02 of Act No. 09-04 on ICT and combat them is specified in key paragraph (a), that: "Offences of infringing on systems for the automatic processing of data specified in the Penal Code and any other crime or it committed easily through a system or electronic communications. ", the text includes a broad legal wording include cybercrime and crimes committed through an electronic means, which is cyber terrorism, referring to the Penal Code, we find that the last clause of Article 87 bis 11 adopted the term "use of information and communication technologies," which is specific to the commission of terrorist acts stipulated in paragraphs 1, 2 and 3 of the similar article, and we treat them as follows:

FIRST REQUIREMENT: Use of ICT to travel terrorist activities

We explain the danger of using technology, as well as the criminalization of the Algerian legislator to these criminal ways, as follows:

Firstly: The danger of using ICT by terrorists

Terrorists acquire the means provided by technology to diversifying their activities, making them efficient, they can be implemented correctly with fewer individuals and better results, and thus one person recruit more recent members, Network technologies characterized by diversity and plurality are largely driven by consumers and commercial markets around the world. It is unpractical to keep these branches of knowledge out of the hands, these technologies can simply be bought off the shelves, From this, the elevated risk of terrorists and their ardent supporters using media technologies to spread extremist ideology that leads to the modern terrorism of all kinds, and to recruit others to commit acts and incite them to do so, through channels including the Internet and financing and facilitating the travel of foreign fighters and the activities they typically attempt after that, Resolution 2178 (2014) adopted by the Security Council in its preamble to Express the grave concern over the acute and growing threat posed by foreign terrorist fighters and defines them as: " individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict, and resolving to address this threat",[xv] it underlines the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts, while respecting human rights and fundamental freedoms and in compliance with other obligations under international law.

Secondly: The position taken by the Algerian legislator

In the penal law the article 87 bis 11 identified many forms of terrorist activities, including the first paragraph is criminalization of travel and stipulated that: "... every Algerian or foreigner residing in Algeria legally or illegally travels or attempts to travel to another country for the purpose of committing, planning, preparing, or participating in terrorist acts", And in the last paragraph: "he uses the information and communication technologies to commit the acts mentioned in this article," therefore ICT used to facilitate the travel to do terrorist activities, it specified the scope of the criminalization of travel for the purpose of terrorism, such a thing applies to the Algerian and the foreigner who commits the crime or use the ICT to commit it.

The ISIS, Al-Qaeda and associated groups leads to implement Resolution 2178 (2014) to limit this spread by preventing and suppressing the recruitment, organization, transfer, or equipping of foreign terrorist fighters and financing their travel and activities, a foreigner is considered a legal resident if he has been in possession of a resident card by the mandate of his residence for a period of two years, which shows that he has proven his actual, habitual

and permanent residence in Algeria, and a non-resident who is considered to be transiting the Algerian territory or residing in it for a period not exceeding ninety days.

we point out that the Algerian legislator had to define the term training or receiving training, as it was included in the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism[xvi], where Article 03 in the first clause states: " For the purpose of this Protocol, "receiving training for terrorism" means to receive instruction, including obtaining knowledge or practical skills, from another person in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of carrying out or contributing to the commission of a terrorist offence".

SECOND REQUIREMENT: use of ICT for the facilitation of terrorist activities

like a means of facilitating travel, through the provision and collection of funds, and financing, as well as organization.

Firstly:ICT is a means of saving and collecting funds or financing for travel

Article 87 bis 11 criminalizes the acts of "saving", "collecting" and"financing" in paragraphs 2 and 3, saving money express the finding of sources from which money is collected, while the collecting means compiling of money from different sources.

In addition, the person who collects the funds not the provider of it, for that there is a necessity to criminalize each act separately. On the other hand, saving and collecting funds are acts that fall under the general concept of "finance",if we compare the "saving" is a direct means, while "collection" is an indirect means of financing, this last is confirmed by Article 05, first paragraph of the Additional Protocol of COE, which defined; "funding travelling abroad for the purpose of terrorism means providing or collecting, by any means, directly or indirectly, funds fully or partially enabling any person to travel abroad for the purpose of terrorism".

we can say that what was mentioned in paragraphs 2 and 3 previously is a direct employment of the resolution 1373 (2001)[xvii], this last adopted under Chapter VII of the United Nations Charter, it's a binded rules urge to: (a) Prevent and suppress the financing of terrorist acts; (b) Criminalize the wilful provision (saving) or collection, by any means, directly or indirectly, of funds by their nationals or in their territories with the intention that the funds should be used, or in the knowledge that they are to be used, in order to carry out terrorist acts.

In fact, there is no definition to concept "finance" in the penal law, so its end for the special laws in the field of criminalization.

In this regard, Prevention and Combating Money Laundering law and Terrorist Financing express in Article 03, that: "Anyone who provides, collects, or conducts willingly, in a legitimate or illegal manner, by any means, directly or indirectly, funds for the purpose of using them personally, wholly or partially, to commit or attempt to commit crimes described as terrorist acts or with his knowledge...the financing of terrorism is an act of terrorism".

Secondly: ICT is a means of organizing or facilitating travel

Article 87 bis 11 in the third paragraph criminalizes the organization and facilitation of travel to commit terrorist activities, however, it did not specify the meaning or scope of the activities of organizing and facilitating, therefore it refers to the general principal of criminal law related to the crime contribution by the aid or assistance.

On the contrary the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism in the first paragraph Article 06, defines; "organising or otherwise

facilitating travelling abroad for the purpose of terrorism", it means any act of organisation or facilitation that assists any person in travelling abroad for the purpose of terrorism.

Conclusion:

I concluded in the research paper that the Algerian legislator criminalized the use of information and communication technology by terrorists in implementation of the Security Council resolutions.

The results I summarize are as follows:

- Cyber terrorism is one of the newly crimes that use cyberspace to achieve the purposes of classic terrorism through the use of information and communication technologies.
- Cyber terrorism is a global crime that transcends the borders, for this a difficult to detect the cybercriminals, they are usually specialists in the field of information technology or have some knowledge in dealing with information networks.
- Algeria applied the Resolution 2178 (2014) by including Article 87 bis 11, it criminalizes the use of ICT in terrorism by terrorists and their supporters to spread extremist ideology, and recruiting others to commit acts of terrorism and inciting them, through channels, including the Internet, financing and facilitating the travel of foreign fighters.

Hence, the study made the following recommandations:

- Enacting a general law related to terrorism and criminalizing all acts of cyberterrorism.

-The need to ratify the Budapest Convention on Cybercrime, due to the development of cybercrime.

- Awareness of youth about the danger of violent and extremist content and their participants in the war on terrorism through seminars, scientific research and advertising on various television channels.

---

[i] Savona, Ernesto U., ed. Crime and technology: New frontiers for regulation, law enforcement and research. Springer Science & Business Media, 2004, p08.

[ii] Wikipedia, Information and communications technology, Available at:https://en.wikipedia.org/wiki/Information_and_communications_technology,accessed10 June 2021.

[iii] UN Security Council, S/RES/2161 (2014), on threats to international peace and security caused by terrorist acts, available at: https://www.undocs.org/S/RES/2161%20(2014), accessed 15 June 2021

[iv] Law 09-04 of August 5, 2009, "the special rules for the prevention and control of crimes related to ICT, Algerian Official Journal, No. 47, issued on August 16, 2009, p. 05.

[v] .COLLIN, Barry C. The future of cyberterrorism: Where the physical and virtual worlds converge. Crime and Justice International, 1997, 13.2: 15-18

[vi] . National Research Council, C. O. R. P. O. R. A. T. E. (1991). Computers at risk: Safe computing in the information age. National Academy Press, p07.

[vii] .Fortin, Francis. Cybercrimes et enjeux technologiques : Contexte et perspectives, Presses internationales polytechnique, 2020, p285.

[viii] .Clough, Jonathan. Principles of cybercrime. Cambridge University Press, 2015, p11

[ix] . RUGGIERO, Vincenzo (ed.). Organized crime and terrorist networks. Routledge, 2019, p60.

[x] . BRUNST, Phillip W. Terrorism and the internet: new threats posed by cyberterrorism and terrorist use of the internet. In: A War on Terror? Springer, New York, NY, 2010. p73.

[xi] .Donn B Parker went on to consider people who misuse the information intentionally They cover a range of criminals Although it is impossible to describe these criminals in one definition, However, there are some interestingcriminal phenomena, that we need to know in order to be effective in protecting of information, and many of these characteristics distinguish cybercriminals from other criminals, it referred In the word S.K.RAM, as an abbreviation to skills, knowledge, resources, authority, and motives.

[xii]. A digital currency, usually abbreviated by (BTC), its prohibited to trade the virtual currencies in Algeria, according to the Article 117 of the Algerian Financial Law of 2018 stipulates that: “It is prohibited to buy, sell, use and possess virtual currency. Virtual currency is the one that Internet users use over the Internet, and it is distinguished In the absence of a physical support such as coins, banknotes and payments by check or bank card.

[xiii].Fortin, Francis, Op. Cit, p304.

[xiv]. GIACOMELLO, Giampiero. Bangs for the buck: A cost-benefit analysis ofcyberterrorism.Studies in conflict & terrorism, 2004, 27.5, p387.

[xv].United Nations, General Assembly, S/RES/2178 (2014). Available at:https://www.undocs.org/en/S/RES/2178%20(2014), accessed19 June 2021.

[xvi]. Council of Europe, Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Available at:https://rm.coe.int/168047c5e,accessed20 June 2021.

[xvii].United Nations, General Assembly, S/RES/1373(2001), Available at: https://undocs.org/en/S/RES/1373(2001), accessed23 June2021.

عنـــوان المداخـــلة : " دور التطور التكنولوجي في أنسنة الأنظمة العقابية–السوار الالكتروني نموذجا–"

The role of Technological Development in The humanization of The Punitive Systems-Electronic Bracelet as a Model-

❖ **المحور الثالث: دور التكنولوجية الحديثة في تطوير آلية تطبيق العقوبات.**

بكـوش محـــمد أمـين

أستـــاذ محاضر قســـم "ب"

بجامعـــة إبـــن خلـــدون تيارت-الجزائر-

كلـية الحقـــوق والعلـــوم السياسية/قســـم: الحقـــوق.

الإنتماء: مخبر البحث في تشريعات حماية النظام البيئي.

كلية الحقوق والعلوم السياسية بجامعة إبن خلدون تيارت-الجزائر-

البريـــد الإلكـــتروني:mohamed.amine.bekkouche@univ-tiaret.dz

مقدمة:

عرف الفكر الإنساني في العصر الحديث تطورات هائلة شملت شتى المعارف والعلوم الإنسانية،ونتيجة هذه التطورات إرتقت الإنسانية في أفكارها ومعيشتها، وإكتشف الفرد آفاق جديدة فيحياته المادية وعلاقاته الاجتماعية، وقد إنعكس كل ذلك على النظام القانوني بصفة عامة، وعلى فكرة العقوبة بوجه خاص، حيث تغير السياسية الجنائية من فكرة الردع إلى فكرة الإصلاح.

فلقدشملت هاته التطورات جميع المجالات والميادينخاصة الميدان التكنولوجي، وبظهور الوسائط الإلكترونية وبقدر ما سهلت الحياة وإختصرت الوقت والجهد وما قدمته للبشرية من تسهيلات وخدمات إيجابية غيرت نمط الحياة للمجتمعات وساهمت في تطورها ورقيها، بقدر ما أثرت إيجابا على تطور المفهوم الحديث للعقوبة، فلقد وجدت آليات جديدة لتنفيذ العقوبة من بينها نظام السوار الإلكتروني كنظام مستحدث لتكيف العقوبة السالبة للحرية في التشريع الجزائري.

يعد إجراء الوضع تحت المراقبة الإلكترونية من الموضوعات المستحدثة في مجال العدالة الجنائية المعاصرة، ويتمثل في توظيف التكنولوجيا الحديثة في مجال السجون بإعادة إدماج المحكوم عليهم في المجتمع مرة أخرى من خلال منحهم الفرصة في الانخراط في المجتمع وذلك تحت رقابة أجهزة العدالة الجنائية، وهو الأمر الذي دفع التشريعات العقابية الحديثة إلى الحد من العقوبات السالبة للحرية والتقليل منها والعمل على الإستفادة من التكنولوجيا الرقمية والتوجه نحو معاملة المجرمين معاملة إنسانية مع مساعدتهم في الوقت ذاته،العمل على تحقيق الهدف من وجود العقوبة، وهو نفس التوجه الذي أخذ به المشرع الجزائري بموجب

القانون رقم: 18-01[1] وذلك في إطار تجسيد و إحترام حقوق الإنسان ومبادئ المحاكمة العادلة وحماية الحريات الفردية.

تكمن أهمية البحث في هذا الموضوع في معرفة دور التكنولوجيا من خلال إستحداث نظام المراقبة الإلكترونية في توفيرالأنسنة داخل قطاع السجون والحفاظ على حقوق المحبوسين وإحترام مبادئ العدالة، وفيالوقت ذاته تحقيق الإصلاح والتأهيل للمحبوسين وعصرنة قطاع العدالة وعليه ومن خلال ما سبق ارتئيناطرحالإشكالية التالية:

هل يمكن أن يحل نظام المراقبة الالكترونية محل العقوبة السالبة للحرية وما مدى نجاعة هذه التكنولوجيا في تحقيق أهدافالعقوبة والحفاظ على إنسانية المحكوم عليه؟

وللإجابة عن هاته الاشكالية قسمنا مداخلتنا إلى مبحثين:الأولحولماهيةنظام المراقبة الإلكترونية عنطريقالسوار الإلكتروني، والثاني : تناولنا فيه شروط وأثارالإستفادةمنهذا النظام.

المبحث الأول : ماهية نظام المراقبة الإلكترونية عن طريق السوار الإلكتروني.

يعد نظام الوضع تحت الرقابة الإلكترونية وسيلة بديلة للعقوبة السالبة للحرية قصيرة المدة وأهم ما أفرزه التقدم التكنولوجي في مجال العقابي والذي إنعكس بدوره على السياسة العقابية في معظم الأنظمة العقابية المعاصرة، التي من بينها النظام العقابي الجزائري الذي حاول مواكبة التطورات المتسارعة التي تشهدها السياسة العقابية الحديثة في مجال محاربة الجريمة وإصلاح المجرمين.

ففي مجال إصلاح قطاع العدالة وعصرنتهاعنطريق إدراج التكنولوجيات الحديثة للإعلام والإتصال في مجال الإجراءات القضائية خطا المشرع الجزائري خطوة هامة بإعتماد نظام المراقبة الإلكترونية للأشخاص المحكوم عليهم نهائيا، بتمكينهم من قضاء كل العقوبة أو جزء منها خارجأسوار المؤسسة العقابية بما يضمن إنسانيتهم كبشر.[2]

و لتحديد مفهوم المراقبة القضائية بواسطة السوار الإلكتروني يقتضي بداية التعرض لمفهوم المراقبة الإلكترونية ثم تعريف السوار الإلكتروني كآلية لتنفيذ نظام المراقبة الإلكترونية وذلك على النحو الآتي:

[1]- القانون رقم: 18-01 المؤرخ في: 30 يناير 2018 المتمم للقانون رقم: 05-04 المؤرخ في: 06 فبراير 2005 والمتضمن قانون تنظيم السجون واعادة الإدماج الاجتماعي للمحبوسين، ج.ر عدد: 05 الصادرة بتاريخ: 30 يناير 2018، ص 10 .

[2]- المادة 150 مكرر من نفس القانون.

المطلب الاول: مفهوم المراقبة الإلكترونية.

لقد عرف البعض المراقبة الالكترونية على أنها: " ترك المحكوم عليه بعقوبة سالبة حرا طليقا مع إخضاعه لعدة إلتزامات ومراقبته إلكترونيا من خلال إشارات يتم التعرف عليها عن طريق سوار إلكتروني يوضع في المعصم أو قدم الخاضع للمراقبة في النطاق الجغرافي المحدد له"[1]، وعرفها بعض الفقه الفرنسي على أنها : " إستخدام وسائط إلكترونية للتأكد من وجود الخاضع لها من خلال فترة محددة في الزمان والمكان السابق الإتفاق عليها بين هذا الأخير والسلطة القضائية الآمرة بها.[2]

ومن التعريفات التشريعية نجد تعريف التشريع الفرنسي الذي عرفها علىأنها : "فرض إلتزامات على شخص محكوم عليه بعدم مغادرة منزله، أو محل إقامته، أو أي مكان أخر محدد، خارج الأوقات التي يحددها القاضي المختص، بحيث يتم متابعة مدى إلتزامه بالواجبات المفروضة عليه الكترونيا، و يرد تحديد الأماكن و الأوقات في متن الحكم أو الأمر أو القرار بصورة عامة بناءا على إعتبارات متعلقة أساسا بممارسة نشاط مهني، أو متابعة الدراسة الجامعية،أو التكوين المهني، أو نشاط يساعده في تحقيق الإدماج الإجتماعي، أو المشاركة في الحياة العائلية، أو متابعة علاج طبي، و بالمقابل يلتزم المدان بالإستجابة بكل الإلتزامات الواقعة على عاتقه، خاصة إستدعاءات السلطات العمومية التي يحددها القاضي المختص ".[3]

أما المشرع الجزائري فقد عرفها بموجب المادة 150مكرر من القانون رقم: 18-01 المتمم للقانون رقم:05-04والمتضمن قانون تنظيم السجون واعادة الإدماج الإجتماعي للمحبوسين على أنه:" إجراء يسمح بقضاء المحكوم عليه كل العقوبة أو جزء منها خارج المؤسسة العقابية من خلال حمل الشخص المحكوم عليه طيلة المدة المحددة في المادة 150مكرر01 من نفس القانون لسوار إلكتروني يسمح بمعرفة مكان تواجده في مكان تحديد الإقامة المبين في مقرر الوضع الصادر عن قاضي تطبيق العقوبات" .

---

[1]-قتال جمال/عقباوي سلمى، بدائل العقوبات السالبة للحرية- السوار الالكتروني-، مجلة الدراسات و البحوث القانونية، المجلد:04 العدد:02/جانفي2022، ص:184 ، مقال منشور على منصة المجلات العلمية الجزائرية، رابط المقال :
https://www.asjp.cerist.dz/en/downArticle/461/4/2/107368

[2]-عبد الحليم موساوي/صورية بورباية، السوار الالكتروني بديل العقوبة السالبة للحرية في التشريع الجزائري والتشريع المقارن، مقال منشور على منصة المجلات العلمية الجزائرية، مجلة الفكر القانوني والسياسي المجلد السادس العدد الأول 2022ص:1318، رابط المقال:https://www.asjp.cerist.dz/en/article/188274/

[3]-Art 132-26-2 du code pénal français;Le placement sous surveillance électronique emporte, pour le condamné, interdiction de s'absenter de son domicile ou de tout autre lieu désigné par le juge de l'application des peines en dehors des périodes fixées par celui-ci. Les périodes et les lieux sont fixés en tenant compte: de l'exercice d'une activité professionnelle par le condamné; du fait qu'il suit un enseignement ou une formation, effectue un stage ou occupe un emploi temporaire en vue de son insertion sociale; de sa participation à la vie de famille; de la prescription d'un traitement médical.Le placement sous surveillance électronique emporte également pour le condamné l'obligation de répondre aux convocations de toute autorité publique désignée par le juge de l'application des peines. Abrogé par LOI n°2019-222 du 23 mars 2019 - art74.

المطلب الثاني:مفهوم السوار الإلكتروني.

يتكون السوار الإلكتروني من شريحة نظام تتبع المواقع، وكذا من بطارية ويستعين مكتب المراقبة بلوحة تحكم معلوماتية تسمح بمراقبة مختلف تحركات حامله، إذ يشترط على حامل السوار الإلكتروني، عدم مغادرة الحدودالإقليمية المحددة له، ويتم تسييره بواسطة برنامج إعلام آلي يربط بين المواقيت والمواقع الجغرافية المعينةلحامله في مقرر الوضع، إذ يمكن تحديد مكان تواجد وتحركات الشخص الذي يضع السوار بدقة عالية وفي حالة تجاوز الشخص الذي يضع هذا السوار على الكاحل للإطار الجغرافي او الزمني المحدد له من قبل السلطة القضائية، تُعطى إشارة تنبيه لقاعة المراقبة المتواجدة على مستوى مركز إعادة التربية وتوجه له إنذاراً أولياً كتنبيه للامتثال وفي حالة الاصرار على المخالفة تتخذ بشأنه احكام المادة 150 مكرر13 التي نصى على انه :" في حالة إلغاء مقرر الوضع تحت المراقبة الإلكترونية، ينفذ المعني بقية العقوبة المحكوم بها عليه داخل المؤسسة العقابية بعد اقتطاع مدة الوضع تحت المراقبة الإلكترونية".

كما أجازت المادة 150 مكرر14 في حالة تملص من المراقبة الإلكترونية، لا سيما عن طريق نزع أو تعطيل الآلية الإلكترونية للمراقبة، يتعرض المستفيد إلى العقوبات المقررة لجريمة الهروب المنصوص عليها في قانون العقوبات.

المبحث الثاني: النظام القانوني للسوار الالكتروني.

يعتبر نظام السوار الإلكتروني أحد الأساليب الحديثة لتنفيذ العقوبة السالبة للحرية قصيرة المدة خارج السجن–أي في وسط مفتوح – بصورة ما يعبر عنه "بالسجن في البيت،"ويقوم هذا النظام على السماح للمحكوم عليه بالبقاء في منزله،مع تحديد تحركاته ومراقبته بواسطة جهاز يشبه الساعة أو السوار مثبت في معصمه أو في أسفل قدمه،ومن هنا جاءت تسمية هذا الأسلوب(السوار الإلكتروني)،وهو الوصف الذي يعتمده بعض فقهاء علم العقاب،كما تعددت المفاهيم والمصطلحات التي أطلقت على نظام المراقبة الإلكترونية،وإن كانت في مجملها تصب في هدف واحد،حيث عبر عنه الفقه الانجليزي بعبارة الإسورة الإلكترونية،بينما إستعمل البعض الآخر مصطلح الرقابة الالكترونية.[1]

حيث يعتبر– السوار الإلكتروني–أسلوب من أساليب المعاملة العقابية التي تبناها المشرع الجزائري بموجب القانون رقم:18–01،المؤرخ في:30يناير2018والمعدل والمتمم لقانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين وذلك في الباب السادس المعنون بـ:"**تكييف العقوبة**" في الفصل الرابع منه

[1] – مهداوي محمد صالح/اسود ياسين،نظام المراقبة الالكترونية في التشريع الجزائري، مجلة دائرة البحوث والدراسات والقانونية والسياسية المجلد:05العدد: 03/ سنة2021، ص:08، مقال منشور على منصة المجلات العلمية الجزائري،رابط المقال:
https://www.asjp.cerist.dz/en/downArticle/693/5/3/168329

بعنوان:"**الوضع تحت المراقبة الإلكترونية**" تحديدا في المواد من:(150مكرر إلى 150مكرر14)، وذلك كأليةمستحدثة لإصلاح وتأهيل المحبوسين وإعادة إدماجهم في المجتمع والتخفيف من ظاهرة التكدس والإزدحام الذي تشهده المؤسسات العقابية عبر الوطنبما في ذلك من ترشيد للنفقات والحد من العودة الى الإجرام.

المطلب الأول: شروط واجراءات تطبيق السوار الإلكتروني كإجراء بديل للعقوبة السالبة للحرية في التشريع الجزائري.

يتم تطبيق نظام السوار الإلكتروني وفقا لإجراءات قانونية، ويعتمد ذلك على توافر مجموعة من الشروط للإستفادة من هذا النظام كإجراء بديل للعقوبة السالبة للحرية، سنحاول تفصيلها كالآتي:

الفرع الاول : الشروط القانونية للإستفادة من نظام السوار الإلكتروني.

يشترط المشرع الجزائري مجموعة من الشروط القانونية التي يتعين توافرها لإصدار أمر الوضع تحت المراقبة ونجد أن هناك شروط ذاتية تتعلق بالأشخاص المحكوم عليهم وشروط موضوعية ترتبط بالعقوبة المطبقة عليهم، إضافة إلى الشروط المادية لتقرير الوضع تحت السوار الالكتروني.

أولا:الشروطالمتعلقة بالعقوبة المحكوم بها.

يشترط لتطبيق نظام السوار الإلكتروني كشرط أساسي أن تكون العقوبة المحكوم بها سالبة للحرية، فلا مجال لتطبيقه علىالعقوبات أخرى كالغرامة، كما يشترط في هاته العقوبة أن لا تتجاوز مدتها ثلاث سنوات نافذة، كما يمكن تطبيق هذا الإجراء في حالة ما إذا كانت العقوبة المتبقية لا تتجاوز هذه المدة، بحيث يصدر قاضي تطبيق العقوبات مقرر الوضع تحت المراقبة الإلكترونية، بعد أخذ رأي النيابة العامة، كما يأخذ رأي لجنة تطبيق العقوبات بالنسبة للمحبوسين.[1]

ثانيا: الشروط المتعلقة بالأشخاص المحكوم عليهم.

ينحصر تطبيق السوار الالكترونيوفقا للتشريع الجزائري على الأشخاص الطبيعية دون غيرهم، إذ

يستحيل تطبيقه على الأشخاص المعنوية نظرا لطبيعته فهو عبارة عن جهاز إلكتروني يوضع على يد أو ساق المحكوم عليه، وفي هذا الصدد نميز بين فئتين:

[1]- المادة 150 مكرر01 من القانون رقم: 18-01 المؤرخ في: 30 يناير 2018 المتمم للقانون رقم: 05-04 المؤرخ في: 06 فبراير 2005 والمتضمن قانون تنظيم السجون واعادة الإدماج الاجتماعي للمحبوسين، المرجع السابق.

أ) بالنسبة للبالغين:

حسب المادة 150 مكرر02 من قانون تنظيم السجون الجزائري، فأنه يمكن وضع السوار الالكتروني كإجراء بديل للعقوبة السالبة للحرية قصيرة المدة، لكل شخص بلغ سن تسعة عشرة كاملة،بشرط ألا يمس ذلك بصحته وسلامته، وهو بذلك يشملالجنسين معا(النساء والرجال).

ب) بالنسبة للقصر:

نصت المادة 150 مكرر02 من نفس القانون على أنه لا يمكن أن يستفيد القاصر الذي لم يبلغ سن الرشد بعد من نظام الرقابة الإلكترونية إلا بعد موافقة ممثله القانوني.

كما إستلزم المشرع لتطبيق هذا النظام الموافقة الصريحة للمحكوم عليه وذلك في حالة تطبيق هذا النظام من جانب القاضي أو بناءا على طلب النيابة العامة.

ثالثا: شروط المادية أو الفنية.

يشترط للإستفادة من نظام الوضع تحت المراقبة الإلكترونية توافر بعض الشروط المادية[1] :

- **أن يثبت المعني مقر سكن أو إقامة ثابتاومزود بخط هاتفي ثابت:**

يشترط المشرع أن يكون الخاضع للمراقبة محل إقامة مستقر وهو ما يستشف من أحكام المادة 150مكرر3وقد يحدد هذا المحل من طرف قاضي تطبيق العقوبات سواء كان خاصا بالمحكوم عليه أو غيره.

كما يجب أن يكون محل الإقامة مزود بخط هاتفي ثابت ويجب هنا أن يكون مهيأ لأداء الخدمة المناطة به أداؤها، أي استقبال الإتصالات الهاتفية المتعلقة بالمراقبة الإلكترونية.[2]

- **أن لا يضر حمل السوار بصحة المعني:**

قبل اللجوء لنظام المراقبة لابد من التأكد من أنه لا يضر بصحة المعني وذلك بعرضه على الطبيب المختص.

- **أن يسدد المعني مبالغ الغرامات المحكوم بها عليه:**

وذلك وفقا لقدرته المالية للخزينة العامة عقب /أو بعد الحكم عليه بالإدانة.

[1]- المادة 150 مكرر03 من القانون رقم: 18-01 المؤرخ في: 30 يناير 2018 المتمم للقانون رقم: 05-04 المؤرخ في: 06 فبراير 2005 والمتضمن قانون تنظيم السجون واعادة الإدماج الاجتماعي للمحبوسين، المرجع السابق.

[2]- المادة 150 مكرر08 من القانون رقم: 18-01، المرجع نفسه.

- **الأخذ بعين الاعتبار الوضعية العائلية للمعني أو متابعته لعلاج طبي أو نشاط مهني أو دراسي أو تكويني أو إذا أظهر ضمانات جدية للاستقامة:**

يستفيد من هذا النظام المراقبة المحكوم عليهم الذين تبرر أوضاعهم فرض هذه الوسيلة وقد يتمثل هذا المبرر في ممارسة المحكوم عليه لنشاط مهني أو متابعته لدراسة أو لضرورة خضوع المحكوم عليه لعلاج طبي[1].

الفرع الثاني: إجراءات تقرير نظام السوار الإلكتروني.

يتم تقرير نظام السوار الإلكتروني وفقا إجراءات قانونية محددة لإصداره، ويترتب على إصدار مقرره عدة آثار وهو ما سنتطرق له في هذا الفرع.

أولا: الجهة القضائية المختصة بتقرير نظام السوار الإلكتروني.

بالرجوع الى نص المادة 150 مكرر01 فإن الجهة التي يصدر عنها تقرير الوضع تحت المراقبة الالكترونية هي قاضي تطبيق العقوبات، ويكون ذلك بشكل تلقائي أو بناء على طلب المحكوم عليه شخصيا، أو عن طريق محاميه، سواء في الحالة ما إذا كانت العقوبة المقرر لا تتجاوز ثلاث سنوات أو كانت العقوبة المتبقية لا تتجاوز هذه المدة، وذلك بإلزامه بالبقاء في منزله أو في مكان معين خارج الفترات المحددة، كما يجوز لقاضي تطبيق العقوبات إخضاع الشخص الحامل للسوار الإلكتروني بتدبير أو أكثر كممارسة نشاط مهني أو متابعة تعليم أو تكوين مهني، وعدم إرتياد بعض الأماكن، وعدم الإجتماع ببعض المحكوم عليهم كالشركاء والفاعليين الأصليين في الجريمة.[2]

أ) صدور مقرر الوضع تلقائيا:

يصدر قاضي تطبيق العقوبات مقرر الوضع تحت المراقبة الالكترونية من تلقاء نفسه، غير أنه لا يمكن تقرير ذلك إلا بموافقة المحكوم عليه أو محاميه أو وليه إذا كان قاصر.

[1] – بوشربي مريم، المراقبة الإلكترونية كأسلوب حديث للمعاملة العقابية "في ظل القانون رقم:18-01 المعدل لقانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، مجلة دائرة البحوث والدراسات القانونيةوالسياسية – مخبر المؤسسات الدستورية والنظم السياسية العدد السادس جانفي 2019،مقال منشور بمنصة المجلات العلمية الجزائرية، رابط المقال:https://www.asjp.cerist.dz/en/downArticle/693/3/6/132154

[2] – المادة 150 مكرر06 من القانون رقم: 18-01 المؤرخ في: 30 يناير 2018 المتمم للقانون رقم: 05-04 المؤرخ في: 06 فبراير 2005 والمتضمن قانون تنظيم السجون واعادة الإدماج الاجتماعي للمحبوسين، المرجع السابق.

ب) صدور مقرر الوضع من قاضي تطبيق العقوبات بناء على طلب المحكوم عليها/أو محاميه:

يقدم طلب الإستفادة إلى قاضي تطبيق العقوبات لمكان إقامة المحكوم عليه أو المكان الذي يوجد به مقرالمؤسسة العقابية المحبوس بها المعنيوعند تقديم الطلب يؤجل تنفيذ العقوبة السالبة للحرية بالنسبة للمحكوم عليهم غير المحبوسين إلى غاية الفصل النهائي في طلب المحكوم عليه، على أن يفصل قاضي تطبيق العقوبات في الطلب في أجل(10) أيام من إخطاره بمقرر غير قابل لأي طعن، غير أنه يحق للمحكوم عليه تقديم طلب جديد بعد مضي (06) ستة أشهر من تاريخ رفض طلبه.[1]

ثانيا: الجهة المختصة بتنفيذ مقرر الإستفادة من نظام السوار الإلكتروني.

تتولي المصالح الخارجية لإدارة السجون المكلفة بإعادة الإدماج الإجتماعي للمحبوسين بمراقبة تنفيذ الوضع تحت المراقبة وذلك تحت إشراف قاضي تطبيق العقوبات عن بعد وعن طريق الزيارات الميدانية ومراقبته عن طريق الهاتف، ولها أن تبلغ قاضي تطبيق العقوبات فورا، بكل خرق قد يقع لمواقيت الوضع تحت المراقبة الإلكترونية.

ويترتب عن الوضع تحت المراقبة الإلكترونية طبقا لنص المادة150 مكرر05 من قانون تنظيم السجون الجزائريإخضاع المعني لمجموعة من الإلتزامات من بينها :عدم مغادرة المعني لمنزله أو للمكان الذي يعينه قاضي تطبيق العقوبات خارج الفترات المحددة في مقرر الوضع، وتحدد هذه الأوقات والأماكن مع مراعاة ممارسة المحكوم عليه لنشاط مهني ومتابعة لدراسة أو تكوين أو تربص أو شغله وظيفة أو متابعة لعلاج، كما

يمكن لقاضي تطبيق العقوبات إخضاع الشخص الموضوع تحت المراقبة الالكترونية لتدبير أو أكثر من التدابير المحددة في المادة 150 مكرر 06 من نفس القانون[2].

المطلب الثاني: الآثار المترتبة على الإستفادة من نظام السوار الإلكتروني.

يترتب على الإستفادة من نظام السوار الإلكتروني عدة أثار، نتناولها كالآتي:

الفرع الأول: خضوع المستفيد للإلتزامات المفروضة عليه.

يمكن إجمال الإلتزامات التي يخضع لها المحكوم عليه حسب نص المادة 150 مكرر05 ومكرر06

[1]- المادة 150 مكرر04 من القانون رقم: 18-01، المرجع السابق.

[2]- القانون رقم: 05-04 المؤرخ في: 06 فبراير 2005 والمتضمن قانون تنظيم السجون واعادة الإدماج الاجتماعي للمحبوسين، المعدل والمتمم.

فيما يلي:

- عدم مغادرة المحكوم عليه منزله أو المكان الذي يعينه قاضي تطبيق العقوبات، وذلك خلال المدة الزمنية المحددة في مقرر الوضع، وتؤخذ بعين الإعتبار الأوقات والأماكن التي يمارس فيها مهنة أو لمتابعة دراسة أو تكوين أو تربص أو متابعة العلاج.
- عدم الإجتماع ببعض المحكوم عليهم، بما في ذلك الفاعلين الأصليين أو الشركاء في الجريمة.
- إلزام المحكوم عليه بعدم الإجتماع ببعض الأشخاص لا سيما القصر والضحايا.
- إلزام المحكوم عليه بالإستجابة لإستدعاءات قاضي تطبيق العقوبات أو الجهة المختصة التي يعينها كمصالح الأمن.

كما يجوز لقاضي تطبيق العقوبات تعديل أو إلغاء التزامات الوضع تحت المراقبة الالكترونية سواء من تلقاء نفسه أو بطلب من المحكوم عليه.[1]

تنقضي المراقبة الإلكترونية كأي عقوبة بإستنفاذ المدة التي قررها قاضي تطبيق العقوباتوبقيام المحكوم عليه بأداء كافة الإلتزامات المفروضة عليه، حيث لا يجب أن تقل مدة المراقبة عن الفترة المحددة وقد يؤخذ بعين الاعتبار في هذه الحالة المدة التي قد يستفيد منها المحكوم عليه من إجراء العفو عن العقوبة حيث تقتطع مدة العقوبة التي تم العفو عنها من مدة المراقبة الإلكترونية.

الفرع الثاني: إخلال المستفيدبالإلتزاماتالمفروضة عليه وحالات إلغائها.

يمكن لقاضي تطبيق العقوبات تلقائيا من نفسه أو بناءا على سماع المعني إلغاء الوضع تحت المراقبة الإلكترونية في حالات التالية:[2]

- ❖ عدم احترام المحكوم عليه للالتزامات المفروضة عليه دون تقديم مبررات مشروعة، وذلك عن طريق التقارير الدورية التي تصل قاضي تطبيق العقوبات عن طريق المصالح الخارجية لإدارة السجون المكلفة بإعادة الإدماج الاجتماعي للمحبوسين، والمكلفة بالمتابعة عن بعد وعن طريق الزيارات الميدانية عن طريق الهاتف.
- ❖ في حالة إدانة المحكوم عليه بعقوبة أخرى، والملاحظ هنا أن المشرع لم يحدد نوع العقوبة الجديدة حتوإن كانت غرامة مالية.

[1]-المادة 150 مكرر09 من القانون رقم: 18-01، المرجع السابق.

[2]- المادة 150 مكرر10، المرجع نفسه.

- ❖ في حالة طلب المحكوم عليه.
- ❖ في حالة الطلب المقدم من النائب العام إلى لجنة تكييف العقوبات، إذا كان الوضع تحت المراقبة الالكترونية يمس بالأمن والنظام العام.[1]

وقد أجاز القانون للشخص المعني التظلم ضد إلغاء مقرر الوضع تحت المراقبة الإلكترونية أمام لجنة تكييف العقوبات والتي يجب عليها الفصل فيه في أجل(15) خمسة عشر يوما من تاريخ إخطارها.[2]

وفي حالة طلب النائب العام إلغائه لمبررات تتعلق بالأمن والنظام العام، هنا وجب على لجنة تكييف العقوبات الفصل في الطلب بمقرر غير قابل لأي طعن وذلك في أجل أقصاه (10) عشر أيام من تاريخ إخطارها.[3]

كما أن المشرع الجزائري أكد على تعرض الشخص الذي يتملص من المراقبة الإلكترونية لاسيما عن طريق نزع أو تعطيل الآلة الإلكترونية للمراقبة إلى العقوبات المقررة بجريمة الهروب المنصوص عليها في المواد 188إلى 194من قانون العقوبات.

ويترتب في كل الأحوال على إلغاء مقررالوضع تحت نظام المراقبة تنفيذ المعني للعقوبة الأصلية المحكوم بها عليه داخل المؤسسة العقابية بعد إقتطاع مدة الوضع تحت المراقبة الإلكترونية.[4]

خاتمة:

وفي ختام مداخلتنا يمكننا القول بأن المشرع الجزائري قد خطى خطوة كبيرة في مجال محاربة الجريمة وإصلاح المجرمين، من خلال تبنيه لبعض الآليات الحديثة في المجال العقابي لمواصلة عصرنة قطاع العدالة وتعزيز الخدمات بإدخال تكنولوجيات الإعلام الحديث، وتجلى ذلك من خلال بعض التعديلات التي عرفها قانون تنظيم السجون من أجل ضمان الحريات المكرسة بالمواثيق الدولية والدستور، وهوما يؤكد محاولته للحاق بالتطورات السريعة التي تعرفها السياسة العقابية الحديثة في هذا المجال، تعزيزا لحقوق الأفراد وحرياتهم، لا سيما قرينة البراءة ومبادئ المحاكمة العادلة، بإستحداث نظام الوضع تحت المراقبة الإلكترونية أو ما يسمى بالسوار الإلكتروني ليكون إجراء جديدا من إجراءات البديلةلعقوبة الحبس قصيرة المدة، غير أن الواقع العملي أسفر عن

[1] – المادة 150 مكرر12، المرجع السابق.
[2] – المادة 150 مكرر11، المرجع نفسه.
[3] – المادة 150 مكرر2/12،نفس المرجع.
[4] – المادة 150 مكرر13، المرجع نفسه.

ضعف البنية التحتية اللازمة للعمل بنظام المراقبة الإلكترونية وكذا الكوادر البشرية المؤهلة والمتخصصة.

وبالإضافة إلى ما يمكن أن ينطوي عليه نظام السوار الإلكتروني من مساس بالحقوق الشخصية للمحكوم عليه مثل التدخل في حياته الخاصة فقد حرص المشرع على إحاطة هذا النظام بالضمانات القانونية الكافية لضمان إنسانية المحكوم عليهم والموضوعينتحت نظام السوار الإلكتروني في جميع مراحل التنفيذ.

الإقتراحات والتوصيات:

رغم كل الإنتقادات الموجهة لنظام السوار الإلكتروني كونه لا يحقق الهدف المرجو من العقوبة من حيث تحقيق الردع بنوعيه،إلا أن هذا النظام يبقى الأصلح للمحكوم عليهم مقارنة بالآثار السلبية التي يحدثها التنفيذ التقليدي للعقوبة السالبة للحرية،وبالمقابل يساهم نظام السوار الإلكتروني في إصلاح المحكوم عليهمن خلال إبعاده عن البيئة الاجرامية من جهة،كما أنه يشكل ضمان من ضمانات حقوق الإنسان الحديثة من جهة أخرى.

غير أنه وفي رأئينا يجدربالمشرع الجزائريمراجعة منظومتنا القانونية وجعل هذا النظام عقوبة بديلة كعقوبة العمل للنفع العام وليس مجرد إجراء من إجراءات تكيف العقوبة لما فيه من مزايا إقتصادية وإجتماعية تساعد فئات كبيرة من الجانحين في إستمرار روابطهم الإجتماعية مع عائلاتهم ومحيطهم الخارجي وتنسجم مع متطلبات برامج إعادةالإدماج الاجتماعي وتجنبهم مخاطرالعود للجريمة وتساعد على الحد من الاكتظاظ في السجون وترشيد النفقات التي تتحملها الدولة في إصلاح المجرمين.

قائمة المصادر والمراجع:

أ- النصوص القانونية :

أولا: الوطنية.

1) القانون رقم: 05-04 المؤرخ في: 06 فبراير 2005 والمتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، المعدل والمتمم.
2) القانونرقم: 18-01 المؤرخفي: 30 يناير 2018 المتمممللقانونرقم: 05-04 المؤرخفي: 06 فبراير 2005 والمتضمنقانونتنظيمالسجونواعادةالإدماجالاجتماعيللمحبوسين،ج.رعدد: 05 الصادرةبتاريخ: 30 يناير 2018.

ثانيا: الأجنبية.

1) LOI n°2019-222 du 23 mars 2019 - art74du code pénal français ، https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417412

ب-المجلات العلمية:

1) بوشربي مريم، المراقبة الإلكترونية كأسلوب حديث للمعاملة العقابية "في ظل القانون رقم:18-01 المعدل لقانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، مجلة دائرة البحوث والدراسات القانونيةوالسياسية – مخبر المؤسسات الدستورية والنظم السياسية العدد السادس جانفي 2019،مقال منشور بمنصة المجلات العلمية الجزائرية، رابط المقال:

https://www.asjp.cerist.dz/en/downArticle/693/3/6/132154

2) مهداوي محمد صالح/اسود ياسين، نظام المراقبة الالكترونية في التشريع الجزائري، مجلة دائرة البحوث والدراسات والقانونية والسياسية المجلد:05 العدد: 03/ سنة2021، ص:08، مقال منشور على منصة المجلات العلمية الجزائري، رابط المقال:

https://www.asjp.cerist.dz/en/downArticle/693/5/3/168329

3) عبد الحليم موساوي/صورية بورباية، السوار الالكتروني بديل العقوبة السالبة للحرية في التشريع الجزائري والتشريع المقارن، مقال منشور على منصة المجلات العلمية الجزائرية، مجلة الفكر القانوني والسياسي المجلد السادس العدد الأول 2022ص :1318، رابط المقال:

https://www.asjp.cerist.dz/en/article/188274/

4) قتال جمال/عقباوي سلمى، بدائل العقوبات السالبة للحرية – السوار الالكتروني-، مجلة الدراسات و البحوث القانونية، المجلد:04 العدد:02/جانفي2022، ص:184 ، مقال منشور على منصة المجلات العلمية الجزائرية، رابط المقال :

https://www.asjp.cerist.dz/en/downArticle/461/4/2/107368

لشهب نادية ليلى . أستاذة مؤقتة – كلية الحقوق – جامعة الجزائر 1

Email : lechehebnadiadroit@gmail.com

انتهاك الخصوصية المعلوماتية للمستخدم عبر المنصات التعليمية الافتراضية: ما بين الحماية التقنية والمسؤولية جنائية

ضمن الملتقى الدولي الموسوم بـ: القانون الجنائي في ظل التطور التكنولوجي – إشكالات ومعالجات –

المحور الأول: التطور التكنولوجي والظاهرة الإجرامية/ التطور التكنولوجي كمتطلب لتحقيق المعرفة

الملخص:

في غضون السنوات الأخيرة، وبسبب بعض النجاحات البارزة وإمكاناته الرائدة، انتقل الذكاء الاصطناعي من منطقة البحث الأكاديمي إلى طليعة المناقشات العامة، بما في ذلك المناقشات على مستوى أكبر الدول. ومن المرجح على مدى السنوات القادمة، أن يتوسع استخدام الذكاء الاصطناعي والتقنيات الأخرى مثل الواقع المعزز (AR) والواقع الافتراضي (VR) والصور المجسمة وبيئات التعلم الافتراضية (VLE) في المدارس والكليات وكذلك في المنزل بشكل كبير.

وعلى مدار العقد الماضي، ازداد استخدام أدوات الذكاء الاصطناعي وتعزيزه بشكل كبير وقد زاد هذا الاستخدام بعد إغلاق المدارس والجامعات بسبب الجائحة التي أصابت العالم (كوفيد–19)، فلقد شهد التعليم عموما، والتعليم الجامعي خصوصا تطورا ملحوظا عبر العالم عامة والجزائر خاصة بعد هذه الجائحة، إذ نجد أن التعليم العالي قد تطور عن المفهوم التقليدي له سابقا، فلم يصبح يعتمد على التعليم الحضوري فقط، بل تطور إلى أكثر من ذلك فأصبح يتم عبر منصات تعليمة افتراضية تعمل ببرامج الذكاء الاصطناعي إلى جانب التعليم الحضوري، وأصبح الأستاذ الجامعي بإمكانه التواصل مع طلبته عبر الفضاء الافتراضي بشكل مباشر وسريع، ليس هذا فحسب بل أصبح أكثر من ذلك إذ يمكن اجتياز عدة اختبارات ويتم التواصل مباشرة.

غير أنه لا يخفى علينا إلى جانب محاسن هذا التطور، ظهور مساوئ تقابله خاصة في مجال انتهاك خصوصية المعلومات المنشورة عبر هذه المنصات التعليمية الافتراضية من سرقة علمية وانتهاك لخصوصية الأفراد العاملين عليها في ظل غياب أطر قانونية تحمي هكذا أنواع من هذا التعليم ، سوى تلك التي تقضي بحماية الملكية الفكرية في مجال الأمن السيبراني، والتي تقيم المسؤولية الجنائية في حالة انتهاك هذه الخصوصية.

مقـــدمة:

أدى التقدم العلمي والتقني في مجال الاتصالات وظهور شبكة الإنترنت[1] وتضخمها وامتدادها إلى أقاليم الدول تقريبا إلى تنوع وتعدد الأنشطة الإجرامية التي ترتكب من خلالها وعبر عدة دول.

[1] - نشأت هذه الشبكة في الولايات المتحدة الأمريكية، وكانت عبارة عن مشروع رعته وأنفقت عليه وكالة مشاريع البحوث المتقدمة في وزارة الدفاع الأمريكية Advance research project agency وذلك في ستينيات القرن الماضي وكان هدف الوزارة آنذاك بناء شبكة متماسكة يمكن أن تصمد في ظل ظروف صعبة كحدوث كارثة نووية وذلك لنقل المعلومات الأمنية والعسكرية في ظل الكارثة وذلك عبر إعداد سلسلة من الوصلات الحاسوبية تعرف

فالانترنت هو مجموعة شبكات وأجهزة الحاسب الالكتروني التي تتواجد في مختلف دول العالم والتي تتصل ببعضها ويجمع بينهما أنظمة الاتصالات الالكترونية التي تستخدم لنقل البيانات أو ما يدعى بنظام TCP/IP[1] أي نظام نقل المعلومات، فهو مجال أضاف نقلة نوعية في مجال التطور التكنولوجي ونقل المعلومات عبر العالم.

لكن هذا التطور السريع والمذهل في عالم تكنولوجية المعلوماتية، من وسائل اتصال وشبكات المعلومات وأجهزة الكمبيوتر وتطور التقنيات الحيوية، جعل البيئة الرقمية في شتى المجالات تعمل على تسهيل وتسريع نقل المعلومات ربحاً للوقت والجهد واقتصاداً للمال، لكن بالمقابل أصبحت هناك مخاطر واعتداءات إلكترونية تستهدف كيانات العالم الرقمي، فبات من الضروري مواكبة ذلك التطور من حيث التشريعات والتنظيمات والإجراءات التي بواسطتها يمكن التحكم في مراقبة وحماية المعلومات المتدفقة في الفضاءات الرقمية لاسيما منها ما يتعلق بالملكية الفكرية والمعلومات الشخصية، التي بدورها تطورت بتطور عصر المعلومات والمعرفة مع ظهور تكنولوجيات الإعلام و الاتصال، حيث صارت المعلومات ذات الطابع الفكري والأدبي و حتى الصناعي من الأمور التي ترد عليها الحقوق، وتُبرم بشأنها العقود، حيث أصبحت من الحقوق التي تستدعي أمنها وحمايتها من المخاطر والتهديدات التي تواجهها خاصة ما يتعلق منها بالجرائم الإلكترونية الماسة بالمعلومات الشخصية.

فقد تم نتيجة هذا التقدم تجريد الإنسان مما تبقى له من خصوصية[2]، حيث أصبح بمقدور الغير الوقوف على أدق تفاصيل الحياة الخاصة للفرد، سواء أكان برغبته أو بغير ذلك[3]، وقد صار بالإمكان مراقبة الشخص بالوسائل الإلكترونية بالصوت والصورة وتسجيل كل كلمة يلفظ بها أو فعل يقوم به، فلم يعد أحد بمنأى عن ذلك، لذلك استوجب استحداث طرق تقنية تعمل على الفضاء الالكتروني لها فعالية كبيرة في حماية هكذا معلومات.

باسم Arpanet لتضمن بذلك بقاء الاتصال فيما بين الأجهزة الأمنية والعسكرية المختلفة, وبعد ذلك في عام 1968 م أدخلت الوزارة أربع جامعات أمريكية عبر الشبكة لتبادل الأبحاث إلى أن غطت معظم الجامعات الأمريكية في عام 1972م إلى أن تخلت الوزارة عن الشبكة نهائيا في ثمانينيات القرن الماضي. بيل بول: انطلق مع الانترنت، ترجمة مركز التعريب والترجمة، الدار الجامعية للعلوم، بيروت، 1996م، ص 12.

Bob Northen and Cathy Smith: understanding business on the internet in week Hodder and Stoughton, 1997, p. 12-15.

[1] - Transmission Control Protocol/ Internet Protocol

[2] - أحمد عبد اللاه عبد الحميد عبد الرحيم المراغي، المسؤولية الجنائية لمقدمي خدمات الإنترنت – دراسة تحليلية خاصة لمسؤولية مزودي خدمات الاتصالات الإلكترونية -، مجلة حقوق حلوان للدراسات القانونية والاقتصادية،كلية الحقوق، جامعة حلوان، ص 110

https://mklse.journals.ekb.eg/article_229442_6f7598aebf816ee2c6667d10f83ae504.pdf

[3] - The Privacy Commissioner of Canada: Genetic testing and privacy, Minister of Supply and Services Canada, 1995, p. 2.

شار إليه لدي .د. أشرف توفيق شمس الدين: الجينات الوراثية والحماية الجنائية للحق في الخصوصية، دراسة مقارنة، ط 2، 2016، ص 3.

وبما أن هذه المعطيات لها قيمة كبيرة لدى الأفراد والمؤسسات، لذا ينبغي أن تكون دائماً بأمان وفي سرية، عملت كل الأجهزة على حمايتها وتسمى هذه العملية بأمن المعلومات، وهو نظام أمني واسع، قائم بذاته في كل الإدارات والمؤسسات العمومية والخاصة، يهدف إلى حماية المعلومات المتواجدة في الوثائق والسجلات المدنية والإدارية والتجارية وغيرها، المتضمنة للبيانات الشخصية أو الفكرية أو الأدبية للأشخاص الطبيعية والمعنوية، سواءاً كانت هذه البيانات رقمية أو غير رقمية، ويمكن لأمن المعلومات الاحتفاظ بها وتخزينها في أماكن متعددة كالمجلدات والمستندات والأقراص المضغوطة والصلبة وأجهزة الكمبيوتر الثابتة والمحمولة ووسائل التخزين الخاصة بشبكات الاتصال السحابية (Les-Claudes)، كما يمكن الوصول إليها بطرق مختلفة.[1]

هذا من جهة، ومن جهة أخرى نجد أن القانون الجنائي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا الحديثة، لاسيما نصوص القانون الجنائي والتي وضعت في عصر لم يكن فيه الانترنت قد ظهر، ولم تظهر بعد المشاكل القانونية الناشئة عن استخدامه، مما يفرض على رجال القانون التدخل لمكافحة الجرائم الناشئة عن استخدام الانترنت ومواجهة هذا النقص التشريعي، بإصدار تشريعات مستقلة للإحاطة بجميع جوانب الجرائم المتعلقة بالحاسوب والإنترنت.

ويقتصر مجال دراستنا هذه فقط على ماهية هذه المنصات التعليمية الافتراضية والانتهاكات التي تمس المعلومات المنشورة على المنصات التعليمة التابعة لوزارة التعليم العالي، حتى لا نضيع في هكذا مجال واسع، والذي لا يسعنا المقام هنا للتفصيل فيه بشكل كبير.

فقبل التطرق للطرق التي يتم بها انتهاك هذه الخصوصية، وجب المرور أولا على تحديد مفهوم هذه المنصات، وطبيعة المعلومات المنشورة على هكذا فضاءات، ثم الطرق التقنية لحماية هكذا معلومات، وصولا إلى المسؤولية الجنائية القائمة نتيجة انتهاك خصوصية هكذا معلومات شخصية.

لذلك سنقسم بحثنا هذا إلى ثلاث محاور وهي كالآتي،

المحور الأول: التعليم الالكتروني الجامعي عبر المنصة التعليمية عبر الخط(Moodel)

المحور الثاني:الوسائل التقنية لحماية المعلومات الشخصية المنشورة عبر هذه المنصات

[1]- منى عبد الله السرحان، منى عبد الله السرحان، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية، جامعة المنصورة، السعودية، 2020، ص13

المحور الثالث: المسؤولية الجنائية عن انتهاك خصوصية المعلومات الشخصية.

المحور الأول: ماهية التعليم عن بعد(التعليم الالكتروني)

أخذ مصطلح التعلم عن بعد شهرة واسعة، خاصة في أواخر الستينات من القرن العشرين، عندما بدأت اليونسكو في الاهتمام بتبني صيغ جديدة في ميدان تعليم الكبار والتربية المستمرة وحاولت تفسير الهيئة العلمية للتربية بالمراسلة (ICCE) إلى إسم جديد هو الهيئة العالمية للتربية من بعد (ICCDE)، وتتعدد مسميات التعلم عن بعد، فيطلق عليه أحيانا مصطلح "Distance Learning" أي التعلم عن بعد، وفي أحيان أخرى "Distance Teaching" التدريس عن بعد، وتارة أخرى التربية عن بعد "Distance Education"[1]، ولعل الاختلاف في تحديد تعريف موحد للتعليم عن بعد هو النشأة الحديثة له، إذ لم يعرف مصطلح التعليم عن بعد بشكل رسمي إلا حديثا وبالتحديد عام 1982[2]، وبذلك يعد مفهوم التعليم عن بعد مفهوما جديد ولا يوجد حتى الآن تعريف ثابت ومحدد له، وتتداخل المفاهيم الخاصة به فيما بينها ولم تستقر على تعريف محدد إن كانت جميعها ترتكز على بعد المسافة بين المعلم والمتعلم وتعدد الوسائل المستخدمة في عملية التعليم[3]،

لدى فالمفاهيم المتعددة للتعليم عن بعد مهما تباينت فيما بينها **(أولا)**، يبقى هدفها واحد وهو تمكين الطالب من تحصيل دروسه ومحاضراته من خلال منصات تعليمية افتراضية تعمل تحت وصاية وزارة التعليم العالي والبحث العلمي **(ثانيا)**

أولا:تعريف التعليم عن بعد

---

[1] – قودة عزيز، دهيمي زينب، التعليم عن بعد في الجامعة الجزائرية في ظل أزمة جائحة covid-19، مجلة الباحث في العلوم الإنسانية والاجتماعية، العدد 4، لسنة 2021، ص 464.

[2] – بوخدوني صبيحة، بن عاشور الزهرة، سياسة التعليم عن بعد في ظل جائحة كوفيد-19، دراسة تحليلية لتعليمات والقرارات الصادرة من وزارة التعليم العالي والبحث العلمي الجزائرية، مجلة مدارات سياسية، المجلد 04، العدد 04، 2020، ص62.

[3] – طارق عبد الرؤوف عامر، التعليم عن بعد والتعليم المفتوح، اليازوري العلمية للنشر والتوزيع، الأردن، بدون سنة نشر، ص 5.

التعليم عن بعد هو عبارة عن عملية تعليمية تربط فيها المعلمين والمتعلمين، بحيث تكون هناك بينهم مسافة جغرافيا (إدارة المكان)، ويديرون نشاطهم بطريقة مرنة ومستقلة تقريبا (إدارة الوقت)[1].

عرف التعليم عن بعد بأنه ذلك التعليم الإلكتروني الذي يقدم محتوى تعليمي عبر الوسائط المتعددة على الحاسوب وشبكات الاتصالات إلى المتعلم بشكل يتيح له إمكانية التفاعل النشط مع المحتوى المدرس والزملاء بصورة متزامنة أو غير متزامنة في الوقت والمكان والسرعة التي تناسب ظروف المتعلم وقدراته، وإدارة كافة فعاليات العملية العلمية والتعليمية ومتطلباتها بشكل الكتروني من خلال الأنظمة المتخصصة بذلك[2].

ويعد تعريف " هولمبرجHolmberg" والذي اقترحه في عام 1977 من أهم التعريفات وأبسطها والأكثر تداولا في دوريات التعلم عن بعد، إذ يقوا بأنه مصطلح يشمل كافة أساليب الدراسة وكل المراحل التعليمية التي لا تتمتع بالإشراف المباشر والمستمر من قبل معلمين يحضرون مع طلابهم داخل قاعات الدراسة التقليدية ولكن تخضع عملية التعليم لتخطيط وتنظيم وتوجيه من قبل مؤسسة تعليمية ومعلمين"[3].

كما يعرف التعليم الإلكتروني بأنه :" التعليم الذي يستهدف إيجاد بيئة تفاعلية غنية بالتطبيقات المعتمدة على تقنيات الحاسب الآلي والأنترنت وتمكن الطلبة المتمدرسين من الوصول إلى مصادر التعليم في أي وقت ومن أي مكان".[4]

هو أيضا تعلم يهدف لإيجاد بيئة تفاعلية غنية بالتطبيقات المعتمدة على تقنيات الحاسب الآلي (الانترنت)، وتمكن الطالب من الوصول إلى مصادر التعلم في أي وقت ومن أي مكان[5].

---

[1] – أكرور مريم، المرفق العمومي للتعليم العالي في الجزائر ووباء كوفيذ 19، حوليات جامعة الجزائر1، المجلد 34، عدد خاص: القانون وجائحة كوفيد 19، 2020، ص 232.

[2]– Watanabe, Keiko, 2005, A study on Needs for E– Learning– Through The Analysis of National Survey And Case studies, National Institute of Informatics, N 2 .

[3] – قودة عزيز، دهيمي زينب، مرجع سابق، ص 464.

[4] – أحمد العويد، محمد الحامد، التعليم الالكتروني في كلية الاتصالات والمعلومات بالرياض، ورقة عمل مقدمة إلى الندوة الأولى للتعليم الإلكتروني، مدارس الملك فيصل بالرياض، متوفر على الموقع : http://www.jeddahedu.gov.sa/

[5] – أمل محمد عبد الله البدو، فعالية المنصات التعليمية في تطبيق التعلم عن بعد بالمرحلة الثانوية بدولة الإمارات، أوراق المجلة الدولية للدراسات الأدبية والإنسانية، مخبر الموسوعة الجزائرية الميسرة، جامعة باتنة1، الجزائر ، المجلد 3، العدد1، 2021،

ويعرف التعليم الإلكتروني بأنه طريقة للتعليم باستخدام آليات الاتصال الحديثة من حاسوب وشبكات ووسائطه المتعددة من صوت وصورة، ورسومات، وآليات بحث، ومكتبات إلكترونية وكذلك بوابات الانترنت سواء كان عن بعد أو في الفصل الدراسي[1]، المهم المقصود هو استخدام التقنية بجميع أنواعها في إيصال المعلومة للمتعلم بأقصر وقت وأقل جهد وأكبر فائدة[2].

كما نجد عدة مصطلحات تشمل التعليم عن بعد، التعليم بالمراسلة، التعليم المفتوح، التعليم الموزع، الدراسة المنزلية، الدراسة من الخارج، والدراسة عبر الخط، **Distance Learning, Distributed Learning, Remote Learning, Distance Education**.

وعرف أيضا بأنه: " نقل برنامج تعليمي من موضعه في حرم مؤسسة تعليمية إلى أماكن متفرقة جغرافيا، ويهدف إلى جدب طلاب لا يستطيعون تحت الظروف العادية الاستمرار في برنامج تعليمي تقليدي"، وأيضا بأنه : " أحد طرق التعليم الحديثة نسبيا ويعتمد مفهومه الأساسي على وجود المتعلم في مكان يختلف عن المصدر الذي قد يكون فيه الكتاب أو المعلم أو حتى مجموعة الدارسين" [3].

هذا من جهة، ومن جهة أخرى نرى ما لتأثير التعليم عن بعد في الجزائر، إذ يعد أحد الأنماط التعليمية التي لم تعد تقتصر على فئة معينة، حيث كان سابقا يطبق فقط على مستوى مرحلة التعليم ما قبل الجامعي عن طريق الديوان للتعليم والتكوين عن بعد، وكذا جامعة التكوين المتواصل، حتى أن مفهومه أصبح شاملا ومتطورا لدرجة أنه تم اعتماده حتى في الجامعة في مرحلة الماستر كتجربة أولى[4]، إذ يعتمد هذا النظام على وسائل تعليمية حديثة تدعم العملية التعليمية التقليدية، تلزم الطالب على متابعة تعليمه عن طريق أرضية الكترونية وهي منصة "مودل moodel"، مستخدما الوسائل

---

[1] – بن عيشي عمار ، بن عيشي بشير، تقرارت يزيد، واقع استخدام منصة التعليم الالكتروني المودل(Moodel) في ظل جائحة كورونا وأثره على اتجاهات طلبة الجامعات الجزائرية من وجهة نظر طلبة كلية العلوم الاقتصادية بجامعة بسكرة، مجلة الباحث للعلوم الرياضية والاجتماعية، جامعة الجلفة، المجلد 04، العدد 07، ص332.

[2] – العنزي فاطمة بنت قاسم، التجديد التربوي التعليم الإلكتروني، دار الراية للنشر والتوزيع، عمان، الأردن، 2011

[3] – ar.m.wikibedia.org . تاريخ الاضطلاع على الموقع : 2022/03/23.

[4] – المنشور رقم 536 المؤرخ في 06 نوفمبر 2016 المكمل للمنشور رقم 536 المؤرخ في 26 أكتوبر 2016، والذي يبين دور جامعة التكوين المتواصل في الماستر عبر الخط، إذ يقع على عاتقها: ضمان المرافقة طيلة مدة التكوين، تسيير وإدارة الأرضية التعليمية المخصصة لهذا النمط من التكوين، ولتحديد صلاحيات ومهام كل الفاعلين في هذا النمط من التكوين، تبرم اتفاقيات بين جامعة التكوين المتواصل والمؤسسات الجامعية المعنية.

التكنولوجية الحديثة، كالحاسوب والشبكة العنكبوتية، وهذا في إطار مواكبة التطور التكنولوجي، وكانت تقتصر هذه التجربة على بعض من فئات الماستر عبر الوطن وبعض الجامعات على وجه الخصوص، من بينها على سبيل المثال لا الحصر جامعة الجزائر1، في تجربتها للماستر عبر الخط، حيث مرت جامعة الجزائر1 بتجربة التعليم عن بعد من خلال تأطير دفعتين متتاليتين في الماستر عبر الخط[1]، وجاء ذالك استنادا على المنشورين الوزاريين المنظمين للتسجيلات في الماستر عبر الخط، وهما على التوالي المنشور 535 المؤرخ في 26 أكتوبر 2016 المتعلق بالتسجيل في دراسات الماستر عبر الخط بعنوان السنة الجامعية 2017/2016 والمنشور المؤرخ في 30 جانفي 2018 المتعلق بالتسجيل في دراسات الماستر عن بعد بعنوان السنة الجامعية 2018/2017، وتم على أساسه فتح فرع للتسجيل به وهو: فرع إدراة ومالية للسنة الجامعية 2017/2016، ثم تلتها السنة الموالية 2018/2017 ليضاف إلى الفرع السابق فرع ثاني وهو القانون جنائي.

وعممت هذه التجربة في مرحلة تالية فيما بعد، أي التعليم عن بعد وهو ما يعرف بالتعليم عبر المنصة التعليمية عبر الخط plateforme pédagogique en ligne ، على مستوى جميع الجامعات الجزائرية خاصة بعد الجائحة التي أصابت العالم عموما والجزائر على الخصوص.

وسنحاول تاليا، تحديد ماهية هذه المنصات وكيفية العمل عليها لتوضيح بعض الإبهام والصعوبات التي واجهت بعض الفاعلين عليها، ولتقريب الصورة أكثر.

ثانيا: ماهية المنصة التعليمية موودل (Moodel)

تعد المنصات التعليمية بيئة رقمية تعليمية جديدة تعتمد على التكنولوجيا الحديثة باستعمال الشبكة العنكبوتية، فهي تسمح للأستاذ بنشر الدروس في شكل محتوى رقمي تفاعلي ونشر النشاطات وتبادل الملفات بكل أنواعها (مكتوبة، صوتية، فيديو)، وإجراء الاختبارات الالكترونية، كما تسمح المنصات التعليمية بتبادل الأفكار ومشاركة المحتوى مع عدد كبير من الطلبة في آن واحد باستخدام تقنيات متعددة[2].

---

[1] – أكرور مريم، حنصالي صابرينة، التعليم العالي عن بعد: تجربة جامعة الجزائر 1 في الماستر عبر الخط، المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 57، العدد الخاص، السنة 2020، ص 73.

[2] - بن رجدال آمال، المنصات الذكية مستقبل التعليم عن بعد – التجربة الإمارتية – المجلة الجزائرية للعلوم القانونية والسياسية، المجلد 58، العدد 02، 2021، ص 512

فمع التقدم التكنولوجي الكبير أصبحت أغلب المؤسسات التعليمية حول العالم تسعى لتبني نظام التعلم الافتراضي أو التعلم عن بعد من خلال شبكة الانترنت، لما توفره من سهولة في التعلم للطلاب وكفاءة أكبر في إيصال المعلومات للطلبة وفعالية أكبر في التواصل بين المدرسين والطلاب، ولعل ما دفع بهذا النظام إلى الظهور للواجهة بقوة هو الجائحة التي شهدها العالم مؤخرا (covid-19)، ولقد اشتهرت عدة منصات تعليمية في هذا المجال، ولعل أهمها منصة مودل التي تعتبر الرائدة في التعلم الالكتروني والتي تعتبر من أفضل بيئات التعلم الالكتروني، وتكتسب شهرة واسعة حول العالم، وهي نفس المنصة التي تبنت التعليم عبرها وزارة التعليم العالي والبحث العلمي الجزائرية.

تستخدم منصة مودل من قبل عدد كبير من المؤسسات التعليمية والأكاديمية في مختلف أنحاء العالم، إذ نجد إضافة لما توفره هذه المنصة التعليمية الإلكترونية من مميزات كثيرة كوسيلة للاتصال عن بعد، فهي أرضيات للتكوين قائمة على تكنولوجيات الويب، وبمثابة الساحات التي يتم بواسطتها عرض الأعمال وجميع ما يختص بالتعليم الإلكتروني، ويعتبر نظام موودل (Moodel) قفزة كبيرة في تطوير العملية التعليمية، فهو نظام صمم على أسس تعليمية ليساعد الأساتذة على توفير بيئة تعليمية الكترونية.

يعرف نظام التعليم الالكتروني موودل (Moodel) بأنه برنامج تطبيقي مجاني على شبكة الانترنت يوفر بيئة تعليمية متكاملة، تتضمن أدوات لتأليف المقررات، متابعة الطلبة وتوجيههم، وإضافة مصادر التعلم مثل: صفحات ويب، وملفات الوسائط المتعددة، وبناء الاختبارات الالكترونية وتصحيحها، وإعلان نتائجها، وأدوات لتحقيق التواصل والتفاعل بين الطلبة والأساتذة مثل المحادثة والمنتديات، وذلك لتحقيق الأهداف التعليمية بكفاءة وفعالية[1].

حيث تمكن خدمات هذا النظام عن طريق أدواته المتعددة تسهيل العملية التعليمية من خلال ما توفره من منتديات للنقاش، وتحميل فيديوهات، والمحاضرات الداعمة لهذا المساق، إضافة إلى تبادل الأسئلة بين الأستاذ والطالب وتقديم واجبات تعليمية وتبادل الآراء والأفكار بين الأساتذة والطلاب، إضافة إلى مشاركة المحتوى العلمي، حيث يتيح للطالب الاطلاع والتفاعل مع المادة التعليمية في أي

[1] – فارس نجلاء محمد وإسماعيل عبد الرؤوف محمد، التعليم الالكتروني مستحدثات في النظرية والإستراتيجية، عالم الكتب، القاهرة، 2017. ص22.

وقت يشاء و يستطيع تعزيز التواصل الإلكتروني بين الأستاذ والمتعلمين أنفسهم، مما يؤدي إلى تحفيز المتعلم والأستاذ على مواكبة النهضة المعلوماتية، باعتباره برنامج حر مفتوح المصدر[1].

وصمم مودل لمساعدة العاملين عليه لإنشاء فضاء يمكن أن يخدم جامعة تضم أكثر من 40000 مشارك، ومن الناحية التقنية فإن هذا النظام قد صمم باستخدام لغة PHP وقواعد البيانات MYSQL[2].

حتى تتضح المفاهيم أكثر يمكن أخذ كنموذج المنصة التعليمية عبر الخط plateforme pédagogique en ligne التابعة لجامعة الجزائر 01[3]، وهي منصة تضم روابط لخمسة كليات وهي: كلية الحقوق – سعيد حمدين –، كلية العلوم الإسلامية – خروبة –، كلية الطب و كلية العلوم وكلية الصيدلة – الجزائر العاصمة –، وتحتوي هذه المنصة كلا حسب مجاله (بالنسبة للكليات التابعة لجامعة الجزائر1) على مواضيع للدروس والمحاضرات، وكذلك نماذج عن الأعمال الموجهة، وصممت هذه المنصة بشكل يسمح للطالب الولوج إليها والاستفادة من موادها التعليمية والتواصل مع أساتذته المختصين كلا في مجاله، إضافة إلى ذلك تمكن هذه المنصة الأستاذ على متابعة طلابه عن طريق تنظيم ومراقبة الحضور والغياب ومتابعة آداء الطلاب باستخدام الاختبارات والواجبات المنزلية وفتح باب المناقشة عن طريق خاصية الرسائل والمنتديات، كل ذلك يدخل في إطار الالتزامات الأكاديمية للأستاذ الجامعي والتي تلقي على عاتقه توفير المعلومة اللازمة والصحيحة لطلابه.

سنحاول تاليا التطرق لكيفية العمل على هذه المنصة وتقريب المفاهيم عن كيفية العمل على هذه المنصة في المبحث الموالي.

المحور الثاني: المتابعة التقنية للعمل عبر المنصة التعليمية الافتراضية مودل

تعد الحصيلة التعليمية من أهم المبادئ التي تسهر عليها الجهات العلمية المختصة، إذ إن المنصة التعليمية عن بعد هي منصة الكترونية يشرف عليها أشخاص مختصين في مجال الإعلام الآلي تابعين لمؤسسات وزارة التعليم العالي والبحث العلمي، يسهرون على تطويرها وتحسينها بشكل

---

[1] – https://ar.wikipedia.org/wiki/ ، تاريخ الاضطلاع على الموقع: 2022/03/23.

[2] – علي شقور السعدي: 2015، ص 08.

[3] – الموقع الخاص بجامعة الجزائر 01 على الموقع التالي: https://cours.univ-alger.dz/ ، تاريخ الاضطلاع: 2022/01/01.

دائم ومستمر، كما يعملون على ترقيتها وضمان صيرورتها واستمرارها، بهدف دعم الأنظمة التعليمية عن بعد، حتى تضمن توفير خدمات الكترونية متطورة تساعد الأستاذ والطالب على الإستفاذة منها بوجه صحيح ونافع.

تعمل جهات مختصة في هذا المجال على إنشاء حسابات خاصة بالأساتذة والطلبة، إلى جانب تسهيل عملية توفير المادة العلمية عبر هذه المنصة، سنعتمد كنموذج كلية الحقوق التابعة لجامعة الجزائر 1. على سبيل المثال لا الحصر كما سبق ذكره.

فيتم إنشاء الحسابات الخاصة بالفاعلين عبر هذه المنصات باتباع خطوات محددة ومعينة، تسهل على كل من الأستاذ الجامعي والطالب الولوج بكل سهولة ويسر سواء لتحميل المادة العلمية من قبل الأساتذة على هذه المنصة، أو لتحميلها للاستفادة منها من قبل الطلاب.

1: الإجراءات التقنية التي تكفل إنشاء حساب خاص بالأستاذ الجامعي على المنصة

يتم إتباع إجراءات تقنية معينة لإنشاء حسابات الكترونية خاصة بكل طالب وأستاذ تربطه علاقة تنظيمية بهذه المنصة، فيعمل المختصين من تقنيين ومهندسين في الإعلام الآلي على إنشاء حساب يمكن الأستاذ ويساعده على آداء مهنته التعليمية بشكل منظم وصحيح وسهل في آن واحد، حيث تسمح المنصات التعليمية بتبادل الأفكار ومشاركة المحتوى مع عدد كبير من الطلبة في آن واحد باستخدام تقنيات متعددة، حيث يتم إخطار الطلبة بكل محتوى جديد، عند إدراج الدروس والنشاطات...الخ[1]، كل ذلك يتم بطريقة منظمة ومدروسة لتسهيل العمل عبر هذه المنصات، بالإضافة إلى كل ذلك فإن ما يميز هذه المنصات التعليمية أنها تعمل بطرق آمنة للإتصال وحفظ خصوصية الأستاذ والطالب معا، وحفظ معلوماتهم في بيئة مغلقة، لا ينظم لها سوى الأساتذة والطلبة المعنيين وذلك باستخدام إسم المستخدم والرقم السري الخاص بكل منهم، وتتم هذه العملية عن طريق إجراءات تقنية تتمثل فيما يلي:

1 – إنشاء إيمايل مهني خاص بكل أستاذ يتكون من إسم ولقب الأستاذ والجامعة التي ينتمي إليها ومثال عن ذلك:la première lettre de prénom.nom@univ-faculté.dz

[1] – بن رجدال آمال، المنصات الذكية مستقبل التعليم عن بعد – التجربة الإمارتية –، مرجع سابق، ص 512.

فمثلا عن نموذج خاص بأستاذ يدرس على مستوى كلية الحقوق جامعة الجزائر نجد الإيمايل الخاص به يكون كالأتي:a première lettre de prénom.nom@univ-alger.dz

2 – إنشاء حساب خاص بالأستاذ يحتوي على كل من اسم المستخدم User Name، والرقم السري الخاص به Mot de passe

3 – يتم ربط حساب الأستاذ ورقمه السري بالسنة الجامعية الخاصة بالتعليم الجامعي مثلا: السنة الجامعية 2022/2021، ثم القسم التابع له مثلا : قسم الماستر، ثم السنة التابعة لها الأستاذ ومثال ذلك: السنة أولى ماستر أو الثانية ماستر، يليه إلحاق حسابه بالفرع التابع له والمادة المدرسة على مستوى هذا القسم.

4 – بعد أن يتم ربط الحساب بالسنة الجامعية التي يقوم على مستواها التدريس فيها، يتم تاليا توجيهه إلى المواد الملزم بها في مسار هذه السنة الجامعية.

5 – يتم تفعيل حسابه على المنصة بغرض تمكين الطلبة الإطلاع على كل ما يتم تحميله من طرف الأساتذة في جميع المواد المكلفين بها خلال السنة الجامعية السارية.

تتم هذه الإجراءات بطريقة منظمة ودورية لكل سنة جامعية محددة، حيث يتم في كل سنة أو سداسي إما إضافة حسابات جديدة، أو تغيير في الحسابات الخاصة بالأساتذة بسبب تغيير المصلحة التابعين لها، أو إلغاء حسابات من المنصة (في حالة التقاعد، الإحالة على الاستيداع...الخ)، وغيرها من العمليات الكثيرة، كل هذا يسهر عليه مختصين تقنيين بهدف منح كل التسهيلات للأستاذ الجامعي للدخول إلى حسابه الخاص وتفعيل خاصية تمكينه من وضع الدروس على المنصة، فيقوم بتحميلها وتفعيلها للظهور لكل من له الحق على الاطلاع عليها[1].

تمنح هذه الإجراءات عدة مزايا للأستاذ تمكنه في التحكم في حسابه الخاص على المنصة، تتمثل فيما يلي:

1 – حرية تغيير اسم المستخدم والرقم السري الخاص به للولوج إلى المنصة، وهذا ضمان للسرية الخاص بالمعلومات الشخصية لكل أستاذ.

[1] – مركز الحسابات التابع لكلية الحقوق، جامعة الجزائر، 2022.

2 – إمكانية تحميل المادة العلمية الخاصة بكل أستاذ بأريحية وسهولة، والتحكم في تقسيماتها داخل الفضاء الخاص بحسابه.

3 – إمكانية الولوج إلى المنتديات الخاصة بالمنصة التعليمية، والإجابة على جميع الاستفسارات الخاصة بالطلبة والفاعلين على هذه المنصة.

4 – التحكم التام بحسابه الخاص وبمعلوماته الشخصية عبر المنصة، بداية من بطاقته المعلوماتية ووصولا إلى مواده العلمية.

في الأخير يمكن القول أن المنصة التعليمية عبر الخط (منصة مودل)، مكنت من التعامل بكل حرية وأريحية في هذا المجال، وإن كان هناك بعض الإشكالات التي تحدث في بعض الأحيان لأغلبية الأساتذة نظرا لقلة الخبرة بالنظام الالكتروني وعدم الدراية الكافية بمجال الإعلام الآلي، إلا أنها ساعدت في تسهيل عملية التعليم وتبسيطها، سواء للأستاذ أو الطالب والذي بدوره هو الآخر معني بعملية إنشاء حساب خاص به على هذه المنصة وهو ما سنتناوله تاليا.

2 – الإجراءات التقنية لإنشاء الحساب الخاص بالطلبة

تتم هذه العملية هي الأخرى بمراحل متتابعة، تشبه إلى حد بعيد الإجراءات الخاصة بالأستاذ فيما يتعلق بالإيمايل المهني وحساب المستخدم والرقم السري، إلا أنها تختلف عنها في بعض الخصوصيات التي لا يمكن منحها للطالب، خلاف الأستاذ وهي محددة بالنقاط التالية:

1 – يمكن للطالب الاطلاع فقط على الدروس الخاصة بالمواد التي يدرسها على مستوى السنة الجامعية التابع لها.

2 – لا يحق للطالب الولوج إلى حساب الأستاذ، بل يكفي الدخول على المنتديات وطرح الإشكالات التي تهمه في مساقه الدراسي.

3 – تحميل الدروس فقط من المنصة والمتعلقة بالمواد المدرسة في السنة الجامعية التابع لها، دون حرية التعديل أو الحذف أو الإضافة عكس الأستاذ الجامعي.

4 – تحميل نماذج الاختبارات عبر الخط، والتي توضع من طرف الأساتذة في بعض من المواد التي استلزمت في بعض الأحيان إجراءها عن بعد خاصة في ظل الظروف التي مرت بها الجامعة والوطن ككل (covid-19).

مما لا يخفى على الكل أن هذه المنصات تعمل بالذكاء الاصطناعي والذي أصبح مجال لا يمكن الاستغناء عنه، فتعتمد هذه المنصات التعليمية على تقنياته وخورزمايات[1] خاصة بها، كل ذلك بهدف إنتاج محتوى تعليمي ذكي، وتسهيل العمل على الأستاذ من خلال أتمته لمهامه.

مما سبق ذكره بخصوص الإجراءات المتبعة لإنشاء الحسابات التقنية على منصة مودل، سواء ما تعلق منها بالأستاذ أو الطالب، تبقى هذه العملية خاضعة لرقابة ومتابعة الهيئات العليا بالمؤسسات الجامعية، والتي تسهر على ديمومة المنصة واستمرارية التعليم عبر مؤسساتها، عبر اتخاذ الإجراءات القانونية اللازمة، بهدف ضبط النظام العام للمؤسسات الجامعية وسيرها، وهذا ما سنتطرق له تاليا.

المحور الثالث: المسؤولية الجنائية عن انتهاك خصوصية المعلومات المنشورة عبر المنصة

رغم الدور الذي تلعبه المنصات التعليمية عبر الخط، والمساهمة في تطوير التعليم العالي عن طريق اعتمادها على تقنيات حديثة ومتطورة تعتمد في مجملها على الذكاء الاصطناعي، من أجهزة كمبيوتر، وشبكة أنترنت...الخ، هذا الأمر بقدر ما هو إيجابي إلا أنه قد يعرض الفاعلين عليه إلى بعض الانتهاكات لخصوصيتهم ومعلوماتهم الشخصية على هذه المنصات، لدى عمل المشرع الجزائري ودراءا لمخاطر هذه الانتهاكات إلى فرض عقوبات جزائية على كل منتهك لهذه الخصوصية، وأقامت عليه المسؤولية الجنائية عن ذلك.

ومن خلال هذا المحور سنحاول التطرق إلى بعض القوانين التي أتى بها المشرع عقابا لكذا جرائم، والتي جاء تسميتها بالجرائم الالكترونية، نظرا لارتباطها بالفضاء الالكتروني، سنحاول تاليا تبيان خصوصية هذه الجرائم وصولا إلى العقوبات المفروضة على انتهاكها.

---

[1] – الخوارزمية هي عبارة عن برنامج أو مجموعة من البرامج المنظمة، لنظام الكمبيوتر، وبشكل البرنامج من الناحية التقنية، الهندسة المنطقية الكيان المعنوي له،

شكلا يكتب بلغة لها رموز يشفرها لإجراء سلسلة متتالية من القرارات، يتم تشغيل هذا البرنامج على جهاز مجسم، أين يتم تثبيت المعلومات في شكل إشارات كهربائية، لمزيد من المعلوماتحول الطبيعة اللامادية للأنظمة الالكترونية الذكية أنظر:

نريمان مسعود بورغدة، المسؤولية عن فعل الأنظمة الالكترونية الذكية، حوليات جامعة الجزائر 1، العدد 31، ص 144.

أولا: تعريف الجريمة الالكترونية

صارت التقنية خاصة في جانب المعلوماتية من أساسيات الحياة في عصرنا الحالي، لكن البعض من مستخدمي هذه التقنية الحديثة استغلتها في أهداف غير مشروعة طبقا لمصالحه الشخصية، حيث أصبح الإعلام الآلي بشكل عام وشبكة الأنترنت على وجه الخصوص، أدوات أو محلا لارتكاب الجريمة بمفهومها الحديث، مع احتراف بعض الجناة عديد الجرائم، بواسطة الحاسب الآلي أو شبكة الأنترنت، وبذلك أصبحت الجريمة الالكترونية من الظواهر الرائجة حديثا، نظرا لارتباطها بتقنية متطورة هي تكنولوجيا المعلومات والاتصال[1]، لدى تعددت وجهات النظر بخصوص هذا النوع المستجد من الجرائم، حيث لا يوجد إجماع على تعريف الجريمة الالكترونية من حيث تحديدها والجرائم التي تشملها، وفيما يلي سنتطرق لبعض التعاريف الخاصة بهذه الجرائم.

عرفت الجريمة الالكترونية بأنها: " كل فعل اجرامي أو متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة بالمجني عليه، أو كسبا يحققه الفاعل"، كما عرفتها منظمة التعاون الاقتصادي والتنمية بأنها: " كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[2].

أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين، فقد تبنى التعريف التالي للجريمة الإلكترونية: " هي أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"[3].

يلاحظ من التعريف الأخير أنه استطاع الإحاطة – قدر الإمكان – بجميع الأشكال الإجرامية للجريمة الإلكترونية، سواء بواسطة النظام المعلوماتي، أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما يشمل التعريف الجرائم التي من الممكن أن تقع في بيئة الكترونية، فهذا التعريف لم يركز على فاعل الجريمة ومقدراته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي

---

[1] – مونة مقلاتي، راضية مشري، الجريمة الالكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مجلة أبحاث قانونية وسياسية، المجلد 6، العدد1، جوان 2021، ص492.

[2] – يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري، في ضوء االاتفاقيات العربية لمكافحة جرائم المعلومات، قانون العقوبات، ق إ ج، قوانين خاصة، دار الجامعة الجديدة، الإسكندرية، 2019، ص50.

[3] - نداء نايل فايز المصري، خصوصية الجرائم المعلوماتية، مذكرة ماجستير، قانون عام، بكلية الدرسات العليا في جامعة النجاح الوطنية، نابلس، فلسطين، 2017، ص03.

تسعى لها الجريمة الإلكتروني، بل حاول عدم حصر الجريمة الإلكترونية في نطاق ضيق يتيح المجال أما إفلات العديد من صور هذه الجريمة من دائرة العقاب.

وباستقرائنا للتعاريف السابقة للجريمة الالكترونية على العموم فهي تقوم على ثلاث عناصر، السلوك ووصفه والنص القانوني على تجريم السلوك وإيقاع العقوبة، ثم محل اعتداء في الظاهرة الإجرامية المستحدثة متمثلا في معطيات الحاسوب، خلافا للجريمة عموما، إذ هي سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الحاسوب الآلي، فالسلوك يشمل الفعل الإيجابي والامتناع عن العمل، مع اعتبار أن إسباغ الصفة الجرمية لا يتحقق في الميدان الجنائي إلا بإرادة المشرع/ ومن خلال النص القانون ومحل الجريمة ذاتها وهو معطيات الكمبيوتر بدلالاتها الواسعة[1].

أما بالنسبة للمشرع الجزائري، فلقد فضل تسميتها تحت مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وكخطوة أولى لمواجهة ما يعرف بجرائم تكنولوجيا الإعلام والاتصال، أجرت الحكومة الجزائرية بعض التعديلات على قانون العقوبات، بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-156، والمؤرخ في 08 يونيو 1966 والمتضمن قانون العقوبات، حيث استحدثت عقوبات تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، وهو ما نصت عليه المواد 394 و 394 مكرر 1 إلى 7 من القسم السابع مكرر، وتراوحت هذه العقوبات من شهرين إلى ثلاث سنوات مع دفع غرامة مالية من 50000 دج إلى 5000000 دج، وذلك حسب حجم ودرجة خطورة الجريمة الالكترونية المرتكبة، كما قام المشرع الجزائري بتجريم الأفعال الماسة بأنظمة الحاسب الآلي بسبب ما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، وهو ما دفعه إلى تعديل قانون العقوبات 15/04، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات[2].

يعد 04/09 أول قانون في الجزائر اهتم بكيفية تبادل المعلومات الرقمية، وتجري فيه كل أنواع المعاملات والخدمات الالكترونية، وقد عرفت المادة 02 منه الجريمة الالكترونية على أنها: جرائم المساس

---

[1] - إدريس النوازلي، موقف القضاء من الجريمة الالكترونية، سلسلة الندوات والأيام الدراسية، التجارة الالكترونية أية حماية؟ أشغال الندوة الوطنية التي نظمها مكتب الدراسات وهيئة المحامين بمراكش، المغرب، أيام 29، 30 ماي 2009، ص 91.

[2] - سعيداني سلامي وطارق طراد، التجربة الجزائرية لمواجهة الجريمة الالكترونية في ظل البيئة التفاعلية الجديدة، عرض تشريعي قانوني، مجلة الحقوق والعلوم السياسية، العدد 12، جوان 2019، ص ص 247.

بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الالكترونية[1].

يتضح من هذه المادة نية المشرع الجزائري في تبني مبدأ المرونة في الصياغة التشريعية، للتمكن من استيعاب الأنشطة الإجرامية الالكترونية التي يتعذر حصرها وتحديدها، نظرا لسرعة وتطور أساليبها، تبعا للتطور التقني، وهو ما يتيح للقاضي حرية واسعة في التقدير[2]، وانطلاقا من فحو ى هذه المادة، يتبين أن المشرع الجزائري قسم هذه الجرائم إلى ثلاث أنواع : جرائم المساس بأنظمة المعالجة الآلية للمعطيات، جرائم ترتكب أو يسهل ارتكابها عن طريق المنظومة المعلوماتية، جرئم ترتكب أو يسهل ارتكابها عن طريق نظام للاتصالات الالكترونية[3].

من خلال استعمال المشرع الجزائري لمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، لدلالة على الجرائم الالكترونية، فهو يزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة، فالأولى تقوم على استخدام الوسائل التقنية لإدارة وتنظيم ومعالجة البيانات، أما تكنولوجيات الاتصال فتقوم على وسائل تقنية لنقل المعلومات بجميع دلالتها، ولذلك فقد وفق –في نظرنا– المشرع الجزائري باختياره مصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي تتوافق مع مصطلح الجرائم الالكترونية بالمفهوم الواسع، وهذا للأسباب التالية:

–الجرائم الناشئة في البيئة الرقمية هي حديثة ، يرتبط مفهومها بظهور التكنولوجيا الحديثة، وما يواكبها من تطور مستمر في تشغيل ونقل وتخزين المعطيات في شكل الكتروني.

– استعمال هذا المصطلح له مفهوم واسع، فهو يشمل كل الاعتداءات التي تتم في بيئة افتراضية، بما فيها الجرائم التي تقع على نظم المعالجة الآلية للمعطيات، وتكون وسيلة لارتكابها.

– يعبر هذا المصطلح عن الطابع التقني والمميز للجرائم الالكترونية.

– لم يحدد المشرع صور السلوك المجرم الذي يرتكب أو يسهل ارتكابه ضمن منظومة معلوماتية، أو نظام للاتصالات.

---

[1] - قانون رقم 04/09 المؤرخ في 2009/08/05، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج.ر 74، الصادرة في 2009/08/16.

[2] - مونة مقلاتي، راضية مشري،الجريمة الالكترونية: دلالة المفهوم وفعالية المعالجة القانونية، مخبر الدراسات القانونية البيئية، مجلة أبحاث قانونية وسياسية، المجلد 06، العدد 01، جوان 2021، ص 495.

[3] -

– تضمن هذا التعريف التكرار، كون أن مفهوم نظام الاتصالات الالكترونية يندرج تحت مصطلح المنظومة المعلوماتية، ذلك أن المشرع الجزائري عرف هذه الأخيرة بموجب أحكام المادة 02، على أنها نظام منفصل، أو مجموعة من الأنظمة المتصلة بعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات، تنفيذا لبرنامج معين، لدى يمكن تعريف الجريمة الالكترونية حسب رأينا بأن : " الجريمة الالكترونية هي كل اعتداء على معلومات أو حقوق شخصية على الفضاء الرقمي، باستخدام أجهزة رقمية نظام معلوماتي، وكان له دور رئيسي في السلوك المجرّم".

ثانيا: البرامج المستعملة في الجرائم المعلوماتية

مع تعدد الجرائم المعلوماتية الالكترونية، تتعدد معها البرامج التي تهدد هذا المجال، ومنها جريمة صناعة ونشر الفيروسات عبر التطبيقات والبرامج المهددة والفتاكة للأجهزة الإلكترونية والشبكات الرقمية وقواعد البيانات، والهدف المباشر من ذلك هو تعطيل الأجهزة وشبكات الاتصالات الالكترونية وقرصنة البيانات المخزنة فيها، بغرض تخريبها أو المتاجرة بها أو استغلالها بطرق غير شرعية، من خلال نقلها من الأجهزة الأصلية المخزنة بها إلى أجهزة أخرى معدة خصيصاً لارتكاب مثل هذه الجرائم؛ وهنا يمكننا أن نذكر أبرز هذه البرامج والتطبيقات الضارة في مجال المعلوماتية:

- **الأدوير (*Adware*)** هو برنامج تجسسي يتم بواسطة الإعلانات المتسللة، يقوم بملاحقة نظام التشغيل عبر الصفحات التي يقوم المستخدم باستطلاعها، لمعرفة اهتماماته وترصد هواياته، وبالتّالي تُعرض له الإعلانات التي تتناسب مع هواياته وأهوائه، فيقوم بمتابعتها وهنا يتم قرصنته، كما يقوم هذا التطبيق بالحصول على المعطيات الشخصية للمستخدم الضحية من جهازه الإلكتروني كالحصول على بريده الإلكتروني لإرسال الإعلانات غير المرغوب فيها إليه المسماة بـ **(*Spam*)** ، ومن ثمة إرسال بريده الإلكتروني إلى الجهات التي سوف تستفيد من محتواه، كما انه بإمكانه تغيير مستعرض الإنترنت المختار، حتى لو أعاد ضبطه فسوف يتغير باستمرار؛ و مثال ذلك نجد برنامج **(*RootKit*)** ؛ لكن يجب أن نشير إلى أنه ليست جميع تطبيقات الأدوير ضارة، فبعضها مفيد في إعداد المشاريع المالية والاقتصادية، حيث يستخدم في بعض الدراسات الإحصائية و المحاسبية على غرار تطبيق **(*SPSS*)**.
- **السبايوير (*Spyware*)** هو برنامج شبيه بالأدوير لكن هدفه مختلف، حيث يسعى إلى التعرف على المعلومات المتعلقة بالمستخدم المُراد قرصنته بدون علمه، كالمعلومات المتعلقة بحساباته الإلكترونية

ككلمات السر الخاصة به أو رقم بطاقته الإئتمانية إذا كان يستخدمها للدفع الإلكتروني، حيث يكون الهدف منه سرقة البيانات الشخصية أو سرقة الأموال أو تحويلها؛ وبالتالي فهو أشد خطورة من برنامج الأدوير[1].

- **الفيروس(*Virus*)** هو تطبيق إلكتروني يهدف إلى تعطيل البرامج الأساسية للحاسوب ويشكل الخطر الأكبر والأشد لأنظمة التشغيل والبرامج المعلوماتية وقواعد البيانات، حتى أن لبعض الفيروسات القدرة على التّسبب بأعطال مستديمة في الحواسيب. ومن بين الفيروسات المنتشرة بكثرة نذكر[2]:

✓ **التروجان: (*Trojan*)** أو ما يعرف بحصان طروادة ***(Cheval-de-Troid)*** وهو برنامج تمويهي وتخريبي، له تسميات عديدة، يجعل من الحاسوب الخاص بمستخدم ما خادماً لحاسوب آخر، أي يتمكن الحاسوب الأخر من التحكم بالحاسوب المصاب بالتروجان، لكن الشرط الأساسي لهذه العملية أن يكون الحاسوب المراد إصابته أو اختراقه موصولًا بالشبكة العنكبوتية.

✓ **الديدان (*Worm*):** هو برنامج إلكتروني ضار لكن خطورته ليست شديدة، يقوم بالتكاثر عبر الشبكة العنكبوتية وينتقل من الحاسوب إلى آخر لتعطيله والتجسس على محواه، حيث يقوم بإستخدام مصادر الحاسوب لإغلاقة أو إثقاله ثم مهاجمته.

أما فيما يخص حقوق الملكية الفكرية والأدبية، فإن هذا المجال يشهد اليوم لاسيما في فضائه الرقمي، العديد من المخاطر والتهديدات التي تسعى إلى خرق وقرصنة نُظُم المعلومات وقواعد البيانات، وكل ما يتعلق بالمصنفات الرقمية، التي تشمل نسخ البرامج أو تقليدها وإعادة إنتاجها أو تداولها بدون وجه حق؛ فالاعتداء على حقوق المؤلف والعلامات التجارية وبراءات الاختراع وكل ما هو في إطار الملكية الفكرية يُعد من الجرائم الإلكترونية الخطيرة. وعلى سبيل المثال نورد بعض النماذج التي ارتبط وجودها بشبكة الإنترنيت، والتي أضفت عليها صفة البيئة العدائية وغير الآمنة، والتي تمس الملكية الفكرية، ومنها:

- **تعطيل الأجهزة المتضمنة لمعطيات الملكية الفكرية والصناعية:**

لقد حملت الإنترنيت التي تضم مجموعة كبيرة من الأجهزة الإلكترونية والشبكات حول العالم فوائد جمة، وأصبحت وسيلة سهلة وممتعة، تتيح لملايين البشر الولوج إلى الكم الهائل من المعلومات المتوفرة في فضائها، ولكن بظهور العديد من المخاطر التي سمحت بها طبيعتها المفتوحة، وعدم وجود قوانين رادعة في كثير من الأحيان، أدت إلى انتشار جرائم العصر الإلكتروني، المتمثلة في الخرق، الانتحال، التقليد، القرصنة، التجسس، وغير ذلك من الجرائم الماسة بشكل أو بمحتوى الأجهزة الإلكترونية والشبكات.

---

[1]- فاطمة شعران، مرجع سابق، ص128.

[2]- جليلة بن عياد، الحماية القانونية للمصنف الالكتروني في القانون الجزائري، مجلة التعليم عن بعد والتعليم المفتوح، جامعة بومرداس، الجزائر، ص17.

- **الإغراق الإلكتروني للحسابات :**

هذه الجريمة انتشرت مؤخراً حيث يقوم مرتكبوها بإرسال مئات بل الآلاف من الرسائل غير المرغوب فيها ***(Spam)***[1]، إلى البريد الإلكتروني لشخص ما قصد إغراق حساباته أو بنك معلوماته الإلكتروني لخرقها والاستحواذ على محتواها المتضمن لمعطيات شخصية أو مهنية، أو أن يقوموا بسد منافذ الاتصال لديه ***(Ports-de-Communication)*** مما ينتج عنه انقطاع في الخدمة وعدم إمكانية تواصله مع الغير، وهذا ما ينجم عنه أضرار مادية ومعنوية تخص الشخص الضحية أو المستفيد من الخدمة أو المستخدم لهذه الجهة.

- **التعدي على الحرية والخصوصية:** إن التقدم التقني و المعلوماتي في الاتصال كان معجزة هذا العصر الذي دخل به كتحد ورهان طرحه مبتكروه كمرحلة انتقالية حاسمة في حياة البشرية، حيث استطاعت هذه التقنيات أن ترفع جميع الحواجز وتقرب المسافات إلى حد جعل العالم وكأنه قرية صغيرة؛ وبقدر ما كان هذا الرهان نعمة على البشرية بقدر ما أصبح نقمة عليها نظرا للتجاوزات العديدة والمختلفة من الاختراقات والسطو، والتعدي الصريح على حرية الأفراد والمؤسسات والمساس بأمن خصوصياتهم؛ وتتجلى لنا مظاهرا هذا التعدي لاسيما في مجال الملكية الفكرية في ما يلي:

✓ **انتحال الشخصية في البيئة الرقمية:** تعتبر جريمة انتحال الشخصية واحدة من بين أهم وأكثر الجرائم المنتشرة في البيئة الرقمية التي سهلت من تواجدها، وتمخضت عنها انعكاسات خطيرة لتنال بذلك من حرية وخصوصية الأفراد والمؤسسات على حد سواء، فانتحال الشخصية في البيئة الرقمية تمس جانبين مهمين و هما[2]:

- **إنتحال شخصية الأفراد :** تعتبر جرائم انتحال شخصية الأفراد من الجرائم القديمة وليست بالمستحدثة، ولكن التنامي المتزايد للشبكة العنكبوتية أعطى المجرمين قدرة أكبر على جمع المعلومات والاستفادة منها، وقد يؤدي انتحال شخصية الأفراد إلى الحصول على حساباتهم الإلكترونية لاستعمالها غير المشروع، كأن يعمل على استعارة مراجع علمية نادرة أو الاتصال المباشر بمراكز وبنوك المعلومات أو الاتصال بناشرين أو مؤلفين والعمل على اقتناء أو شراء نُسخ من مؤلفاتهم باسم أو لحساب الضحية، والانعكاسات هنا تكون خطيرة لأنها تعدي على شخصية وخصوصية الأفراد وحرياتهم.
- **انتحال شخصية المواقع الإلكترونية:** يعتبر هذا النوع من الانتحال، جديد وأشد خطورة في اكتشافه أو تقفي أثره، بالنظر إلى حجم المخاطر التي تنجر عنه، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع التي يتم تأمين نُظم الاتصالات بها (***Secured Server***)، إذ يمكن اختراق مثل هذه الحواجز الأمنية بسهولة، وتتم عملية الانتحال كأن يقوم مرتكب الجريمة باختراق موقع لأحد مقدمي الخدمة المشهورين

---

[1]- محمد رحيلي، حقوق المؤلف والحقوق المجاورة في البيئة الرقمية، كلية الحقوق، جامعة قسنطينة، 2015، ص319.

[2]- محمد رحيلي، مرجع سابق، ص322.

أو بنك للمعلومات، يتسم بالمصداقية وبإتاحته لمصادر المعلومات الغنية أو موقع لمكتبة رقمية يكثر عليها الرواد، وهذا بتثبيت برنامجه الخاص به هناك، مما يؤدي إلى توجيه أي زائر إلى موقعه بمجرد كتابة إسم هذا الموقع، ويتوقع العديد من الخبراء أن انتشار مثل هذا النوع من الجرائم مستقبلا سوف يكون بكثرة، نظرا لصعوبة اكتشافه و تقفي أثره .

- ✓ **التشويش وتحوير المعلومات داخل محيط الإنترنيت:** لقد مكنت شبكات الاتصالات داخل فضاء الإنترنيت من الوصول المباشر إلى الأوعية الفكرية المنتشرة في مختلف دول العالم وتصفح محتوياتها بصفة آنية، من خلال الإتصال ببنوك المعلومات للمكتبات الرقمية الموصلة بمحركات البحث المعروفة، الشيء الذي سهل من عملية تحوير المعلومات والاعتداء على الوثائق من طرف مجرمي الشبكات الرقمية؛ وهي من أكثر الجرائم الإلكترونية انتشاراً في عالمنا المعاصر، حيث يلجأ المخرب بالتشويش على المعلومات أثناء عملية بثها أو إرسالها وذلك من خلال الاستحواذ عليها، و القيام بتحميلها من أجل تحوير محتواها، ليقوم فيما بعد بإنزالها إلى المستفيد منها بعد أن مرت بعملية تعديل في المحتوى تتماشى مع أهواء أو رغبة المخرب.
- ✓ **جرائم النصب والاحتيال الإلكتروني في مجال النشر:** لقد أصبحت الإنترنيت، الفضاء الواسع والرحب في عملية الإتاحة والتداول والاتصال والتواصل بين مختلف شرائح مستخدمي الشبكة بمختلف توجهاتهم العلمية، التجارية، الإقتصادية والسياسية، فاسحة المجال للراغبين في تقديم خدماتهم أو بيع منتجاتهم أو عرض أفكارهم وإبداعاتهم؛ ولم يكن في الحسبان أبداً أن يُساء استخدام هذه الوسائل والتقنيات في عمليات النصب والاحتيال الرقمي، التي تمس بأمن المعلومات المراد تنزيلها أو تحميلها على الإنترنيت؛ ومن بين جرائم النصب و الاحتيال المنتشرة بقوة، نجد مثلا تقديم خدمات وهمية لمؤلفين أو لناشرين وهميين أو سرقة معلومات لبطاقات الائتمان واستخدامها للسطو على الحسابات البنكية، أو العمل على اختلاق دائنين وهميين لهم حقوق مستحقة الدفع أو اختلاق فواتير وهمية يجب سدادها وهذا بالتحوير و التزوير في بياناتها الرقمية[1].

- **التقليد للمصنفات الرقمية:** هذه الجريمة تعتبر من أكبر الجرائم المعلوماتية ومن أخطرها وأشدها فتكاً بالمصنفات الرقمية للملكية الفكرية، ويُعد من التقليد، نسخ كل منتوج فكري في شكل رقمي دون إذن صاحبه، حيث حدد المشرع الجزائري جرائم التقليد للمصنفات الرقمية في نصوص المواد151 و152 من القانون 03-05 سالف الذكر[2] وهي كالآتي:

---

[1]- محمد رحيلي، مرجع سابق، 323.

[2]- القانون 03-05، مرجع سابق، المواد 151-152.

- الكشف غير المشروع للمصنف (رقمي)
- المساس بسلامة المصنف (رقمي)
- استنساخ مصنف (رقمي) بأي أسلوب من الأساليب في شكل نسخ مقلدة
- تبليغ المصنف (رقمي) بأي منظومة معالجة معلوماتية
- استيراد أو تصدير نسخ مقلدة من مصنف (رقمي)
- بيع نسخ مقلدة لمصنف (رقمي)
- تأجير أو وضع رهن التداول لنسخ مقلدة من مصنف (رقمي).

ثالثا: التقنيات المستعملة للوقاية من الجرائم الالكترونية.

فرض المشرع عقوبات على هكذا أنواع من الجرائم الالكترونية، غير أن هذا غير كافي إذ يجب توفير حماية تقنية لتفادي هكذا انتهاكات على الفضاء الرقمي تتمثل في برامج تعمد في الأساس على الجانب الالكتروني حماية للمعلومات الشخصية والحقوق الخاصة بهذا الفضاء، من بينها:

– **إبقاء البرنامج ونظام التشغيل محدّثَين:** يضمن إبقاء البرنامج ونظام التشغيل لديك محدّثَين استفادتك من أحدث تصحيحات الأمن لحماية جهاز الكمبيوتر الخاص بك.

–**استخدام برنامج مكافحة الفيروسات وإبقائه محدّثًا:** يشكّل استخدام برنامج لمكافحة الفيروسات أو حل شامل لأمن الإنترنت مثل Kaspersky Total Security طريقة ذكية لحماية النظام من الهجمات.

ويتيح برنامج مكافحة الفيروسات فحص الجهاز واكتشاف التهديدات وإزالتها قبل أن تتطور لتصبح مشكلة. يساعد وجود مثل هذه الحماية في حماية جهاز الكمبيوتر الخاص والبيانات من الجرائم الالكترونية، مما يوفّر راحة البال، ويجب التأكد من إبقائه محدّثًا للحصول على أفضل مستوى من الحماية.

– **استخدام كلمات مرور قوية:** يجب التأكد من استخدام كلمات مرور قوية لا يمكن للأشخاص معرفتها ولا يتم تسجيلها في أي مكان. أو استخدم برنامج حسن السمعة لإدارة كلمات المرور وذلك من أجل إنشاء كلمات مرور قوية بشكل عشوائي لتسهيل هذا الأمر.

– **عدم فتح المرفقات في رسائل البريد الالكتروني العشوائية أبدًا:** تشكّل مرفقات البريد الالكتروني في رسائل البريد الالكتروني العشوائية طريقة تقليدية لإصابة جهاز الكمبيوتر ببرامج ضارة وغيرها من أشكال الجرائم الالكترونية. إذ لا يجب تفتح أبدًا مرفقًا من مرسِل لا تعرفه.

أما بالنسبة للانتهاكات التي تواجهها حقوق الملكية الفكرية، وخاصة منها المصنفات الرقمية، حيث لم تعد الوسائل القانونية وحدها قادرة على التصدي لها وتوفير الحماية المطلوبة لهذه الحقوق، مما أدى إلى وجوب إيجاد آليات تقنية تقوم بمواجهة هذه الاعتداءات وتضع حداً لمختلف عمليات الخرق والتخريب والقرصنة للمصنفات الرقمية، عن طريق إعداد برامج معلوماتية قوية ومتكاملة لتأمين وحماية شبكة الإنترنيت، وتتمثل هذه التقنيات في استخدام مايلي:

أ – العلامات المائية (*Water Marking Digital*): وهي مجموعة بيئات تمثل صورة يتم تضمينها في الملف لتحديد معلومات حقوق الملكية الفكرية لذلك المصنف، وعلى العكس من الوثائق المطبوعة المرئية، يتم توزيع وتثبيت البيانات الممثلة للعلامات المائية الرقمية، حيث يصعب تحديدها ومعالجتها بعد إنشائها، ويستخدم برنامج خاص لتجميع هذه البيانات المشتتة والتحقق منها ومن صحتها ومطابقتها للأصل، ولا يقتصر تصميم العلامات المائية الرقمية فقط على المحتوى النصي كمثيلتها المطبوعة، وإنما تنسحب على جميع أشكال الملفات الرقمية من رسومات وصور وفيديوهات، ووسائط متعددة[1]، ونجد أنه يمكن أن يضاف علامات مائية للمحتوى، وهذا لتوثيق ملكية تلك المصنفات بشكل واضح يجعل من إعادة استخدامها بشكل غير قانوني أمراً ملحوظ لمتصفح ذلك المحتوى، لاسيما في إدارة المواقع مثل مواقع التواصل الاجتماعي، حتى تسهل عملية حذف المحتوى المنسوخ من الآخرين.

ب– نظام الوشم والتسيير الإلكتروني لحقوق المؤلف: يقصد بنظام الوشم تلك التقنية التي تسمح بالتعرف على كل المعلومات الخاصة بالمصنف وتعتمد هذه التقنية على تضمين المصنف الرقمي لعلامة أو رمز تسمح بتعين المصنف نفسه وكذا أصحاب الحقوق، بحيث أية تغييرات يقوم بها المستعمل أو أي استغلال غير مرخص يتم اكتشافه، أما نظام التسيير الإلكتروني لحقوق المؤلف يهدف إلى المراقبة الدائمة والمستمرة لطلبات النفاذ التي تسجل أوتوماتيكيا على المصنف المنشور على الإنترنت، وهذا ما يسمح باستخراج التقارير الخاصة بمحاولات القرصنة، وتتم عن طريق النقاط التالية:

1– **تحديد الهوية والمصداقية:** باستخدام كلمة السر أو أي شكل آخر لتحديد هوية المستفيدين المرخص لهم الدخول على النظام.

2– **مراقبة الدخول (*ACCESS CONTROL*):** لإبعاد كل من المستفيدين المرخص لهم وغير المرخص لهم عن الوصول إلى مواد معلومات غير مسموح لهم بالإطلاع عليها.

3– **المسؤولية (*ACCOUNTABILITY*):** وذلك عن طريق ربط كل النشاطات على الشبكة بهويات المستفيدين، واعتبار كل شخص مخول بالاستخدام مسئولا عن المعلومات في النظام.

4– **سجل المراجعة (*AUDIT TRAILS*):** وذلك لمتابعة وتقرير ما إذا كان هناك خرق أمني، أو ضياع جزء من المعلومات، ومن هو الشخص الذي قام بذلك.

---

[1]– نادر شافي ، أنواع التوقيع الالكتروني، منشور على المرقع الالكتروني التالي: https://twitmail.com/fullview

5- **استخدام المواد (*OBJECT REUSE*)**: بمعنى تأمين مصادر المعلومات للاستخدام من قبل المستفيدين المرخص لهم.

6- **الدقـة (*ACCURACY*)**: الحماية ضد الأخطاء أو التعديلات غير المرخص بها.

7- **الاعتمادية (*RELIABILITY*)**: حماية المعلومات من الاحتكار من قبل أي مستفيد.

8- **تبادل البيانات (*DATA EXCHANGE*)**: تأمين بث المعلومات عبر قنوات اتصال مأمونة[1].

ج – التشفير[2]: لم يعرف المشرع الجزائري التشفير وإنما اكتفى فقط إلى التطرق إلى أنواعه المتمثلة في التشفير العام والخاص ضمن المادة 02 فقرة 8 و9 من قانون 15-04 المؤرخ في 01 فبراير 2015، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين[3]، بحيث تنص على أن " مفتاح التشفير الخاص، هو عبارة عن سلسلة من الأعداد يحوزها حصرياً الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح التشفير العمومي، أما مفتاح التشفير العمومي، هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من التوقيع الالكتروني، وتُدرج في شهادة التصديق الالكتروني".

د – التوقيع الالكتروني[4] : أما بالنسبة للتوقيع الالكتروني فعكس التشفير، عرَّفه المشرع الجزائري في المادة 02 فقرة1 من قانون 15-04 السالف الذكر على أنه " بيانات في شكل الكتروني مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى، تستعمل كوسيلة للتوثيق"، ويشمل التوقيع الالكتروني نوعين هامين هما: التوقيع الرقمي (***Digital Signature***)، والتوقيع البيوميتري (***Biometric Signaleur***).

وعليه فإن عملية الحفاظ على حقوق المؤلف داخل البيئة الرقمية، عبارة عن عملية صعبة ومعقدة، ولكنها هامة للغاية، خاصة مع انتشار الانفجار الكبير في عالم التقنية، لذلك وجب الحفاظ على نتاج العلماء والمبدعين حتى تستمر عملية التطوير والتحسين للبشرية أجمع، فالأمر ليس متعلقا فقط بالناحية الاقتصادية، وإنما بكافة نواحي الحياة.

---

[1] – عبد الرزاق مصطفى، حقوق التأليف والملكية الفكرية في البيئة الرقمية والتجربة الأردنية، ص24، مقال، منقول بتاريخ 2021/10/11:، من الموقع: https://jordan-lawyer.com

[2] – يعرَّف التشفير على أنه "استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها"، تعريف منشور على الموقع : https://www.e-justice.tn>references-juridiques

[3] – قانون رقم 15-04، مؤرخ في01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، الجريدة الرسمية رقم 06، مؤرخة في 10 فبراير 2015.

[4] – عرفه المشرع المصري في المادة الأولى فقرة ج من قانون رقم 15-2004 المتعلق بالتوقيع الالكتروني على أنه " التوقيع الالكتروني هو ما يوضع على المحرر الالكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد الشخص وتمييزه عن غيره"، نادر شافي، أنواع التوقيع الالكتروني، منشور على الموقع الإلكتروني التالي: https://twitmail.com>fullview.

خاتمة:

نتيجة التطور السريع والمذهل في عالم تكنولوجية المعلوماتية، من وسائل اتصال وشبكات المعلومات وأجهزة الكمبيوتر وتطور التقنيات الحيوية، جعل البيئة الرقمية في شتى المجالات تعمل على تسهيل وتسريع نقل المعلومات ربحاً للوقت والجهد واقتصاداً للمال، لكن بالمقابل أصبحت هناك مخاطر واعتداءات إلكترونية تستهدف كيانات العالم الرقمي، فبات من الضروري مواكبة ذلك التطور من حيث التشريعات والتنظيمات والإجراءات التي بواسطتها يمكن التحكم في مراقبة وحماية المعلومات المتدفقة في الفضاءات الرقمية لاسيما منها ما يتعلق بالملكية الفكرية والمعلومات الشخصية، التي بدورها تطورت بتطور عصر المعلومات والمعرفة مع ظهور تكنولوجيات الإعلام و الاتصال، حيث أصبحت من الحقوق التي تستدعي أمنها وحمايتها من المخاطر والتهديدات التي تواجهها خاصة ما يتعلق منها بالجرائم الإلكترونية الماسة بالمعلومات الشخصية.

لذلك استوجب استحداث طرق تقنية تعمل على الفضاء الالكتروني لها فعالية كبيرة في حماية هكذا معلومات، إلى جانب النصوص القانونية فرضها المشرع الجزائري لاسيما نصوص المتعلقة بالجريمة المعلوماتية، غير أن هذا لا يعد كافيا في مواجهة مثل هكذا جرائم ، إذ لابد على رجال القانون التدخل لمكافحة الجرائم الناشئة عن استخدام الانترنت بإصدار تشريعات مستقلة للإحاطة بجميع جوانب الجرائم المتعلقة بالحاسوب والإنترنت.

السوار الالكتروني كآلية تكنولوجية لتنفيذالعقوبة السالبة للحرية قصيرة المدة

د/ بن جدو آمال – كلية الحقوق –جامعة الجزائر 1.

Amel.bendjeddou@yahoo.fr

ط د/ ابراهيمي رابح–كلية الحقوق –جامعة الجزائر 1.

Brahimi.rabah@hotmail.com

ملخص:

لجأت مختلف التشريعات خصوصا الأجنبية إلى اعتماد السوار الالكتروني مستعينة بأحدث التقنيات والتكنولوجيات لتحقيق التطبيق الفعال له كإجراء لتنفيذ العقوبة السالبة للحرية قصيرة المدة ،لان هذه الأخيرة أفرزت آثار سلبية أكثر منها إيجابية ،مست بأغراض السياسة العقابية التي أصبحت تهدف لتأهيل وإصلاح المحكوم عليه بدلا من مجرد عقابه والثأر منه ،فبعد النص عليه قانونا وفرت كل ما من شأنه المساعدة على نجاحه ميدانيا ،كما نص عليه المشرع الجزائري عام 2015 ،وصدر القانون المنظم له عام 2018 إلا أن تطبيقه واقعيا يبقى منعدم لمواجهته مشاكل تقنية.

الكلمات المفتاحية:

السوار الالكتروني،المراقبة الالكترونية،إنسانية العدالة الجنائية.

Abstract:

Various legislations, especially foreign ones, have resorted to the adoption of the electronic bracelet using the latest techniques and technologies to achieve its the effective application of it as a measure to implement the short-term deprivation of liberty penalty, because the latter has produced negative effects more than positive, affecting the purposes of the punitive policy, which has become aimed at rehabilitating and reforming the sentenced person instead of just punishing him and taking revenge on him.

After stipulating it as a law, it provided everything that would help its success on the ground, as stipulated by the Algerian legislator in 2015, and the law regulating it was issued in 2018, but its application in reality remains non-existent because it faces technical problems.

Key words :

Electronic Bracelet, Electronic monitoring, Criminal Justice Humanity.

مقدمة:

تعد العقوبات السالبة للحرية رد فعل على ارتكاب الجريمة وهي الأكثر شيوعا في المجال الجنائي وجدت لعقاب الجاني وتحقيق الزجر،الايلام والردع، وقد حققت ذلك في وقت ما ،إلا أنه مع كثرة الجرائم وتطورها تكنولوجيا ،وازدياد عدد المجرمين المحكوم عليهم بسلب الحرية من جهة، وتطور أغراض السياسة العقابية من جهة أخرى من مجرد الايلام والردع إلى الإصلاح والتأهيل، أصبحت العقوبة السالبة للحرية غير صالحة لكل الجرائم ،ولا يمكن تطبيقها على كل المجرمين ،لأن المبتدئ ليس كالمحترف والجريمة البسيطة ليست كالخطيرة ،كما أن كثرة الحكم بها أفرز تكدس وتضخم في المؤسسات العقابية ،إذ لم تعد تستوعب الكم الهائل من المجرمين سواء من حيث المساحة والنفقات، أو من حيث برامج الإصلاح والتأهيل

انطلاقا من ذلك كان لابد من البحث عن بدائل تحل محل العقوبة السالبة للحرية قصيرة المدة للتخفيف والتقليل من كثرة الحكم بها، فوجدت عقوبات بديلة لعقوبة الحبس منها العمل للنفع العام، وقف التنفيذ، وغيرها ،ونظرا لأن الحياة البشرية تطورت تكنولوجيا فقد تم الاعتماد على ذلك لايجاد إجراءات جديدة لتنفيذ عقوبة سلب الحرية تتميز بالتكنولوجية الحديثة من خلال تقنيات متطورة ،ومنه ظهر ما يعرف بالسوار الالكترونيأو المراقبة الالكترونية ،إذ تعتبر الدول الأجنبية لاسيما الأمريكية أول ما جاء به ،أين استعانت به في المجال الجنائي كاجراء جديد لتنفيذعقوبة سلب الحرية ،ولقى ذلك نجاحا باهرا ،لينتقل إلى التشريع الجزائري ،وهو أول تشريع عربي ينص على إمكانية اللجوء للسوار الالكتروني أين أصدر عام 2018 قانونا يعدل القانون 04/05 المتعلق بتنظيم السجون وإعادة الادماج الاجتماعي للمحبوسين ،يتضمن أحكام الاستعانة به كاجراء يسمح بقضاء المحكوم عليه كل العقوبة أو جزء منها خارج المؤسسة

العقابية عن طريق حمل الشخص المحكوم عليه لسوار الكتروني يسمح بمعرفة مكان تواجده المحدد من طرف قاضي تطبيق العقوبات، كما تضمنت مواده النص على أن يتم تطبيق نظام المراقبة الالكترونية تديريجيا متى توفرت الشروط الضرورية لذلك ،ولنجاح تطبيقه لابد من الاستعانة بأحدث الوسائل التقنية والتكنولوجية.

هل شهد تطبيق السوار الالكتروني نجاحا في التشريع والقضاء الجزائري؟

المبحث الأول:

دور السوار الالكتروني فيتنفيذ العقوبة السالبة للحرية قصيرة المدة

تتجه السياسة الجنائية المعاصرة نحو الحد من العقوبات السالبة للحرية لاسيما قصيرة المدة بالاعتماد على أسلوب الحد من العقاب إما بتسليط عقوبات غير جنائية أو عقوبات جنائية غير سالبة للحرية من خلال استغلال التكنولوجيا الحديثة التي أنتجت وجود السوار الالكتروني وهو الذي يساعد على مراقبة المحكوم عليه دون الحاجة لسلب حريته.

المطلب الأول:

مبررات استخدام السوار الالكتروني

انطلاقا من العقوبات البديلة لعقوبة الحبس والتي تسلط على المحكوم عليه بدل سلب حريته، فتكون بديلا للعقوبة السالبة للحرية قصيرة المدة مثل العمل للنفع العام ووقف التنفيذ، تمت الاستعانة كذلك بالسوار الالكتروني أو كما يحبذ البعض استخدام مصطلح المراقبة الالكترونية، إذ هو الاجراء الأبرز الذي يعتمد على التكنولوجيا الحديثة من خلال استخدام تقنيات رقمية تساعد أجهزة القانون من متابعة المحكوم عليه خارج المؤسسة العقابية عن طريق خضوعه لمجموعة من الالتزامات والشروط[1]

حيث عرف على أنه نظام الكتروني عن بعد يمكن بموجبه التأكد من وجود أو غياب شخص عن المكان المخصص لإقامته بموجب حكم قضائي يسمح للمحكوم عليه بالبقاء في المنزل، ولكن تحركاته محدودة

---

[1] حورية بورابة، عبد الحليم موساوي، السوار الالكتروني بديل للعقوبة السالبة للحرية في التشريع الجزائري والتشريع المقارن، مجلة الفكر القانوني والسياسي ،المجلد06 ،العدد01 ،2022 ،ص1318.

ومراقبة بمساعدة جهاز مثبت في معصمه أو في أسفل قدمه[1]، كما أنه مصطلح عام يشير إلى أشكال المراقبة التي يتم من خلالها مراقبة الموقع وحركة وسلوك شخص محدد وفق إجراءات العدالة الجنائية[2].

وراء ظهور السوار الالكتروني مجموعة من الأسباب تتمحور أولا حول مساوئ العقوبة السالبة للحرية لاسيما قصيرة المدة إذ لم تعد تحقق الغرض الذي وجدت لأجله ولم يعرف تأهيل الجاني بقدر ما عرف احترافه داخل المؤسسات العقابية واندماجه فيها بدل اندماجه في المجتمع واختلاط المجرم المبتدئ مع المحترف والخطير[3] مما يصعب عملية التأهيل لاحقا.

ثانيا مشكلة اكتظاظ وتكدس المؤسسات العقابية حيث أصبحت جميع السجون تعاني من هذه المشكلة بسبب كثرة الحكم بعقوبات سالبة للحرية ،فتعجز المؤسسات العقابية عن استيعاب الكم الهائل للمسجونين وبذلك تضعف أو تنعدم عملية إصلاح وتأهيل الجاني كغرض حديث للسياسة العقابية.

كما أثر التطور التكنولوجي على ظهور السوار الالكتروني إذ يعرف العالم الحديث تطور تكنولوجي بتقنيات متطورة أثرت على جميع المجالات ،ومنها عالم القانون الجنائي ،من جانب المجرمين والجهات القانونية القضائية ،إذ أصبح المجرمون يعتمدون على وسائل تكنولوجية حديثة في تنفيذ العمليات الإجرامية ،كرد فعل واجهتهم جهات التحقيق بوسائل متطورة في البحث، التحري والتحقيق ثم في المحاكمة، وامتد التطور التكنولوجي إلى ما بعد مرحلة المحاكمة ،في مرحلة تنفيذ الحكم ،ومنه وجد السوار الالكتروني كبديل عن العقوبة السالبة للحرية قصيرة المدة[4].

كما ظهر السوار الالكتروني لتحقيق الأغراض الحديثة للعقاب والتي تتمثل خصوصا في الإصلاح والتأهيل ،لأن العقوبة السالبة للحرية أصبحت تحقق فقط غرض الثأر منالجاني والانتقام منه ،فلم تعد تأهله ولا تعيد اندماجه في المجتمع ،بينما السوار الالكتروني كبديل عن العقوبة السالبة للحرية قصيرة المدة يحقق التأهيل والاندماج ،بأن لا يختلط المجرم المبتدئ مع المحترف ،ولا يكتسب خبرات إجرامية إذ

---

[1] عباسة طاهر ،عامر جوهر، السوار الالكتروني اجراء بديل للعقوبة السالبة للحرية في التشريع الجزائري ،مجلة الاجتهاد القضائي ،العدد16 ،مارس2018 ،ص187.

[2] MIKE NELLIS . DOMINIK LEHMER . scope and definitions electronic monitoring ,Eouropean comitteé on crime problems ,council for penological cooperation ,16 octobre 2012.

[3] عباسة طاهر ،المرجع السابق ،ص186.

[4] صورية بوربابة ،عبد الحليم موساوي ،المرجع السابق ،ص1319.

يبقى كالشخص الحر الفرق فقط في أنه مراقب من طرف الجهات المختصة إذ يمنع عليه مغادرة المكان المحدد لأن حريته مقيدة وليست مسلوبة مثلما هو الحال في العقوبات السالبة للحرية وبالتالي يستطيع ممارسة حياته بكل حرية، كما أن نفسية المحكوم عليه بسوار الكتروني تكون معتدلة مقارنة بمن هو محبوس في مؤسسة عقابية إذ تكون نفسيتها منهارة.

كما أن السوار الالكتروني يقلل من النفقات التي تنفقها الدولة على المؤسسات العقابية فكلما كان عدد المحبوسين أقل كانت تكلفة النفقات تقل ،وكلما زاد عدد المحبوسين زادت الأموال التي تنفقها الدولة لاسيما من أجل تطبيق برامج الإصلاح والتأهيل بينما السوار الالكتروني يقتصد النفقات ،فهو يهدف لسياسة ترشيد وإنسانية العقاب[1].

المطلب الثاني :

الشروط القانونية للاستعانة بالسوار الالكتروني

السوار الالكتروني كإجراء قانوني لتنفيذ العقوبة السالبة للحرية قصيرة المدة يخضع لجملة من الشروط بعضها يرتبط بشخص المحكوم عليه ،والبعض الآخر مرتبط بالعقوبة المحكوم بها، فأولا يطبق السوار الالكتروني على الشخص الطبيعي البالغ سن الرشد الجزائي، كما يطبق على القاصر كلما وافق عليه ممثله القانوني ،ويستفيد منه كذلك المسبوق قضائيا ،وفي جميع الحالات يشترط الحصول على موافقة المحكوم عليه شأنه شأن العمل للنفع العام إذ لا يوضع غصبا عنه ،إنما بعد الحصول على رضاه وبعدما يحدد المعني مقر إقامته[2] ،كما يسدد ما عليه من التزامات مالية .

أيضا يجب أن لا يتعارض السوار الالكتروني مع صحة المحكوم عليه ،فإن كان يضر بصحة وسلامة المعني يستبعد تطبيقه ومنه يتوجب على الجهة المختصة بتنفيذ السوار الالكتروني التأكد أولا وقبل كل شيء من أنه لا يتعارض ولا يمس صحة المحكوم عليه بأي شكل من الأشكال ،كما تأخذ بعين الاعتبار عند الوضع تحت المراقبة الالكترونية الوضعية العائلية للمعني أو متابعته لعلاج طبي أو نشاط مهني أو

---

[1] ويزة بلعسلي ،الوضع تحت نظام المراقبة الالكترونية باستعمال السوار الالكتروني (آليات ترشيد السياسة العقابية المعاصرة)، مجلة الحقوق والحريات ،تيزي وزو ،العدد05 ،2018 ،ص147.

[2] هارون نورة، تأثر السياسة العقابية الجزائرية بالتطور التكنولوجي :الوضع تحت المراقبة الالكترونية ،المجلة الأكاديمية للبحث القانوني ،المجلد11 ،العدد04 ،2020 ،ص89.

دراسي أو تكويني، فقبل حبس المحكوم عليه في مكان معين يتعين النظر إلى دراسته أو مهنته ،أو التكوين الذي يزاوله حتى لا ينقطع عن إكمال ما يمارسه لأن الغرض من السوار الالكتروني هو إعادة إدماج الجاني في المجتمع دون إبعاده عن بيئته الطبيعية ،كما يطبق السوار الالكتروني كلما أظهر المحكوم عليه ضمانات جدية للاستقامة[1]، فبدل حبسه في مؤسسة عقابية يتم مراقبته الكترونيا بواسطة السوار، يتبين من ذلك أن السوار الالكتروني يطبق كبديل للعقوبة السالبة للحرية ،أو لتنفيذ الجزء المتبقي من العقوبة السالبة للحرية إن سبق الحكم بها على المحكوم عليه.

أما فيما يخص الجهات المعنية بالسوار الالكتروني فيجب أن تحترم خصوصية المحكوم عليه لأن الحق في الحياة الخاصة[2] من الحقوق المكفولة قانونا ودستورا ،وهو امتداد لوجوب الحصول على رضا المحكوم عليه .

أيضا لتطبيق السوار الالكتروني لابد من توافر جملة من الشروط المتعلقة بالعقوبة أولها أن تكون العقوبة الأصلية من العقوبات السالبة للحرية ،لأن السوار الالكتروني إجراء بديل لعقوبة الحبس للتخفيف من الآثار السلبية لها ،فلا يكون بديلا لعقوبة مالية[3]، ولا بديلا للبدائل الأخرى من عمل للنفع العام وغيرها ،كما يشترط في العقوبة السالبة للحرية أن لا تتجاوز 3 سنوات حتى يمكن استبدالها بالسوار الالكتروني ،وإن كان المحكوم عليه سبق وأن حكم عليه بعقوبة سالبة للحرية ودخل المؤسسة العقابية فيشترط أن تكون المدة المتبقية تساوي أو تقل عن 3 سنوات ،أما فيما يخص الحكم فلابد أن يكون نهائيا ،ومنه لا يمكن تطبيقه على المتهم المحبوس مؤقتا ،ويطبق على الجرائم البسيطة إن كانت عقوبتها السجن بناءا على حكم من طرف قاضي تطبيق العقوبات وبعد أخذ رأي لجنة تطبيق العقوبات، أو بطلب من المحكوم

---

[1] المادة 150 مكرر3 من القانون رقم 01/18 المعدل للقانون 04/05 المتعلق بتنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين "تؤخذ بعين الاعتبار عند الوضع تحت المراقبة الالكترونية الوضعية العائلية للمعني ،أو متابعته لعلاج طبي أو نشاط مهني أو دراسي أو تكويني أو إذا أظهر ضمانات جدية للاستقامة.

[2] ويزة بلعسلي ،المرجع السابق، ص150.

[3] محمود محمد بهجت عبد الرحمان محمد، التكييف الفقهي والقانوني للسوار الالكتروني كعقوبة مستحدثة ،مجلة كلية الشريعة والقانون،دقهلية، مصر ،العدد23 ،2021

عليه أو محاميه الذي يرسل الطلب إلى قاضي تطبيق العقوبات، وهذا الأخير يفصل فيه خلال مدة 10 أيام[1] .

أما الجهة المختصة بتطبيق اجراء السوار الالكتروني فهو قاضي تطبيق العقوبات إما من تلقاء نفسه أو بطلب من المحكوم عليه أو محاميه، يقرر إخضاع المحكوم عليه لسوار الكتروني بموجب مقرر بعد أخذ رأي النيابة العامة، وأخذ رأي لجنة تطبيق العقوبات بالنسبة للمحبوسين الذين تكون المدة المتبقية لهم أقل من 3 سنوات، يتم إلزام المحكوم عليه بالبقاء في المكان المحدد من طرف قاضي تطبيق العقوبات، وغالبا ما يكون المنزل ،إذ يسمى السوار الالكتروني " الحبس المنزلي" نظرا لحبس المعني بمنزله وعدم مغادرته، كما يمكن إخضاع المعني لتدبير أو أكثر من التدابير المحددة في المادة 150 مكرر6 من القانون 01/18[2]":ممارسة نشاط مهني أو متابعة تعليم أو تكوين مهني ،عدم ارتياد بعض الأماكن، عدم الاجتماع ببعض المحكوم عليهم بما في ذلك الفاعلين الأصليين أو الشركاء في الجريمة، عدم الاجتماع ببعض الأشخاص لاسيما الضحايا والقصر، الالتزام بشروط التكفل الصحي أو الاجتماعي أو التربوي أو النفسي التي تهدف إلى إعادة إدماجه اجتماعيا ".

إن التزم المحكوم عليه بالالتزامات المفروضة عليه من طرف قاضي تطبيق العقوبات تنتهي عقوبته المحكوم بها عليه بواسطة السوار الالكتروني بمجرد انتهاء المدة التي حددها القاضي ،أما إن أخل بالتزاماته بتغيبه عن المكان المحدد في مقرر الإدانة أو إذا حاول تعطيل الأجهزة ،فيقوم المؤهلين المختصين بإثبات المخالفة، تتم إدانة المحكوم عليه إن ارتكب جريمة جديدة أثناء وضعه تحت المراقبة الالكترونية، أو في حال رفضه الامتثال لتعديل التزامات المراقبة الالكترونية[3].

المبحث الثاني:

السوار الالكتروني بين النص عليه وتطبيقه

---

[1] صورية بوربابة ،عبد الحليم موساوي ،المرجع السابق ،ص1323

[2] قانون رقم 01/18 المؤرخ في 2018/01/30 يتمم القانون 04/05 المؤرخ في 2005/02/06 المتضمن قانون تنظيم السجون وإعادة الادماج الاجتماعي للمحبوسين ،الجريدة الرسمية العدد05 ،مؤرخ في 2018/01/30.

[3]صورية بوربابة ،عبد الحليم موساوي ،المرجع السابق ،ص1323

يعتبر السوار الالكتروني من أهم ما أفرزه التطور التكنولوجي في مجال السياسة العقابية حيث اتجهت التشريعات الغربية أولا إلى تطبيق فكرة المراقبة الالكترونية كإجراء بديل عن العقوبة السالبة للحرية ،ولقى ذلك استحسان معظم الدول الأجنبية أين لجأت للنص على إمكانية اللجوء للسوار الالكتروني ،وخصصت كل ما يلزم من أساليب ووسائل لتطبيقه وامتد هذا الاهتمام إلى الدول العربية وإن كان تطبيقه مقيد ومحصور مقارنة مع الدول الأجنبية ،كما حبذ المشرع الجزائري النص عليه قانونا في قانون تنظيم السجون وإعادة الادماج الاجتماعي للمحبوسين ،وإن كان تطبيقه بأرض الواقع لم يتم بقوة .

المطلب الأول:

تطبيق السوار الالكتروني في الدول الغربية

أول ظهور للسوار الالكتروني كان في الدول الأجنبية ،الأمريكية بالضبط حيث بحلول عام 1982، كان قاضي أمريكي(judje love) مقتنعا بأنه يمكن استخدام مزيج من سوار إرسال، وجهاز قريب لقراءة البطاقات للتحقق من أن الشخص الذي يخضع للمراقبة كان في مكان معين،حاول اقناع العديد من شركات الكمبيوتر إلا أنها لم تقتنع، لكن ممثل المبيعات في شركة هانيويل لأنظمة المعلومات ، مايكل تي جوس ،وهو ضابط سابق في البحرية وشرطيأحب الفكرة[1]،أين اقتنع بصنع سوار الكتروني يوضع على معصم اليد ،وبالفعل تم التوصل عام1983 إلى أول نظام يسمح بذلك من خلال رصد الحركة ،وتم تطبيق هذه التجربة كبديل للحبس المؤقت ،ولقت نجاحا ،وبعد ذلك تم تعميم التجربة إلى باقي الولايات الأمريكية .

انتقلت التجربة لاحقا إلى الدول الأوروبية بدأت في بريطانيا عام1989 وانتشرت لباقي الدول وصولا لفرنسا بموجب القانون 1159/97 المعدل لقانون الإجراءات الجزائية[2]

يعرف السوار الالكتروني في الدول الغربية ثلاث أنواع لكل منها خاصيتها وطرق خاصة لتطبيقها ،أولا الترددات الإذاعيةradio Frequency)(تستخدم خصيصا في اسكتلندا وهي تقنية بسيطة يتم استخدامها

---

[1] Robert S. GableThe Ankle Bracelet Is History: An Informal Review of the Birth and Death of a Monitoring Technology ,The Journal of Offender Monitoring , 2015 Civic Research Institute.p5.

[2] صورية بوربابة ،عبد الحليم موساوي ،المرجع السابق ،ص1325.

بشكل شائع لمراقبة حالات حظر التجول التي يتم من خلالها تقييد الأشخاص الخاضعين للمراقبة في مكان معين عادة ما يكون منزلهم أو تقييدهم بعيدًا عن مكان ما مثلا متجر في حالات السرقة المتكررة لفترات زمنية محددة،ثانيا جهاز التعريف الشخصي (a tag) ، يوصل بكاحل الشخص الذي يخضع للمراقبة أو بمعصمه يكتشف محاولة الشخص لإزالتهالجهاز، ترسل علامة التردد اللاسلكي إشارة إلى صندوق وحدة المراقبة المركب في منزلهم أو في مكان آخر محدد ، والذي يراقب وجود المعني أو غيابه عن هذا الموقع خلال الفترات الزمنية المحددة ،ثالثا نظام تحديد المواقع العالميتعد تقنية (GPS) نظامًا عالميًا يستخدم الأقمار الصناعية لتتبع الموقع في الوقت الفعلي، علامة GPS عبارة عن جهاز إرسال مقاوم للعبث يتم ارتداؤه حول الكاحل ويستقبل الإرسال من الأقمار الصناعية ويحدد الموقع بناءً على القوة النسبية للإشارات[1].

المطلب الثاني:

تطبيق السوار الالكتروني بين القانون والقضاء الجزائري

بعدما لقت المراقبة الالكترونية بواسطة السوار الالكتروني استحسان التشريعات الأجنبية عهدت بعض التشريعات العربية إلى تطبيقه في قوانينها مثل التشريع السعودي[2] ،أما التشريع الجزائري فقد نص على إمكانية اللجوء للسوار الالكتروني عام 2015 بموجب القانون رقم 02/15[3]المعدل للأمر 155/66 المتضمن قانون الإجراءات الجزائية كإجراء لتنفيذ العقوبة السالبة للحرية موازاة مع تأهيل المحكوم عليه وإدماجه في المجتمع كغرض حديث للسياسة العقابية ،وفي إطار احترام حقوق الإنسان وتوفير المحاكمة العادلة ،إلا أنه منذ ذلك الوقت لم يصدر أي تنظيم يبين شروط وإجراءات وكيفية اللجوء للسوار

---

[1]HANNAH GRAHAM , GILL MCIVOR ,Electronic monitoring in the criminal justice system,INSIGHTS A SERIES OF EVIDENCE SUMMARIES ,november 2017 ,p4,5.

[2] تضمن مشروع نظام العقوبات البديلة النص على السوار الالكتروني الذي قدم لوزارة العدل ،كما طبقت وزارة الداخلية بالمملكة عام2011 فكرة استخدام السوار الالكتروني كبديل عن الحبس المؤقت على المجرمين غير الخطرين ،خصوصا الحالات التي تستدعي مغادرة المحكوم عليه لمدة معينة مثل زيارة مريض أو حضور عزاء ،وذلك بمتابعة جهات أمنية.

[3] المادة 125 مكرر1 "يمكن لقاضي التحقيق أن يأمر بأخذ ترتيبات من أجل المراقبة الالكترونية لتنفيذ التزامات الرقابة القضائية".

–محمد بن حميد المزمومي، المراقبة الالكترونية كبديل للعقوبة السالبة للحرية ،دراسة في ضوء النظام السعودي والأنظمة المقارنة، مجلة ضوت القانون، المجلد7 ،العدد2، 2020.

الالكتروني لغاية 2018 بموجب القانون 01/18 المعدل للقانون 04/05 بموجب المواد 150 مكرر إلى 150 مكرر16 الباب السادس الفصل الرابع ،أين بين ووضح كيفية القيام بتطبيق سوار الكتروني والجهة المختصة بذلك والتي تتمثل في قاضي تطبيق العقوبات ،وقد نص في المادة 150 مكرر على أن الوضع تحت المراقبة الالكترونية اجراء يسمح بقضاء المحكوم عليه كل العقوبة أو جزء منها خارج المؤسسة العقابية" بمعنى أنها تتجنب وضع المتهم في الحبس كبديل عن العقوبة السالبة للحرية ،أو يمكن أن يكون اجراء تأهيلي بعد دخول المتهم للمؤسسة العقابية ،يفضل إكمال الجزء المتبقي خارجا لإعادة إدماج المجرمين ،والتخفيف من النفقات المالية التي تتطلبها السجون ،والتقليص لأكبر حد من سلبيات العقوبة السالبة للحرية.

أما على المستوى التطبيقي فقد طبق لأول مرة بتاريخ 2016/12/25 على مستوى المحكمة الإبتدائية لتيبازة ،أين أصدر قاضي التحقيق حكما بتطبيق السوار الالكتروني على متهم بجريمة ضرب وجرح بالسلاح الأبيض[1] ،وذلك قبل صدور القانون المنظم له 01/18 ،أما بعد ذلك قلم يحقق تطبيقه نجاحا قد يعود ذلك لأسباب تقنية وتكنولوجية ،وهو ما صرح به وزير العدل بلقاسم زغماتي عندا قال بصريح العبارة" أن العملية اعترضتها مشاكل تقنية حالت دون مواصلة اعمل بهاته الوسيلة ،والعملية متوقفة لغاية إعادة النظر في المسألة"

خاتمة:

السوار الالكتروني من أساليب المراقبة الالكترونية وهو اجراء قانوني بديل عن العقوبة السالبة للحرية ،وجد للتخلص أو التقليل من النتائج السلبية لها ،خصوصا بعدما تطورت أغراض السياسة العقابية إلى إصلاح ،وتأهيل المحكوم عليه وإعادة إدماجه في المجتمع ،بينما سلب الحرية لم يعد كافيا لتحقيق ذلك ،ومنه وجب التخلي نوعا ما عن القواعد الجنائية التقليدية وإدخال قواعد جنائية حديثة تتسم بالإنسانية والتأهيلية والتكنولوجية كذلك، نظرا لعصرنة العدالة وتطور الحياة البشرية تكنولوجيا من جميع نواحيها .

النتائج.:

---

[1] محمد المهدي بكراوي،حباس عبد القادر ،جامع مليكة، نظام الوضع تحت المراقبة الالكترونية في التشريع الجزائري ،مجلة آفاق علمية ،المجلد11، العدد3، 2019،ص275.

-واكب المشرع الجزائري كأول تشريع عربي المجتمعات الغربية من حيث النص على إمكانية اللجوء للسوار الالكتروني.

-وجد السوار الالكتروني لتحقيق الأغراض الحديثة للسياسة العقابية من إصلاح وتأهيل ،والتقليل من سلبيات العقوبات السالبة للحرية.

-يحقق السوار الالكتروني عصرنة العدالة ويتجه نحو تحقيق عدالة تصالحية اجتماعية من خلال إنسانية العقاب .

-على غرار العقوبات السالبة للحرية فإن السوار الالكتروني يحقق نتائج إيجابية للمحكوم عليه سواء نفسيا ،اجتماعيا ،أو جنائيا ،ويحقق الإيجابية كذلك بالنسبة للدولة من خلال تقليل النفقات .

التوصيات:

-ضرورة حل المشاكل التقنية التي تعترض التطبيق السليم للسوار الالكتروني ،والأخذ بتجارب الدول الأجنبية أثناء الاستعانة به.

-التقليل لأكبر حد ممكن من الحكم بعقوبات سالبة للحرية لما أفرزته هذه الأخيرة من سلبيات على المحكوم عليه ،والاعتماد على البدائل التي تركز على الإصلاح والتأهيل .

-توفير الإمكانيات من أجل تحقيق تطور تكنولوجي على مستوى القانون الجنائي ليستفيد منه السوار الالكتروني من أجل تحقيق نتائج فعالة.

-الاتجاه نحو إنسانية العقاب من خلال التركيز على إعادة ادماج المجرمين تحقيقا لعدالة تصالحية اجتماعية بدلا من عدالة عقابية محضة .

قائمة المراجع:

النصوص القانونية :

-القانون رقم 01/18 المؤرخ في 2018/01/30 يتمم القانون 04/05 المؤرخ في 2005/02/06 المتضمن قانون تنظيم السجون وإعادة الادماج الاجتماعي للمحبوسين ،الجريدة الرسمية العدد05 ،مؤرخ في 2018/01/30.

-القانون رقم 02/15 المعدل للأمر 155/66 المتضمن قانون الإجراءات الجزائية.

المقالات العلمية:

- حورية بورابابة، عبد الحليم موساوي، السوار الالكتروني بديل للعقوبة السالبة للحرية في التشريع الجزائري والتشريع المقارن، مجلة الفكر القانوني والسياسي ،المجلد06 ،العدد01 ،2022

- محمد المهدي بكراوي،حباس عبد القادر ،جامع مليكة، نظام الوضع تحت المراقبة الالكترونية في التشريع الجزائري ،مجلة آفاق علمية ،المجلد11، العدد3، .2019

-محمد بن حميد المزمومي، المراقبة الالكترونية كبديل للعقوبة السالبة للحرية ،دراسة في ضوء النظام السعودي والأنظمة المقارنة، مجلة ضوت القانون، المجلد7 ،العدد2، 2020

- محمود محمد بهجت عبد الرحمان محمد، التكييف الفقهي والقانوني للسوار الالكتروني كعقوبة مستحدثة ،مجلة كلية الشريعة والقانون،دقهلية، مصر ،العدد23 ،2021.

- ويزة بلعسلي ،الوضع تحت نظام المراقبة الالكترونية باستعمال السوار الالكتروني (آليات ترشيد السياسة العقابية المعاصرة)، مجلة الحقوق والحريات ،تيزي وزو ،العدد05 ،2018 .

- هارون نورة، تأثر السياسة العقابية الجزائرية بالتطور التكنولوجي :الوضع تحت المراقبة الالكترونية ،المجلة الأكاديمية للبحث القانوني ،المجلد11 ،العدد04 ,2020.

- عباسة طاهر ،عامر جوهر، السوار الالكتروني اجراء بديل للعقوبة السالبة للحرية في التشريع الجزائري ،مجلة الاجتهاد القضائي ،العدد16 ،مارس2018.

- MIKE NELLIS . DOMINIK LEHMER . scope and definitions electronic monitoring ,Eouropean comitteé on crime problems ,council for penological cooperation ,16 octobre 2012.

-HANNAH GRAHAM , GILL MCIVOR , Electronic monitoring in the criminal justice system, INSIGHTS A SERIES OF EVIDENCE SUMMARIES ,november 2017.

-Robert S. Gable The Ankle Bracelet Is History: An Informal Review of the Birth and Death of a Monitoring Technology , The Journal of Offender Monitoring , Civic Research Institute, 2015.

مداخــلة مشتركة للمشاركة في الملتقى الدولي الافتراضيحول:

"القانون الجنائي في ظل التطور التكنولوجي"

-اشكالات ومعالجات-

***الاســم واللقب:** خـالـد بوكتاب

المؤهل العلمي:طـالـب دكـتـوراه وعضو في مخبر "الدراسات القانونية المغاربية" –عنابة

التخصص: قانون المرفق العام

الوظيفة: أستاذ مشارك

المهنة: محام معتمد لدى مجلس قضاء عنابة

المؤسسة: جامعة باجي مختار، كلية الحقوق والعلوم السياسية – عنابة

الهاتف:06.74.51.01.04

البريد الإلكتروني:boukettab.khaled@gmail.com

***الاسم واللقب:** بلفار شوقي

المؤهل العلمي:طالب دكتوراه وعضو في مخبر "الدراسات القانونية البيئية" –قالمة.

التخصص: قانونعام

الوظيفة: أستاذ مشارك

الهيئة المستخدمة:كلية الحقوق والعلوم السياسية، جامعة 08 ماي 1945 – قالمة.

الهاتف: 06.61.86.78.36

البريد الالكتروني: Belfar.chaouki@univ-guelma.dz

محور المداخلة :المحور الثالث (التطور التكنولوجي عامل تطور في تطبيق العقوبات السالبة للحرية)

عنوان المداخلة: "انعكاسات التطور التكنولوجي على تنفيذ الأحكام الجنائية"

ملخص:

مع اتجاه السياسة الجنائية الحديثة إلى تبني فكرة تأهيل وإصلاح المحكوم عليهم كغرض مهم للجزاء الجنائي، وثبوت فشل تلك السياسة في تحقيق هذا الهدف، اتجهت للبحث عن بدائل للعقوبات التي ثبت فشلها في تحقيق غاية الاصلاح والتأهيل، وبالأخص عقوبة الحبس قصير المدة، وقد كان من نتائج البحث عن بدائل لتلك العقوبات، ابتكار بعض الوسائل والأدوات التي ساهمت بشكل كبير في الحد من مساوئ سلب الحرية قصير المدة، وقد اعتمدت بعض تلك الخيارات على وسائط الكترونية، وهو ما يشير بشكل أو بآخر إلى استخدام التحول الرقمي في تنفيذ العقوبات، كما اعتمدت خيارات أخرى على آليات أخرى يمكن تنفيذها من خلال توظيف التكنولوجيا الحديثة وربطها بمعلومات وبيانات المحكوم عليه المسجلة لدى الجهات المختلفة داخل الدولة، ومن خلال هذه المداخلة سنعرض بعض الخيارات القائمة على استخدام التكنولوجيا والتي تبنتها السياسة الجنائية الحديثة في تنفيذ العقوبات.

Abstract:

As modern criminal policy has tended to adopt the idea of rehabilitating and reforming convicts as an important purpose of criminal punishment, and proving that it has failed to achieve this goal, it has sought alternatives to sanctions that have proven to have failed to achieve the goal of reform and rehabilitation, particularly short-term imprisonment, and one of the results of the search for alternatives to such penalties has been the creation of some means and tools that have contributed significantly to reducing the disadvantages of short-term deprivation of liberty, some of which have relied on electronic media, This indicates in one way or another the use of digital transformation in the implementation of sanctions, and other options have relied on other mechanisms that can be implemented through the use of modern technology and linking it to the information

and data of the convict registered with various entities within the state, and through this intervention we will present some of the technology-based options adopted by modern criminal policy in the implementation of sanctions.

مقدمة:

مرت السياسة الجنائية على مدى العقود المنصرمة بعدة أزمات، كان أبرزها على الإطلاق تراكم القضايا الجنائية في المحاكم المختلفة، فضلا عن المشكلات المتعلقة بعدم تنفيذ أحكام الإدانة في العديد من القضايا، إذ تصدر المحاكم الجنائية آلاف الأحكام بالإدانة بشكل يومي، غير أن القليل من هذه الأحكام ما يصادف التنفيذ، ومن المعلوم أنه لا قيمة لحق لا نفاذ فيه، وفيما يتعلق بالأحكام التي تنفذ فعليا فيلاحظ أن أغلبها تصدر بعقوبات سالبة للحرية قصيرة المدة، وقد تبث فشل هذه العقوبات في تحقيق أغراض العقوبة.

ومع اتجاه السياسة الجنائية الحديثة إلى تبني فكرة تأهيل وإصلاح المحكوم عليهم كغرض مهم للجزاء الجنائي، وثبوت فشل تلك السياسة في تحقيق هذا الهدف، فقد اتجهت للبحث عن بدائل للعقوبات التي تبث فشلها في تحقيق غاية الإصلاح والتأهيل، وعلى الأخص عقوبة الحبس قصير المدة[1]، وقد كان من نتائج البحث عن بدائل لتلك العقوبات ابتكار بعض الوسائل والأدوات التي ساهمت بشكل كبير في الحد من مساوئ سلب الحرية قصيرة المدة، وقد اعتمدت بعض تلك الخيارات على وسائط الكترونية، وهو ما يشير بشكل أو بآخر إلى استخدام التحول الرقمي في تنفيذ العقوبات، كما اعتمدت خيارات أخرى على آليات أخرى يمكن تنفيذها من خلال توظيف التكنولوجيا الحديثة وربطها بمعلومات وبيانات المحكوم عليه المسجلة لدى الجهات المختلفة داخل الدولة.

---

[1] أحمد فتحي سرور، المشكلات المعاصرة للسياسة الجنائية الحديثة، مطابع جامعة القاهرة، 1983، ص 31.

على ذلك فقد أمكن استخدام التطور التكنولوجي الرقمي في تنفيذ العقوبات بتبني بعض السياسات المتعلقة بتصرفات المحكوم عليه، وكانت البداية في التشريع الأمريكي الذي ابتكر نظام الوضع تحت المراقبة الالكترونية بالسوار الالكتروني، او الحبس في البيت، أو الحبس المنزلي المراقب الكترونيا كأحد البدائل والحلول سنة 1983، ثم أخذت به كل من كندا سنة 1987، وانجلترا سنة 1994، وأيضا فرنسا منذ سنة 1997 بموجب قانون 19 ديسمبر 1997.[1]

ومحاولة من المشرع الجزائري اللحاق بركب التطور التشريعي العقابي، فقد تبنى بعض الآليات الحديثة مثل "الأمر الجزائي" و"المثول الفوري"، وكذا العمل للمنفعة العامة والمصالحة في المواد الجزائية، واستحداث نظام المراقبة الالكترونية في مرحلة التحقيق القضائي وذلك كبديل للحبس المؤقت وإجراء من إجراءات الرقابة القضائية، بموجب المادة 125 مكرر 1 من الأمر رقم 02/15 المعدل لقانون الإجراءات الجزائية، ثم تطور هذا الإجراء سنة 2018 ليشمل مرحلة تنفيذ العقوبة، حيث نصت المادة الثانية من القانون رقم 01/18 المتعلق بتنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين[2]، تنفيذا لأحكام

---

[1] ليلى طلبي، الوضع تحت المراقبة الالكترونية، مقال منشور بمجلة العلوم الانسانية، مجلة علمية محكمة تصدر عن جامعة منتوري، قسنطينة، العدد 47، المجلد –أ– جوان 2017، ص 255–256.

[2] قانون رقم 18–01 مؤرخ في 12 جمادى الأولى عام 1439 الموافق لـ 30 يناير سنة 2018، يتمم القانون رقم 05–04 المؤرخ في 27 ذي الحجة عام 1425 الموافق لـ 06 فبراير 2005 والمتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، ج ر عدد 47، 2018.

القانون رقم 03/15 المتعلق بعصرنة العدالة[1]، على أنه يتمم الباب السادس من القانون رقم 05-04 بفصل رابع عنوانه "الوضع تحت المراقبة الالكترونية" يتضمن المواد من 150 مكرر إلى 150 مكرر 16.

بذلك تعتبر الجزائر أول بلد عربي وثاني بلد إفريقي بعد جنوب افريقيا يشرع في العمل بنظام الوضع تحت المراقبة الالكترونية كإجراء بديل للعقوبة السالبة للحرية قصيرة المدة، ومن هنا يمكننا طرح الإشكالية التالية: "إلى أي مدى ساهم التحول الرقمي في تطوير منظومة العدالة خصوصا في مسألة تنفيذ العقوبة سالبة الحرية؟

وتندرج تحت هده الاشكالية الرئيسية، تساؤلات فرعية على النحو الآتي:

- هل يمكن اعتبار المراقبة الالكترونية آلية فعالة وبديلة لتنفيذ العقوبات السالبة للحرية؟

- وكيف يمكن للتحول الرقمي جعل المحكوم عليه بعقوبة سالبة للحرية أن يبادر إلى تنفيديها؟

للإجابة عن هاته الإشكالية المطروحة، ارتأينا تقسيم خطة الدراسة إلى محورين أساسين وهما:

المحور الأول: المراقبة الالكترونية كوسيلة لتنفيذ لتنفيذ العقوبات السالبة للحرية

المحور الثاني: مبادرة المحكوم عليه في تنفيذ العقوبة السالبة للحرية

المحور الأول: المراقبة الالكترونية كآلية لتنفيذ العقوبات السالبة للحرية

[1] قانون رقم 15-03 المؤرخ في 01 فبراير 2015 والمتعلق بعصرنة العدالة، ج ر عدد 06 لسنة 2015.

فضلا عن استخدام أسلوب المراقبة الالكترونية كوسيلة لتنفيذ إجراء الحبس الاحتياطي كإجراء من إجراءات التحقيق، استخدمت بعض النظم العقابية "المراقبة الالكترونية" كطريقة حديثة لمعالجة مساوئ تنفيذ العقوبات السالبة للحرية داخل المؤسسات العقابية، وذلك عن طريق حبس المحكوم عليه في محل إقامته خلال ساعات محددة، مع خضوعه لرقابة الكترونية[1].

ويفترض أسلوب التنفيذ من خلال المراقبة الالكترونية أن يتم الاتصال بين الشخصين –المحكوم عليه– وأجهزة المراقبة المثبتة في المؤسسة العقابية، بحيث يقوم السوار الالكتروني بالاتصال المستمر بالكومبيوتر المركزي في حالة تجاوز المحكوم عليه للحدود المسموح له بها، ويمكن القول بانه بهذهالطريقة تحل التكنولوجيا محل الحارس، بحيث تكون العلاقة مباشرة بين الإدارة العقابية والمحكوم عليه[2].

أولا: مفهوم الوضع تحت المراقبة الالكترونية

لقد عرف البعض المراقبة الالكترونية بأنها: "استخدام وسائل الكترونية للتأكد من وجود الخاضع لها خلال فترة محددة في المكان والزمان السابق الاتفاق عليها بين هذا الأخير والسلطة القضائية الآمرة بها"[3].

---

[1] عماد الفقي، النظم البديلة للحبس قصير المدة –دراسة مقارنة، الطبعة الأولى 2017، دار النهضة العربية. ص30.

[2] عمر سالم، المراقبة الالكترونية طريقة حديثة لتنفيذ العقوبات السالبة للحرية خارج السجن، دار النهضة العربية، الطبعة الثانية، د ت ن، ص 02.

[3] أسامة حسنين عبيد، المراقبة الجنائية الالكترونية –دراسة مقارنة، مجلة القانون والاقتصاد، كلية الحقوق جامعة القاهرة، العدد 82، ص 06.

كما ذهب رأي آخر إلى أنها: "احد البدائل الرضائية للعقوبات السالبة للحرية التي بمقتضاها يتم متابعة الشخص الخاضع لها من خلال استخدام تقنيات حديثة من قبل أجهزة إنفاذ القانون خارج السجن في أماكن وأوقات محددة سلفا، ومن خلال إخضاعها لمجموعة من الالتزامات والشروط، ويترتب عن مخالفة هذه الالتزامات معاقبته بعقوبة سالبة للحرية"[1].

وتعتبر المراقبة الالكترونية نوعاً من الحرية المراقبة أو المقيدة[2]، إذ تفرض المراقبة على الخاضع لها عدة التزامات، أهمها: عدم مبارحة المكان المحدد لدى الجهة المسؤولة التي تتولى متابعة التنفيذ، ولا يجوز للخاضع لهذا الإجراء الخروج عن ذلك إلا بعد الرجوع للقاضي المختص بمتابعة التنفيذ، وفي حالة ثبوت مخالفة المحكوم عليه هذا الالتزام فإنه يجوز للقاضي إلغاء المراقبة والعودة إلى تنفيذ العقوبة السالبة للحرية، ولا يطبق هذا الأسلوب على الجميع المحكوم عليهم بعقوبات سالبة للحرية، وإنما تطبق على من يثبت جدارته للاستفادة بها[3].

على ذلك، فإن نظام المراقبة الالكترونية يفترضاستخدام التكنولوجيا الحديثة في تنفيذ العقوبات السالبة الحرية، ويمكن من خلاله تفادي المساوئ المترتبة على هذه العقوبات، حيث يجنب المحكوم عليه شر الاحتكاك بغيره من المحكوم عليهم، مما يساهم في الحد من خطورته الإجرامية، ويمنع من اكتسابه

---

[1] رامي متولي القاضي، المراقبة الالكترونية في القانون الفرنسي والمقارن، مجلة الشريعة والقانون، كلية الحقوق، جامعة الإمارات، العدد 63، يوليو 2015، ص264.

[2] عماد الفقي، النظم البديلة للحبس قصير المدة، مرجع سابق، ص 51.

[3] أسامة حسنين عبيد، المراقبة الجنائية الالكترونية –دراسة مقارنة، مجلة القانون والاقتصاد –كلية الحقوق، جامعة القاهرة، العدد 82، 2009، ص 88.

ألوان جديدة من الإجرام، كما يساعد هذا النظام في سرعة تأهيل المحكوم عليه وذلك من خلال الحفاظ على صلاته الأسرية والاجتماعية، كما يتيح له الحفاظ على عمله، وهو ما يحافظ على حالته النفسية، وينجم عنه سهولة اندماجه مع أقرانه داخل المجتمع.

1- إدخال نظام المراقبة الالكترونية في القانون الجزائري

تبنى المشرع الجزائري نظام المراقبة الالكترونية، فاعتبره أسلوبا أو طريقة لتنفيذ البعض من تدابير الرقابة القضائية وهو ما سنتطرق إليه أولا، واعتبره أيضا نظاما لتنفيذ العقوبة وهو ما سنتناوله ثانيا.

1- 1: المراقبة الالكترونية كآلية لتنفيذ تدابير الرقابة القضائية

أدخل المشرع الجزائري نظام المراقبة الالكترونية لأول مرة في قانون الإجراءات الجزائية باعتباره آلية لتنفيذ تدابير الرقابة القضائية وذلك بتعديل المادة 125 مكرر 01 منه، ولقد منح المشرع طبقا لنص هذه المادة سلطة تقديرية لقاضي التحقيق لإصدار أمر باتخاذ ترتيبات من أجل المراقبة الالكترونية، وذلك للتحقق من مدى الالتزام ببعض التدابير المنصوص عليها في هذه المادة[1].

---

[1] فنصت المادة 125 مكرر 01 منه: "... يمكن قاضي التحقيق أن يأمر باتخاذ ترتيبات من أجل المراقبة الالكترونية للتحقق من مدى التزام المتهم بالتدابير المذكورة في 1 و2 و6 و9 و10 أعلاه..."، وتتمثل هذه التدابير في:- عدم مغادرة الحدود الاقليمية التي حددها قاضي التحقيق إلا بإذنه.- عدم الذهاب إلى بعض الأماكن المحددة من طرف قاضي التحقيق.- الامتناع عن رؤية الأشخاص الذين يعنهم قاضي التحقيق أو الاجتماع ببعضهم.- المكوث

1-2: المراقبة الالكترونية لتنفيذ العقوبة الجزائية

لقد عرفت المادة 150 مكرر الوضع تحت المراقبة الالكترونية بأنه: "... إجراء يسمح بقضاء المحكوم عليه كل العقوبة أو جزء منها خارج المؤسسة العقابية...".

وحددت هذه المادة أسلوب تنفيذ المراقبة الالكترونية وذلك بأن يحمل المحكوم عليه طيلة المدة المحكوم بها عليه، سوارا الكترونيا يسمح بمعرفة مكان تواجده والمحدد في مقرر الوضع الصادر عن قاضي تطبيق العقوبات، فيمكن لهذا الأخير إما تلقائيا أو بناء على طلب المحكوم عليه شخصيا أو عن طريق محاميه، أن يقرر تنفيذ العقوبة تحت هذا النظام في حالة الإدانة بعقوبة سالبة للحرية لا تتجاوز مدتها ثلاث سنوات، أو في حالة ما إذا كانت العقوبة المتبقية لا تتجاوز هذه المدة[1].

يكون الوضع تحت نظام المراقبة الالكترونية بموجب مقرر يصدره قاضي تطبيق العقوبات، وذلك بعد أخذ رأي النيابة العامة، هذا بالنسبة للمحكوم عليهم بعقوبة سالبة للحرية لا تتجاوز مدتها ثلاث سنوات، أما المحكوم عليهم

في إقامة محمية يعينها قاضي التحقيق وعدم مغادرتها إلا بإذنه.- عدم مغادرة مكان الإقامة إلا بشروط وفي مواقيت محددة،الأمر رقم 15-02،المعدل والمتمم للأمر رقم 66-155، المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج ر عدد 40 لسنة 2015، المعدل والمتمم.

[1] نص القانون على تنفيذ العقوبة تحت نظام المراقبة الالكترونية، وحدد العقوبة المحكوم بها دون أن ينص على نوع الجرائم التي تسمح بتطبيق هذا النظام، انظر نص المادة 150 مكرر 01 من القانون رقم 15-02،نفسه.

المحبوسين فبالإضافة إلى رأي النيابة العامة يأخذ قاضي تطبيق العقوبات رأي لجنة تطبيق العقوبات، وهي موجودة على مستوى كل مؤسسة وقاية، وكل مؤسسة إعادة التربية، وكل مؤسسة إعادة التأهيل، وفي المراكز المخصصة للنساء[1].

ثانيا: إجراءات الوضع تحت المراقبة الإلكترونية والالتزامات المترتبة عنه

حددت المادة150 من قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين 18-01، الشروط التي تسمح للمحكوم عليه للاستفادة منه، وهو ما سنتطرق إليه من خلال الحديث عن إجراءات الوضع تحت المراقبة الالكترونية، وكذا الالتزامات المترتبة عنه.

1- إجراءات الوضع تحت نظام المراقبة الالكترونية

يوضع المحكوم عليه تحت نظام المراقبة الالكترونية، إما تلقائيا من طرف قاضي تطبيق العقوبات بشرط موافقة المحكوم عليه إذا كان بالغا، أو موافقة ممثله القانوني إذا كان قاصراّ، أو بناء على طلبه الشخصي أو عن طريق محاميه، وذلك إذا توافرت شروط معينة[2].

[1]انظر نص المادة 24 من القانون رقم18-01، سالف الذكر.

[2]وهي: - أن يكون الحكم نهائيا، -أن يثبت المعني مقر سكن أو إقامة ثابتة، -ألا يضر حمل السوار الالكتروني بصحة المحكوم عليه، -أن يسدد المحكوم عليه مبلغ الغرامات المحكوم بها عليه، انظر نص المادة 150 مكرر 3 من القانون رقم 18-01، نفسه..

إذا توافرت تلك الشروط القانونية، وقد الطلب المعني يتم إرجاء تنفيذ العقوبة المحكوم بها إلى حين الفصل في الطلب، حيث يفصل فيه القاضي في أجل عشرة أيام من اخطاره، ويصدر مقررا غير قابل لأي طعن[1].

يتحقق القاضي تلقائيا أو بناء على طلب المعني، وذلك قبل وضع السوار الالكتروني وفي أي وقت أثناء تنفيذ نظام المراقبة الالكترونية من أن السوار لا يمس بصحة المعني وذلك تطبيقا لنص المادة 150 مكرر 2 فقرة 2 من قانون تنظيم السجون وإعادة الادماج الاجتماعي للمحبوسين.

يتم وضع السوار الالكتروني بالمؤسسة العقابية، ويتم متابعته ومراقبة تنفيذه تحت إشراف قاضي تطبيق العقوبات من قبل المصالح الخارجية لإدارة السجون المكلفة بإعادة الادماج الاجتماعي للمحبوسين عن بعد، وعن طريق الزيارات الميدانية والمراقبة عن طريق الهاتف، وتبلغ المصالح الخارجية لإدارة السجون، قاضي تطبيق العقوبات فورا بكل خرق لمواقيت الوضع تحت المراقبة الالكترونية، وترسل إليه تقارير دورية عن تنفيذ الوضع تحت المراقبة الالكترونية[2].

2- الالتزامات المترتبة على وضع السوار الالكتروني

يترتب على وضع السوار الالكتروني عدم مغادرة المحكوم عليه لمنزله أو للمكان الذي يعينه قاضي تطبيق العقوبات خارج الفترات المحددة في مقرر

---

[1] إذا تم رفض طلب المحكوم عليه، فله أن يقدم طلبا جديدا بعض مضي ستة أشهر من تاريخ رفض طلبه الأول، انظر نص المادة 150 مكرر 4 من نفس القانون.

[2] نص المادة 150 مكرر2، مكرر4 ومكرر7 ومكرر 8 من القانون 18-01، سالف الذكر.

الوضع، حيث يؤخذ بعين الاعتبار لتحديد هذه الأوقات والأماكن ممارسة المحكوم عليه لنشاط مهني أو متابعته لدراسة أو تكوين أو تربص أو شغله وظيفة أو متابعة لأي علاج، وكل هذه الأمور ينص عليها مقرر الوضع[1].

كما تضيف المادة 150 مكرر 14 أنه في حالة ما إذا تملص المحكوم عليه من المراقبة الالكترونية، وذلك بنزع أو تعطيل الآلية الالكترونية للمراقبة، فإنه يتعرض لجريمة الهروب المنصوص عليها في قانون العقوبات[2].

المحور الثاني: مبادرة المحكوم عليه لتنفيذ الأحكام الجنائية الصادرة بالإدانة

---

[1] بالإضافة إلى ذلك يمكن لقاضي تطبيق العقوبات أن يخضع المعني إلى تدبير أو أكثر من التدابير الآتية:- ممارسة نشاط مهني أو متابعة تعليم أو تكوين مهني.- عدم ارتباط بعض الأماكن، -عدم الاجتماع ببعض المحكوم عليهم، بما في ذلك الفاعلين الأصليين أو الشركاء في الجريمة، -عدم الاجتماع ببعض الأشخاص لا سيما الضحايا والقصر، -الالتزام بشروط التكفل الصحي، والاجتماعي، والتربوي، أو النفسي، والتي تهدف إلى إعادة إدماجه اجتماعيا، -إلزام المحكوم عليه بالاستجابة إلى استدعاءات قاضي تطبيق العقوبات، أو السلطة العمومية التي يعينها القاضي، انظر نص المادة 150 مكرر 3 من القانون رقم 18-01، نفسه.

[2] وبتفحص نصوص هذه الأخيرة نجد المادة 188 منه تنص: "يعاقب بالحبس من شهرين إلى ثلاث سنوات كل من كان مقبوضا عليه أو معتقلا بمقتضى أمر أو حكم قضائي، يهرب أو يحاول الهرب من الأماكن التي خصصتها السلطة المختصة لحبسه أو من مكان العمل أو أثناء نقله، ويعاقب الجاني بالحبس من سنتين إلى خمس سنوات، إذا وقع الهروب أو الشروع فيه بالعنف أو بالتهديد ضد الأشخاص أو بواسطة الكسر أو تحطيم باب السجن".

أصبح واضحا اليوم أن التقدم العلمي المادي ليس له حدود ولا تبدو له نهاية، فالدول المتقدمة تزداد تقدمًا باستخدام تقنية المعلومات والاتصالات– والتي تبث بالتجربة أنها مفتاح التنمية المتواصلة– بينما تحاول الدول النامية اللحاق بالركب، واستخدام هذه التقنيات لعبور ما يسمى بالفجوة العلمية والتكنولوجية الواسعة التي تفصل ما بين الدول المتقدمة والدول النامية[1].

لقد كشفت التطورات التكنولوجية الحديثة عن امكانيات هائلة لأجهزة الحاسب الآلي وشبكات المعلومات الدولية "الانترنت"، وكان منم بين ما أسفرت عنه هذه التطورات امكانية ربط أجهزة ومصالح الدولة بنظام الكتروني واحد، بحيث يمكن استخدامه في تنفيذ العديد من المهام بين المؤسسات وبعضها البعض، فتستطيع الأجهزة والمؤسسات على مستوى الدولة أن تتواصل فيما بينها، وتنجز أعمال الأفراد أو توقفها بحسب الحاجة إلى ذلك.

وقد ساهم إدخال ورفع بيانات الأفراد والمؤسسات على شبكة المعلومات الدولية في تحسين بيئة العمل في كثير من الدول، وذلك من خلال قيام كل مؤسسة باستخدام تطبيقات تكنولوجية لأعمالها على الشبكة، بحيث يتمكن

---

[1]ظهرت في إطار العولمة فجوات جديدة بين الدول غير ما يسمى الفجوة الرقمية المعروفة بين الشمال والجنوب، ومن ذلك مثلا: (Divide Digital) التي أسفرت عنها محاولات التزاوج بين العقل البشري والعقول الالكترونية، ويقصد بها الفجوة بين المجتمعات والأفراد الذين يستخدمون بكفاءة وفعالية تكنولوجيا المعلومات والاتصالات وبين المجتمعات والأفراد الذين لا يستخدمون هذه التكنولوجيا، وهذه الفجوة الرقمية قد تتطور إلى فجوة كمية (DivideQuantu) وهي الفجوة التي تنجم عن استخدام الحاسبات العملاقة والكمية في حل أعقد المسائل في ثوان فيما كان يعجز عن حله علماء الرياضيات والطبيعة حتى زمن قريب، الحكومة الالكترونية، كتاب صادر عن جامعة الملك عبد العزيز آل سعود، ضمن سلسلة عالم المعرفة، ص09.

الأفراد من الولوج لهاته التطبيقات والإبلاغ عن ما يحتاجونه، ثم اتباع التعليمات المقدمة بمعرفة تلك المؤسسات للحصول على الخدمات المتاحة لهم بمعرفة المؤسسة صاحبة الموقع أو التطبيق.

يعتبر نظام الحكومة الالكترونية مثالا فعالا على ذلك، إذ تستطيع الحكومة الالكترونية أن تقدم خدماتها لجمهور من خلال تطبيقات الكترونية مختلفة، صممتها بواسطة الخبراء والمختصين، بحيث يتمكن الأفراد من الولوج إلى هذه التطبيقات والبرامج للحصول على الخدمات التي تقدمها تلك الحكومات، وفي ذات الوقت تستطيع الحكومات حجب هذه المواقع أو منع استخدامها عن بعض الأفراد بضوابط معينة[1].

والحكومة الإلكترونية اصطلاح مستحدث يشير إلى استخدام تقنيات المعلومات والاتصالات بأسلوب يسهل من الاتصال والتواصل والتعامل مع الحكومة ويجعل من التعاملات بين المصالح الحكومية أكثر فعالية، فالحكومات تستخدم تلك التقنيات في توفير الخدمات بين المصالح الحكومية والمواطنين، والأعمال، والموظفين، والوكالات الأخرى غير الحكومية، ولا شك

[1]أتاحت سرعة تطور التقنية الرقمية والاتصال بالإنترنت فتح المجال لما هو معروف الأن بنظام الحكومة الرقمية أو الحكومة الإلكترونية، فأصبح من الممكن تقديم الطلبات وتخليص الكثير من المعاملات مباشرة عن طريق الحاسوب الآلي والإنترنت، كما أصبح بمقدور المواطن الحصول على كل النماذج الخاصة بالمعاملات الحكومية من الموقع الخاص بالمصلحة الحكومية من الموقع الخاص بالمصلحة الحكومية المتصلة على الشبكة العنكبوتية العالمية، وقد انتشرت فكرة الحكومة الالكترونية في أنحاء العالم وخاصة في دول أوروبا وآسيا، حتى أن سنغافورة أصبحت في مقدمة الدول التي حولت معظم المصالح الحكومية إلى المعاملات الإلكترونية.

- Pavlichev A and Garson G .D: Digital Government , Principles and Best Practices. Idea Group publishing G, Septemper 2003.

أنها تتضمن توفير مدخل أفضل للمعلومات الحكومية، وتشجيع تداخل المجتمع في فعاليات الحكومة، ووضعها في خاضع أكثر للمساءلة، واتاحة الفرص لمزيد من التنمية والحوكمة والشفافية.

جدير بالذكر، أنه مع انتشار جائحة كورونا في أغلب دول العالم بدأت الحكومات –حتى غير المؤهلة– تفكر في تطبيق فكرة الحوكمة الإلكترونية، كوسيلة لاستدامة تقديم خدماتها للأفراد من ناحية، وطريقة لضمان وصول وجهة نظر الحكومة لهم من ناحية أخرى، وقد اعتبرت بعض الدول هذه الأزمة بمثابة تنبيه لإعادة النظر في تحسين أعمالها من خلال استغلال التكنولوجيا وربط أعمالها بها.

بعيدا عن مزايا وعيوب التحول إلى نظام الحكومة الإلكترونية، فإن ما يهمنا هو كيفية استخدام معطيات التحول الرقمي والتكنولوجيا الحديثة كوسيلة تساعد على تيسير تنفيذ الأحكام الجنائية؟.

للإجابة عن هذا التساؤل يمكننا القول بأن ما يقدمه التحول الرقمي من امكانات تتعلق بتخزين بيانات الأفراد ومعلوماتهم أولا، وتحليل هذه البيانات والربط بينهما، مع وجود نظام الكتروني يربط بين الجهات والمصالح المختلفة داخل الدولة، سوف يُمّكن الحكومات من معرفة ورصد كل المعلومات الهامة عن مواطنيها، والمقيمين على أراضيها، كما يمكن من خلال ما تحصله من معلومات عن تقديم أي خدمة من معرفة مواطن إقامة المواطنين ومعاملاتهم.

كما تستطيع الحكومة الالكترونية –ذات الجهات والمصالح الحكومية المترابطة من خلال نظام الكتروني واحد أن تستخدم هذا النظام الالكتروني في تسجيل كافة البيانات والمعلومات– أن تستخدم هذا النظام الالكتروني في

تسجيل كافة البيانات والمعلومات عن المواطنين والمقيمين، وعناوينهم وممتلكاتهم، وتستطيع من خلال البرامج الخاصةبالأرشيف الالكتروني أو الرقمي أن تسجل ما يصدر من أوامر خاصة بالتحقيقات الجنائية والأحكام الصادرة بالإدانة على النظام، ومن خلال الربط بين نظام الأرشيف الخاص بوزارة الداخلية والربط الشبكي على مستوى الدولة، يتم منع أي شخص يصدر ضده حكم قضائي بالإدانة من مباشرة أي إجراء يتعلق بمستنداته أو معلوماته أو ممتلكاته قبل أن يتخذ إجراء فيما يتعلق بالحكم الصادر ضده، أيًا كان مكان صدور الحكم وزمانه.

ومن خلال التحكم الالكتروني في أنشطة الأجهزة المختلفة القضائية والإدارية، ومن خلال الرفع اليومي لسجلات المحاكم الجنائية، وما يصدر عنها من أحكام جنائية، يكون بإمكان الدولة أن تستفيد من عملية التطور التكنولوجي في تنفيذ الحكم، ففرض بعض القيود على تصرفات الأفراد عندما تتطلب حياتهم اليومية ذلك، بسبب وجود حكم جنائي بالإدانة عليهم، يسبب نوعا من الشلل الإداري للفرد –إن جاز التعبير–، وعليه فإنه سيبادر بنفسه إلى تنفيذ الحكم الصادر بالإدانة، أو على الأقل سيقوم باتخاذ إجراء الطعن أو التصالح بحسب الأحوال، وبذلك تكون فكرة التحول الرقمي قد ساهمت بشكل كبير في تقديم علاج ناجح وناجع لأزمة العدالة الجنائية المتمثلة في تراكم القضايا والأحكام، وعدم تنفيذ الأحكام الجنائية الصادرة بالإدانة.

وجدير بالذكر أن المشرع الفرنسي قد طور نظاما يتعلق بالأحكام القضائية، من شأنه أن يمنع المحكوم عليه من إبرام أي تصرف يتعلق بأمواله وممتلكاته أو التصرفات العادية التي يكون أحد أطرافها جهة حكومية، إلا بعد

أن يتم تنفيذ الحكم إذا كان صادرا بعقوبة مالية "كالغرامة"، أو بعد اتخاذ إجراء بشأن الحكم، كالطعن مثلا إذا كان الحكم قابلا للطعن، أو التصالح إذا كان موضوع الحكم مما يجوز التصالح فيه، أو التنفيذ إذا كان الحكم باتا وغير قابل للتصالح في موضوعه[1].

وقد نظم المشرع الفرنسي إجراءً شبيها بذلك وهو إجراء الحجز الجنائي على الأموال Les saisies en matière pénale أو ما يعرف بالحجوزات الخاصة Les saisies spécialesبالمادة 706-30 من قانون الإجراءات الجنائية الفرنسي، فأجاز لقاضي التحقيق بناءً على طلب وكيل الجمهورية (النيابة العامة) أن يصدر أمرا بالحجز الجنائي التحفظي على أموال المتهم كلها أو بعضها بغية كشف الحقيقة وضمان تنفيذ العقوبات المالية[2].

فقد جاء نص المادة 706-30 إجراءات -فرنسي المضافة بالقانون رقم 94-89 الصادر في أول فبراير 1994 بالنص على أنه: في حالة توافر معلومات أثناء التحقيق على (مخالفة المواد 222-34، 222-38، 324-1، 324-2 من قانون العقوبات) أو (الفقرة الثانية من المادة 222-49 والفقرة 12 من المادة 324-7 من قانون العقوبات) فإنه لضمان دفع الغرامات المستحقة وتنفيذ المصادرة يجوز لرئيس المحكمة الابتدائية أو من يفوضه بناء على طلب المدعي العام أن يأمر وفقا لقانون أصول المحاكمات المدنية بفرض تدابير تحفظية Des Mesures Conservatoires ضد ممتلكات الشخص

[1]**Eric. Camous**, **Les saisies en procédure pénale** ; un régime juridique modernise, commentaire des dispositions pénales de droit interne de la loi n 2010-768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale, Droit Pénal .,n 1, 2011,p.1.

[2]**Frederick DUPUIS,** Les saisies en matière pénale, de l'opportun a l'opportunisme, Rev. Procédures n 5, Mai 2014, P1 ; **Gaston Stefani, George Levasseur et Bernard Bouloc**: Procédure Pénale, op. Cit. N 686. P 606.

محل التحقيق، فإذا صدر حكم بالبراءة أو الإفراج أو انقضت الدعوى الجنائية فإنه يترتب عليه تلقائيا زوال التدابير المتخذة قبله، مع تحمل الخزانة العامة تكاليف ذلك[1].

خاتمة:

يتضح من خلال عرضنا لانعكاسات التطور التكنولوجي على السياسة الجنائية المعاصرة عموما وعلى مرحلة تنفيذ الأحكام خصوصا، أن لهذا التحول أثر كبير ليس فقط في دفع التشريعات الجنائية إلى تطوير ذاتها، سواء كان ذلك من خلال تطوير وتنقيح القواعد العامة (قوانين العقوبات والإجراءات الجزائية) أو من خلال القوانين الخاصة التي تكمل ما تعجز القوانين العامة عن الالمام به، وذلك بغرض استيعاب النتائج المذهلة التي أسفر عنها، وإنما كذلك قاد إلى تطور كبير في الجوانب الإجرائية المتعلقة بالإجراءات الجنائية، والذي امتدت آثار التحول كذلك إلى مرحلة تنفيذ الأحكام الجنائية، فوجدنا استخدام بعض آلياته في مرحلة التنفيذ، واستلهم البعض هذه الآليات لاستخدامها في الحد من مساوئ سلب الحرية، بصفة خاصة قصير المدة، واستطاعت بعض التشريعات أن تطور –من خلال الربط الالكتروني بين أجزاء أقاليم دولها– أن

[1]En cas d'information ouverte pour infraction (Loi n 94-89 du 1 er févr. 1994), aux articles 222-34 a 222-38,324-1 et 324-2 du code pénal , et afin de garantir le paiement des amendes encourues, ainsi que l'exécution de la confiscation prévue (loi n 2001- 420 du 15 mai 2001),au deuxième alinéa de l'article 222-49 et au 12 de l'article 324-7 du code pénal , le président du tribunal de grande instance ou un juge délégué par lui, sur requête du procureur de la République, peut ordonner, aux frais avances du Trésor et selon les modalités prévues par le code de procédure civile, des mesures conservatoires sur les biens de la personne mise en examen.
La condamnation vaut validation des saisies conservatoires et permet l'inscription définitive des suretés. La décision de non-lieu, de relaxe ou d'acquittement emporte de plein droit, aux frais du Trésor, mainlevée des mesures ordonnées.

تبتكر أساليب جديدة تساهم في معالجة مسألة تنفيذ الأحكام الصادرة بالإدانة، وهو ما شكل صعوبة لدول كثيرة لفترات طويلة.

كل هذه التطورات وغيرها مما لم يكن بالإمكان إحصاؤه كانت ناتجة عن التحول الرقمي، أو بشكل أصح ناتجة عن إرهاصات التطور التكنولوجي، ونتصور أن يسفر هذا التحول في المستقبل القريب عن تغيير شامل في القواعد الموضوعية والإجرائية في القوانين الجنائية، بما يتواءم مع متطلبات هذا التحول، وبما يتيح لقواعد القانون الإحاطة بالتقدم الذي تحرزه التكنولوجيا الحديثة كل يوم، كما نأمل أن يسفر تطبيق التطور التكنولوجي في صورته النهائية –والتي تظن أنها لم تتبلور بعد ولن تأتي في المستقبل –قواعد إدارة العدالة الجنائية بما يساهم في تحسين بيئة العمل داخل المؤسسات الأمنية والمحاكم وأماكن التنفيذ العقابي.

يعتبر نظام المراقبة الالكترونية من أهم الأساليب الحديثة التي تبنتها التشريعات الجنائية لمعاملة المحكوم عليه خارج المؤسسات العقابية، حيث يمكن للمحكوم عليه أن يمارس عمله خارج هده المؤسسات مع فرض نوع من التدابير والالتزامات عليه، وهدا الأسلوب يتماشى والدعوة إلى وضع حل لمشكل العقوبة السالبة للحرية قصيرة المدة، والحد من اكتظاظ السجون، رغم أن هدا النظام لم يلق القبول من قبل بعض الفئات التي ترى فيه تقييدا لحرية التنقل بالنسبة للمحكوم عليه.

كما نود أن نشير إلى وجود العديد من النصوص التقليدية التي تعد من موروثات القرون الماضية، والتي نرى ضرورة تطويرها وإعادة النظر فيها، لتنسجم مع تطورات المجتمع، وأن يكون النظر في هذه القوانين بشكل دوري،

على الأقل كل خمس سنوات، بحيث يتاح مراجعتها وتنقيحها، كما نقدم الاقتراحات الآتية:

–التوصية بدراسة امكانية الاستفادة من المراقبة الالكترونية كوسيلة لتنفيذ الحبس الاحتياطي والعقوبات السالبة للحرية، على أن يكون ذلك بضوابط تحقق أغراض العقاب، بصفة خاصة تأهيل وإصلاح المحكوم عليه، وألا يتاح إلا في الجرائم التي لا يمثل خروج المتهم فيها من المؤسسة العقابية خطرا على الأمن العام.

– التوصية بدراسة أثر التطور التكنولوجي الرقمي في ربط كافة مؤسسات الدولة من خلال الشبكة المعلوماتية، بحيث يتاح تسجيل الأحكام الجنائية الصادرة بالإدانة على مواقعها، وحجب الخدمات الحكومية عن المحكوم عليهم بأحكام نهائية بالإدانة إلا عقب اتباع إجراءات تنفيذ الحكم، أو التصالح فيه، وبذلك يبادر الأفراد إلى تنفيذ العقوبات المحكوم بها من تلقاء أنفسهم، يساهم التحول الرقمي في حل أزمة عدم تنفيذ الأحكام الجنائية.

قائمة المصادر والمراجع:

أ) النصوص القانونية:

1- الأمر رقم 15-02، المعدل والمتمم للأمر رقم 66-155، المؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج ر عدد 40 لسنة 2015، المعدل والمتمم.

2- قانون رقم 15-03 المؤرخ في 01 فبراير 2015 والمتعلق بعصرنة العدالة، ج ر عدد 06 لسنة 2015.

3- قانون رقم 18-01 مؤرخ في 12 جمادى الأولى عام 1439 الموافق لـ 30 يناير سنة 2018، يتمم القانون رقم 05-04 المؤرخ في 27 ذي الحجة عام 1425 الموافق لـ 06 فبراير 2005 والمتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، ج ر عدد 47، 2018.

ب) المراجع باللغة العربية:

أ-1/ الكتب:

1- أحمد فتحي سرور، المشكلات المعاصرة للسياسة الجنائية الحديثة، مطابع جامعة القاهرة، 1983.

2- عماد الفقي، النظم البديلة للحبس قصير المدة -دراسة مقارنة، الطبعة الأولى 2017، دار النهضة العربية.

3- عمر سالم، المراقبة الالكترونية طريقة حديثة لتنفيذ العقوبات السالبة للحرية خارج السجن، دار النهضة العربية، الطبعة الثانية، د ت ن.

ب-2/ المقالات العلمية:

1- أسامة حسنين عبيد، المراقبة الجنائية الالكترونية -دراسة مقارنة، مجلة القانون والاقتصاد، كلية الحقوق جامعة القاهرة، العدد 82، ص 06.

2- رامي متولي القاضي، المراقبة الالكترونية في القانون الفرنسي والمقارن، مجلة الشريعة والقانون، كلية الحقوق، جامعة الإمارات، العدد 63، يوليو 2015.

3- ياسر محمد اللمعي، إصلاح العدالة الجنائية عن طريق رقمنة الإجراءات الجنائية– دراسة تحليلية مقارنة، بحث منشور بمجلة كلية الشريعة والقانون، جامعة الأزهر بدمنهور، العدد 02، الربيع 2021.

4- ليلى طلبي، الوضع تحت المراقبة الالكترونية، مقال منشور بمجلة العلوم الانسانية، مجلة علمية محكمة تصدر عن جامعة منتوري، قسنطينة، العدد 47، المجلد –أ– جوان 2017، ص 255–256.

ت) المراجع باللغة الأجنبية:

1- Michèle-Laure Rassat : Droit pénal spécial, PRECIS, DALLOZ, 3e édition, 2001.

2- Pavlichev A and Garson G .D: Digital Government , Principles and Best Practices. Idea Group publishing G, Septemper 2003.

3- Eric. Camous, Les saisies en procédure pénale; un régime juridique modernise, commentaire des dispositions pénales de droit interne de la loi n 2010-768 du 9 juillet 2010 visant à faciliter la saisie et la confiscation en matière pénale, Droit Pénal .,n 1, 2011,p.1.

4- **Frederick DUPUIS,** Les saisies en matière pénale, de l'opportun a l'opportunisme, Rev. Procédures n 5, Mai 2014, P1 ; **Gaston Stefani, George Levasseur et Bernard Bouloc**: Procédure Pénale, op. Cit. N 686. P 606.

5- (Loi n 94-89 du 1 er févr. 1994), aux articles 222-34 a 222-38,324-1 et 324-2 du code pénal , et afin de garantir le paiement des amendes encourues, ainsi que l'exécution de la confiscation prévue (loi n 2001- 420 du 15 mai 2001),au deuxième alinéa de l'article 222-49 et au 12 de l'article 324-7 du code pénal

تقنية السوار الالكتروني
بين مقاصد العقوبة السالبة للحرية والإصلاح الجنائي

د. غناي زكية **أ.د. جمال زيد الكيلاني**
كلية الحقوق، جامعة بومرداس، الجزائر **عميد كلية الشريعة، جامعة النجاح، نابلس، فلسطين**
shar@najah.eduz.ghanai@univ-boumerdes.dz

مقدمة:

إن المقصود من تطوير القانون الجنائي التوصل إلى القضاء أو على الأقل التقليل من نسبة الإجرام في المجتمع، والرفع من مستوى الأمن الاجتماعي، والنجاح في نشر الأمان ومحو الرعب لدى المواطنين بالعمل بكل الوسائل المشروعة للقضاء على ملكة الإجرام من النفوس البشرية، ولا يتأتى هذا إلا بتطبيق سياسة جنائية عادلة ومعقولة بحيث تطبق العقوبة المناسبة على الجريمة المناسبة.

وقد كانت الشريعة الإسلامية السباقة في هذا المجال، إذ قسّمت الجرائم وعقوباتها إلى حدود وقصاص وتعزير، وقد أسفر التطبيق الفعلي لها إلى تحقيق العدل والأمن في المجتمع في زمن النبي صلى الله عليه وسلم وزمن صحابته بعده، كيف لا وهي تستمد مصدرها من القرآن الكريم والسنة النبوية. ومع توالي الأزمنة وضعف الوازع الديني بدأ التخلي عن العقاب الشرعي بوصفه بالقاسي واللاإنساني، وأصبحت عقوبة قطع يد السارق ورجم الزاني المحصن وغيرها مستحيلة التطبيق بسبب ضعف هيبة الحكم والقضاء اليوم، مما نجم عنه في المقابل تصاعد رهيب للإجرام في كل أنحاء العالم، فاستعصى على الحكومات التصدي له.

أما وبعد أن تعطّل تطبيق الشرع في المجال الجنائي، وفشلت سياسة العقاب الوضعي على وجه الأرض، طفق الكل يبحث باستمرار عن حلول بديلة تعمل على إصلاح العدالة الجنائية، ومن بين هذه الحلول تقنية السوار الالكتروني التي ظهرت حديثا مع التطور التكنولوجي الذي اقتحم مجال القانون الجنائي، حيث أُريد استبدالها بالعقوبة السالبة للحرية، وقد اخترعتها الحاجة إلى تخفيف الضغط على السجون التي امتلأت بنزلائها فلم تعد تقدر على تحقيق مقاصدها.

وتعتبر الجزائر أول بلد عربي يلجأ لتقنية السوار الالكتروني، كما حذت حذوه دول أخرى كالسعودية والإمارات، وبغض النظر عن الحاجة التي دفعت العالم إلى استحداث هذه التكنولوجيا كضرورة مسايرة التطور التكنولوجي في المجال الجنائي، وضرورة حل مشكل الاكتظاظ في السجون، أو حتى الحكم بعدم

فعالية العقوبات التقليدية في تحقيق العدالة الجنائية؛ فإن أول سؤال يتبادر إلى الذهن هو: ما الذي يضمن امتثال المحكوم عليه ارتداء السوار الالكتروني طيلة فترة العقوبة؟ ألا يمكن لمجرم مارق التخلص من السوار والفرار من المراقبة الإلكترونية؟ وما مدى فعالية هذه التقنية المستحدثة في تطوير السياسة العقابية؟

وعلى صعيد آخر، تجدر الإشارة إلى أن العقوبة السالبة للحرية تملك مقاصد بالغة الأهمية في تحقيق الردع الجنائي المطلوب لتوفير سياسة جنائية فعالة في حماية المجتمع من الإجرام، وإذا تم استبدالها بعقوبة تكنولوجية مستحدثة فيفترض في هذه الأخيرة مادامت بديلة أن تحقق نفس مقاصد العقوبة الأصلية، وألاّ تفرط في أي منها، فهل نجحت تقنية السوار الالكتروني في تحقيق مقاصد عقوبة الحبس الاحتياطي؟

الإجابة على هذا السؤال تتطلب البحث والتمحيص المعمق في تقنية السوار الالكتروني ومدى شرعيتها وتحقيقها لمقاصد العقوبة السالبة للحرية؛ كما تتطلب من جانب آخر القيام بدراسة ميدانية بخصوص تجربة السوار الالكتروني للإحاطة بمدى فعاليتها ومدى مساهمتها في إصلاح السياسة العقابية.

المبحث الأول: مدى شرعية استبدال العقوبة السالبة للحرية بالسوار الالكتروني

إن الخوض في موضوع تقنية السوار الالكتروني كبديل عن العقوبة السالبة للحرية يتطلب عدم الارتجال في تقبل كل ما هو جديد باسم التقدم العلمي والتكنولوجي، بل يجب تحرير الفكر من عادة الانبهار بالتطور، والتركيز بموضوعية في مسألة شرعية استبدال عقوبة حبس مجرم داخل أسوار سجن بمجرد ارتداء جهاز رقابة عن بعد، ما يعني استبدال عقوبة مقيدة للجاني ضامنة نوعا ما عدم فراره بأخرى مطلقة لسراحه مهيئة له فرصة الفرار.

إن المنطق السليم يقتضي أن يكون البديل أفضل من المبدل أو على الأقل في نفس مكانته، ولهذا فإن التساؤل الذي يطرح لأول وهلة يكمن في مدى تحقق الغرض من الحبس في عقوبة السوار الالكتروني.

نبدأ بالتعريف بالسوار الالكتروني، حتى إذا اتضحت التقنية ندرس مدى شرعية حلولها كبديل عن الحبس الاحتياطي.

المطلب الأول: التعريف بتقنية السوار الالكتروني

تعتمد تقنية السوار الالكتروني على ارتداء الجاني سوارا يشبه الساعة في معصمه أو كاحله، ويسمح هذا السوار، الذي يكون مبرمجا رقميا، بإرسال واستقبال موجات لا سلكية تعمل على مراقبة تحركات حامله عن بعد، وترصد مكان تواجده تماما كما يعمل نظام تحديد المواقع في الأجهزة الالكترونية، وكما يقال: الحاجة أم الاختراع، لم تكن هذه التقنية لتظهر لولا حاجة أجهزة العدالة عبر العالم إلى التصدي لظاهرة اكتظاظ السجون.

الفرع الأول: نشأة تقنية السوار الالكتروني

نبين أولا نشأة تقنية السوار الالكتروني عبر العالم، ثم في الجزائر.

أولا: نشأة تقنية السوار الالكتروني عبر العالم

كانت كندا في الحقيقة هي السباقة في إجراء تجارب التحكم عن بعد في حركات الجاني مع إبقائه في المنزل، وكان ذلك عام 1946 حيث ظهرت فكرة الحبس في المنزل، وفي أوت 1979 كان القاضي جاك لوف يطالع جريدة تتحدث عن مقطع من المسلسل المشهور سبايدر مان أين استحضر فكرة إمكانية استعمال سوار كجهاز إرسال عندما طالع لقطة تتحدث عن تمكن أحد اللصوص من تتبع الرجل العنكبوت بواسطة سوار وضع في معصمه، وهذه الفكرة ألهمت القاضي، وعلى الفور اتصل بمهندس الكتروني وطلب منه تطوير نظام المراقبة عن بعد، وفي عام 1983 جرّب هذا القاضي السوار بنفسه لمدة عدة أسابيع ثم أصدر أمرا بوضع خمسة مخالفين تحت هذه الرقابة الالكترونية. وبسرعة كبيرة انتقلت هذه التقنية إلى الولايات المتحدة في شكل مشاريع تجريبية، وبعد أقل من أربع سنوات تم الشروع في استخدامها في 26 ولاية أمريكية، وبسبب التقدم التقني وتطور نظام الرقمنة، انتقلت تقنية السوار الالكتروني إلى بلدان أخرى حول العالم قبل نهاية القرن العشرين.[1]

أما البلدان العربية فلم تعمد إلى تفعيل تقنية السوار الالكتروني، ففي المملكة العربية السعودية اقتصر إعماله على الحالات الضرورية والاستثنائية التي يغادر فيها السجين لمدة معينة من أجل العلاج

1. Jean Paul CERE, La surveillance électronique: Une réelle innovation dans le procèspénal, Revue de la faculté de droit de Campos, Vol VII n 8, 2006, P 107.

أو حضور جنازة، وليس كبديل لعقوبة الحبس.[1]وفي مصر تم تقديم اقتراح إلى البرلمان المصري من طرف النائبة سميرة الجزار، ويهدف الاقتراح إلى التخفيف من مشكلة اكتظاظ السجون.[2]

ثانيا: نشأة تقنية السوار الالكتروني في الجزائر

في الجزائر، وإن كانت التكنولوجيا الرقمية ظهرت حديثا، غير أن تقييد حرية الجاني عن بُعد أي خارج أسوار السجن كان معروفا تحت اسم "تحديد الإقامة" المنصوص عليه كعقوبة تكميلية بموجب نص المادة 9 من قانون العقوبات،[3] وقد عرّفت المادة 11 من نفس القانون تحديد الإقامة كما يلي: "تحديد الإقامة هو إلزام المحكوم عليه بأن يقيم في منطقة يعينها الحكم .."، وبالتالي فهو لا يختلف عن الرقابة الالكترونية إلا بزيادة تركيب سوار الكتروني.

وأما نظام الرقابة الالكترونية فأحدثه المشرع بموجب الفقرة 11 من المادة 125 مكرر 1 من قانون الإجراءات الجزائية[4] التي تنص على ما يلي: "يمكن لقاضي التحقيق أن يأمر بأخذ ترتيبات من أجل المراقبة الالكترونية للتحقق من مدى التزام المتهم بالتدابير المذكورة في الفقرة 1 و2 و6 و9 و10 أعلاه ... تحدد كيفيات تطبيق المراقبة الالكترونية المنصوص عليها في هذه المادة عن طريق التنظيم."

ما يلاحظ على هذا النص أنه نص على الرقابة الالكترونية دون أن يحدد وسيلتها، فهو بهذا لم ينص صراحة على السوار الالكتروني، وحتى قانون عصرنة العدالة[5] وجدته ينص في المادة 14 منه على إمكانية استجواب وسماع الأطراف عن طريق المحادثة المرئية عن بعد، ولم أجد نصا يقضي صراحة بالسوار الالكتروني، ورغم ذلك أصدر قاضي تحقيق محكمة تيبازة بتاريخ 25 ديسمبر 2016 أمرا لأول مرة بالوضع تحت المراقبة الالكترونية في حق جاني متهم بتهمة الضرب والجرح العمدي.

---

1. عامر جوهر وعباسة طاهر، السوار الالكتروني إجراء بديل للعقوبة السالبة للحرية في التشريع الجزائري، مجلة الاجتهاد القضائي، جامعة بسكرة، مج 10، عدد 2، 2018، ص 183.

2. هبة أنيس، هل ينجح السوار الالكتروني في إنهاء دائرة الحبس الاحتياطي، منشور على الموقع حقوق وحرياتwww.masr/net-360 بتاريخ 2021/04/04 20:30

3. أمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد 49، المؤرخة في 11 يونيو 1966.

4. أمر رقم 15-02مؤرخ في 23 جويلية 2015 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 08 جوان 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40، المؤرخة في 23 جويلية 2015، ص 28.

5. قانون رقم 15-03 مؤرخ في 01 فبراير 2015 يتعلق بعصرنة العدالة، الجريدة الرسمية عدد 06، المؤرخة في 10 فبراير 2015، ص 4.

هذا وإن كان أمر قاضي التحقيق هو الآخر لم يبين صراحة أنه يقصد بالمراقبة التقنية استخدام السوار الالكتروني إلا أنه حسب المدير العام لعصرنة العدالة فقد أعلن عن انطلاق عملية الرقابة الالكترونية بولاية تيبازة من خلال استخدام سوارين الكترونيين.[1]

وفي سنة 2018، صدر قانون رقم 18-01 مؤرخ في 30 يناير 2018 يتمم القانون رقم 05-04 المؤرخ في 06 فبراير 2005 والمتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين،[2] حيث طبقا للمادة 2 منه يتمم الباب السادس بفصل رابع عنوانه "الوضع تحت المراقبة الالكترونية"، يتضمن المواد 150 مكرر إلى 150 مكرر 16، بموجبها نص المشرع صراحة على تقنية السوار الالكتروني، وبهذا تم تكريسه ضمن السياسة الجنائية في الجزائر، ولعل تحليل نصوص هذا الفصل يساعدنا في فهم النظام القانوني للسوار الالكتروني.

الفرع الثاني: النظام القانوني للسوار الالكتروني

تبين أن السوار الالكتروني هو جهاز يركب في يد أو قدم المحكوم عليه، مزود بنظام تحديد المواقع لرصد تحركاته عن بعد بدلا من حبسه، وهذه هي الرقابة الالكترونية، وقد بين المشرع شروطه وآثاره.

أولا: شروط تطبيق السوار الالكتروني

وضع قانون تنظيم السجون شروطا لتطبيق السوار الالكتروني يمكن إجمالها في صنفين: شروط موضوعية، وأخرى شكلية.

1- الشروط الموضوعية

للسوار الالكتروني شروط موضوعية، منها ما هو خاص بالعقوبة، ومنها ما هو خاص بالمتهم.

أ- الشروط الموضوعية الخاصة بالعقوبة[3]

- عدمتجاوز مدة العقوبة ثلاث سنوات، وبالتالي لا يستفيد من السوار من تجاوزت عقوبته هذه المدة.

---

1. محمد. ب، انطلاق العمل بالسوار الالكتروني من تيبازة، جريدة المساء، مؤرخة في 26 ديسمبر 2016، أنظر: www.el-massa.com/dz

2. قانون رقم 18-01 مؤرخ في 30 يناير 2018 يتمم القانون رقم 05-04 المؤرخ في 06 فبراير 2005 والمتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، الجريدة الرسمية عدد 05، المؤرخة في 30 يناير 2018، ص 10.

3. نظمتها المادة 150 مكرر 1 من قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين.

– لا يطبق السوار الالكتروني إلا على العقوبات السالبة للحرية، وبالتالي لا يكون بديلا على غيرها من العقوبات كالإعدام أو الغرامة أو الأشغال الشاقة.

ب– الشروط الموضوعية الخاصة بالمتهم[1]

– رضا المحكوم عليه أو وليه، مما يفهم منه أن عقوبة السوار الالكتروني عقوبة اختيارية رضائية لو رفضها المتهم واختار الحبس لم تنفذ عليه.[2]

– ثبوت مقر المحكوم عليه، ولعل هذا من صعوبات تطبيق السوار الالكتروني لكون العديد من المحكوم عليهم لا يملكون مقرا.

– عدم تعرض صحة المحكوم عليه للضرر، وذلك لأن السوار يعمل لا سلكيا، وهذه التقنية قد تضر من يحملون بطاريات تنظيم نبضات القلب أو غيرها.

– سداد المحكوم عليه مبالغ الغرامات المحكوم بها عليه، مما يعني أن السوار الالكتروني ليس بديلا عن عقوبة الغرامة.

2– الشروط الشكلية

تطبيق السوار الالكتروني يستلزم توافر شروط شكلية تتمثل فيما يلي:

– وجوب أخذ رأي النيابة العامة.

– وجوب كون الحكم نهائي، ومعناه أن المحكوم عليه الذي مازالت الخصومة سارية بشأنه لا يستفيد من السوار.

ثانيا: آثار تطبيق السوار الالكتروني

إذا توفرت شروط السوار الالكتروني، وارتدى المحكوم عليه السوار، ترتبت التزامات وجب عليه عدم الإخلال بها وإلا تعرض لجزاءات.

1– التزامات المحكوم عليه

يخضع المحكوم عليه الحامل للسوار الالكتروني لتدابير، منها ما هو إلزامي ومنها ما هو جوازي.

أ– التدابير الإلزامية

1. نظمتها المادة 150 مكرر 2 من قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين.

2. ولعل هذا من غرائب السوار الالكتروني لأن المعروف في العقوبات الشدة والصرامة والإكراه لا التخفيف واللين والرضائية.

نصت عليها المادة 150 مكرر 5، وطبقا لهذا النص، بعد أن يحمل المحكوم عليه السوار الالكتروني، يعين له القاضي مكانا يقضي فيه عقوبته قد يكون منزله أو غيره، أين يتم تركيب جهاز مستقبل ثابت مزود بتقنية GSM وهي تقنية عالية يمكنها اختراق الجدران،[1] ثم يمنع المحكوم عليه من مغادرته.

وطبقا للنص المذكور يسمح للمحكوم عليه بمغادرة مكانه استثناء وفي أوقات محددة لفري شغله من علاج أو دراسة أو شغل، ولعل هذا أحد أهداف استبدال عقوبة الحبس بالسوار الالكتروني، حيث لا يحبس المحكوم عليه من فري ما يؤمن مستقبله، وهذا ما يزيد في إصلاحه وتهيئته للاندماج في المجتمع.

ب- التدابير الجوازية

نظمتها المادة 150 مكرر 6 حيث قضت بأنه يجوز للقاضي إخضاع المحكوم عليه لواحد أو أكثر من هذه التدابير:

- ممارسة نشاط مهني أو متابعة تعليم أو تكوين مهني.
- عدم ارتياد بعض الأماكن.
- عدم الاجتماع ببعض المحكوم عليهم، فاعلين أصليين كانوا أو شركاء في الجريمة.
- عدم الاجتماع ببعض الأشخاص لا سيما الضحايا والقصر.
- الالتزام بشروط التكفل الصحي أو الاجتماعي أو التربوي أو النفسي التي تهدف إلى إعادة إدماجه اجتماعيا.

وهذه التدابير المذكورة باعتبارها جوازية تخضع للسلطة التقديرية للقاضي، قد يحكم بكلها أو بعضها وقد لا يحكم بأي منها، غير أنه لا يمكنه الحكم بغيرها على أساس أنها وردت على سبيل الحصر.[2]

2- جزاء الاخلال بالتدابير

إن السوار الالكتروني كعقوبة بديلة يدفع لأول وهلة إلى الاستغراب حول الثقة الممنوحة للمحكوم عليه وإطلاق سراحه بالاعتماد على جهاز يكشف مكان تواجده، مع أنه قد يخطر على بال أي كان

1. بن يوسف القينعي، نظام المراقبة التقنية في التشريع الجزائري، حوليات جامعة الجزائر 1، مج 35، عدد 2، 2021، ص 80.
2. بن يوسف القينعي، المرجع السابق، ص 81.

إمكانية التخلص منه بسهولة والفرار، ولهذا السبب لم يترك المشرع هذه المسألة دون تنظيم، فقرّر جزاءات على الإخلال بالتدابير المذكورة أعلاه، منها جزاءات تأديبية وأخرى عقابية.[1]

أ- الجزاءات التأديبية

تتمثل طبقا للمادة 150 مكرر 10 في إلغاء الوضع تحت المراقبة التقنية وبالتالي إلغاء الاستفادة من السوار الالكتروني، حيث ينزع من المحكوم عليه ثم ينفذ بقية العقوبة داخل المؤسسة العقابية مع اقتطاع المدة المقضية تحت رقابة السوار.[2] وهذا ما يدل على أن الحبس هو العقوبة الأصلية يرجع إليه كلما لم تنفع العقوبة البديلة. ويقرر هذا الجزاء عند عدم احترام المحكوم عليه لالتزاماته دون مبرر مشروع أو عند إدانته من جديد.[3]

ب- الجزاءات العقابية

نظمتها المادة 150 مكرر 14 حيث قضت بما يلي: "يتعرض الشخص الذي يتملص من المراقبة الالكترونية لا سيما عن طريق نزع أو تعطيل الآلية الالكترونية للمراقبة إلى العقوبات المقررة لجريمة الهروب المنصوص عليها في قانون العقوبات." وبالرجوع إلى هذا الأخير[4] نجده ينص في المادة 188 منه على ما يلي: "يعاقببالحبسمنشهرينإلىثلاثسنواتكلمنكانمقبوضاعليهأومعتقلاقانونا بمقتضىأمرأوحكمقضائيوبهربأويحاولالهروبمنالأماكنالتيخصصتهاالسلطةالمختصةلحبسهأومن مكانالعملأوأثناءنقله.ويعاقبالجانيبالحبسمنسنتينإلىخمسسنواتإذاوقعالهروبأوالشروعفيهبالعنفأوبالتهديدضدالأشخا صأوبواسطةالكسرأوتحطيمباالسجن." وبهذا يعتبر التخلص من السوار جريمة هروب من العدالة يعاقب عليها بالحبس، ويقتضي المنطق أن يعاقب عليها بالحبس داخل المؤسسة العقابية رجوعا للأصل لاستحالة تطبيق العقوبة البديلة، ويبدو فرار المحكوم عليه نتيجة طبيعية لا يتحملها وحده بل تتحمل التقنية جزء من مسؤولية هروب المحكوم عليه إذ هي من فتحت له الباب واسعا للتفكير فيه،فمسألة الهروب تبدو متوقعة، فمن الطرائف الميدانية أن قد وصلت جرأة أحد المحكوم عليهم إلى التخلص من السوار وإعادة تركيبه في رأس دجاجة ثم الهروب،[5] وهذه قضية أخرى أثارت السخرية من تقنية السوار

1. بن يوسف القينعي، المرجع السابق، ص 82.
2. راجع المادة 150 مكرر 13 من قانون تنظيم السجون وإعادة الادماج الاجتماعي للمساجين.
3. راجع المادة 150 مكرر 10 من قانون تنظيم السجون وإعادة الادماج الاجتماعي للمساجين.
4. أمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد 49، المؤرخة في 11 يونيو 1966.
5. مقابلة مع بعض قضاة مجلس تيبازة.

الالكتروني كعقوبة بديلة عن الحبس داخل المؤسسات العقابية، مما نجم عنه عزوف أغلب قضاة التحقيق عن تطبيقها، واختيارهم عقوبة الحبس التي بقيت في نظرهم أكثر ضمانا وأصدق ردعا.

المطلب الثاني: مدى مشروعية إبدال عقوبة الحبس بالسوار الالكتروني

بعد أن تبينت تقنية السوار الالكتروني كتكنولوجيا حديثة في مجال العقاب الجنائي، وقد ظهرت كبديل عن العقوبة السالبة للحرية، وجب الوقوف عند هذه المسألة بالذات والبحث عما إذا كان جائز شرعا إبدال عقوبة بأخرى بديلة عموما، واستبدال الحبس بالسوار الالكتروني خصوصا؟

إن الإجابة على هذا التساؤل يتطلب دراسة مدى مشروعية إبدال العقوبة عموما، ليتضح بعدها مدى مشروعية السوار الالكتروني كعقوبة بديلة.

الفرع الأول: مدى مشروعية إبدال العقوبة كقاعدة عامة

لا يمكن الإحاطة بحكم العقوبات البديلة ومدى مشروعيتها دون إيضاح الجرائم والعقوبات المقررة لها في الشريعة الإسلامية، فالجريمة في الشريعة الإسلامية منها ما شرع لها عقوبات محددة لا يجوز استبدالها بأخرى بديلة؛ ومنها ما لم يحدد لها عقوبات بل تركت لاجتهاد ولي الأمر، وهذه اجتهد العلماء القدامى في تقرير عقوبات لها، اختلف اليوم في مدى مشروعية إبدالها بعقوبات بديلة على النحو الذي نبينه فيما يلي.

أولا: العقوبات غير المشروع إبدالها

العقوبات غير المشروع إبدالها بغيرها هي تلك المقدرة شرعا، وتنقسم إلى حدود وقصاص.

1- الحدود

الحدود "هي عقوبات محددة بنص شرعي في القرآن الكريم أو السنة النبوية الشريفة على وجه ثابت ذات حد واحد لا تقبل عفوا أو تعديلا أو تشديدا أو تخفيفا"،[1] ويفهم من هذا أنها لا تقبل بديلا أيضا، ومن المهم جدا معرفة الجرائم المستوجبة لإقامة الحد،ومعرفة نوع الحد في كل منها حتى يستبعد عنها البديل.

فالحدود في الشريعة الإسلامية مقررة للجرائم التالية على النحو المبين أمامها.

- جريمة الزنا: حد مائة جلدة لغير المحصن مع التغريب، وحد الرجم حتى الموت للمحصن.

1. عمران محمد، أغراض العقوبة والمبادئ الأساسية التي ترتكز عليها في النظام العقابي الإسلامي، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، مج 14، عدد 2، 2021، ص 77.

- جريمة السرقة: حد القطع.
- جريمة القذف: حد ثمانين جلدة.
- جريمة شرب الخمر: حد ثمانين جلدة.
- جريمة البغي: حدها القتل.
- جريمة الردة: حدها القتل.
- جريمة الحرابة: حدها القتل أو الصلب أو قطع اليد اليمنى والرجل اليسرى أو النفي.

فهذه الجرائم لا يمكن استبدال الحدود المقررة لها ببديل مهما كان في أي زمان ومكان، لأنها جرائم تمس بحق من حقوق الله تعالى.[1]

2- القصاص

القصاص "إسم لما يجنيه المرء من شر اكتسبه"[2]، وعقوبة القصاص هي الأخرى مقدرة بنص شرعي على وجه ثابت، وبديلها المقرر شرعا هو الدية، ولا يجوز استبدالها بغير ما جاء في الشرع، مثلها مثل الحدود، غير أنها تختلف عن هذه الأخيرة في أن القصاص يجوز فيه للمجني عليه أو لوليه العفو، لأن جرائم القصاص تمس بحقوق العباد، فيجوز للعباد العفو عنها.

والقصاص مقرر للجرائم التالية:

- القتل العمدي.
- المساس بسلامة الجسم عمدا.
- الجروح.

فالقصاص إذن ثابت شرعا، وإن كان يجوز العفو فيه، غير أنه لا يجوز استبداله بعقوبة بديلة.[3]

ثانيا: العقوبات المشروع إبدالها

العقوبات المشروع إبدالها بغيرها هي تلك التي لم تقدّر شرعا، وتسمى التعزير.

1- مفهوم التعزير

1. أحمد فتحي بهنسي، الحدود في الإسلام، مؤسسة المطبوعات الحديثة، القاهرة، د.س.ن، ص 166 وما يليها.
2. أحمد فتحي بهنسي، القصاص في الفقه الإسلامي، ط 5، دار الشروق، القاهرة، 1989، ص 11.
3. عمران محمد، المرجع السابق، ص 78.

كل جريمة لم ينص الشرع على عقوبة محددة لها، فلم يشرع فيها حد ولا قصاص تدخل في مفهوم التعزير. فتختلف جرائم التعزير عن جرائم الحدود والقصاص في أنها لم ينص على عقوبتها وترك أمر الاجتهاد فيها لولي الأمر، كما أنه يجوز العفو فيها ويجوز إبدالها بعقوبات بديلة، حيث أن مشروعية العقوبات البديلة تستند أصلا إلى مشروعية التعزير.[1]

يقول الدكتور أحمد فتحي بهنسي: "نص الشارع على ضرورة عقاب مرتكب الجريمة، فنص على العقوبة بالنسبة للحد والقصاص، أما في التعزير فترك ذلك للمشرع الوضعي يحدد العقوبات في مختلف الجرائم سوى ما حدده الله سبحانه وتعالى."[2]

2- الجرائم المعاقب عليها بالتعزير وعقوباتها

بما أن جرائم التعزير لا يمكن حصرها، فقد قال الفقيه بهنسي أنه "يعزّر كل من يرتكب جرما ليس فيه حد من الحدود المذكورة على سبيل الحصر، وهي السرقة والحرابة والزنا والقذف وشرب الخمر والبغي والردة. فإذا ارتكب الجاني جريمة خلاف هذه الجرائم المحددة العقوبة لا يحد بل يعزّر، وذلك مثل الرشوة وشهادة الزور وأكل الربا وجميع الجرائم غير الحدود."[3]

هذا وإن كانت جرائم التعزير لا يمكن حصرها، فإنه يستتبع ذلك عدم إمكانية حصر عقوباتها، بل يمكن إعطاء عقوبات على سبيل المثال كما جاء في الذخيرة عن التعزير: "وأما قدره فلا حد له فلا يقدّر أقله ولا أكثره بل بحسب اجتهاد الإمام على قدر الجناية ... وأما جنسه فلا يختص بسوط أو حد أو حبس أو غيره بل باجتهاد الإمام."[4]

الفرع الثاني: مدى مشروعية السوار الالكتروني كعقوبة بديلة للحبس

الآن بعدما تبين أنه لا تشرع العقوبات البديلة في الحدود ولا في القصاص فيما تشرع في التعزير، والقوانين الوضعية إنما قرّرت السوار الالكتروني كبديل عن العقوبة السالبة للحرية، فنتسائل هل العقوبة السالبة للحرية تدخل في مفهوم التعزير؟ فإن كانت كذلك فإنه مبدئيا يشرع إبدالها بالسوار الالكتروني؛

---

1. سلمان دعيج حمد بوسعيد، العقوبات البديلة للحبس في الفقه الإسلامي وصورها المعاصرة في قانون العقوبات، مجلة دراسات، الجامعة الأردنية، مج 48، عدد 4، 2021، ص 119.

2. أحمد فتحي بهنسي، التعزير في الإسلام، ط 1، مؤسسة الخليج العربي، القاهرة، 1988، ص 12.

3. أحمد فتحي بهنسي، التعزير في الإسلام، المرجع السابق، ص 18.

4. شهاب الدين أحمد بن إدريس القرافي، الذخيرة، دار الغرب الإسلامي، بيروت، 1994، ط 1، ج 12 (الجنايات والجراح)، ص 118.

غير أنه تبقى هناك مسألة أهم وهي أنه لا يمكن القول بجواز استبدال العقوبة السالبة للحرية في القانون الوضعي بالسوار الالكتروني إلا إذا كانت فعلا مقرّرة في جرائم تعزيرية ولم تقرّر خطأ في جرائم حدية، فجريمة السرقة مثلا هي جريمة حدية حدها القطع ولا يشرع فيها البديل، فإذا قرر لها المشرع الوضعي عقوبة تعزيرية خطأ فهذا لا يشفع في أن يُشرع فيها السوار الالكتروني كبديل.

أولا: مفهوم العقوبة السالبة للحرية ومدى دخولها في مفهوم التعزير

"عرف الإسلام سلب الحرية في صورة واحدة هي الحبس أو السجن بمعنى منع الحرية بقصد تعويق الشخص ومنعه من التصرف بنفسه ... وكان الحبس على نوعين: حبس كعقوبة، وحبس استطهار، أي على ذمة قضية معينة على سبيل الاحتياط."،[1] ولعل هذا ما يعرف عندنا بالحبس الاحتياطي، وكل من السجن والحبس هما معوقان للحرية وللفرار.[2]

والحبس الاحتياطي لا يعد من الحدود ولا من القصاص، مما يدخله في مفهوم التعزير، وبما أنه تعزير فجائز إبداله بعقوبة بديلة، مما يستنتج منه مبدئيا أن مسألة جعل السوار الالكتروني كعقوبة بديلة للعقوبة السالبة للحرية هي مسألة مشروعة وليست مخالفة لقواعد العقاب الشرعي الإسلامي.

ثانيا: إشكالية تقرير العقوبة السالبة للحرية في القانون الوضعي

توصلنا إلى أن العقوبة السالبة للحرية تتمثل كقاعدة عامة في الحبس، وهي تدخل في مفهوم التعزير مما يجعل إبدالها بعقوبة بديلة أمرا مشروعا، غير أن المشكل يكمن في الخطأ الفادح الذي يرتكبه المشرع الوضعي في وقتنا الحالي في أغلب الدول، حيث أنه يقرّر عقوبة الحبس التي هي تعزير في جريمة تدخل في حد من الحدود، كما فعله المشرع الجزائري الذي قرّر عقوبة الحبس في جريمة السرقة.[3]

فتجدر الإشارة ههنا إلى هذه المسألة البالغة الأهمية بمكان، وهي أن الشرعية هنا تضفى فقط على مسألة السوار الالكتروني كبديل عن العقوبة السالبة للحرية فحسب، ويفترض في هذه الأخيرة ما دامت تعزيرا أن لا يُقضى بها في جرائم الحدود أو القصاص، أما لو حصل أن وجدنا نصا وضعيا يقضي بالحبس في حد السرقة مثلا فلا يمكن القول بجواز استبدال عقوبة الحبس بالسوار الالكتروني، فمدار

---

1. عبد الفتاح خضر، تطور مفهوم السجن ووظيفته، جامعة نايف العربية للعلوم الأمنية، الرياض، 1984، ص 26.

2. محسنة بنت سعيد بن سيف القحطاني، العقوبات البديلة في قضايا الأحداث، رسالة ماجستير، قسم الشريعة والقانون، كلية العدالة الجنائية، جامعة نايف، الرياض، 2014، ص 27 و28.

3. راجع المادة 350 من قانون العقوبات الجزائري التي تعاقب على جريمة السرقة بالحبس وبالغرامة، مع أن السرقة حد عقوبته القطع لا الحبس.

الأمر كله هو النظر في مشروعية تقنين العقوبة المناسبة على الجريمة المناسبة قبل النظر في مشروعية العقوبة البديلة، فلا يكون السوار الالكتروني كبديل عن الحبس مشروعا إلا إذا كان الحبس مقررا في جريمة تعزيرية، لا حد ولا قصاص، وهذه مسألة تتطلب إعادة النظر في العقوبات المقرّرة للجرائم في القوانين الوضعية، لأن الجرائم المعاقب عليها بالحبس لا تدخل كلها في التعزير، بل منها ما يدخل للأسف في الحدود.

المبحث الثاني: مدى مساهمة تقنية السوار الالكتروني في تطور القانون الجنائي

بعدما تبين جواز إبدال العقوبة السالبة للحرية بالسوار الالكتروني بشرط أن تكون مقررة بحق في جريمة تعزيرية، فيمكن القول أن هذه العقوبة البديلة والحديثة غير مخالفة للشرع، ولكن هل تكريسها يساهم في الإصلاح الجنائي؟

إن معرفة ما إذا كان السوار الالكتروني يصلح أن يكون بديلا عن الحبس الاحتياطي تتطلب معرفة ما إذا كان يحقق أغراض عقوبة الحبس من جهة؛ ومن جهة أخرى لنفرض أنه حققها، هل سيكون تفعيله ناجحا؟

المطلب الأول: مدى تحقيق السوار الالكتروني لمقاصد الحبس

سبق وأن رأينا أن عقوبة الحبس هي من العقوبات التعزيرية المتروك الاجتهاد في تقديرها لولي الأمر يختار من البدائل العقابية ما يراه صالحا لمكافحة الجريمة وتقويم وتأهيل مرتكبيها،[1] فإن كان المشرع يرى السوار الالكتروني بديلا عن الحبس، فيجب الوقوف على مسألة مدى تحقيقه لأغراض الحبس من جهة، ومن جهة أخرى التحقق من مدى تحقيقه لضوابط تنفيذه.

الفرع الأول: مدى تحقيق السوار الالكتروني لأغراض عقوبة الحبس

تتمثل أغراض عقوبة الحبس في الردع وإصلاح المحبوس وتحقيق العدالة الجنائية في المجتمع.

أولا: الردع

1. عليان بوزيان وحبشي لزرق، بدائل العقوبة السالبة للحرية من منظور إسلامي، مجلة المعيار، تيسمسيلت، مج 5، عدد 9، 2014، ص 246.

المقصود بالردع هو تهديد وتخويف العامة تحذيرا من الاقتراب للجريمة أو التفكير في ارتكابها،[1] فحد قطع اليد يلقي الخوف في نفسية من تحدثه نفسه بارتكاب جرم السرقة مما يجعله يعدل عنها خوفا من العقاب. ولهذا غالبا ما نجد الردع في الحدود، وهي عقوبات يغلب عليها طابع التشدد الذي يحقق غرضها، فالرجم والجلد والقطع وغيرها من الحدود تلعب دورا كبيرا في الوقاية من وقوع الجريمة أصلا، ناهيك عن الأثر الذي تخلّفه في الجاني وفي المجتمع عند تطبيقها حال وقوع الجريمة، مما يجعلها نادرة.

لكن قد يصل التعزير بالحبس هو الآخر إلى الردع، سواء ردع الجاني نفسه أو العامة، فالحبس داخل أسوار المؤسسات العقابية عقوبة مقيدة للحرية مقلقة للنفس البشرية التي جُبلت على حب الحرية وعدم إطاقة القيود، فهو بالتالي يهدف إلى الحد من الجريمة بالحد من حرية مرتكبيها الذين سيكرهون العودة إلى الإجرام كما يكرهون العودة إلى الحبس.

وإذا ما عدنا إلى عقوبة السوار الالكتروني فلا نرى فيها شدة، بل نجدها يغلب عليها طابع السهولة واللين، فهي مجرد مراقبة عن بعد للمحكوم عليه، وليست حبسا مقيدا للحرية، فالمحكوم عليه طليق خارج أسوار المؤسسة العقابية وبين أفراد عائلته مما يعطيه أكثر حرية من المحبوس، وبالتالي فلا يبدو السوار الالكتروني محققا للردع الذي يحققه الحبس، فإن صلح قد يصلح لجاني مبتدئ في جريمة لا تعدو أن تكون مخالفة خفيفة، ولا يصلح تطبيقه في الجنايات والجنح ما دام لا يحقق الردع الذي يحققه الحبس.

ثانيا: إصلاح الجاني

المقصود بإصلاح الجاني "استئصال الخطورة الاجرامية الكامنة في شخصه وإعادة تأهيله للحياة الاجتماعية"،[2] وعموما قد يتحقق إصلاح الجاني بتعزيره، وذلك ببعث الندم في نفسه وتعويده على النظر الجدي في أفعاله، ويمكن أن يتحقق هذا بالسوار الالكتروني حيث منحه الثقة يعزّز كرامته ويسهل عزوفه عن العودة لسلك طريق الإجرام مرة أخرى، غير أن هذه المسألة هي الأخرى يجب التعامل فيها بحذر لأن الواقع يعكس أنواعا كثيرة من الجناة، فمنهم من لا ينفع معه الإصلاح، ولهذا وجب عند تطبيق العقوبة بغرض إصلاح الجاني النظر قبل ذلك إلى شخصيته إن كان أهلا للصلاح، وكذا ظروفه ومدى تهيؤ

1. جمال زيد الكيلاني، مقاصد العقوبة في الشريعة الإسلامية، مجلة جامعة النجاح للأبحاث، فلسطين، مج 28، عدد 1، 2014، ص 111.

2. عمران محمد، المرجع السابق، ص 85.

ملكة الخير لديه،[1] ولهذا يبقى السوار الالكتروني بمثابة تجربة تضفى على المحكوم عليه، قد تنجح وقد تفشل، وفي حالة فشله لا مناص من الرجوع إلى العقوبة الأصل وهي الحبس داخل المؤسسة العقابية.

ثالثا: تحقيق العدالة الجنائية

تتحقق العدالة الجنائية عندما توقع على الجريمة العقوبة المناسبة لها، أي لما يتحقق التوازن بين العقوبة والجريمة، ولا يمكن أن تتحقق إذا كانت العقوبة أخف من الجريمة أو العكس، فلو كانت العقوبة أشد من الجريمة كان ظلما، ولوكان أخف منها لم يتحقق الردع المطلوب، واستخف بها المجتمع مما يزيد في استفحال الإجرام.[2]

وتبدو العقوبة المقتصرة على مجرد حمل سوار دون حبس فعلي وجسدي للجاني خفيفة نوعا ما، تكاد لا تناسب الإجرام الذي يشهده العصر اليوم، لأن السوار في يد المحكوم عليه يمكنه التخلص منه بسهولة والفرار، عكس الحبس داخل المؤسسة العقابية الذي يضمن التحكم فيه عن قرب وتوجيهه ومراقبته ورصد مدى توفر ملكة الصلاح في نفسه، وبالتالي مدى استعداده قبول إعادة التأهيل والاندماج في المجتمع.

الذي يبدو لنا بعد هذه الدراسة المتواضعة أن السوار الالكتروني يبقى مجرد تجربة لا ترقى لمفهوم العقوبة الحقيقي إلا في حالات نادرة يكون فيها الجاني إما حدثا يُرجى إعادة تربيته، أو مبتدئا يُرجى إعادة تأهيله، أو مخطئا يُرجى توبته، ولهذا فلا يرفض قطعا تطبيقه، ولكنه لا يطبق كعقوبة بل كوسيلة إصلاح لمن يمكن إصلاحه، ولهذا حبذا لو حدد المشرع أشكال الإصلاح عن طريق السوار الالكتروني، وأشكال الخاضعين له على سبيل المثال لا الحصر، لتسهل مهمة القاضي في الأمر به، ويتضح أكثر الغرض من السوار كوسيلة لإصلاح العدالة.

الفرع الثاني: مدى تحقيق السوار الالكتروني لضوابط تنفيذ عقوبة الحبس

تتمثل ضوابط تنفيذ العقوبة بصفة عامة، وعقوبة الحبس بصفة خاصة في عدم تضرر المجتمع وعدم تضرر المحكوم عليه وعدم المساس بسياسة العقاب.

أولا: عدم تضرر المجتمع

1. عمران محمد، المرجع السابق، ص 85.
2. عمران محمد، المرجع السابق، ص 86.

يجب أن يضمن تطبيق السوار الالكتروني عدم تضرر المجتمع، فالمحكوم عليه لن يكون محبوسا عن قرب بل طليقا مراقبا عن بعد، فلو سوّلت له نفسه ارتكاب جريمة أخرى، قد لا يتوصل إلى منعه وحماية المجتمع منها إلا بعد فوات الأوان، مما يجب معه توخي الحذر في منح الاستفادة منه للفئة الخطيرة من المجرمين كالمغتصبين وخاطفي الأطفال والمتعاطين للمخدرات وغيرهم ممن يشكّلون خطرا على المجتمع، وما أكثرهم اليوم.

ثانيا: عدم تضرر المحكوم عليه

المحكوم عليه حتى وإن كان جانيا لا يجوز الإضرار به، إذ الهدف من العقوبة تهذيبه وإصلاحه لا تعذيبه والإضرار به.[1]ويشمل عدم الإضرار بالمحكوم عليه عدم المساس بسمعته وكرامته من جهة؛ وبصحته من جهة أخرى، ولعل هذا ما قصده المشرع من نص الفقرة الثانية من المادة 150 مكرر 2 حيث قضى: "يجب احترام كرامة الشخص المعني وسلامته وحياته الخاصة عند تنفيذ الوضع تحت المراقبة الالكترونية."

وبالنسبة للحرص على السلامة البدنية للمحكوم عليه، الانتباه إلى كون تقنية السوار الالكتروني متماشية مع الوضع الصحي للمحكوم عليه غير ضارة به، لأن منهم من يحمل بطاريات تنظم دقات القلب وغيرها مما لا يتماشى وتقنية التكنولوجيا الرقمية، ولهذا وجب قبل الحكم بالسوار الأخذ في الحسبان الملف الصحي للمحكوم عليه.[2]

ثالثا: عدم المساس بسياسة العقاب

تقتضي سياسة العقاب أن تكون العقوبة على قدر الجريمة من جهة؛ ومن جهة أخرى لا يقضى بالعقوبة التعزيرية كبديل لعقوبة حدية أو قصاص.[3]

فأما عن وجوب كون العقوبة على قدر الجريمة،فيقتضيه مبدأ العدل والمساواة الذي يلزم أن تكون العقوبة لا أخف ولا أقسى من الجريمة، وقد سبق الحديث عن هذه المسألة، إلا أنه يجب التنبيه هنا إلى أنه على القاضي عند أمره بالسوار الالكتروني أن يراعي تساوي مدة حمل السوار مع مدة العقوبة السالبة للحرية المحكوم بها على الجاني.

---

1. سلمان دعيج حمد بوسعيد، المرجع السابق، ص 128.
2. المرجع السابق.
3. سلمان دعيج حمد بوسعيد، المرجع السابق، ص 128 و129.

وأما عن وجوب عدم القضاء بعقوبة تعزيرية كبديل لعقوبة حدية أو قصاص،فهو ضابط بالغ الأهمية، إذ علاوة على وجوب عدم الحكم بالسوار في جرائم الحدود، يجب أيضا عدم الحكم به في الجرائم المعاقب عليها خطأ بعقوبة سالبة للحرية كجريمة السرقة مثلا، فمعلوم أن جرائم السرقة في جُلّ التشريعات العربية لا يطبق بشأنها عقوبة القطع، مثلها مثل جريمة الزنا التي تستحق عقوبة الرجم أو الجلد، فهذه الجرائم عقوباتها الشرعية معطّلة للأسف،[1] مما لا يمكن معه تطبيق بديل السوار الالكتروني فيها حتى وإن كانت عقوباتها الوضعية هي الحبس.

المطلب الثاني: مدى مساهمة السوار الالكتروني في الإصلاح الجنائي

إن إثارة مسألة الإصلاح الجنائي توحي حتما للتساؤل حول دوافع التفكير في بديل عن العقوبات السالبة للحرية، فهل فشل الحبس في تحقيق أهدافه؟

ومن جهة أخرى، ما دامت تقنية السوار الالكتروني قد تم تقريرها قانونا كبديل للعقوبة السالبة للحرية، فهل نجح السوار في الإصلاح الجنائي؟

الفرع الأول: حقيقة فشل العقوبة السالبة للحرية

أعطى الكثير من شُرّاح القانون أسباباعامة لفشل العقوبة السالبة للحرية في الإصلاح الجنائي، غير أننا نرى أن هناك حقيقة أخرى وراء فشلها كما سنبين أدناه.

أولا: الأسباب العامة لفشل العقوبة السالبة للحرية

يُرجع العديد من الشُّرّاح فشل العقوبات السالبة للحرية لأسباب عامة منها ما يلي:[2]

– إساءة تطبيق عقوبتي الحبس والسجن، وبالتالي ظُلم الكثير من الأبرياء لعدم إمكانية ثبوت براءتهم رغم اقتناع القاضي ببراءتهم.

1.محمد عيشوبة، العقوبات بين الشريعة الإسلامية والقانون الجزائري –دراسة مقاصدية–، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، مج 15، عدد 1، 2022، ص 808.

2. محسنة بنت سعيد، المرجع السابق، ص 35 وما يليها، راجع أيضا: وداعي عز الدين، العقوبات البديلة كضمان للحد من مساوئ العقوبة السالبة للحرية قصيرة المدة في الجزائر، المجلة الأكاديمية للبحث القانوني، جامعة بجاية، مج 11، عدد 1، 2020، ص 52 و53. راجع أيضا: جلال الدين بانقا أحمد بشير، العقوبات البديلة للسجن، مجلة جامعة شندي للبحوث والدراسات الشرعية والقانونية، السودان، عدد 2، 2020، ص 53.

– اكتظاظ المؤسسات العقابية بالمساجين،وعدم كفاية السجون لاستيعاب المزيد، وعدم نجاح سجون اليوم في ردع نزلائهم ومنعهم من العود.
– إرهاق خزينة الدولة بسبب تضاعف الأموال الواجب صرفها على نزلاء السجون من أجل نفقتهم بكل أنواعها من مأكل وملبس وعلاج.
– التواصل السلبي بين السجناء وما يتمخض منه من آثار خطيرة على المبتدئين منهم، فعوض التوصل لتحسين سلوك أكابر المجرمين انعكس سلوكهم على أصاغرهم مما زاد في انتشار الملكة الإجرامية.
– تضرّر أُسر المساجين بابتعاد ذويهم ممن قد يكونون مُعيلين لهم، مما يؤدي في كثير من الأحيان إلى تفكك أُسرهم وتشرد ذراريهم.

لكن المتمعن جيدا في هذه الأسباب يجدها ليست سببا في فشل العقوبة السالبة للحرية بحد ذاتها، وإنما سببا في عدم القدرة على تطبيقها تطبيقا جيدا، فالفشل لا ينسب إلى الحبس في حد ذاته وإنما إلى إساءة تطبيقه، فسجون اليوم صارت كالفنادق لا تحقق ردعا، ولا تذيق نزيلها طعم السجن، مما لم يعد معه خوفٌ في نفوس المجرمين من دخولها، بل من الفقراء من يفتعل الإجرام كي يدخل السجن ليجد مأوى لهحيث أصبحت سياسة حياة، كيف وقد أضحت المؤسسات العقابية مهيئة حتى بأجهزة التلفاز زعما بإصلاح الجاني، مع أن المعروف عرفا أن ليونة العيش لا تصنع الرجال فكيف بإصلاحها، ألا يوصي ديننا بوجوب تربية الطفل على خشونة العيش ليكبر على طينة الرجال؟

لهذه الأسباب، يبدو أن فشل العقوبة السالبة للحرية لا يعود إليها بالذات، بل إلى تطبيقها السيء، كما أن هناك سبب جدي آخر وراء استفحال الجريمة وعدم القدرة على الإصلاح الجنائي، وهو تعطيل الحدود الشرعية.

ثانيا: فشل سياسة العقاب بتعطيل الحدود الشرعية

أفادت دراسات عديدة تزايد معدل الإجرام يوميا، وارتفاع نسبة المجرمين بوتيرة سريعة، مما تسبب في عجز الدولة عن التصدي لها من جهة، وعن احتواء المجرمين من جهة أخرى، ما أوقعها في ورطة التعامل مع الموقوفين صعب عليها الخروج منها لكثرتهم وقلة إمكانيات التعامل معهم ومواجهتهم، وقد أرجع بعض الباحثين السبب الرئيسي إلى "عدم تطبيق العقوبات الشرعية المقدرة والمحددة من قبل الشريعة الإسلامية لبعض الجرائم وليس لكلها، بالإضافة إلى بعض التعازير التي لا تتناسب مع نوع الجريمة

المرتكبة".[1] فعقوبة السرقة هي القطع وليس الحبس، وعقوبة القتل العمد هي القصاص، وإن كان المشرع الوضعي ينص على الإعدام فهو غير مُفعّل بجدية، بل نحن الآن في عصر تعالت فيه الأصوات المطالبة بإلغائه لعدم انسانيته على حد زعمهم، فكيف بعد هذا لا تستفحل الجريمة؟!

وعلى هذا، فالحل الوحيد للوصول إلى تحقيق مقاصد عقوبة الحبس بصفة خاصة، والإصلاح الجنائي بصفة عامة، هو تطبيق الحدود المشروعة بالقرآن والسنة.

ولكن إذا بقينا في التعازير المخول الاجتهاد فيها، وأدخلنا السوار الالكتروني ضمنها، هل سيساهم في حماية المجتمع من الإجرام؟

الفرع الثاني: آثار تقنية السوار الالكتروني على المجتمع

لو فرضنا أن استجاب المشرع الوضعي لأحكام الشريعة الإسلامية في المجال الجنائي، وقرّر الحدود والقصاص على الجرائم الخاصة بها، واجتهد في التعزير سواء بالإبقاء على العقوبة السالبة للحرية، أو باستحداث السوار الالكتروني كبديل لها، فما مدى مساهمة هذه التقنية التكنولوجية في الإصلاح الجنائي؟

أولا: مزايا السوار الالكتروني

السوار الالكتروني تكنولوجيا حديثة لا يمكن التنبؤ بمدى نجاحها إلا مع مرور مدة كافية، ولا يمكن الحكم بدقة على مدى مساهمتها في الإصلاح الجنائي إلا بعد توسيع تطبيقها على عينة كافية، ومع ذلك فقد نسبت لها بعض المزايا هي في الحقيقة لم تكن نتيجة استخدامها بل ما كان مرجوا من استخدامها، ويمكن إجمالها فيما يلي:[2]

– التخفيف من الاكتظاظ في السجون، وهي النتيجة الرئيسية المرجوة من السوار الالكتروني، ومازالت لم تتحقق بعد نظرا للتفعيل المحتشم له.

– التخفيف من جريمة العود، وهذه أيضا مجرد فرضية وضعها مؤيدو السوار، إذ على حد قولهم عدم تقييد الجاني يساهم في منحه الثقة في نفسه وعدم التفكير في العودة للإجرام، ولكن تبقى هذه مجرد فكرة غير مبررة.

1. محمد عيشوبة، العقوبات بين الشريعة الإسلامية والقانون الجزائري –دراسة مقاصدية–، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، مج 15، عدد 1، 2022، ص 808.

2. Pierrette PONCELLA, La surveillance électronique de fin de peine, R.S.C D.P.C, 2011, n 3, P 685.

– السوار الالكتروني يكلف نفقات أقل من نفقات الحبس، أي هو أكثر اقتصادي منه، غير أن هذه الميزة انتقدت هي الأخرى على أساس أن تطبيق السوار يتطلب علاوة على اقتناءه تكوين العاملين عليه وإنفاق أموالا معتبرة على المكالمات الهاتفية وغيرها من الاتصالات اللازمة.

– اعتبر السوار تدبيرا أكثر إنسانية من الحبس، ولكن هذه الفكرة التي تعني عدم إنسانية السجون لا يمكن اعتبارها صحيحة إذ طبيعة السجن تقتضي تقييد الجناة، ولا يعد هذا عملا غير إنساني إذا لم يظلم السجين.

– السوار يسمح بحماية فعالة للمجتمع من الجاني، وهذه الميزة الغريبة انتقدت على أساس أن المحكوم عليه يمكنه بالعكس التخلص من السوار للهروب من العدالة والإضرار بالمجتمع.[1]

وبهذا يبدو أن الوقت جد متقدم للحكم على السوار الالكتروني بأنه أداة فعالة للإصلاح الجنائي.

ثانيا: عيوب السوار الالكتروني

سمحت دراسة تقنية السوار الالكتروني كعقوبة بديلة عن الحبس بالاطلاع على العديد من الآراء الفقهية الرافضة لهذه التكنولوجيا، ويمكن إجمال النظرات السلبية الموجهة له فيما يلي:[2]

– خلو السوار الالكتروني من أسلوب الردع والزجر، وعدم تقبله من المجتمع كعقوبة، والاستخفاف به، وعدم الثقة فيه.[3]

– السوار الالكتروني يخرق حقا من حقوق الإنسان، وهو حقه في الخصوصية وفي احترام حياته الخاصة،وذلك باختراقه الجدران لمراقبة المحكوم عليه في أدنى تحركاته.

– السوار الالكتروني قد يكون سببا في إلحاق الضرر بصحة حامله، إذ يعتمد على التكنولوجيا الرقمية التي تعمل بإشعاعات قد لا تظهر عواقبها إلا بعد مدة.

– صعوبة تطبيق تقنية السوار تبعا لصعوبة توفير مكان لعزل المحكوم عليه، خصوصا منهم الذين لا يملكون إقامة معلومة.

1. Olivier LEGRAND, La surveillance électronique des justiciables, Wallonie-Bruxelles, 2015, p 13.
2.Olivier LEGRAND, op.cit., p 17.
3. صفاء أوتاني، الوضع تحت المراقبة الالكترونية –السوار الالكتروني في السياسة العقابية الفرنسية– مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج 25، عدد 1، 2009، ص 154.

– خطر إساءة تطبيق السوار الالكتروني، خصوصا إذا كان المحكوم عليه من المجرمين الخطرين الذين لا يصح تركهم أحرارا لغلبة أذيتهم للمجتمع.

خاتمة:

خلصت دراسة تقنية السوار الالكتروني ومدى تحقيقها لمقاصد العقوبة السالبة للحرية من جهة، ومدى مساهمتها في الإصلاح الجنائي من جهة أخرى إلى النتائج التالية:

– تدخل العقوبة السالبة للحرية ومنها الحبس في مفهوم التعزير الذي لم يشرع فيه حد ولا قصاص، وإنما ترك للاجتهاد فيه بتقرير عقوبة على قدر الجريمة.

– يجوز شرعا إبدال العقوبة السالبة للحرية بعقوبات بديلة لها، بشرط أن تكون مقررة في تعازير فقط.

– العقوبات السالبة للحرية في قانون العقوبات الجزائري مقررة خطأ في بعض جرائم الحدود، وبالتالي لا يمكن تطبيق السوار الالكتروني فيها كبديل.

– تقنية السوار الالكتروني هي من النوازل الفقهية التي يجوز مبدئيا جعلها كبديل للعقوبة السالبة للحرية.

– تقنية السوار الالكتروني لا تحقق كل مقاصد عقوبة الحبس، إذ أن هذا الأخير لا يسهل هروب الجاني، فيما يفتح السوار الباب واسعا للهروب؛ كما أن الحبس يحمي المجتمع من الجاني بينما لا يحقق السوار هذه الحماية.

– السوار الالكتروني قد يساهم في إصلاح بعض الجناة، ولكنه لا يساهم أبدا في زجر ولا ردع، ولهذا السبب فهو يبدو كوسيلة إصلاح، لكن لا يمكن أبدا اعتباره وسيلة عقاب.

– أثبت الميدان العملي استخفاف بعض المحكوم عليهم بعقوبة السوار الالكتروني مما جعل العديد من قضاة التحقيق يعزفون عن تطبيقه.

وعلى أساس هذه النتائج نقترح التوصيات التالية:

– يمكن الاستئناس بالسوار الالكتروني واعتباره وسيلة لإصلاح الجناة لا وسيلة لعقابهم، إذ لا يمكن اعتباره عقوبة.

– يمكن منح الاستفادة من السوار الالكتروني للمبتدئين والأحداث والمتورطين خطأ في جرائم مخففة ممن يثبت في العادة اقتناع شخصي لدى القضاة ببراءتهم، ولا يمكن تطبيقه على من يشكّل خطورة على

المجتمع من مجرمي الاغتصاب والسرقة والقتل وخطف الأطفال وغيرها، ولا على من يتوسم فيه عدم جدوى الإصلاح، ولا على من يستخفون به.

– الإصلاح الجنائي حسب الرأي العام والمعقول يأتي من تغليظ العقوبة لا من تخفيفها، مما يستوجب العودة إلى الشريعة الإسلامية،بتفعيل الحدود والقصاص لإقامة العدل وحماية المجتمع وإعادة إحياء الزجر والردع الميتين في نفوس المجرمين.

– لا مانع من القضاء على الاكتظاظ في السجون بتشييد المزيد منها، كما أنه لا مانع من الاستفادة من العدد الهائل للمساجين بتشغيلهم فيما يعود بالنفع على الدولة كالفلاحة والصناعة، بل ويمكن تحويل بعض المؤسسات العقابية إلى ورشات تشغيل للاستفادة من النزلاء ذوي الكفاءات العالية.

– إخلاء السجون من وسائل الترفيه كالتلفاز ليتحقق الغرض منها، والأفضل تعويضها بوسائل أخرى كالمكتبات والمصليات، مع تعزيز الخطاب الديني الدوري لإعادة إحياء الوازع الديني في نفوس المجرمين والقضاء على النزعة الإجرامية لديهم.

المراجع:

المراجع العربية:

الكتب:

1. أحمد فتحي بهنسي، الحدود في الإسلام، مؤسسة المطبوعات الحديثة، القاهرة، د.س.ن.

2. أحمد فتحي بهنسي، القصاص في الفقه الإسلامي، ط 5، دار الشروق، القاهرة، 1989.

3. أحمد فتحي بهنسي، التعزير في الإسلام، ط 1، مؤسسة الخليج العربي، القاهرة، 1988.

4. شهاب الدين أحمد بن إدريس القرافي، الذخيرة، ط 1، ج 12 (الجنايات والجراح)، دار الغرب الإسلامي، بيروت، 1994.

5. عبد الفتاح خضر، تطور مفهوم السجن ووظيفته، جامعة نايف العربية للعلوم الأمنية، الرياض، 1984.

الرسائل:

1. محسنة بنت سعيد بن سيف القحطاني، العقوبات البديلة في قضايا الأحداث، رسالة ماجستير، قسم الشريعة والقانون، كلية العدالة الجنائية، جامعة نايف، الرياض، 2014.

المقالات:

1. عامر جوهر وعباسة طاهر، السوار الالكتروني إجراء بديل للعقوبة السالبة للحرية في التشريع الجزائري، مجلة الاجتهاد القضائي، جامعة بسكرة، مج 10، عدد 2، 2018، ص ص 177-196.

2. بن يوسف القينعي، نظام المراقبة التقنية في التشريع الجزائري، حوليات جامعة الجزائر 1، مج 35، عدد 2، 2021، ص ص 69-86.

3. عمران محمد، أغراض العقوبة والمبادئ الأساسية التي ترتكز عليها في النظام العقابي الإسلامي، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، مج 14، عدد 2، 2021، ص ص 74-88.

4. سلمان دعيج حمد بوسعيد، العقوبات البديلة للحبس في الفقه الإسلامي وصورها المعاصرة في قانون العقوبات، مجلة دراسات، الجامعة الأردنية، مج 48، عدد 4، 2021، ص ص 116-133.

5. عليان بوزيان وحبشي لزرق، بدائل العقوبة السالبة للحرية من منظور إسلامي، مجلة المعيار، تيسمسيلت، مج 5، عدد 9، 2014، صص 246-272.

6. وداعي عز الدين، العقوبات البديلة كضمان للحد من مساوئ العقوبة السالبة للحرية قصيرة المدة في الجزائر، المجلة الأكاديمية للبحث القانوني، جامعة بجاية، مج 11، عدد 1، 2020. ص ص 48-69.

7. محمد عيشوبة، العقوبات بين الشريعة الإسلامية والقانون الجزائري –دراسة مقاصدية–، مجلة الحقوق والعلوم الإنسانية، جامعة الجلفة، مج 15، عدد 1، 2022، ص ص 803-820.

8. صفاء أوتاني، الوضع تحت المراقبة الالكترونية – السوار الالكتروني في السياسة العقابية الفرنسية– مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مج 25، عدد 1، 2009، ص ص 129-162.

9. جلال الدين بانقا أحمد بشير، العقوبات البديلة للسجن، مجلة جامعة شندي للبحوث والدراسات الشرعية والقانونية، السودان، عدد 2، 2020، ص 53.

10. جمال زيد الكيلاني، مقاصد العقوبة في الشريعة الإسلامية، مجلة جامعة النجاح للأبحاث، فلسطين، مج 28، عدد 1، 2014، ص ص 91-126.

القوانين:

1. أمر رقم 66-156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات، الجريدة الرسمية عدد 49، المؤرخة في 11 يونيو 1966.

2. أمر رقم 15-02 مؤرخ في 23 جويلية 2015 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 08 جوان 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40، المؤرخة في 23 جويلية 2015، ص 28.

3. قانون رقم 15-03 مؤرخ في 01 فبراير 2015 يتعلق بعصرنة العدالة، الجريدة الرسمية عدد 06، المؤرخة في 10 فبراير 2015، ص 4.

4. قانون رقم 18-01 مؤرخ في 30 يناير 2018 يتمم القانون رقم 05-04 المؤرخ في 06 فبراير 2005 والمتضمن قانون تنظيم السجون وإعادة الإدماج الاجتماعي للمحبوسين، الجريدة الرسمية عدد 05، المؤرخة في 30 يناير 2018، ص 10.

المراجع الأجنبية:

1.Jean Paul CERE, La surveillance électronique : Une réelle innovation dans le procès pénal, Revue de la faculté de droit de Campos, Vol VII n 8, 2006, pp 105-122.

2. Pierrette PONCELLA, La surveillance électronique de fin de peine, R.S.C D.P.C, 2011, n3, pp681-689.

3. Olivier LEGRAND, La surveillance électronique des justiciables, Wallonie-Bruxelles, 2015.

مصادر الانترنت:

1. هبة أنيس، هل ينجح السوار الالكتروني في إنهاء دائرة الحبس الاحتياطي، منشور على الموقع حقوق وحريات www.masr/360-net بتاريخ 2021/04/04 20:30

2. محمد. ب، انطلاق العمل بالسوار الالكتروني من تيبازة، جريدة المساء، مؤرخة في 26 ديسمبر 2016، www.el-massa.com/dz

التصوير الضوئي
كوسيلة لتسجيل معاينة مسرح الجريمة

د . يحيى عبد الحميد / أستاذ محاضر قسم " أ "
كلية الحقوق والعلوم السياسية / جامعة مستغانم

الملخص :

يعد التصوير الضوئي وسيلة مهمة من الوسائل المستعملة في البحث الجنائي، لأنه يسمح بتسجيل الآثار المادية التي يعثر عليها الباحث الجنائي بمسرح الجريمة، وتقديمها لسلطات القضاء الجزائي في شكل صور لتكون أدلة أو قرائن على وقوع الجريمة ونسبتها إلى مرتكبها. ويخضع تصوير مسرح الجريمة لجملة من الضوابط الفنية التي تضمن إنجاز صور واضحة ودقيقة، تكشف الحقيقة كاملة عن هذا المسرح والآثار المادية التي تمت معاينتها بعد الحادث الإجرامي. وتزداد أهمية وفعالية التصوير الضوئي في مجال البحث الجنائي بفضل التطور التكنولوجي الذي تشهده الآلات والأجهزة المستخدمة في إنجازه، و كذلك بفضل المزايا التي ينفرد بها عن باقي أساليب المعاينة في المجال الجزائي.

الكلمات المفتاحية : التصوير الضوئي – مسرح الجريمة – الآثار المادية – البحث الجنائي

Summury :

Photography is an important instrument used in criminal investigation, because it enables recording the physical traces found by the criminal investigator at the crime scene in order to present them to the criminal justice authorities in the form of images to be evidence or clues to the occurrence of the crime and relating it to the perpetrator. Taking photography of a crime scene is subject to a set of technical standards that garantee the accomplishment of clear and accurate images that must reveal the full truth about this scene and the physical effects that were examined after the criminal incident.The importance and effectiveness of photography in the field of criminal investigation increases thanks to the technological development witnessed by the machines and devices used to achieve it, as well as thanks to the advantages that are unique to the photography comparing to other methods of inspection in the criminal field.

Keywords : Photography – crime scene – physical effects – criminal investigation

مقدمة

يشكل تسجيل مسرح الجريمة عملا أساسيا من أعمال البحث الجنائي، ذلك أن هذا المسرح هو المصدر الرئيسي لمعظم الأدلة المادية على وقوع هذه الجريمة ، ونسبتها إلى مرتكبها، وتحديد ظروف ارتكابها. وعلى هذا الأساس ينبغي لضابط الشرطة القضائية أن يسجل معاينته لهذا المسرح عن طريق الوصف الدقيق للحالة التي وجده عليها، حيث أن هذا الوصف ينطوي على فوائد كبيرة في مرحلتي التحقيق والمحاكمة، فسلطة التحقيق تباشر عملها على نحو سليم متى قدم لها وصف كامل ودقيق لحالة مسرح الجريمة مباشرة بعد وقوعها، كما أن جهة الحكم لا غنى لها عن هذا الوصف عندما تجري تحقيقها النهائي بالجلسة.

ويتم وصف مسرح الجريمة بثلاث طرق هي : والوصف الكتابي ضمن المحاضر، وتصوير مسرح الجريمة، والرسم التخطيطي للواقعة.

ويتعلق موضوع هذه المداخلة بإحدى هذه الطرق الثلاثة وهي طريقة تصوير مسرح الجريمة، وقد أصبح هذا التصوير يكتسي أهمية كبرى في ميدان البحث الجنائي نظرا للتطور التكنولوجي الهائل الذي بلغته الآلات والأساليب الفنية المستخدمة في هذا الشأن. وسوف نتناول هذا الموضوع وفق خطة تراعي الترتيب المنهجي لعناصره، والتقسيم المتوازن لمحتوياته، وبمقتضاها نتناول ماهية التصوير الضوئي لمسرح الجريمة (مبحث أول) ثم نتناول مزايا التصوير الضوئي لمسرح الجريمة.

المبحث الأول : ماهية التصوير الضوئي لمسرح الجريمة

لتحديد ماهية التصوير الضوئي لمسرح الجريمة على أكمل وجه، ينبغي أن نقوم بتعريفه (مطلب أول)، ثم نبين الضوابط الفنية التي تجب مراعاتها عند القيام به (مطلب ثان).

المطلب الأول : تعريف التصوير الضوئي لمسرح الجريمة

التصوير الضوئي عموما هو التصوير الفوتوغرافي، ويسمى أيضا " التصوير الشمسي " ،أو "التصوير الثابت " ويعرف بأنه " طريقة عملية لإنتاج صورة عن غرض ما بالاستفادة من التأثير الذي يحدثه الضوء في مادة حساسة "[1].

[1] نوفل علي عبد الله وخالد عوني خطاب، دور أجهزة التصوير الحديثة في الإثبات الجنائي– دراسة مقارنة – ، مجلة الرافدين للحقوق، المجلد(15) ، العدد (55) ، السنة (17).

ويتم التقاط الصورة الضوئية بواسطة آلة التصوير وهي : " عبارة عن صندوق محكم لا ينفذ منه الضوء، في أحد أطرافه عدسة مجمعة يقابلها في الطرف الآخر للصندوق اللوح الحساس أو الفلم. بالإضافة إلى أجزاء أخرى تضمن حدة تفاصيل الصورة وتحدد كمية الضوء المارة خلال العدسة وتتحكم فيه "[1].

وتتكون آلة التصوير من عدة أجزاء أساسية هي العدسة والفتحة والغالق والصندوق المظلم أو الممر المظلم، وهي مكونات لا يمكن الاستغناء عنها مهما حدث تطور العلم والتكنولوجيا في مجال التصوير الضوئي، وذلك لأنها عناصر أساسية في هذا التصوير سواء أكان إنتاج الصورة فيه يعتمد على المعالجة الكيميائية أو على التقنيات الرقمية، فالكاميرات الرقمية الحديثة والمتطورة تعتمد أيضا على هذه العناصر، وأساس عملها يقوم على ذات المبدأ الذي يقوم عليه التصوير الضوئي (الفوتوغرافي) ، ولا يختلف عنه إلا من ناحية طبع الصورة، فالتصوير الضوئي يعتمد على المعالجة الكيميائية لإنجاز هذا الطبع، أما التصوير بواسطة الكاميرات الرقمية فيعتمد على المعالجة الإلكترونية لإخراج الصورة[2].

وقد تم اختراع التصوير الضوئي عام 1839م من طرف العالم الإنجليزي " وليم هنري فوكس " ولم يكن هذا التصوير غداة اختراعه ينتج صورا ذات جودة كبيرة، وفي عام 1890م ظهرت إلى الوجود عدسات تصوير أكثر تطورا، وفي عام 1906م تم إنتاج أفلام تصوير ذات حساسية عالية. وبعد ذلك كان لأحداث الحرب العالمية الثانية أثر بارز في الدفع نحو الاستعانة بالتصوير، وخاصة في مجال تصوير أراضي الأعداء والأهداف العسكرية والوثائق الهامة[3].

---

[1] مديحة فؤاد الخضري و أحمد بسيوني أبو الروس ، الطب الشرعي والبحث الجنائي، بدون طبعة ، دار المطبوعات الجامعية ، الإسكندرية، 1989، ص 595.

[2] نوفل علي عبد الله و خالد عوني خطاب، مرجع سابق، ص 402.

[3] عمار عباس الحسيني، التصوير المرئي وحجيته في الإثبات الجنائي، بحث منشور على الشبكة الدولية للمعلومات (الإنترنت).
https://www.iasj.net/iasj/download/b1afc5c91bc88b9e
تاريخ الدخول إلى الموقع : 2022/8/5 على الساعة 1.30.

وفي المجال الجزائي، يقصد بالتصوير الضوئي لمسرح الجريمة استخدام آلات التصوير الفوتوغرافي أو كاميرات الفيديو لتسجيل الآثار والأدلة المرئية وغير المرئية الموجودة بمسرح الجريمة وتقديمها لسلطات القضاء الجزائي في شكل صور لتكون أدلة أو قرائن حسب قوتها في الإثبات[1].

ولما كان المقصود بالصورة الضوئية (الفوتوغرافية) في اللغة اللاتينية هو الكتابة بواسطة التصوير، فإنه من الضرورة بما كان أن تتم الاستعانة بالصورة لدعم وتعزيز معاينة مسرح الجريمة من أجل أن تقدم أمام القضاء الحقيقة الكاملة عن هذا المسرح[2] .

ويعتبر هذا التصوير ضروريا في الحالات التي يقدم لنا فيها نتائج في البحث الجنائي أفضل مما يمكن الحصول عليه بالعين المجردة، وكذلك في كل الحالات التي تتطلب الرجوع مستقبلا إلى الصور. ولذلك أصبح البحث الجنائي الحديث يعتمد اعتمادا كبيرا على التصوير الضوئي لمكان وقوع الحادث الإجرامي، لأن وصف هذا المكان، مهما بلغت دقته، تكون الصورة الضوئية أقوى منه في بيان الحقيقة، وخاصة أنه في بعض الحالات، يكون المحقق مضطرا إلى بذل جهد كبير في شرح المعاينة ، ووصف كل شيء عن مكان الحادث، والحرص الشديد على عدم نسيان أي أثر من الآثار التي وجدت بمسرح الجريمة، وكل هذا يتطلب منه تدوين محاضر من صفحات كثيرة، بينما تستطيع الصورة الضوئية أن تجنبه بذل هذا الجهد بما تعبر عنه من حقائق ، وما تحمله من صدق ووضوح[3].

المطلب الثاني : الضوابط الفنية لتصوير مسرح الجريمة

ينادي المختصون في مجال البحث الجنائي الفني بضرورة مراعاة جملة من الضوابط الفنية عند القيام بالتصوير الضوئي لمسرح الجريمة، وهي تتمثل في مجموعة من الأساليب والكيفيات التي يعتبر اتباعها ضمانا فعالا لإنتاج صور تعكس بدقة ووضوح حقيقة الأشياء والآثار المراد تصويرها، غير أنه تنبغي الإشارة إلى أن عدم الالتزام بها لا يترتب عليه إهدار قيمة وأهمية الصور المنتجة وعدم

---

[1] مباركي جمال الدين لزرق، إجراءات البحث الفني والتقني للشرطة العلمية بمسرح الجريمة، مجلة متون، مجلة علمية محكمة تصدرها كلية العلوم الاجتماعية والإنسانية بجامعة الدكتور مولاي الطاهر– سعيدة ، المجلد الثامن ، العدد الرابع ، جانفي 2017، ص 683.

[2] مديحة فؤاد الخضري و أحمد بسيوني أبو الروس، مرجع سابق، ص 629.

[3] سالم حسين الدميري و عبد الحكم فودة ، الطب الشرعي ، بدون طبعة ، دار المطبوعات الجامعية ، الإسكندرية، 1996 ، ص 971.

الاعتداد بها مطلقا، وإنما يحتمل معه أن يكتنف تلك الصور غموض وتداخل يجعلها غير معبرة عن التسجيل الدقيق والصادق للأشياء والآثار على حالتها الطبيعية، وهو أمر ينبغي تفاديه نظرا لارتباط التصوير الجنائي بأدلة الإثبات وما يترتب عليها من آثار على حقوق الأطراف في المسائل الجزائية. وسوف نبين فيما يأتي أهم تلك الضوابط :

أولا : التقاط صور متعددة حسب أهمية موضوع الصورة، ويكون ذلك من جهات مختلفة وزوايا متعددة[1]. والهدف من ذلك هو اخذ العدد الكافي من الصور، لأن ما يمكن تصويره في فترة معينة قد يستحيل تصويره في فترة أو مرحلة لاحقة، لأن مسرح الجريمة معرض للتغير سواء بفعل الطبيعة أو بفعل الإنسان، كما أن التحفظ على مسرح الجريمة لا يمكن فرضه لمدة زمنية غير محدودة، فمن اللازم بعد إجراء المعاينة إزالة آثار الجريمة حتى لا تبقى عاملا لاستمرار إثارة مشاعر الألم التي أحدثتها الجريمة. إضافة إلى أنه يجب رفع التحفظ على المكان الذي تمت فيه المعاينة والتصوير، وتسليمه لمن له الحق في استعماله، ولا يجوز حرمانه من هذا الحق دون مبرر قضائي[2].

ثانيا : استعمال أكثر من آلة أو وسيلة للتصوير، فإذا فشل أو اخفق العمل الذي تم بإحدى الآلات، يمكن اللجوء إلى نتيجة العمل الذي تم بواسطة الآلات الأخرى، دون حاجة لإعادة التصوير، خاصة وأن مسرح الجريمة يكون قد تعرض للتغيير مع مرور الزمن، فتصبح هذه الإعادة بدون جدوى.

إضافة إلى ذلك فإن بعض الوقائع الإجرامية يكون هدف التصوير فيها متغيرا وغير ثابت، مثل المظاهرات وأعمال الشغب ، وتستحيل إعادة تصويره إذا ظهر أن التصوير الول كان فاشلا ، وقد تم بآلة أو وسيلة واحدة[3].

ثالثا : ينبغي وضع علامات أو إشارات واضحة بجانب الأجسام والآثار المراد تصويرها بمسرح الجريمة، وخاصة إذا كانت غير واضحة بذاتها حسب لونها ودرجة دكانتها[1]. وكذلك إذا كانت بعض

---

[1] عبد الله محمد اليوسف، التصوير ودوره في القضايا الجنائية، مجلة الأمن والحياة ، مجلة إعلامية أمنية ثقافية تصدر بشكل دوري عن جامعة نايف العربية للعلوم الأمنية، العدد (341) ، شوال 1431 هـ ، سبتمبر / أكتوبر 2010 م ، ص 59.

[2] برهامي أبو بكر عزمي، الشرعية الإجرائية للأدلة العلمية – دراسة تحليلية لأعمال الخبرة – ، بدون طبعة، دار النهضة العربية ، القاهرة ، 2006 ، ص 307.

[3] المرجع السابق، الموضع نفسه.

الأشياء ذات الصلة بالجريمة تظهر صغيرة ويصعب تمييزها، فيمكن وضع حوامل عندها، وتكون هذه الحوامل بقاعدة صغيرة ، ويوضع رقم واضح على كل حامل ، بحيث تسهل الإشارة إليه من خلال الوصف التعريفي للصور. وتكون الأرقام الموضوعة على الحوامل مسلسلة بحيث يوضع كل منها عند كل جسم أو أثر يتوقع أن يظهر في الصورة العامة لمسرح الجريمة[2].

رابعا : ينبغي أن تؤخذ الصور من زوايا متعددة أفقية ورأسية، لأن ما تظهره الصورة الملتقطة من زاوية معينة، أفقية أو رأسية، يختلف عما تظهره الصورة الملتقطة من زاوية اخرى[3].

خامسا : إذا كان التصوير يتعلق بمناظر متشابهة، أو يصعب تحديد مواقعها من خلال الصور، ينبغي ترتيب هذه الصور بشكل تسلسلي وذلك بوضع رقم بطرف كل صورة، وكتابة البيانات الجوهرية للمناظر حسب تسلسل الصور في ورقة مستقلة أو خلف الصورة إن كان هناك متسع، أو وضع سهم يشير إلى كل اثر تم التقاطه، وذلك لتسهيل شرح مضمون كل صورة، وبيان الموقع الذي أخذت فيه تفاديا لحدوث خلط بين مضامين الصور، أو تشابه بينها يثير الغموض حول ما يظهر فيها[4].

سادسا : إلى جانب التصوير الضوئي، يمكن استخدام الأشعة غير المنظورة في تصوير ما لا تراه عين الإنسان، فهذه العين تتأثر فقط بموجات ضوئية ذات أطوال في مدى معين، ولا تتأثر بالموجات التي تكون أكثر أو أقل طولا من ذلك المدى كالأشعة فوق البنفسجية وتحت الحمراء[5].

وتستعمل الأشعة فوق البنفسجية في التصوير الجنائي، ولا تعتبر الشمس مصدرا هاما لهذه الأشعة، ولذلك ينبغي استخدام المصادر الصناعية في الحصول عليها، وقد تمكن العلماء من تحقيق ذلك بطرق مختلفة. وتحدث الأشعة فوق البنفسجية توهجا بالأجسام المراد تصويرها، ولكنه توهج لا يظهر واضحا لعين الإنسان في الضوء الطبيعي، ولذلك ينبغي تصوير الأجسام التي تعرض لهذه الأشعة في مكان مظلم ليبدو توهجها واضحا. وهناك حالات كثيرة تتم فيها الاستعانة بهذه الأشعة في

---

[1] عبد الله محمد اليوسف ، مرجع سابق ، ص 59

[2] برهامي أبو بكر عزمي، مرجع سابق، ص 309.

[3] المرجع السابق، الموضع نفسه.

[4] عبد الله محمد اليوسف، مرجع سابق، ص 59.

[5] برهامي أبو بكر عزمي، مرجع سابق، ص 311.

التصوير الجنائي، ومنها تصوير بصمات الأصابع، والمواد المنبعثة من الحريق، وبقع الدم، والوثائق المختلفة، واللوحات الزيتية وغيرها[1].

وفيما يتعلق بالبصمات، كثيرا ما تفشل المساحيق التي تستخدم في إظهارها على الأسطح بغرض تصويرها، وذلك عندما يمضي عليها وقت طويل، فيتم اللجوء إلى استخدام الأشعة فوق البنفسجية لإظهارها، وهي من أهم الوسائل المستخدمة لهذا الغرض[2].

وتؤدي الأشعة البنفسجية دورا هاما في الكشف عن إفرازات جسم الإنسان في القضايا الجزائية التي يكون فيها هذا الجسم محلا للاعتداء، فبعض هذه الإفرازات ، ومن بينها الإفرازات المنوية، لها خاصية التألق الفلوري إذا عند تعريضها للأشعة فوق البنفسجية، وقد تظل آثارها متألقة حتى بعد تعرضها للإزالة حين تعجز عين الإنسان عن رؤيتها، ولذلك ينبغي للباحث الجنائي في هذه المسائل أن يبحث في مسرح الجريمة عن أي آثار تظهر تألقا حين تسلط عليها الأشعة فوق البنفسجية، ثم يحولها إلى المخبر المختص لتحليلها والتحقق من جوهرها[3].

سابعا : تدوين كافة الملاحظات المتعلقة بلقطات التصوير كوقت ومكان التقاطها[4]، فعنصر الزمن مهم جدا في تفسير أي تغيير طبيعي يكون قد مس الآثار المادية التي تم تصويرها بمسرح الجريمة، فالفترة الزمنية التي تنقضي منذ لحظة ارتكاب الجريمة إلى وقت تصوير آثارها المادية، يمكن أن تكون سببا في حدوث ذلك التغيير الطبيعي على مسرح الجريمة.

المبحث الثاني : مزايا التصوير الضوئي لمسرح الجريمة

سبقت الإشارة إلى أن المقصود بالصورة الضوئية في اللغة اللاتينية هو الكتابة بواسطة التصوير، وأنه من الضرورة بما كان أن تتم الاستعانة بالصورة لدعم وتعزيز معاينة مسرح الجريمة من أجل أن تقدم الحقيقة الكاملة عن هذا المسرح أمام القضاء . ولذلك صار التحقيق الجزائي الحديث

---

[1] سالم حسين الدميري و عبد الحكم فودة، مرجع سابق، ص 979.

[2] رمسيس بهنام ، البوليس العلمي أو فن التحقيق ، بدون طبعة، منشأة المعارف، الإسكندرية ، 1996 ، ص 125.

[3] عبد الفتاح رياض، الأدلة الجنائية المادية، بدون طبعة، دار النهضة العربية، القاهرة، 2000 ، ص 478.

[4] قدري عبد الفتاح الشهاوي، فن البحث الجنائي وطبيعته الذاتية ، بدون طبعة، دار النهضة العربية ، القاهرة ، بدون سنة نشر ، ص 80.

يعتمد اعتمادا كبيرا على تصوير مسرح الجريمة بما يحويه من أشياء وآثار مادية لها صلة بالواقعة الإجرامية، ثم إدراج الصور المتحصل عليها ضمن مكونات ملف القضية لتكون مرجعا أساسيا يتم الرجوع إليه كلما دعت الحاجة إلى ذلك في وقت تكون فيه الآثار والمعالم بذلك المسرح قد تغيرت، أو اندثرت واختفت إلى الأبد.

وبالنظر إلى العناصر الأساسية التي يعتمد عليها تسجيل معاينة مسرح الجريمة وهي : الوصف بالكتابة، والتصوير الضوئي، والرسم التخطيطي، نجد أن التصوير الضوئي ينفرد عن بقية العناصر بجملة من المزايا ، بعضها يتعلق بالناحية الفنية لهذا التسجيل، وبعضها الآخر يتعلق بإثبات الجريمة وظروف ارتكابها، أي بالإثبات الجزائي، وبناء على هذا سنتناول ضمن هذا المبحث مزايا التصوير الضوئي من الناحية الفنية (مطلب أول) ، ثم نتناول مزايا التصوير الضوئي في مجال الإثبات الجزائي (مطلب ثان).

المطلب الأول : مزايا التصوير الضوئي من الناحية الفنية

يحقق التصوير الضوئي لمسرح الجريمة جملة من المزايا الفنية في تسجيل معاينة هذا المسرح يعجز الوصف بالكتابة عن تحقيقها، وهي تتمثل فيما يأتي :

أولا : إن الصورة الضوئية تكفي بذاتها لتسجيل ونقل تفاصيل المشهد الذي تسجله مما يغني عن وصف بالكتابة لتلك التفاصيل قد يستغرق صفحات طويلة، وتظهر أهمية ذلك مثلا : في وصف هيئة الأشخاص وملامح وجوههم، وآثار التحطيم والإتلاف الناتج عن حريق أو حادث سير أدى إلى تهشم السيارات المتصادمة على نحو معين، وغير ذلك من المشاهد التي تعجز الكتابة عن وصفها بدقة ونقل تفاصيلها للأذهان على نحو يعطي الانطباع الصادق عنها، ذلك أن الكتابة هي في جوهرها تعبير ينطوي على محاولة لنقل ما هو منطبع ومستقر في الأذهان إلى الغير، تتفاوت فيها قدرات البشر على هذا التعبير. ومهما بلغت هذه القدرات، لا تستطيع الكتابة نقل المشاهد نقلا ومتكاملا ومطابقا للواقع مطابقة تامة[1].

[1] برهامي أبو بكر عزمي، مرجع سابق، ص 303.

ثانيا : إن الصورة الضوئية قادرة على نقل المنظر من واقعه الطبيعي إلى ساحة القضاء، فيكون لها في نفس القاضي ذات الأثر الذي شعر به المحقق الذي عاين مسرح الجريمة عقب وقوعها، وذلك مهما طالت المدة الزمنية الفاصلة بين إجراء المعاينة وعرض الأمر على القضاء، ويمثل ذلك ميزة للصورة الضوئية لا تتوافر في الوصف عن طريق الكتابة مهما كان دقيقا، فهو لا ينقل بشاعة الجريمة وفظاعة آثارها إلى ذهن القاضي كما تنقلها الصورة. يضاف إلى ذلك أن الإحساس بالمظاهر التي يلمسها المحقق حينما يعاين مسرح الجريمة يتلاشى بمضي المدة، وخاصة إذا تم نظر القضية بعد مدة طويلة، أما الصورة الضوئية فتبقى معبرة طيلة وجودها عن الواقع كما جرت معاينته[1].

ثالثا : إن التصوير الضوئي له ميزة خاصة في تسجيل الحوادث التي لا يمكن استيعاب مظهرها بالوصف الدقيق مثل حوادث التصادم والحريق والتظاهر غير القانوني والمشاجرات والسطو والأفعال المخلة بالحياء، وكل الحالات التي تتغير فيها المظاهر بمرور الزمن، مثل الجروح على اختلاف درجاتها، وخاصة عند السعي إلى معرفة الأداة التي استعملت في إحداثها، أو تحديد الاتجاه الذي وقع منه الاعتداء[2].

المطلب الثاني : مزايا التصوير الضوئي في مجال الإثبات الجزائي

يحقق التصوير الضوئي لمسرح الجريمة جملة من المزايا فيما يتعلق بإثبات وقوع الجريمة، وظروف ارتكابها، ونسبتها إلى من ارتكبها، وتتمثل هذه المزايا فيما يأتي :

أولا : أن من يقوم بمعاينة مسرح الجريمة يركز عادة على على الأمور التي يراها ذات أهمية حسب تقديره الشخصي، وفي ظل تعدد الأشياء والآثار فإنه قد يغفل وصف بعضها ، ثم يبدو أن ما لم يذكره يكتسي أهمية في مرحلة لاحقة من مراحل الفصل في الدعوى العمومية متى أثار الخصوم هذه الأهمية، أو أثارها المتهم في دفاعه. وذلك في الوقت الذي قد يكون فيه مسرح الجريمة قد تغير بفعل عوامل الطبيعة أو بفعل الإنسان. ولمواجهة هذه الحالة، يتم اللجوء إلى الصور الضوئية التي تم

---

[1] سالم حسين الدميري و عبد الحكم فودة، مرجع سابق، ص 971.

[2] المرجع السابق، ص 971 – 972.

التقاطها لمسرح الجريمة ، فهي المرجع الوحيد الذي ينقل بصدق معالم هذا المسرح وما وجد به من آثار، سواء أكان الوصف بالكتابة قد تناولها أو لم يتناولها لأي سبب كان[1].

ثانيا : تعد الصور الضوئية لمسرح الجريمة أحسن دليل إثبات للحالة التي وجد عليها هذا المسرح عند معاينته، ولكل الأشياء والآثار التي وجدت به، ومن حق الخصوم أن يحتجوا بما تضمنته هذه الصور لإثبات ادعاءاتهم، وتعزيز وجهات نظرهم في شأن وقائع الدعوى وظروف حدوثها، فهم يلجئون إليها باعتبارها دليلا ماديا يثبت الوقائع التي يؤسسون عليها طلباتهم، أو يعززون بها دفوعهم. ومن ناحية أخرى، يستند المحقق إلى صور مسرح الجريمة أن ما تم تدوينه في المحاضر وصفا لهذا المسرح مطابق للحقيقة، وذلك ليواجه أي طعن أو تجريح في إجراءات المعاينة[2].

ثالثا : يعد التصور الضوئي وسيلة لإثبات قيام حالة التلبس في بعض الجرائم كالتظاهر غير المشروع ، وإشعال الحرائق عمدا ، وتحطيم أملاك الغير، والقيام بأعمال الشغب وغيرها[3]. وميزة التصوير بالنسبة لهذه الجرائم أنه يظهر صور الجناة حال قيامهم بجرائمهم ، ويبين بوضوح تفاصيل أعمالهم التي تشكل الركن المادي للجريمة ، وبذلك يكون من الصعب عليهم إنكار قيامهم بتلك الأعمال عند مواجهتهم بما تظهره الصور[4].

خاتمة

بعد تناولنا لموضوع التصوير الضوئي كوسيلة لتسجيل معاينة مسرح الجريمة تبين لنا أن استخدام هذا التصوير في المجال الجزائي كان نتيجة للتطور التكنولوجي الذي طرأ على الآلات والوسائل المستخدمة في هذا الشأن. وقد أصبح يكتسي أهمية كبيرة في مجال البحث الجنائي، وذلك بفضل المزايا التي يوفرها من الناحية الفنية في تسجيل معاينة مسرح الجريمة على نحو دقيق ومطابق للواقع، والأدلة التي يوفرها في مجال الإثبات الجزائي خدمة لمصالح الخصوم، وصونا لحقوقهم.

---

[1] برهامي أبو بكر عزمي، مرجع سابق، ص 304.

[2] المرجع السابق، الموضع نفسه.

[3] سالم حسين الدميري و عبد الحكم فودة، مرجع سابق، ص 972.

[4] برهامي أبو بكر عزمي، مرجع سابق، ص 305.

قائمة المراجع

أولا : المؤلفات

– برهامي أبو بكر عزمي، الشرعية الإجرائية للأدلة العلمية – دراسة تحليلية لأعمال الخبرة – ، بدون طبعة، دار النهضة العربية ، القاهرة ، 2006.

– رمسيس بهنام ، البوليس العلمي أو فن التحقيق ، بدون طبعة، منشأة المعارف، الإسكندرية ، 1996.

– سالم حسين الدميري و عبد الحكم فودة ، الطب الشرعي ، بدون طبعة ، دار المطبوعات الجامعية، الإسكندرية، 1996.

– عبد الفتاح رياض، الأدلة الجنائية المادية، بدون طبعة، دار النهضة العربية، القاهرة، 2000.

– قدري عبد الفتاح الشهاوي، فن البحث الجنائي وطبيعته الذاتية ، بدون طبعة، دار النهضة العربية ، القاهرة، بدون سنة نشر.

– مديحة فؤاد الخضري و أحمد بسيوني أبو الروس ، الطب الشرعي والبحث الجنائي، بدون طبعة ، دار المطبوعات الجامعية ، الإسكندرية، 1989.

ثانيا : البحوث والمقالات العلمية

– عبد الله محمد اليوسف، التصوير ودوره في القضايا الجنائية، مجلة الأمن والحياة ، مجلة إعلامية أمنية ثقافية تصدر بشكل دوري عن جامعة نايف العربية للعلوم الأمنية، العدد (341) ، شوال 1431 هـ ، سبتمبر / أكتوبر 2010 م .

– عمار عباس الحسيني، التصوير المرئي وحجيته في الإثبات الجنائي، بحث منشور على الشبكة الدولية للمعلومات (الإنترنت) على الموقع الآتي :
https://www.iasj.net/iasj/download/b1afc5c91bc88b9e
تاريخ الدخول إلى الموقع : 2022/8/5 على الساعة 1.30.

– مباركي جمال الدين لزرق، إجراءات البحث الفني والتقني للشرطة العلمية بمسرح الجريمة، مجلة متون، مجلة علمية محكمة تصدرها كلية العلوم الاجتماعية والإنسانية بجامعة الدكتور مولاي الطاهر– سعيدة ، المجلد الثامن ، العدد الرابع ، جانفي 2017.

– نوفل علي عبد الله وخالد عوني خطاب، دور أجهزة التصوير الحديثة في الإثبات الجنائي– دراسة مقارنة – ، مجلة الرافدين للحقوق، المجلد(15) ، العدد (55) ، السنة (17).

ملخص مداخلة للمشاركة في

المؤتمر الدولي الإفتراضي الموسوم بـ " القانون الجنائي في ظل التطور التكنولوجي

" اشكالات ومعالجات "

عنوان المداخة

" **استخدامتقنية المحادثة المرئية عن بعد في سماع الشهود في مرحلتي التحقيق القضائي والمحاكمة** "

جامعة الجزائر 1 يوسف بن خدة

كلية الحقوق

يومي 28 و29 سبتمبر 2022

1) الاسم واللقب : **تومي يحـي**

الرتبة العلمية : **أستاذ محاضر قسم(ا)**

القسم : قانون عام : التخصص : قانون جنائي وعلوم جنائية

مؤسسة العمل : كلية الحقوق والعلوم السياسية . جامعة يحي فارس . المدية

المحور الرابع : استخدام التقنيات الحديثة في مجال العدالة الجنائية

البريد الالكتروني : yahiatoumi943@gmail.com

2) الإسم واللقب : **مهاد قانة**

الرتبة العلمية : طالبة دكتوراه

القسم : قانون عام : التخصص : قانون جنائي وعلوم جنائية

المؤسسة الأصلية : كلية الحقوق والعلوم السياسية . جامعة يحي فارس . المدية

المحور الرابع : استخدام التقنيات الحديثة في مجال العدالة الجنائية

البريد الالكترونيMihad GN t.mi12@hotmail.com

مقدمة

لا شكأن العالميعيش ثورة معلوماتية هائلة من المفترض أن ينعكس ذلك على مرفق القضاء ككل ، ومدى اسهام تطورات عصر التكنولوجيا في تحقيق سرعة الفصل في الدعاوى ،ورغم مظاهر تأثيرثورة تكنولوجيا المعلومات والإتصالات الحديثة على كافة مناحي الحياة بما فيها المنظومة القضائية، فقد تولد عن ثورة المعلوماتية كثير من التطبيقات التي أثرت تأثيرا بالغا في شتى نواحي الحياة الإجتماعية والإقتصادية والعلمية ، والتي كان من بينها الحكومة الالكترونية ، والتعليم الالكتروني ، والتجارة الالكترونية ،وعلى غرار التشريعات المقارنة نص المشرع الجزائري على جواز استخدام وسائل الإتصال المسموعة والمرئية عن بعد في الإجراءات الجزائية في مرحلتى التحقيق القضائي ومرحلة المحاكمة ، وتبيين الشروط والضوابط الواجب مراعاتها عند استخدام هذه الوسائل الذي يؤدي إلى الوصول إلى الحقيقة وتطبيق مبدا سيادة القانون دون المساس بحقوق الدفاع .

فدخول تكنولوجيا المعلومات والإتصالات مجال العدالة الجنائية أتاح إمكان سماع شهادة الشهود عن طريق تقنية المحادثة المرئية عن بعد Vidéoconférence، الأمر الذي جعل المشرع الجزائري يسارع إلى اصدار القانون بموجب القانون رقم 15-03 المؤرخ في 01 فيفري 2015 المتعلق بعصرنة العدالة، وأخيرا القانون رقم 20-04 المؤرخ في 30 غشت 2020 المعدل لقانون الاجراءات الجزائية، حيث يتم استعمالها أثناء الإجراءات في مرحلتي التحقيق القضائي والمحاكمة الجزائية عموما وفي سماع الشهود خصوصا، و يعد هذا امتدادا لمصادقة الجزائر بتحفظ من خلال المرسوم الرئاسي 02-55 الصادر سنة 2002 على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية التي نصت في فحوى موادها على امكانية استعمال هذه التقنية في مجال مكافحة الجريمة دعما للتعاون الدولي .

و بما أن الطرق التقليدية أصبحت لا تواكب تقدم العصر ،أصبح من الضروري عصرنة مرفق العدالة بما يتماشى وتطور تكنولوجيا المعلومات والإتصلات ، مما يعكس ارادة المشرع نحو الإستفادة من تكنولوجيا الاتصالات الحديثة في العدالة الجنائية نظرا لمحاسنها المتعددة كأداة لترشيد الإجراءات الجنائية والسرعة في تنفيذها ومن ثم مواكبة مستجدات العصر الرقمي بإدخال تقنية المحادثة المرئية عن بعد في الإجراءات القضائية في مرحلتي التحقيق القضائي والمحاكمة، ومنها سماع الشهود عن بعد، فهي وسيلة جديدة تدخل المنظومة القضائية الجزائرية تسمح باستجواب وسماع الأطراف عن بعد والمتعاونين مع العدالة الجزائية من شهود وخبراء ، ويتم اللجوء لسماع الشهود عن بعد وفق ما نصت عليه أحكام القانون السالف الذكر. كما يجب أن تضمن الوسيلة المستخدمة في المحادثة سرية الإرسال وأمانته. علما أن المحادثات المرئية يمكن استعمالها أيضا للاستماع للشهود في الجنايات لأنهم مجرد شهود وليسوا متهمين لربح الوقت إذا استدعى أمر تنقلهم مدة طويلة لتفادي تأجيل المحاكمة. والتي مازالت تواجه معارضة شديدة بسبب ما قد يترتب عنها من إخلال بحقوق الدفاع ومبدأ المواجهة، واستعمال تقنية

المحادثة عن بعد بالنسبة للشهود سواء كانوا موقوفين في مؤسسات عقابية أو غير موقوفين ، ومنه يمكن أن أن نطرح الإشكالية التالية : **ما مدى فعالية تقنية المحادثة المرئية عن بعد في سماع الشهود وانعكساتها على السير الحسن للعدالة الجنائية وتأثيرها على المبادئ الأساسية للدعوى الجزائية بخصوص حقوق الدفاع ومبدأ المواجهة بين الخصوم ؟ وهل الحضور الالكتروني للشخص الشاهد يغني عن الحضور الجسدي فعلا ؟**

ولمعالجة هذه الاشكالية إرتأينا تقسيم هذه الدراسة إلى محورين هما :

المحور الأول : مفهوم سماع الشهود عبر تقنية المحادثة المرئية عن بعد أمام المحاكم الجزائية

المحور الثاني : إجراء سماع الشهود عبر تقنية المحادثة المرئية عن بعد ومبادئ حقوق الدفاع

المحور الأول : مفهوم سماع الشهود عبر تقنية " المحادثة المرئية عن بعد" أمام المحاكم الجزائية

يعتبر سماع الشهود بواسطة تقنية المحادثة المرئية عن بعد انطلاقة نوعية في مجال العدالة الجنائية لما له من أهمية في تبسيط وسرعة الإجراءات القضائية ، حيث أدى تطور تكنولوجيا المعلومات والإتصالات الحديثة إلى خدمة العدالة الجزائية إلى ظهور ما يسمى بالجلسات الإلكترونية ، فبصدور القانون رقم 15-03 والمتعلق بعصرنة العدالة ، لا شك يعد خطوة ايجابية للجزائرفي إدخال الرقمنة إلى جهاز العدالة مقارنة بالدول العربية الأخرى التي لا تزال رهينة للوسائل التقليدية في عملية التقاضي،ونعتقد أن لجائحة فيروس كورونا المستجد آثارا عميقة على الصعيدين الدولي والوطني، حيث غيرت هذه الجائحة العديد من الأنماط السلوكية والعادات التي درج عليها الناس، ومن أهم هذه المجالات نجد المجال القضائي، الذي أصبح عاجزا عن أداء وظيفته التي كان عليها من قبل، الأمر الذي جعل وزارة العدل الجزائرية تبحث عن حل لإعادة الروح للجهاز القضائي، وذلك عن طريق استغلال القانون رقم 03/15 [1]، ومؤخرا إصدارالقانون رقم 04/20 ، بحيث كان اللجوء لوسائل الاتصال الحديثة هو الحل الوحيد الذي يمكن أن يعيد الروح من جديد للمؤسسة القضائية، وذلك في إطار الإجراءات الاحترازية التي تقوم بها الجزائر لمحاربة تفشي فيروس كورونا المستجد ، حيث تم اعتماد هذه الأخيرة في العديد من محاكم الجمهورية الجزائرية ، وقصد تكريس العملية وإعطائها المزيد من المشروعية القانونية، تم صدور

[1] القانون رقم 15-03 المؤرخ في أول فبراير 2015 ، يتعلق بعصرنة العدالة ، الجريدة الرسمية الجزائرية ، عدد 06 الصادر بتاريخ 10 فبراير سنة 2015 .

قانون رقم04/20 والمتضمن استعمال وسائل الاتصال المسموعة والمرئية في الإجراءات القضائية.وعليه سوف نتعرض أولا بالتعريف بتقنية المحادثة المرئية عن بعد ، ثم ثانيا شروط استعمالها .

أولا : التعريف بتقنية المحادثة المرئية عن بعد (الاتصال المرئي المسموع)

1- إن مصطلح video conférence يرجع أصله إلى اللغة الفرنسية ، حيث يتكون من كلمتين، الكلمة الأولى vidéo يقصد بها في اللغة العربية (الرائي) أو تلفزيوني وهي تطلق على جهاز نقل الصور والأصوات عن طريق الأمواج الكهربائية [2].أما بالنسبة لكلمة conférence المقصود بها اجتماع عدد من الأفراد لإجراء مناقشة أو حوار حول موضوع معين ، هذا وتستخدم للتعبير عن المؤتمر [3] .

2- أما من الناحية الفنية للمصطلح فهو وسيلة من وسائل الاتصال المرئي المسموع لاجتماع شخصين أو عدد من الأشخاص في أماكن مختلفة سواء داخل الدولة أو بين عدة دول ، بحيث تمكنهم هذه التقنية من المشاركة في النقاش والحوار بصورة فعالة ، الأمر الذي يجعل جميع الأطراف المتحاورين من رؤية الآخرين وسماعهم والحديث معهم في نفس الوقت ، وبالتالي يمكن في إطار الاجراءات الجزائية سماع اقوال الشهود والخبراء وفي بعض الأحيان المتهم عبر هذه التقنية [4] ونظرا لأهمية هذه التقنية فهي تستعمل كذلك في مجالات عديدة كالصحة والتعليم والقضاء وفي المؤتمرات العلمية .الخ .

ووفق تقنية المحادثة المرئية عن بعد ، الشاهد لا يكون فيها حاضرا جلسة التحقيق أو المحاكمة بذاته المادية ، وإنما يكون حضوره من خلال الاتصال المباشر بين قاعة الجلسة بالمحكمة ومكان اجراء المحادثة المرئية عن بعد الذي يفترض أنه يبعد عنها بمئات الأميال ، ويتم ذلك من مقر المحكمة الأقرب إلى إقامة الشخص المطلوب تلقي تصريحاته بحضور وكيل الجمهورية المختص إقليميا وأمين الضبط .

كما يجوز أن تتم المحادثة المرئية عن بعد من المؤسسة العقابية التي يوجد بها المحبوس [5] بحيث يتم الحصول على أقواله بشكل سمعي مرئي عن بعد وفق طرق الاتصال المرئي المسموع المعمول بها لدى كثير من الدول التي كانت سباقة إلى استعمال هذه التقنية كالولايات المتحدة الأمريكية وإيطاليا وبلجيكا وفرنسا [6].

---

[2] قاموس المعجم الوجيز ، طبعة خاصة بوزارة التربية والتعليم (المصرية) ، 1990 ، ص 76.

[3] د، سهيل إدريس ، المنهل قاموس فرنسي عربي، دار الأدب للنشر والتوزيع ، بيروت ، لبنان 2005 ، ص 1267 .

4د ، عادل يحي ، التحقيق والمحاكمة الجنائية عن بعد ، دراسة تحليلية تأصيلية لتقنية ال Video Conference ، دار النهضة العربية . 2006 ، ص 25 .

5 تنص المادة 16 /ف3من القانون 15-03 على أنه " إذا كان المسموع محبوسا تتم المحادثة المرئية عن بعد من المؤسسة العقابية التي يوجد فيها المحبوس وفقا للكيفيات المحددة في الفقرة السابق مع مراعاة الأحكام المنصوص عليها في المادة 14 منهذا القانون ."

[6] أنظر المادة 706 مكرر 71 من قانون الاجراءات الفرنسي المعدلة بموجب القانون رقم 1436 لسنة 2009 الصادر في 24 نوفمبر 2009 .

3-انعكاسات التقدم التكنولوجي على سير العدالة بوجه عام ، والعدالة الجنائية بصفة خاصة من خلال تأثير استخدام التقنيات الحديثة على اجراءات الدعوى الجزائية ، كتقنية المحادثة المرئية عن بعد (الاتصال المرئي المسموع) vidéo conférence في مجال التحقيق والمحاكمة الجزائية [7]، والتشريع الجزائري كالتشريعات العربية لم يكن يعرف قبل صدور قانون رقم 15-03 المؤرخ في أول فبراير سنة 2015 المتعلق بعصرنة العدالة إمكانية نقل الأقوال الشفهية الصادرة من المتهم أو الشهود أو الخبراء أو غيرهم إلى قاعة الجلسة بوسيلة أخرى غير حضورهم الجسدي لمكتب قاضي التحقيق أو قاعة الجلسة للمحكمة وإدلائهم بأقوالهم شفهيا في حضرة المحكمة ، و أمام الخصوم والسماح بمناقشة أقوالهم من طرف الخصوم الحاضرين فعليا، غير أن دخول التكنولوجيا مجال العدالة أتاح إمكانية سماع شهادة الشهود عن طريق استخدام تكنولوجيات الاتصال والإعلام أي " المحادثة المرئية عن بعد " [8] ، وهذا ما أجازه المشرع الجزائري قي الفصل الرابع من القانون المذكور سالفا في المواد 14 . 15 .16 منه، حيث نص على استعمال تلك التقنية الحديثة(المحادثة المرئية عن بعد) حيث تنص المادة15 منه على " يمكن قاضي التحقيق أن يستعمل المحادثة المرئية عن بعد في استجواب أو سماع شخص وفي اجراء مواجهات بين عدة أشخاص. يمكن جهة الحكم أيضا أن تستعمل المحادثة المرئية عن بعد لسماع الشهود والأطراف المدنية والخبراء . ويمكن جهة الحكم التي تنظر في قضايا الجنح أن تلجأ إلى نفس الألية لتلقى تصريحات منهم محبوس إذا وافق المعني والنيابة العامة على ذلك " كما أصدر قانون رقم 20-04 المعدل والمتمم لقانون الإجراءات الجزائية واضافة الكتاب الثاني مكرر تحت عنوان " استعمال وسائل الاتصال المسموعة والمرئية أثناء الإجراءات" وبهذا يكون المشرع قد ساير التشريعات المقارنة في توظيف هذه التقنيات الحديثة في مجال العدالة الجزائية ، وذلك بتطبيق نظام الاتصال المرئي المسموع في مجال الاجراءات القضائية سواء على مستوى قاضي التحقيق في استجواب أو سماع الشهود كما يمكن لجهة

---

[7]- استعملت تقنية vidéoconférence لأول مرة بايطاليا في مجال التحقيق بموجب القانون رقم 306 لسنة 1992 المعدل بالقانون رقم 356 لسنة 1992 ، ومن ثم اتسع نطاق استخدام هذه التقنية ليشمل اجراءات محاكمة المجرمين الخطرين بموجب القانون الصادر في 7 جانفي 1998 . حيث أتاحت لهم هذه التقنية مباشرة اجراءات التحقيق والمحاكمة عن بعد وبصفة خاصة سماع الشهود والمتعاونين مع العدالة وغيرهم . أنظر

dixième Congrès des Nations Unies Sur la prévention du Crime et le traitement des délinquants Vienne ,10-17avril2000,le Procès à distance au moyen de la vidéoconférence.l'expérienceItalienne,p,1,http://www.uncjin.org/Documents/10thcongress/10cStatements/italy.pdf

[8]حاتم محمد فتحي أحمد البكري ، مبدأ الشفهية والتقنيات الحديثة في المحاكمات الجنائية ، مجلة البحوث القانونية والاقتصادية ، عدد 49 ، أبريل 2011 ، ص 5.

الحكم استخدام تقنية المحادثة المرئية عن بعد لسماع الشهود. فما المقصود بالمحادثة المرئية عن بعد أو ما يسمى video conference ؟

ثانيا : شروط استعمال " تقنية المحادثة عن بعد "

لقد أجاز المشرع الجزائرياستعمال تقنية المحادثة المرئية عن بعد (الاتصال المرئي المسموع) لسماع الشهود لمقتضيات نصت عليها المادة 441 مكرر من القانون رقم 20-04 [9]منها حسن سير العدالة أو الحفاظ على الأمن أو الصحة العمومية أو أثناء الكوارث الطبيعية أو لدواعي مبدأ الأجال المعقولة أو بعد المسافة المنصوص عليها في المادة 14 من القانون رقم03/15 ، وذلك بناء على شروط معينة مع مراعاة الحقوق والقواعد المنصوص عليها في قانون الاجراءات الجزائية وهذه الشروط بناءا على ما ورد في المادة 441 مكرر هي على الشكل الأتي :

1- يجب أن تضمن الوسائل المستعملة سرية الإتصال وأمانته وكذلك التقاط وعرض كامل وواضح لمجريات الإجراء المتخذ وفق هذه التقنية . .

2-تسجيل التصريحات على دعامة تضمن سلامتها وترفق بملف الاجراءات .

3- يحرر أمينالضبط محضرا عن سير عملية استعمال المحادثة المرئية عن بعد ويوقعه ثم يرسله بمعرفة وكيل الجمهورية إلى الجهة القضائية المختصة لإلحاقة بملف الإجراءات .

ثالثا:اجراءات استخدام تقنية المحادثة المرئية عن بعد

أجار القانون رقم 20-04 المؤرخ في 30أوت 2020 المعدل لقانون الاجراءات الجزائية لجهات التحقيق استعمال المحادثة المرئية عن بعد أثناء القيام باجراء سماع شخص أو استجوابه ، كما يمكن أيضا للمحكمة استخدام تقنية المحادثة المرئية عن بعد لسماع الشهود والخبراء والأطراف المدنية وتتم ألية المحادثة المرئية عن بعد على النحو التالي :

أ- يتم سماع الشاهد غير المحبوس باستعمال تقنية المحادثة المرئية عن بعد بمقر المحكمة الأقرب من مكان إقامة الشخص المطلوب تلقي تصريحاته[10] أو من خلال المؤسسة العقابية التي يوجد فيها إذا كان الشخص محبوسا،بحيث يمكن جهة التحقيق بعد إخطار مدير المؤسسة العقابيةسماع الشاهد عن طريق استعمال المحادثة المرئية عن بعد بحضور أمين ضبط المؤسسة العقابية ويحرر محضرا عن

[9] ألامر رقم 20-04 المؤرخ في 30 غشت 2020 المعدل لقانون الإجراءات الجزائية ، الجريدة الجزائرية الرسمية . عدد 51 الصادر في 13 غشت 2020.

[10] أنظر المادة 441 مكرر من القانون رقم 04/20 المعدل لقانونالاجراءات الجزائية

سيرعملية استعمال هذه التقنية [11]ويقتضي نظام المحادثة المرئية عن بعد تجهيز الأماكن التي يتحدث فيها الأطراف عن بعد بكاميرات فيديو لنقل الصورة وكذلك قاعة المحكمة بشاشات عرض للصورة بالإضافة إلى الأجهزة الأخرى التي بواسطتها يتم رؤية وسماع صوت من يتكلم مع المشتركين في الجلسة بصورة متزامنة وواضحة في حال ضمان جودة الاتصال[12].

ب- حضور وكيل الجمهورية المختص إقليميا وأمين الضبط أثناء القيام بالعملية ، بحيث يجب أن يتحقق وكيل الجمهورية من هوية الشخص الذي يراد سماع شهادته وهذا ما نصت عليه المادة 441 مكرر1 الفقرة الأولى. أما إذا كان الشخص المراد سماع شهادتهمحبوسافإن عملية سماعه تتم عن طريق استعمال المحادثة المرئية عن بعد بحضور أمين ضبط المؤسسة العقابية وفق ما نصت عليه المادة 441 مكرر4 ق إ ج.

ج- تحرير محضر من طرف أمين الضبط عنسير عملية استعمال الحادثة المرئية عن بعد ويوقعه ويرسله بمعرفة وكيل الجمهورية إلى الجهة القضائية المختصة لاإلحاقه بلمف الاجراءات .ويحررأمين ضبط المؤسسة العقابية محضرا عن عملية سير استعمال هذه التقنية ويوقعه ثم يرسله بمعرفة رئيس المؤسسة العقابية إلى الجهة القضائية المختصة إذا كان الشاهد محبوسا ورأت جهة الحكم سماع شهادته .

ونتيجة لما سبق ، فإن اللجوء إلى الاستعانة بهذه التقنية لسماع أقوال الشهود أو الخبراء حال توفر بعد المسافة أو حسن سير العدالة أوالحفاظ على الأمن أو الصحة العمومية أو أثناء الكوارث الطبيعية ..ألخ حسب ما نصت عليه المادة 441 مكرر ق ا ج .

ويلزم لاستخدام تلك التقنية إعداد قاعة المحكمة وتجهيزها ، حيث يفترض بديهيا لاستخدام تلك التقنية قي سماع أقوال الشهود عن بعد توافر شبكة اتصال مرئي ومسموع جيدة وفعالة في قاعة الجلسة التي تتم فيها اجراءات المحاكمة أو التحقيق ، والمكان أو الأماكن التي يوجد بها الشهود بحيث يظهرون أثناء تواجدهم في تلك الأماكن وتتم محادثتهم في الجلسة أمام أطراف الدعوى. فالمحاكمة الجنائية يجب أن تبنى على التحقيق الشفوي لذي تقوم به المحكمة بالجلسة وتسمع فيه الشهود مادام ذلك ممكنا ، وعليه ظهر ما يسمى بالحضور الالكتروني عن طريق تقنية المحادثة المرئية عن بعد[13]. غير أنه بعد ظهور

---

[11] أنظر المادة 441 مكرر4 مرجع سابق .

[12]حاتم محمد فتحي أحمد البكري ، المرجع السابق ، ص 25 ، ولمزيد من التفصيل راجع د ، رامي متولي عبد الوهاب ابراهيم ، حماية الشهود في القانون الجنائي ، مجلة الفكر الشرطي ، م 24 ، ع 95 ، الامارات العربية المتحدة ، اكتوبر 2015 ، ص 109.

[13]حاتم محمد فتحي أحمد البكري ، المرجع السابق ، ص 15.أنظر أيضا، د ، عادل يحي ، المرجع السابق، ص 36.

هذه تقنيات الاتصال الحديثة عن بعد [14] أثير جدل حول مدى امكانية قبول الشهادة الفورية عبرها وهو الأمر المقبول فقها لاسيما وأن الشاهد يظهر في هيئته الكاملة ، فيظهر و كأنه حاضرا حيث تتجلى مظاهر حضوره في ردة فعله الطبيعية حين تلقيه لأسئلة الدفاع أو الاتهام أو القاضي أثناء سير الجلسة [15].

المحور الثاني : إجراءسماع الشهود عبر تقنية المحادثة المرئية عن بعد ومبادئ حقوق الدفاع

المحادثة المرئية عن بعد هي وسيلة مستحدثة يتم استخدامها أثناء الإجراءات القضائية منها إجراء سماع الشهود ، لما لها من ايجابيات في حماية الشهود وتدعيم وسائل المساعدة القضائية المتبادلة بين الدول للحد من مخاطر الإجرام المنظم ، إلا أن استعمال هذه التقنية لقي جدلا في الفقه الجنائي بشأن المساس بمبدئ حقوق الدفاع هذا من جهة ومن جهة أخرى هناك من رحب باستخدام هذه التقنية في اطار عصرنة قطاع العدالة وهو ما سوف نتعرض له من خلال مطلبين :

أولا : الفريق القائل باخلال سماع الشهود عن بعد أمام المحاكم الجزائية بمبادئ حقوق الدفاع

يرى أصحاب هذا الفريق أن سماع الشهود عن طريق تقنية الاتصال المرئي والمسموع عن بعد من شانه إحداث تغيرات في القواعد الإجرائية الجزائية لمساسها بشكل اساسي لحقوق الدفاع ومبدأ المواجهة .

لم يعرف المشرع الجزائري المواجهة في قانون الاجراءات الجزائية ، حيث ترك ذلك للفقه مما وردت في هذا الشان العديد من التعريفات إلا أنها لا تخرج عن كون المواجهة إجراء مستقل من اجراءات التحقيق بواسطته يجمع قاضي التحقيق بمكتبه أو أي مكان أخر ، بين متهم ومدعي مدني وشاهد أو بين متهمين أو أكثر أو مدعيين مدنيين وشهود ، وذلك حسب ما يظهر له من تعارض وتناقض اقوال متعلقة بالوقائع التي تخص القضية التي بين يديه ، فقاضي التحقيق يستهدف جراء المواجهة استخلاص من مجموع الاقوال التي تصدر عن المواجهة بينهم تلك التي ترسم مسار الحقيقة [16].

---

[14] تتمثل هذه التقنيات في الدوائر الاتصالية الالكترونية سواء كانت مفتوحة أو مغلقة ، أو المحادثة المرئية عن بعد أو ما يسمى بالاتصال السمعي البصري vidéo conférence .

[15] خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، المرجع السابق ، ص 262.

[16] عمارة فوزي ، قاضي التحقيق ، أطروحة دكتوراه ، جامعة الإخوة منتوري قسنطينة ، 2009-2010 . ص 116 .

ومعلوم أن مبدأ المواجهة يتيح الفرصة للمواجهة المباشرة (وجها لوجه) بين القاضي والخصوم من جهة والمواجهة بين أطراف الدعوى الجزائية من جهة أخرى ،الأمر الذي يقتضي ضرورة الحضور الجسدي للمتهمين والشهود وكافة أطراف الدعوى الجزائية في جلسة التحقيق أو المحاكمة ، بحيث يتيح ذلك للقضاء سواء في مرحلة التحقيق القضائي أو المحاكمة أن تلمس الحقيقة عن قرب من خلال ما يدلي به الشهود من أقوال وما يصدر عنهم من أفعال وردود أفعال نفسية وعصبية أثناء المواجهة، وهذا لا يتم إدراكه إذا ما جرت العملية عن بعد بواسطة تقنية المحادثة عن بعد [17].

كما أن سماع الشهود عن بعد عن طريق تقنية المحادثة المرئية يسمح لهم بالكذب أو يجعل تحديد كذبهم أمرا صعبا ، إذ قد يجد الشهود أكثر سهولة في قاعات التسجيل عنه في قاعات المحكمة [18]، ويرى الكتور أحمد يوسف السولية أن الشهادة عن طريق التسجيل المرئي والمسموع يحرم القاضي من ملاحظة التغيرات والانفعالات التي تصدر عن الشاهد وطريقة أداؤه للشهادة والتي قد تكون من شأنها عوامل مهمة بالنسبة للقاضي في تقييم شهادته .

وفي الأخير يخلص أصحاب هذا الفريق أنه أمام عجز سماع الشهود طريق المحادثة المرئية عن بعد عن تحقيق الغايات التي يسعى إليها المشرع من كفالة مبدا المواجهة بين الأطراف ومساسه بحقوق الدفاع علاوة على الصعوبات الفنية التي يطرحها استعمال هذه التقنية تصبح المواجهة الشخصية وجها لوجه بالحضور الجسدي لا الإلكتروني بين الخصوم خيار لا بديل عنه عند مباشرة الإجراءات القضائية في مرحلة التحقيق والمحاكمة [19]

ثانيا : الفريق القائل بقبول سماع الشهودعن طريق المحادثة المرئية عن بعد

يعتمد أنصار هذا الفريق استعمالهم لتقنية المحادثة المرئية عن بعد في سماع الشهود يرجع إلى ضرورة تطوير أداء مرفق العدالة الجنائية وعصرنته مع تكنولوجيات المعلومات والإتصالات الحديثة الأمر الذي ضرورة جعل القواعد الإجرائية في التحقيق والمحاكمة مرنة تتماشى والتطور الحاصل في مرفق العدالة الجنائية ، مما يسمح حسبهم بسماع الشهود عن طريق تقنية المحادثة المرئية عن بعد لما تفضي إليه من نتائج إيجابية يتمثل اهمها ، في تبسيط الإجراءات الجزائية وسرعتها ،وتمكين الشهود من

---

[17] خالد موسى توني ، الحماية الجنائية الإجرائة للشهود دراسة مقارنة ، ط1 ، 2010

د . أحمد يوسف محمد السولية، الحماية الجنائية والأمنية للشاهد ، دراسة مقارنة ،دار الفكر الجامعي ، ط 1 ، الاسكندرية 2007 [18].ص 250 .

[19] خالد موسى توني ، المرجع السابق ، 137 .

المشاركة الإيجابية في الدعوى الجزائية بما توفره المحادثة المرئية عن بعد لهم في أمان ، إضافة إلى ذلك فإنها تكفل مبدا المواجهة بين أطراف الخصوم في الدعوى الجزائية بالقدر الذي يسمح بحماية الشهود دون إهدار حق كافة الأطراف في الدعوى في مواجهتهم ومناقشتهم [20]

ويرى جانب من الفقه أن سماع شهود عن طريق المحادثة المرئية عن بعد في نطاق الدعوى الجزائية لا يخلو من فائدة حيث أن اعتبارات تمكين مرفق العدالة الجنائية من تفعيل دوره في ملاحقة المجرمين وتطبيق أحكام القانون تقتضي الخروج عن المفهوم التقليدى لسبل مباشرة الإجراء الجزائي وهو ما نؤيده إذ لا بد من تبني سبل اكثر حداثة وتطورا لمباشرة هذه الإجراءات بحيث يمكن الاستفادة من التقدم العلمي والتقني في مجال الاتصالات ، كما أن استخدام هذه التقنية لا يتعارض بشكل صريح مع المبادئ الحاكمة للدعوى الجزائية لاسيما كفالة حقوق الدفاع ومبدا المواجهة [21]

وفي هذا الإطار قد تم إجراء المحاكمة "علنية" بحضور هيئة الدفاع و مفتوحة للمواطنين بإحدى قاعات الجلسات فيما بما خصصت قاعة مجهزة بالوسائل السمعية البصرية بالمؤسسة العقابية بالقليعة وتعمل بالألياف البصرية وفق نظام الشبكة الداخلية لوزارة العدل.

و رُبطت قاعة جلسات الأحداث بمحكمة القليعة بتجهيزات تكنولوجية حديثة خاصة بنظام النقل المباشر للصورة و الصوت و جميع زوايا قاعة أخرى متواجدة بمقر المؤسسة العقابية بالقليعة ،و التي إمتثل فيها ثلاثة متهمين في ثلاث جنح، خضعوا لمحاكمة علنية عادية ، دون الحاجة إلى نقلهم خارج أسوار السجن

وقد تم إجراء المحاكمة "علنية" بحضور هيئة الدفاع و مفتوحة للمواطنين بإحدى قاعات الجلسات فيما خصصت قاعة مجهزة بالوسائل السمعية البصرية بالمؤسسة العقابية بالقليعة وتعمل بالألياف البصرية وفق نظام الشبكة الداخلية لوزارة العدل.

خاتمة

تبين لنا من خلال هذه الدراسة اتجاه المشرع نحو اصلاح مرفق العدالة وتحسين أداءه عن طريق إصدار قوانين تتيح للمؤسسة القضائية استخدام تكنولوجيات الاعلام والاتصال الحديثة من خلال القانون

[20] محي الدين حسيبة ، سماع الشهود عن طريق المحادثة عن بعد بين الحق في الحماية وحقوق الدفاع ، مجلة الدراسات والبحوث القانونية والسياسية ، عدد10 ، سنة 2018، ص 292 .

[21] أحمد يوسف محمد السولية ، المرجع السابق ، ص 251.

رقم 03/15 المتعلق بعصرنة العدالة ، والقانون رقم 20-04 لاسيما في الإجراءات القضائية لدواعي أمنية وصحية وظروف طبيعية وحسن سير العدالة باستخدام تقنية المحادثة المرئية عن بعد في الإجراءات القضائية من بينها سماع الاشخاص والشهود عن بعد، و بعرضنا لحالتي اللجوء لآلية المحاكمة عن بعد يمكن أن نستشف أن الغاية من إستعمالها هو بمثابة إعلان صحوة من المشرع الجزائريللإتحاق بركب التشاريع التي كرست تلك الآلية نظرا لكونها أصبحت ضرورة ملحة وليست خيارا إستراتيجيا الغاية منه تطوير مرفق العدالة وتمكين كل المتداخلين في المشهد القضائي من مسايرة الدعاوى وفصلها دون ضرورة لتواجدهم المادي الجسدي بقصور العدالة، وهو ما من شأنه أن يساهم في تخفيف العبء على المحاكم وسرعة الفصل في النزاعات والقضايا وتقريب القضاء من المواطن.

أما الغاية الأخرى من إستعمال آلية المحادثة المرئية عن بعد في لا سيما في إجراء سماع الشهود فإن ذلك يأتي في إطار حمائي يتناسق ولو نسبيا مع الظرف الحالي الذي تمر به البلاد في ظل إنتشار فيروس كورونا،وكان اللجوء لوسائل الاتصال المسموعة والمرئية هو الحل الوحيد الذي يمكن أن يعيد الروح من جديد للمؤسسة القضائية، وذلك في إطار الإجراءات الاحترازية التي تقوم بها الجزائر لمحاربة تفشي فيروس كورونا المستجد حيث تم اعتماد هذه الأخيرة في العديد من محاكم الجمهورية الجزائرية.

وأخيرا يمكننا القول أن استخدام تقنية المحادثة المرئية في سماع الشهود عن بعد سواء كان ذلك على مستوى التحقيق القضائي أو المحاكمة لا يمس بمبدأ المواجهة مادام أنه يمكن للمتهم أن يناقش تلك الشهادة وما دام يمكن للقاضي أن يتابع ردود الأفعال أثناء المناقشات التي تتم من خلاتل مواجهة الخصوم ولو عن بعد ، بحيث يمكن للقاضي ان يكون قناعته من خلال طرح أمامه أدلة في الجلسة وهو الغرض من إقرار مبدأ المواجهة .

الهوامش

1-القانون رقم 15-03 المؤرخ في أول فبراير 2015 ، يتعلق بعصرنة العدالة ، الجريدة الرسمية الجزائرية ، عدد 06 الصادر بتاريخ 10 فبراير سنة 2015 .

2-قاموس المعجم الوجيز ، طبعة خاصة بوزارة التربية والتعليم (المصرية) ، 1990 ، ص 76.

3-د، سهيل إدريس ، المنهل قاموس فرنسي عربي، دار الأدب للنشر والتوزيع ، بيروت ، لبنان 2005 ، ص 1267 .

4- د ، عادل يحي ، التحقيق والمحاكمة الجنائية عن بعد ، دراسة تحليلية تأصيلية لتقنية ال Video Conference ، دار النهضة العربية . 2006 ، ص 25 .

5- تنص المادة 16 /ف3من القانون 15-03 على أنه " إذا كان المسموع محبوسا تتم المحادثة المرئية عن بعد من المؤسسة العقابية التي يوجد فيها المحبوس وفقا للكيفيات المحددة في الفقرة السابق مع مراعاة الأحكام المنصوص عليها في المادة 14 منهذا القانون ."

6- أنظر المادة 706 مكرر71 من قانون الاجراءات الفرنسي المعدلة بموجب القانون رقم 1436 لسنة 2009 الصادر في 24 نوفمبر 2009 .

7–استعملت تقنية vidéoconférence لأول مرة بايطاليا في مجال التحقيق بموجب القانون رقم 306 لسنة 1992 المعدل بالقانون رقم 356 لسنة 1992 ، ومن ثم اتسع نطاق استخدام هذه التقنية ليشمل اجراءات محاكمة المجرمين الخطرين بموجب القانون الصادر في 7 جانفي 1998 . حيث أتاحت لهم هذه التقنية مباشرة اجراءات التحقيق والمحاكمة عن بعد وبصفة خاصة سماع الشهود والمتعاونين مع العدالة وغيرهم . أنظر

dixième Congrès des Nations Unies Sur la prévention du Crime et le traitement des délinquants Vienne ,10-17avril2000,le Procès à distance au moyen de la vidéoconférence.l'expérienceItalienne,p,1,http://www.uncjin.org/Documents/10thcongress/10cStatements/italy.pdf

8-حاتم محمد فتحي أحمد البكري ، مبدأ الشفهية والتقنيات الحديثة في المحاكمات الجنائية ، مجلة البحوث القانونية والاقتصادية ، عدد 49 ، أبريل 2011 ، ص 5.

9- ألامر رقم 20-04 المؤرخ في 30 غشت 2020 المعدل لقانون الإجراءات الجزائية ، الجريدة الجزائرية الرسمية . عدد 51 الصادر في 13 غشت 2020.

10–أنظر المادة 441 مكرر من القانون رقم 04/20 المعدل لقانونالاجراءات الجزائية

11– أنظر المادة 441 مكرر4 مرجع سابق .

12-حاتم محمد فتحي أحمد البكري ، المرجع السابق ، ص 25 ، ولمزيد من التفصيل راجع د ، رامي متولي عبد الوهاب ابراهيم ، حماية الشهود في القانون الجنائي ، مجلة الفكر الشرطي ، م 24 ، ع 95 ، الامارات العربية المتحدة ، اكتوبر 2015 ، ص 109.

13-حاتم محمد فتحي أحمد البكري ، المرجع السابق ، ص 15.أنظر أيضا، د ، عادل يحي ، المرجع السابق، ص 36.

14-تتمثل هذه التقنيات في الدوائر الاتصالية الالكترونية سواء كانت مفتوحة أو مغلقة ، أو المحادثة المرئية عن بعد أو ما يسمى بالاتصال السمعي البصري vidéo conférence .

15-خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، المرجع السابق ، ص 262.

16–عمارة فوزي ، قاضي التحقيق ، أطروحة دكتوراه ، جامعة الإخوة منتوري قسنطينة ، 2009–2010 . ص 116 .

17–خالد موسى توني ، الحماية الجنائية الإجرائة للشهود دراسة مقارنة ، ط1 ، 2010

18– د . أحمد يوسف محمد السولية، الحماية الجنائية والأمنية للشاهد ، دراسة مقارنة ،دار الفكر الجامعي ، ط 1 ، الاسكندرية 2007 .ص 250 .

19– خالد موسى توني ، المرجع السابق ، 137 .

20– محي الدين حسيبة ، سماع الشهود عن طريق المحادثة عن بعد بين الحق في الحماية وحقوق الدفاع ، مجلة الدراسات والبحوث القانونية والسياسية ، عدد10 ، سنة 2018، ص 292 .

21– أحمد يوسف محمد السولية ، المرجع السابق ، ص 251 .

الملتقى الدولي الإفتراضي "القانون الجنائي في ظل التطور التكنولوجي –إشكالات ومعالجات–"

الأستاذة/ الدكتورة فرحاتي صبرينة

أستاذ محاضر أ

كلية الحقوق جامعة الجزائر 1 بن يوسف بن خدة

رقم الهاتف: 0661770064

البريد الإلكتروني: s.ferhati@yahoo.com

عنوان المداخلة "مخاطر استعمال الدليل العلمي على السلامة العقلية للشخص في ظل التطور العلمي والتكنولوجي"

محور المداخلة "تحديات استعمال الدليل العلمي بالنسبة لحقوق الإنسان"

ملخص:

إن ثبوت عدم كفاية الوسائل التقليديةوأحيانا فشلها في الكشف عن الجريمة، خاصة بعد التطور التكنولوجي الذي شهدته هذه الأخيرة، أصبحت الضرورة ملحة الى البحث عن وسائل وتقنيات علمية حديثة تتواءم وهذا التحول، إلا أن استعمال الدليل العلمي الذي قد يكون قطعيا كوسيلة للإثبات الجنائي في مواجهة القاضي الجزائي، قد يكون فيه في كثير من الأحيان مساسا بالحرية الشخصية للأفراد وتعديا على حقوق الإنسان بصفة عامة، مالم يتم ضبط ذلك بنصوص قانونية صارمة وواضحة المعالم لتحقيق التوازن بين أمن المجتمع ونظامه من جهة وبين أسس حماية حقوق وحريات المتهم الأساسية بالتعامل معه بوصفه إنسانمن ناحية أخرى.

الكلمات المفتاحية: التنويم المغناطيسي– التخذير الموضعي– حقوق الإنسان– التطور التكنولوجي– الجريمة–الحرية الشخصية للمتهم.

Summary:

The proven insufficiency of traditional means and their failure to detect crime, especially after the technological development witnessed by the latter, has become an urgent necessity to search for modern scientific methods and techniques that are compatible with this transformation, but the use of scientific evidence, which may be definitive as a means of criminal proof in the face of The criminal judge, in which it may often be a violation of the personal freedom of individuals and an infringement of human rights in general, unless this is controlled by strict and clear legal texts to achieve a balance between the security and system of society on the one hand and the foundations for protecting the basic rights and freedoms of the accused by dealing with him as a human being another side.

Keywords:sleep hypnosis - local anesthesia - human rights - technological development - crime - personal freedom of the accused.

مقدمة:

بعد التطور العلمي والتكنولوجي الرهيب في مجال الجريمة، أصبحت وسائل الإثبات التقليدية غير كافية، فباتت الضرورة ملحة الى البحث عن وسائل علمية حديثة، تتواءم وهذا التطور، فتم إرساء سياسة جنائية قائمة على الأساليب العلمية الحديثة التي تشمل مختلف جوانب الجريمة، التي تساعد القاضي الجزائي في الوصول الى الحقيقة وإثباتها، حيث أصبح القضاء يعتمد عليها كأدلة علمية للإثبات، كما تأسس عليها الكثير من الأحكام بالإدانة أو البراءة.

حيث يعتبر كل من التنويم المغناطيسي والتخذير الموضعي إحدى أدوات الإثبات الجنائي، إلا أن مشروعية هذه الأدلة يبقى مرتبط بعدة ضوابط، لأن مجرد الحصول على الدليل العلمي لا يمكن الأخذ به، إلا إذا خضع لمبدأ المشروعية، وهو من أهم القيود التي تحد من استعمالها للإثبات الجنائي، كما ما ورد في نص المادة 44 من الدستور الجزائري لسنة 2020، ومن أجل صحة استعمال هذه الأدلة لا يجب تجاهل تحقيق التوازن بين مصلحة المجتمع من جهة ومصلحة المتهم من ناحية أخرى، وعليه لا يمكن للقاضي أن

يعتمد على أدلة لم تراعى فيها القواعد القانونية، التي تحترم حقوق وكرامة الإنسان، خاصة عندما تكون ماسة بالسلامة العقلية والجسدية للشخص.

لأدلة الإثبات دورا مهما وأساسيا في الإثبات الجنائي مما يجعل موضوع دراستنا من المواصيع بالغة الأهمية، لما لها من دور في تحقيق العدالة الجنائية، والتي تزيل في كثير من الأحيان الغموض في قناعة القاضي سواء الحكم بالبراءة أو الإدانة.

نظرا لتنوع الأدلة العلمية للإثبات نجد من أهمها التنويم المغناطيسي والتخذير الموضعي للمتهم، من أجل الكشف عن الحقيقة، إلا أن أهم أهداف هذه الدراسة هو البحث في مدى مشروعية هذه الأدلة، ومدى تأثيرها على السلامة العقلية والجسدية للشخص، ومدى الأخذ بها.

لذلك فرضت الإشكالية التالية نفسها والتي كانت على النحو التالي:

- **مامدى مشروعية التنويم المغناطيسي والتخذير الموضعي كأداة للإثبات الجنائي؟.**

للإجابة على هذه الإشكالية قمنا بتقسيم خطة العمل الى مبحثين أساسين، المبحث الأول جاء بعنوان ماهية الإثبات الجنائيبالدليل العلمي، والمبحث الثاني بعنوان التنويم المغناطيسي والتخذير الموضعي كأداة للإثبات الجنائي.

المبحث الأول: ماهية الإثبات الجنائي بالدليل العلمي

إن الغاية من الإثبات في المادة الجزائية هو كشف الحقيقة حول الجريمة ومرتكبها، عن طريق البحث في الأدلة المتحصل عليها بمختلف الوسائل والطرق العلمية الحديثة، لما لها من قيمة قانونية في الإثبات الجنائي، بدلا من تلك الوسائل التقليدية التي لم تعد كافية نظرا للتطور الحاصل في مجال الجريمة.

لذلك سنتطرق لمفهوم الإثبات الجنائي في المطلب الأول ومفهوم الدليل العلمي في المطلب الثاني.

المطلب الأول: مفهوم الإثبات الجنائي

يقوم الإثبات الجنائي على كشف الغموض حول واقعة معينة، من أجل الوصول الى الحقيقة وذلك بإثباتها أو نفيها، عن طريق البرهان أو الدليل، فسنتطرق لكل مايتعلق بالإثبات الجنائي من تعريف وخصائص وأهمية من خلال الفروع التالية:

الفرع الأول: تعريف الإثبات الجنائي

يعرف الإثبات الجنائي بأنه إقامة الدليل علر وقوع جريمة أو عدمها ونسبتها للشخص المشتكى عليه فهو الدليل أو البرهان أو الحجة لإثبات الوقائع لدى السلطات المختصة، وفق قواعد مشروعة وقانونية حددها القانون.

حيث يهدف الإثبات في المجال الجنائي الى ضبط الجريمة ومرتكبيها، فنطاق الإثبات الجنائي لا يقتصر على إقامة الدليل أمام المحكمة فقط، بل يشمل أيضا إقامته أمام جهات التحقيق وأمام سلطات جمع الأدلة أيضا، هذا يعني أن نطاق نظرية الإثبات الجنائي أوسع من أن ينحصر في مرحلة المحاكمة، فإقمة الدليل في المواد الجزائية هو تعبير يشمل على معنى التنقيب عنه، ثم تقديمه الى الجهة المختصة، ثم تقديره.

وعليه فإن طرح الدعوى الجزائية أمام القضاء يكون إما بعد جمع الإستدلالات، وإما بعد التحقيق الذي جرى بمعرفة جهة مختصة، وإما بعد تمام الأمرين معا، وكليهما مرحلة أولية من مراحل الإثبات في الأمور الجزائية. هذا يعني أن الإثبات الجنائي قد يشمل في نطاقه كل مراحل الدعوى الجزائية[1].

أما المفهوم الواسع للإثبات ينصرف الى مجموع الوسائل المستعملة للوصول الى الحقيقة، حول سلوك معين، فكلمة الإثبات هنا تعني الوسائل التي يتذرع بها أطراف الدعوى لكشف الحقيقة، كالمعاينة والخبرة، الشهادات والقرائن وغيرها من الوسائل، فهو عملية تسمح بتكوين اقتناع أمام الجهات المختصة حول مسألة محل الشك أو النزاع[2].

الفرع الثاني: خصائص الإثبات الجنائي بالوسائل العلمية الحديثة

تتميز أدلة الإثبات الجنائي بعدة خصائص أهمها:

أولا/ يجب أن يكون الدليل متضمنا أكبر قدر من الحقيقة لكي يكون الحكم المعتمد عليه أقرب الى العدالة.

---

[1]– نسيم بلحو، محاضرات في مقياس الإثبات الجنائي، ملقاة على طلبة السنة أولى ماستر، تخصص قانون جنائي، جامعة محمد بوضياف، المسيلة، قسم الحقوق، السنة الجامعية 2018/2017، ص 05.

[2]– محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، ديوان المطبوعات الجامعية، 1999، ص 105، 106.

ثانيا/يجب أن لا يتعارض البحث عن الدليل مع الحريات العامة والكرامة البشرية كالسلامة العقلية والجسدية للمتهم، مع استبعاد التعذيب والإحتيال.

ثالثا/ بالرجوع الى قانون الإجراءات الجزائية الجزائري نجده لم يحدد لنظرية الإثبات في المجال الجنائي موضعا محددا، بل تشمل كل مراحل الدعوى[1].

رابعا/إن الإثبات بهذه الوسائل يتميز بالحداثة، التي فرضها التطور السريع في مجال الجريمة.

الفرع الثالث: أهمية الإثبات الجنائي بالوسائل العلمية

تكمن أهمية الإثبات الجنائي في الآتي:

- يعتبر مفتاح الوصول الى الحقيقة في أسرع وقت ممكن، وبدونه يصبح الحق بعيد المنال، وعليه فنظرية الاثبات من أهم النظريات القانونية التي تلقى تطبيقا يوميا في المحاكم على مختلف أنواعها ودرجاتها.
- تعتبر نظرية الإثبات الأسلوب السليم أمام القاضي والمتقاضين برسم الطريق التي يجب سلكها، عند تقديم دليل الإثبات وتحقيقه.
- للإثبات الجنائي أهمية خاصة، فالمتهم بريء حتى تثبت إدانته، اعتمادا على الأدلة الواقعية والقانونية التي تتضمنها قوانين الإجراءات الجنائية والتي تضمنت قواعد خاصة تتميز عن قواعد الإثبات في القانون المدني.
- من مظاهر خصوصية وأهمية الإثبات الجنائي، سواء من حيث هدف الدليل أو طبيعة الموضوع الذي يرد عليه عبء الإثبات أو الأدلة المقبولة أو قواعد البحث والتنقيب عنها أو الدول المخول للقاضي الجنائي في الإثبات، أين تظهر أهمية الإثبات في إحاطة القاضي بقواعد الاثبات والتمكن منها يجعل حكمه أكثر رصانة وأقرب للعدالة[2].

---

[1]– نسيم بلحو، مرجع سابق، ص 06 ومايليها.

[2]– أحمد فتحي سرور، الإثبات الجنائي، بحث في مجلة القانون والإقتصاد، عدد خاص سنة 1980.

المطلب الثاني: مفهوم الدليل العلمي

لقد تأثر العالم بأسره بالتقدم العلمي والتكتولوجي الحاصل بصورة سريعة، دون أن نخفي مدى تأثر القانون الجنائي هو الآخر لما أحدثه ذلك التحول في مجال الجريمة، وبالمقابل في مجال الكشف عنها بكل الأدلة العلمية الحديثة لعدم كفاية الأدلة التقليدية ، لذلك سنتطرق لكل مايتعلق بالدليل العلمي وفقا للنقاط التالية:

الفرع الأول: تعريف الدليل العلمي

يمكن تعريف الدليل العلمي على أنه ذلك الدليل الذي يكون مصدره تقدير علمي من أهل الخبرة والإختصاص، والتي تساعد القاضي في تشكيل قناعتهوإصدار حكمه النهائي، على اعتبار أن القاضي لا يمكنه أن يلم بكل الأمور الفنية المتعلقة بالدليل فيلجأ الى للخبراء لأجل الحصول الى الحقيقة[1].

فالدليل العلمي ماهو إلا أداة لربط الجريمة بالفاعل، ومنع القاضي من الوقوع في الخطأ أثناء كشف الحقيقة وإصدار الحكم، تحقيق للعدالة الجنائية والإجتماعية[2].

الفرع الثاني: خصائص الدليل العلمي

يتميز الدليل العلمي بعدة خصائص نذكر أهمها:

- يملك الدليل العلمي دور مهم في إثبات الجريمة، خلال كل مراحل الإجراءات ومراحل الدعوى.
- تتميز الأدلة العلمية بالثبات والإستقرار كونها قائمة على أسس علمية مستقرة تعطي نتائج مستقرة وثابتة.
- بما أن الخبير أثناء تكوين رأيه فإنه يخضع للرقابةمن رئيسه ومن طرف القضاء، مما يجعل الدليل المتوصل إليه يتميز بالحياد والأصالة.
- الأدلة العلمية في تطور مستمر.

---

[1]– سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، دار شتات للنشر والبرمجات، القاهرة، 2011، ص 33.

[2]– عبد الناصر محمد محمود فرغلي، الإثبات العلمي لجرائم تزوير المحررات التقليدية والإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2010، ص 116.

الفرع الثالث: تمييز الدليل العلمي عن غيره من الأدلة الأخرى

يمكن القول بأن وسائل الإثبات في المواد الجنائية يمكن أن تحصر في الآتي:

- وسائل إثبات ناتجة عن الإجراءات وعلى رأسها المحاضر والتقارير[1]. المحاضر الإدارية والتقارير الطبية.
- وسائل إثبات موضوعية مباشرة[2]، فهي تسهم في عملية الإثبات بصورة مباشرة وواضحة،
- وسائل إثبات موضوعية غير مباشرة[3]، فالقرينة مثلا من حيث قيمتها القانونية وقوتهاالثبوتية، لا تعتبر دليل إثبات ولا يمكن بناء الحكم الجنائي عليها، بل تتطلب العديد من القرائن حتى يمكن استنباط أمر مجهول يفيد في الموضوع.

وأمام تلك الوسائل يمكن القول أن مايميز الوسائل العلمية في الإثبات الجنائي، عن الوسائل الأخرى، أنه مع التطور العلمي والتكنلوجي الذي طال مجال الجريمة وأساليبها لم تعد وسائل الإثبات التقليدية كافية لمواجهتها مما تطلب الأمر من ذوي الإختصاص أن يواجهوا ذلك بأساليب علمية متطورة وحديثة تساعدهم في الكشف عن الحقيقة، فأصبحت بذلك هذه الوسائل الحديثة ذات أهمية في مجال الإثبات الجنائي دون الإستغناء عن وسائل الإثبات التقليدية[4].

المبحث الثاني: التنويم المغناطيسي والتخذير الموضعي كأداة للإثبات الجنائي

لقد ظهرت وسائل علمية حديثة تستعمل للإثبات الجنائي، حيث تستخدم بصورة مباشرة على الشخص إلا أنها تظهر تأثيرها على كيانه النفسي والمادي بشكل ظاهر، حيث تستعمل من أجل استنطاق المشتبه فيهم

---

[1]– ويمكن حصرها هي الأخرى في أنواع: محاضر استدلال، محاضر التحقيق ومحاضر الجلسات، ولكل نوع قيمته وقوته القانونية وحجيته الإثباتية.

[2]– كالإعتراف وشهادة الشهود والكتابة،

[3]– في مقدمتها القرائن والدلائل، التي هي مجموعة من الأمارات وهي أقل قيمة من القرائن.

[4]– سامي حارب المندري، موسوعة العلوم الجنائية، تقنية الحصول على الآثار المادية، الجزء الأول، مركز البحوث للشرطة، الشارقة، 2007، ص 71.

– بالرجوع الى نص المادة 212 من قانون الإجراءات الجزائية الجزائري نجد أن المشرع اعتبر الدليل العلمي كبقية الأدلة الأخرى.

بعد استجوابهم مثل الدليل المستمد من التنويم المغناطيسي وكذا التخذير الموضعي، لذلك اخترنا هاتين الوسلتين كنموذج للدراسة يتم مناقشتهما من خلال النقاط التالية:

المطلب الأول:التنويم المغناطيسي

يعتبر كل من التنويم المغناطيسي ، من الأدلة العلمية المستحدثة من أجل استنطاق المتهمين والوصول الى الحقيقة وربطها بالجاني أو نفيها عنه، تحقيقا للعدالة الجنائية التي يقوم عليها أساس القضاء، خاصة في مجال القضاء الجزائي، وعليخ سيتم الطرق إليه من بناء على العناصر التالية:

الفرع الأول: التعريف بالتنويم المغناطيسي

يعتبر التنويم المغناطيسي كوسيلة للإثبات، فهو عملية افتعال نوم غير طبيعي يصاحبه تغيير في الحالة النفسية والجسمانية للنائم، تتغير معه إرادة العقل الطبيعي وملكاته العليا، فالمنوم مغناطيسيا يتغير إدراكه الطبيعي ولا يستطيع إخضاع تصرفاته أثناء النوم للنقد الذاتي، يكون غير قادر على التحكم الإرادي في أفعاله أو الهيمنة عليها وتقدير نتائجها، عكس ما يحدث أثناء وعيه[1].

كما يمكن تعريفه بأنه عملية إيحائية يتمكن من خلالها المنوم من السيطرة على الشخص المنوم، على نحو يكون عقله الواعي معطلا فيما يبقى عقله الباطن مستيقظا[2].

الفرع الثالث: الهدف من التنويم المغناطيسي كأداة للإثبات الجنائي

إن الهدف من التنويم المغناطيسي يبدو واضحا، من حلال الإستفادة منه في الإستدلال من خلال إمكانية استدعاء المعلومات و الأفكار التي قد تكون عميقة في اللاشعور غند نسيانها أو في الشعور عند الإمتناع عن البوح والإقرار بها، والتي لا يمكن الوصول إليها بواسطة إجراءات التحقيق الإعتيادية،[3] وذلك

---

[1]– أسعد زروق، موسوعة علم النفس، الطبعة الأولى، المؤسسة العربية للدراسات والنشر، مطابع الشروق، لبنان، بيروت، 1977، ص 54.

[2]– محمد حمدي حجاز، التنويم السريري ومجالات استخدامه، مجلة الفكر الشرطي، مجلد 13، عدد 02، جويلية 2004، ص – يمكن تسميته أيضا بالتنويم الإيحائي أو الإصطناعي.

[3]– محمد سامي التبراوي، إستجواب المتهم، دار النهضة العربية، مصر القاهرة، الطبعة العالمية 1969/1968، ص 485.

عن طريق التأثير في إرادة المنوم بحيث يصبح في النائم في وضع المستجيب لأيحاء المنوم بواسطة إحداث نوم مصطنع يصاحبه حالة من الفراغ والإرتخاء والراحة النفسية المتحررة من العوائق التي توقف الأفكار[1].

الفرع الثالث: الآثار الجانبية للتنويم المغناطيسي

أن استخدام التنويم المغناطيسي كوسيلة للإثبات الجنائي، لها آثار جانبية وخيمة تهدد السلامة العقلية للشخص، لما فيها من اعتداء على الحرية الشخصية للإنسان والإضرار بحقه في الدفاع عن نفسه، كما فيه اعتداء على الكرامة الإنسانية لدخولها كوسيلة الى مكنونات النفس، فهي تشكل إكراه مادي ومعنوي، نتيجة للآثار النفسية والفيسيولوجية غير الطبيعية التي تخلفها على الشخص المنوم مغناطيسيا[2].

المطلب الثاني:التخذير الموضعي

يعتبر التحليل التخذيري أو مايسميه البعض بالتخذير الموضعي الوسيلة الثانية التي سنتطرق إليها بالدراسة، لما لها من تأثير نفسي ومادي على سلامة الشخص، مع التعرض لكل تلك الجوانب ذات الصلة من خلال العناصر التالية:

الفرع الأول: تعريف التخذير الموضعي

هو حقن المتهمبعقار مخدر الغرض منه التأثير على العقل الباطن للمحقون، من أجل إحداث نوع من التخفيض أو التعطيل في التحكم الإرادي لهذا الشخص، ونزع حوادز عقله الباطن للتعرف على المعلومات المختزنة في داخل النفس، كما يدخل هذا الأخير في حالة نوم عميق أو إسترخاء لمدة تصل من عشرين الى أربعين دقيقة تسلب فيها إرادته مما تجعله أكثر قابلية للإيحاء ورغبة في المصارحة والتعبير عن خوالجه[3].

الفرع الثاني: الآثار الجانبية للتخذير الموضعي

---

[1]– مصطفى العوجي، حقوق الإنسان في الدعوى الجزائية، الطبعة الأولى، مؤسسة نوفل، بيروت، لبنان، 1989، ص 610.

[2]– محمد حمدي حجار، المرجع نفسه، ص

[3]– سامي الملا، إعتراف المتهم، إعتراف المتهم، رسالة دكتوراه، الطبعة الثالثة، المطبعة العالمية مصر، القاهرة، 1986، ص 178.

– من المواد المستخدمة في التخذير الموضعي مادة الكلوروفروم، التي تسلب الشخص الرقابة على وعيه وتسهل على مستعملها إستنطاقه بكل سهولة.

إن للتخذير الموضعي آثار جانبية قد تصيب سلامة المحقون في دماغه والجهاز العصبي وبعض الأعضاء الحيوية الأخرى من جسمه كالكبد كما تؤثر على كريات الدم، مما يشكل اعتداءا على جسده كما تمثل تهديدا لصحته وعلى الحرية الشخصية للإنسان والإصرار بمصلحته في الدفاع على نفسه، كما تمس بكرامته بسبب الدخول الى مكنونات نفسه لما فيها من إكراه مادي ومعنوي يخالف أخلاقيات الكرامة الإنسانية[1].

الفرع الثالث: القيمة الثبوتية لوسيلتي التنويم المغناطيسي والتخدير الموضعي

يعتبر كل من التنويم المغناطيسي والتخذير الموضعي وسيلتان فيهما اعتداء على الحرية النفسية والسلامة الجسدية للمتهم، لما فيهما من سلب لإرادته بسبب تأثيرهما في إضعاف الحاجز القائم بين العقل الواعي والعقل الباطن، وفيهما مساس بشعوره الداخلي بالإضافة للأضرار الجسدية، وعليه حرمت أغلب التشريعات استخدامهما في أعمال الإستدلال أو التحقيق الجنائي، لذات الأسباب لدينا على رأسها القانون البرتغالي والقانون الألماني وكذا القانون الأرجنتيني والقانون الفرنسي وغيرها من القوانين الأخرى.

خاتمة:

إن للإثبات في المادة الجنائية أهمية بالغة، لأنه يشكل المادة الأساسية والمهمة في قناعة القاضي الجزائي، لما ينطوي عليه من أدلة ووسائل مهمة، خاصة وأنه بعد التطور العلمي الحاصل في مجال الجريمة، فرض حتمية البحث عن وسائل إثبات أكثر تطورا ودقة بما يتناسب والتطور العلمي المشهود، وذلك وفق ضوابط علمية للإستدلال والبحث على المتهم وكشف الحقيقة، بما لا يتعارض والشرعية القانونية.

إلا أن استخدام بعض هذه الوسائل الحديثة للحصول على دليل قاطع، قد يشكل اعتداءا على السلامة الشخصية العقلية والنفسية وأحيانا الجسدية، كالتنويم المغناطيسي والتخذير الموضعي، فحقيقة معيار قبول أي وسيلة علمية من هذه الوسائل، يقوم على أساس عدم الإعتداء على الحرية الفردية أو الكرامة الإنسانية للشخص مما يجعل هذا الدليل غير مقبول في مجال الإثبات، حتى أن القاصي ذاته لا يستطيع الأخذ به

[1]– محمد فالح حسن، مشروعية الوسائل العلمية في الإثبات الجنائي، الطبعة الرابعة،العراق، بغداد، 1987، ص 72.

لتعارضه مع القانون وقيم العدالة، اما فيه من مساس بحق المتهم في الدفاع عن نفسه، ومساس بالحقوق الإساسية للإنسان وكذا السلامة العقلية للفرد.

التوصيات:

- لا بد من قبول الأدلة المتحصل عليها عن طريق التنويم المغناطيسي والتخذير الموضعي بالرغم من الآثار الجانبية لهما مع تضييق مجال استعمالهما، ولكن حتى نحقق التوازن بين قيمتهما كدليل قطعي في الكشف عن الحقيقة وبين مخاطرهما على السلامة العقلية والجسدية للمتهم، يجب تحديد مجال استعمالها ونوع الجرائم المسموح بهما.
- لابد من ترك هاتين الوسيلتين كآخر فرصة لكشف الحقيقة بعد فشل كل السبل والطرق.
- لابد من البحث في مخاطر استعمال هاتين الوسيلتين وسبل تجنبها وكيفية التخفيف منها بإشراف مختصين، بما أنه يسمح باستعمالها كعلاج طبي في كثير من الأنظمة القانونية.
- لا بد من وضع نظام قانوني يسمح باستعمال هاتين الوسلتين ولكن بعد موافقة المتهم وبمقابل مادي.

قائمة المراجع:

1/ الكتب:

1. أسعد زروق، موسوعة علم النفس، الطبعة الأولى، المؤسسة العربية للدراسات والنشر، مطابع الشروق، لبنان، بيروت، 1977
2. سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، دار شتات للنشر والبرمجات، القاهرة، 2011.
3. سامي حارب المندري، موسوعة العلوم الجنائية، تقنية الحصول على الآثار المادية، الجزء الأول، مركز البحوث للشرطة، الشارقة، 2007.

4. محمد سامي التبراوي، إستجواب المتهم، دار النهضة العربية، مصر القاهرة، الطبعة العالمية 1969/1968.
5. محمد فالح حسن، مشروعية االوسائل العلمية في الإثبات الجنائي، الطبعة الرابعة،العراق، بغداد، 1987.
6. محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، ديوان المطبوعات الجامعية، 1999.
7. مصطفى العوجي، حقوق الإنسان في الدعوى الجزائية، الطبعة الأولى، مؤسسة نوفل، بيروت، لبنان، 1989.

2/ **أطروحات:**

1. عبد الناصر محمد محمود فرغلي، الإثبات العلمي لجرائم تزوير المحررات التقليدية والإلكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة القاهرة، مصر، 2010.

3/ المقالات:

1. أحمد فتحي سرور، الإثبات الجنائي، بحث في مجلة القانون والإقتصاد، عدد خاص سنة 1980.
2. محمد حمدي حجاز، التنويم السريري ومجالات استخدامه، مجلة الفكر الشرطي، مجلد 13، عدد 02، جويلية 2004.
3. سامي الملا، إعتراف المتهم، إعتراف المتهم، أطروحة دكتوراه، الطبعة الثالثة، المطبعة العالمية مصر، القاهرة، 1986.

4/ المحاضرات:

1. نسيم بلحو، محاضرات في مقياس الإثبات الجنائي، ملقاة على طلبة السنة أولى ماستر، تخصص قانون جنائي، جامعة محمد بوضياف، المسيلة، قسم الحقوق، السنة الجامعية 2018/2017.

الأستاذ: عباسي محمد الحبيب

رئيس فرقة التنمية وحقوق الإنسان – مخبر القانون والتنمية–

أستاذ محاضر أ، كلية الحقوق والعلوم السياسية –جامعة طاهري محمد بشار–

البريد الالكتروني: habibmed08@gmail.com

الهاتف: 0660943382

عنوان المداخلة: استخدام التكنولوجيا الحديثة...آلية إستراتيجية في تفعيل التعاون الدولي في مجال مكافحة الإجرام

مقدمة للمشاركة في الملتقى الدولي الافتراضي الموسوم ب:

القانون الجنائي في ظل التطور التكنولوجي – إشكالات ومعالجات.

يومي 28– 29 سبتمبر 2022

المحور الرابع المعنون ب: استخدام التقنيات الحديثة في مجال العدالة الجنائية.

الملخص:

يعد التعاون الدولي في المسائل الجزائية من أهم الآليات التي يمكن الاعتماد عليها من قبل الدول في مجال مكافحتها للإجرام، نظرا لما يحققه من نتائج إيجابية في تعقب الأنشطة الإجرامية وتتبع المجرمين. تزداد فعاليته بإتباع وسائل التكنولوجيا الحديثة وتسخيرها في مختلف الميادين التي يشملها هذا التعاون، سواء كانت على المستوى المؤسسي ببناء قدرات الدولة وتدعيمها والرفع من كفاءة أجهزتها المعنية بمحاربة الجريمة، أو على المستوى العملياتي، من خلال اللجوء إلى أساليب التحري والتحقيق الخاصة أو استخدام وسائل الاتصال الحديثة لضمان التواصل الدائم بين الأجهزة الوطنية للدول وتيسير ذلك.

الكلمات المفتاحية:

التكنولوجيا الحديثة– التعاون الدولي – وسائل الاتصال والتواصل– الرقمنة – المراقبة الإلكترونية – الترصد الالكتروني.

Sammary

International Cooperation is considered as an important mechanism countries rely upon in matters of penal issues to prevent and combat crime, taking into account the significant results in detecting and tracking criminal activities. By following the means of modern technology its effectiveness is increased and harnessed in several fields recommended by the mentioned cooperation. Whether at the institutional level by constructing state capabilities and enhancing policing efficiency in the defense against crime , or at the operational level by resorting to special investigative measures or the use of modern technology to ensure and facilitate the constant communication among national agencies.

Key words:

Modern Technology, International cooperation, Communication, digitization, electronic monitoring, Computer and network surveillance.

مقدمة:

لا شك أن ما وصل إليه حال الإجرام في الوقت الراهن، بفضل التقدم التكنولوجي وتطور وسائل الاتصال والمواصلات، يعد من أهم المعضلات المتربصة بالدول وبتقدمها، نظرا لتفاقم الآثار السلبية المترتبة عن ارتكاب الجرائم، بشكل لا يستهان به، لاسيما في مجال إفشال مشاريع التنمية وإفسادها وتغيير مسارها، إلى درجة يمكن أن تؤدي إلى تدهور الدولة وتردي الأوضاع فيها.

وإذا كان الأصل في مكافحة الجرائم الوطنية أنها شأن داخلي للدول، ترتبط بسيادتها على إقليمها وما يستتبع ذلك من اتخاذ تدابير وإستراتيجيات داخلية، تتعلق خاصة بالجوانب الأمنية والقضائية، التي تعمل على منع وقوع الأنشطة الإجرامية وتضييق نطاقها. فإن تطور الإجرام وسبله، فرضا منطقا آخر على الدول ودفعها إلى عدم التقيد بالمعنى الضيق لمبدأ السيادة والبحث عن أفضل السبل لتحقيق فعالية خططها المنتهجة في مكافحة الجريمة، فراحت تبحث لها عن شراكة جزائية دولية من خلال إقامة اتفاقيات ثنائية أو متعددة الأطراف قصد التعاون فيما بينها.

فالتعاون الدولي، إذا، ضرورة تضاف إلى اعتبار السياسة الوطنية القائمة على مبدأ السيادة الوطنية في مجال مكافحة الإجرام، تزداد ضرورته إذا تعلق الأمر بتسخير المجرمين لآخر ما وصل إليه التقدم العلمي والتطور التكنولوجي في أنشطتهم الإجرامية، الأمر الذي شجع على زيادة حدة الإجرام وانتشاره بين الدول والقارات.

يقصد بالتعاون الدولي الجزائي، ذلك الصنف من التعاون الذي يعتمد بالأساس على تقديم المساعدة المتبادلة في المسائل الأمنية والقضائية التي تتعلق إما بالمجال المؤسسي أو العملياتي. ولأهميته يجب أن يحظى باهتمام بليغ، ليس من الجانب النظري بإبرام الاتفاقيات أو الترتيبات القائمة على الاعتراف به فحسب بل حتى من الجانب الميداني والتطبيقي، بتطوير مجالاته والوسائل المستعملة فيه، بغية بناء إستراتيجية كاملة ومتكاملة ضامنة لتحقيق الحماية المرجوة لمصالح الدول محل التعاون، فبدون توفر وسائل التكنولوجيا الحديثة في الدول والرفع من كفاءة أجهزة ومؤسساتها وتبادل الخبرات والمهارات والفنيات المتطورة في متابعة الأنشطة الإجرامية واستقصاء المعطيات المرتبطة بها وبالأشخاص الضالعين فيها، لا مجال للبحث عن أي فعالية تذكر في مكافحة الإجرام.

كما أن الدول لا تستطيع النهوض ومواجهة تحديات ومهددات العصر دون الدخول في علاقات وروابط تشاركية لتحقيق مصالحها الوطنية، تتجسد في ميدان التعاون الجزائي العملياتي في اتخاذ الإجراءات اللازمة للبحث والتحري والتحقيق، باستعمال أساليب متطور في ذلك، وكذلك إقامة منظومة اتصال وتواصل دائمين بتسخير أقصى ما وصلت إليه تكنولوجيات الإعلام والاتصال، على أن يكون ذلك بكل مرونة ويسر، بغية الوصول إلى تدفق المعلومات اللازمة في أوانها وإيصالها إلى الدولة المعنية بها في وقتها.

أمام حتمية التعاون الدولي في مكافحة الإجرام والبحث عن متطلبات تفعيله، تبرز التكنولوجيا الحديثة كوسيلة ضرورية في ذلك، فإلى أي مدى يمكن أن تساهم هذه التكنولوجيا في تحقيق الأهداف المرجوة من التعاون الدولي الجزائي؟

هذا ما تسعى هذه الورقة البحثية إلى الوصول إليه، من خلال إبراز أهمية استعمال وسائل التكنولوجيا الحديثة في تدعيم التعاون الدولي في مجال مكافحة الإجرام، سواء على المستوى المؤسسي أو على المستوى العملياتي.

وللإجابة على هذه الإشكالية تم الاعتماد على المنهج الوصفي، بتشخيص واقع استخدام التكنولوجيا الحديثة في العلاقات بين الدول في مكافحة الأنشطة الإجرامية، وكذلك المنهج التحليلي بتحليل مختلف المعطيات القانونية المتوفرة وصلاحياتها للاعتماد على هذه التكنولوجيا في مختلق مجالات التعاون.

تم التطرق إلى هذا الموضوع في محورين، تناول المحور الأول مظاهر استخدام التكنولوجيا الحديثة في التعاون الدولي المؤسسي في مكافحة الإجرام، بينما تم التطرق في المحور الثاني إلى هذه المظاهر في القطاع العملياتي من هذا التعاون.

المبحث الأول: استخدام التكنولوجيا الحديثة في التعاون الدولي المؤسسي في مكافحة الإجرام

ترتبط السياسة الجزائية بالأوضاع السائدة في الدولة والعالم ككل[1]، إذ يتصل نجاحها بمدى قدرتها على مواكبة ما وصل إليه حال الإجرام، وذلك باستيعاب الظواهر الإجرامية الحديثة أو المتجددة عن طريق أجهزة إنفاذ القانون.

يشهد العالم تبلور شكل جديد لنظام دولي قائم على حركة متسارعة وقوة مؤثرة وفعالة في العلاقات الدولية، مردها إلى ما يعرف بظاهرة العولمة التي استطاعت أن تؤثر على مبدأ السيادة الجامد، الذي يعني بسط الدولة لسيطرتها على إقليمها وما يقع فيه دون تقبل أي تدخل أجنبي[2].

إلى وقت ليس ببعيد، كانت الدول تعتمد على مؤسساتها في مكافحة الإجرام الواقع في حدود إقليمها معتبرة في ذلك أن هذه المهمة تدخل ضمن الشؤون الداخلية، وبالتالي لا يجوز لغيرها التدخل لارتباط ذلك بفكرة السيادة الوطنية. لكن ما وصل إليه حال الإجرام جعل الدول عاجزة عن تحقيق مكافحة فعالة دون نسج علاقات تشاركية فيما بينها قائمة على تقديم الدعم والمساندة والمساعدة للدول في مجالها المؤسسي المرتبط بمكافحة الأنشطة الإجرامية المختلفة.

إن تطبيق وسائل التكنولوجيا الحديثة في مجال التعاون الدولي المؤسسي يتخذ عدة صور، بعضها يتعلق ببناء القدرات حتى تستطيع الدول التصدي للجريمة، والبعض الآخر يرتبط بالرفع من كفاءة الدول وأجهزتها حتى تكون قادرة على ذلك.

المطلب الأول: استخدام التكنولوجيا الحديثة في بناء قدرات الدول على مكافحة الإجرام.

يحقق استخدام التكنولوجيا الحديثة ووسائلها من قبل الدول والأجهزة الدولية التي تعني بمكافحة الإجرام قفزة نوعية في مجال التعاون القائم بينها، بما يضمن الوقاية من الأنشطة الإجرامية أو تحديد نطاقها وكذلك ضمان عدم إفلات المجرمين من العقاب، بتعقبهم وتعقب حركاتهم.

---

[1]– علي محمد جعفر، السياسة الجزائية في ظل نظام العولمة، المؤسسة الجامعية للدراسات والنشر والتوزيع لبنان، الطبعة الأولى 2013، صفحة 13.

[2]– عثمانية لخميسي، عولمة التجريم والعقاب، دار هومه للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية 2008، صفحة 5 و6.

يستلزم التعاون الدولي وجود قاعدة متينة قائمة على استخدام وسائل التكنولوجيا الحديثة، ولا يتحقق ذلك إلا من خلال إيجاد المعطيات القانونية وتوفيرها على المستوى الوطني، من خلال تدعيم التشريعات الوطنية بنصوص تسمح باستخدام هذه الوسائل وإضفاء المشروعية عليها، تحسبا للاعتراف بمشروعية العمليات المنتهجة وما تفرزه من أدلة ووسائل إثبات. هذا من جهة، ومن جهة أخرى، فإن التعاون الدولي لا يمكن أن يأتي أكله في غياب التكنولوجيا في بعض الدول أو عدم تطور وسائلها فيها، أين يصير مد أواصر هذا التعاون شبه مستحيلا معها، خصوصا مع تراجع الآليات التقليدية المقررة في مكافحة الجريمة ونقص فعاليتها.

<u>الفرع الأول:</u> التكريس التشريعي لوسائل التكنولوجيا الحديثة في مكافحة الإجرام.

تلعب التشريعات الوطنية دورا مهما في تحديد فعالية التعاون الدولي، ذلك أن وجود نصوص قانونية تدعم هذا التعاون وتعترف بمشروعية الوسائل المستعملة فيه يؤدي إلى تحقيق النتائج المرجوة فيه، غير أن غياب مثل هذه النصوص يشكل عقبة تجعل من الصعوبة بمكان اللجوء إلى هذا التعاون، وحتى في حالة اللجوء إليه يبقى ذلك مجرد إجراء شكلي لا يحقق أي نتيجة.

كما أن وسائل التكنولوجيا الحديثة تعد وسائل علمية ثبت مدى دقتها في استخلاص النتائج من المعطيات المتوفرة لديها، وفي مجال الإجرام هي وسائل مساعدة على كشف الأنشطة الإجرامية، إلا أن المشكلة تكمن في إصباغ المشروعية عليها، إذ أن تأخر التشريعات في مواكبة التطور الحاصل في المجتمع يفسح المجال كثيرا أمام المجرمين للإفلات من العقاب لصعوبة ضبطهم بالوسائل التقليدية المقررة في البحث والتحري[1].

إيمانا منها بأهمية التكنولوجيا الحديثة في الحد من النشاط الإجرامي، حاولت الدول من خلال الاتفاقيات المبرمة بينها والمتعلقة بمكافحة بعض صور الإجرام التأكيد على ضرورة إنفاذ القانون، بالتكريس التشريعي لهذه الوسائل ولاستخدامها. فمثلا، أشارت اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية صراحة إلى ضرورة التعاون في مجال إنفاذ القانون، وذلك بتعزيز قنوات الاتصال والتواصل بين الدول الأعضاء وإيجاد الوسائل القانونية الكفيلة بضمان التعاون في مجال التحقيق والتحري[2]، وكذلك اتخاذ ما يلزم من تدابير لإتاحة استخدام وسائل الإثبات الحديثة في هذا المجال[3].

كما أكد الفريق العامل المعني بالتعاون الدولي التابع للأمم المتحدة على ضرورة أن تعزز الدول الأعضاء في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية كفاءة آليات التعاون في مجال إنفاذ القانون بوسائل، منها استحداث نظم فعالة لتبادل المعلومات وإنشاء قنوات اتصال، وكذلك اكتشاف السبل والوسائل الكفيلة باستخدام الأدلة الإلكترونية وحفظ هذه الأدلة والتعجيل بعمليات المساعدة القانونية المتبادلة[4].

---

[1] – نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، بدون دار نشر، الطبعة الأولى سنة 2011، صفحة 11.

[2]– أنظر المادة 26 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتخذة رقم 25، الدورة 55، المؤرخة في تشرين الثاني/نوفمبر 2000، وثيقة رقم A/RES/55/25.

[3]– أنظر المادة 20 من نفس المرجع.

[4]– أنظر المطة (ج) و(د)من الفقرة 2 من وثيقة: تقرير عن اجتماع الفريق العامل المعني بالتعاون الدولي، المعقود في فيينا يومي 27 و28 أكتوبر 2015، مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، صفحة 2، رمز الوثيقة CTOC/COP/WG.3/2015/4.

في مجال الجرائم الإلكترونية، نصت الاتفاقية العربية المتعلقة بمكافحتها أن تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها لإقرار السلطات والإجراءات اللازمة لأغراض التحقيقات والبحث في هذه الجرائم[1]. بمعنى آخر، أن التعاون الدولي في هذا المجال يعتمد على القوانين الخاصة الوطنية المنسقة، المجرمة لهذه الجرائم وكذلك القوانين الإجرائية الوطنية التي تحدد قواعد الإثبات والإجراءات الجزائية المطبقة عليها[2].

تعد عملية سن قوانين وطنية حديثة واستحداث نظم جديدة بمثابة تبني أحكام المعاهدات والاتفاقات المصادق عليها وهو ما ينعكس بالإيجاب على أدوات التعاون الدولي في مكافحة الجريمة ويحقق الانسجام القانوني بين الدول فيسمح بتطبيق مختلف الآليات الضرورية في ذلك[3].

أسوة بذلك، ونتيجة لمصادقة الجزائر على اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية وبسبب قصور وسائل البحث والتحري التقليدية، المتمثلة أساس في الكمائن والتتبع والتفتيش، في تحقيق نتائج إيجابية في مكافحة الجريمة، عمد المشرع الجزائري إلى تبني وسائل التكنولوجيا الحديثة في البحث والتحري عن بعض صور الجرائم التي تمتاز بخطورة خاصة وذلك من خلال تعديل قانون الإجراءات الجزائية في سنة 2006 بموجب القانون 06-22[4]، كما هو الحال في أسلوب المراقبة الإلكترونية.

في ذات السياق قام المشرع الجزائري بإيجاد قانون خاص بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وذلك من خلال قانون رقم 09-04، الذي يهدف إلى وضع قواعد خاصة للوقاية من هذه الجرائم ومكافحتها[5]. إذ نص القانون المذكور أعلاه على استخدام وسائل التكنولوجيا الحديثة في البحث والتحري عن الجرائم المحددة فيه، بما في ذلك حالات مرتبطة بالتعاون الدولي[6].

<u>الفرع الثاني:</u> نقل التكنولوجيا الحديثة لتعزيز التعاون الدولي في مكافحة الإجرام.

أخذت التكنولوجيا الحديثة مكانتها في المجتمعات كركيزة من الركائز الأساسية في الحياة اليومية التي لا يمكن الاستغناء عنها، لكن بالموازاة أدت أيضا، إلى تطوير أساليب الإجرام والوسائل المساعدة عليه، وهو ما يقتضي أيضا الاعتماد عليها كطريقة مشروعة في اكتشاف الجرائم وضبط الأدلة المتعلقة بها، وتتبع حركة المجرمين ومنع إفلاتهم من العقاب[7].

---

[1]- أنظر المادة 32 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، المصادق عليها بموجب المرسوم الرئاسي رقم 14-252 مؤرخ في 8 سبتمبر 2014، الجريدة الرسمية، عدد 57، بتاريخ 28 سبتمبر 2014.

[2]- أنظر آليات التعاون الدولي الرسمية، الوحدة التعليمية 7: التعاون الدولي على مكافحة الجريمة الإلكترونية، متاح على موقع مكتب الأمم المتحدة المعني بالمخدرات والجريمة.

[3]- مختار شبلي، الإجرام الاقتصادي والمالي الدولي وسبل المكافحة، دار هومه للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية منقحة ومزيدة 2012 صفحة 106.

[4]-القانون 06-22 مؤرخ في 20 ديسمبر2006، يعدل ويتمم الأمر رقم 55-166، المؤرخ في 5 جوان 1996، المتضمن قانون الإجراءات الجزائية الجريدة الرسمية، عدد 84، بتاريخ 24 ديسمبر 2006.

[5]- القانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية، عدد 47، بتاريخ 16 أوت 2009.

[6]- أنظر المادة 16 من نفس القانون.

[7]- نصر شومان، مرجع سابق، صفحة 15 ومايليها.

والمؤكد أن أمن أي دولة يرتبط بأمننة باقي الدول، بمعنى أن الأمن الوطني لم يعد مفهوما ذاتيا يقتصر على الحدود الإقليمية للدولة وإنما تعداه ليدخل تحت نظام الأمن المشترك للدول فيما بينها، فيفرض بذلك التزام الدول فيما بينها في تحقيق الأمن الداخلي لكل دولة.

وفي العصر الحالي، تنطلق الجرائم غالبا من الدول النامية أو السائرة في طريق النمو بفضل ما توفره من مناخ يساعد على ارتكاب الأنشطة الإجرامية، ناتج عن ضعف آليات الرقابة ووسائل التكنولوجيا اللازمة للتعامل مع الأساليب المتطورة المستعملة في هذه الأنشطة، لتلحق في الأخير بالدول المتقدمة.

إن الاهتمام بتحقيق التنمية للدول فيما بينها يساهم بقدر كبير في تحقيق الأمن الداخلي لها، ذلك أن الإجرام لم يعد يعترف بالحدود السياسية لها، فالجريمة يمكن أن ترتكب في دولة معينة، وتنتج أضرارها في دولة أخرى، وبالتالي لابد من تضافر الجهود للقضاء على أسباب استغلال بعض الدول في ارتكاب بعض الأنشطة الإجرامية، والتعاون في مجال البحث والتحري عن الجرائم ومنع وقوعها، لاسيما من حيث نقل التكنولوجيا وتطوير الدول، خاصة النامية منها، في هذا المجال.

يعرف نقل التكنولوجيا بأنه العملية التي تمكن بلد ما من الاستفادة من التكنولوجيا المنتجة في بلد آخر عن طريق التحويل، الذي قد يكون تحويلا جزئيا عندما يقتصر على نقل الآلات والتجهيزات والوسائل التقنية، أو يكون كليا، بنقل حتى الأساليب التنظيمية والإدارية والطرق المعتمدة في التدريب[1].

من بين الاتفاقيات الدولية التي نصت على ضرورة نقل التكنولوجيا بين الدول، اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، إذا جاء فيها أنه يتعين على دول الأطراف أن تبدل جهودا ملموسة في المساعدة التقنية، وذلك من خلال تعزيز تعاونها على مختلف المستويات مع البلدان النامية، بغية تدعيم قدرات تلك البلدان على منع هذه الجريمة ومكافحتها، وكذلك تقديم المساعدة التقنية لهذه البلدان التي تمر اقتصاداتها بمرحلة انتقالية لمساعدتها على تلبية ما تحتاج إليه[2]، بما في ذلك تقديم مساعدات مالية في هذا الخصوص، كل ذلك لضمان فعالية وسائل التعاون الدولي[3].

وفي مجال مكافحة الجرائم الإلكترونية، نصت الاتفاقية العربية المتعلقة بها على اتخاذ العديد من الإجراءات المتعلقة بالكشف والتحري عن هذه الجرائم والتحقيق فيها ضمن سياق التعاون الدولي، بما فيها النفاذ العابر للحدود إلى بيانات الكمبيوتر المخزنة عبر الموافقة أو حيثما تكون متاحة للعموم[4]، ولا يتحقق ذلك إلا بتملك كلا الدولتين الطالبة أو المطلوب منها لوسائل التكنولوجيا.

من هنا تظهر أهمية نقل التكنولوجيا بين الدول، خاصة بالنسبة للدول النامية، أين تكون هذه الأخيرة في أمس الحاجة لها من أجل الرفع من كفاءتها وكفاءة أجهزتها في التصدي للجريمة، وبدون هذه المساعدة التقنية

---

[1]–سهى حمزاوي، نقل التكنولوجيا إلى الدول النامية بين حتمية مدرسة التبعية ومنطق الخصوصية التاريخية، مجلة العلوم الاجتماعية، جامعة عمار ثليجي الأغواط، عدد 21، نوفمبر 2016، صفحة 64.

[2]–أنظر الفقرة 3 من المادة 30 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المرجع السابق.

[3]–أنظر الفقرة 4 من نفس المادة.

[4]–انظر المادة 40 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المرجع السابق.

يبقى التعاون الدولي غير قادر على تحقيق الفعالية المرجوة منه، وبالتالي فتح المجال أمام المجرمين من أجل الزيادة في أنشطتهم الإجرامية واستغلال الدول ذات البنية التكنولوجيا الهشة، ليس فقط من أجل التعدي على مصالح هذه الدول، وإنما بتوجيه ضرباتهم حتى إلى الدول المتقدمة دون أن تستطيع هذه الأخيرة ترصد حركاتهم وكشفهم.

المطلب الثاني: استخدام التكنولوجيا الحديثة في رفع كفاءة الدول على مكافحة الإجرام

أصبح الإجرام يشكل رهانا للدول في مدى قدرتها على مكافحته، ذلك أن التحدي المفروض عليها يتمثل في مسايرة أجهزة إنفاذ القانون للحال الذي وصل إليه الإجرام، وذلك عن طريق تملك التكنولوجيا والأساليب الحديثة والتحكم فيها.

زيادة على ذلك، فإن الرفع من كفاءة أجهزة إنفاذ القانون لا يكون فقط من خلال ما تتخذ الدول على المستوى الوطني، وإنما حتى على المستوى الدولي، عن طريق التعاون في مجال التدريب وتبادل الخبرات.

الفرع الأول: التعاون الدولي في مجال التدريب للرفع من كفاءة الدول في استخدام التكنولوجيا الحديثة.

انشغلت الدول منذ ظهورها بأمر مكافحة الإجرام، وتسعى دائما إلى البحث عن أفضل السبل التي تقيها من شروره، بما في ذلك الرفع من كفاءة أجهزة إنفاذ القانون عن طريق التدريب بغية ضمان عدم إفلات الجناة من العقاب وكشف مختلف الأنشطة التي تم ارتكابها.

ويقصد بالتدريب في هذا المجال: "نشاط مخطط يهدف إلى إحداث تغييرات في الفرد والجماعة، وهذه التغييرات تشمل المعلومات والخبرات والمهارات ومعدلات الأداء، وطرق العمل والسلوك والاتجاهات بما يؤهل الفرد والجماعة إلى القيام بمهامهم بكفاءة وإنتاجية عالية و إحساس متزايد بالأمن والاستقرار المهني والوظيفي»[1].

وينطلق التدريب الفعال في مجال مكافحة الإجرام من ضرورة توفير أجهزة ومعدات وآليات تفوق من حيث التقنية الأجهزة المستخدمة من قبل المجرمين، مع الاعتماد على أساليب البحث العلمي، عن طريق توفير المعلومات والبيانات اللازمة واستغلالها في جميع المراحل الإجرائية[2].

يجسد التعاون الدولي في مجال التدريب سياسة الدول المنتهجة في مكافحة الإجرام، ذلك أنه يؤدي إلى الرفع من قدرات وكفاءات الأجهزة الأمنية الوطنية ومختلف الأجهزة الأخرى، عن طريق تمكينها إن التكنولوجيا الحديثة وإمدادها بمختلف الوسائل التقنية والعملية الحديثة وكذا المهارات العملياتية، وهو ما يجعل هذه الأجهزة على أهبة الاستعداد لمواجهة الإجرام ولو كان في حالة متطورة[3].

نصت العديد من الاتفاقيات التي تعنى بصنف معين من الجرائم على التعاون الدولي في مجال التدريب كآلية إستراتيجية للرفع من كفاءة الأجهزة الوطنية، عن طريق تزويدها بأحدث الوسائل والتقنيات والمهارات، نذكر

---

[1]–أحمد بدري، دور الشرطة في مكافحة جريمة غسل الأموال، الطبعة الأولى، دار النهضة العربية، القاهرة مصر، سنة 2012 صفحة 258.

[2]–كمال بوعباية– السعيد برابح، التدريب ودوره في مكافحة الجريمة عبر الوطنية، مجلة الدراسات والبحوث القانونية، مجلة علمية محكمة جامعة المسيلة CISSN 2676–1688، المجلد السادس، العدد الثاني 2021، صفحة 148.

[3]– محمد علي رهف القحطاني، الجريمة المنظمة، مطابع الحميضي، الرياض المملكة العربية السعودية، الطبعة الثالثة سنة 2013 صفحة 146.

منها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، التي حثت الدول الأطراف على أن التعاون فيما بينها في مجال التدريب والمساعدة التقنية بإعارة الأجهزة المكلفة بمكافحة الجرائم وتبادلهم، في إطار برنامج تتناول مختلف الطرائق والدروب والأساليب المستعملة، خاصة فيما يتعلق منها بالتكنولوجيا الحديثة[1].

ولا يقتصر التعاون الدولي في مجال الرفع من كفاءة أجهزة إنفاذ القانون على ما تقدمه الدول لبعضها البعض، وإنما يشمل حتى ما يمكن أن تقدمه أشخاص المجتمع الدولي الأخرى والهيئات الفاعلة فيها. فعلى سبيل المثال، تساعد المنظمة الدولية للشرطة الجنائية أجهزة الشرطة الوطنية والجهات الشريكة في تنمية كفاءاتها في مكافحة الاتجار بالسلع غير المشروعة، بتقديم دورات تدريبية للبلدان الأعضاء والشركاء في جميع أنحاء العالم لتعزيز الكفاءات وإرساء المعارف لدى جميع الأجهزة المعنية بمكافحة هذا النوع من الإجرام[2]، كذلك عقد دورات تدريبية عملية لتعزيز المهارات لتكون أجهزة الشرطة الوطنية قادرة على مواكبة التطورات التكنولوجية، وذلك بالحصول على الخبرات والكفاءات اللازمة للتعامل مع الجريمة الرقمية المتطورة على الأصعدة الدولية والإقليمية والوطنية[3].

بفضل اهتمام الجزائر بتبادل المؤهلات المتعلقة بمكافحة الإجرام وبعض سبله، تم عقد العديد من الاتفاقيات الثنائية، من أهمها الاتفاقية المبرمة مع إسبانيا في مجال الأمن ومكافحة الإرهاب والإجرام المنظم[4] إذ تضمنت هذه الاتفاقية العديد من صور التعاون في مجال التدريب المتعلق بالتكنولوجيا الحديثة، منها:

– التعاون على شكل تدابير بوليسية منسقة وتدابير المساعدة المتبادلة فيما يخص المستخدمين والعتاد على أساس ترتيبات تكاملية موقع عليها من طرف السلطات المختصة[5].

– تبادل مختصين بهدف اكتساب المعارف المهنية ذات المستوى الرفيع واكتشاف الوسائل والمناهج والتقنيات الحديثة لمكافحة الإجرام[6].

كذلك بالنسبة لاتفاق التعاون بين الجزائر وإيطاليا في مجال محاربة الإرهاب والإجرام المنظم والاتجار غير المشروع في المخدرات والمؤثرات العقلية والهجرة غير الشرعية[7]، حيث اشتمل هذا الاتفاق التزام الطرفين بالتعاون في مجال التكوين والتدريب، لاسيما التكوين المخصص وكذا ترقية هذا التعاون بين مؤسسات تكوين الشرطة في كلا البلدين[8].

---

[1]– أنظر المادة 29 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المرجع السابق.

[2]– التدريب في مجال مكافحة السلع عير المشروعة، متاح على الموقع الرسمي للإنتربول: interpol.int/ar/4/13/6

[3]– تطوير القدرات في مجال مكافحة الجريمة السيبرية، متاح على الموقع الرسمي للإنتربول: interpol.int/ar/4/6/3

[4]– اتفاقية بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا في مجال الأمن ومكافحة الإجرام المنظم، المصادق عليها بموجب المرسوم الرئاسي رقم 08–427 مؤرخ في 28 ديسمبر 2008، الجريدة الرسمية، عدد 05، بتاريخ 21 جانفي 2009.

[5]– الفقرة ب من المادة 2 من نفس المرجع.

[6]– الفقرة هـ من نفس المادة.

[7]– اتفاق التعاون بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الإيطالية في مجال محاربة الإرهاب والإجرام المنظم والاتجار غير المشروع في المخدرات والمؤثرات العقلية والهجرة غير الشرعية، المصادق عليه بموجب المرسوم الرئاسي رقم 07–374 مؤرخ في 01 ديسمبر2007 الجريدة الرسمية، عدد77، تاريخ 09 ديسمبر2007.

[8]– الفقرة 1 من المادة2 من نفس المرجع.

إضافة إلى ما سلف قد تساهم الهيئات الوطنية للبحث العلمي في تقديم المساعدة التقنية لدول أخرى عن طريق التدريب، كما هو الحال بالنسبة لجامعة نايف العربية للعلوم الأمنية، إذ تقدم برامج تدريبية متخصصة للعديد من الدول، تغطي الاحتياجات التدريبية للمستفيدين من العاملين في أجهزة الأمن الوطني ومكافحة الجريمة، قائمة بالأساس على تحليل المعلومات باستخدام التقنيات المتطورة والتحكم في وسائل الإثبات الحديثة كل ذلك من أجل الرفع من جاهزية هذه الأجهزة وإعداد كوادر مؤهلة في هذا المجال[1].

الفرع الثاني: التعاون الدولي في مجال تبادل الخبرات المتعلقة باستخدام التكنولوجيا الحديثة.

يسعى المجرم المعاصر إلى وضع مخطط أكثر تعقيدا لجرائمه، من أجل تجنب اكتشاف السلطات المختصة له وتجنب إلقاء القبض عليه، وهو بذلك أصبح ملما بسائر متطلبات النشاط الإجرامي، ومكتسبا لمهارات، محققا لما يصبوا إليه، ليس همه فقط الإفلات من العقاب، وإنما تجاوز الأجهزة المكلفة بمكافحة الإجرام في التسلح بالتكنولوجيا الحديثة[2].

والدول بهذا المعنى تكون غير قادرة بمفردها على تحقيق فعالية كبرى في مكافحة الإجرام، ما لم تتضافر الجهود فيما بينها لتطوير قدراتها للتحكم في التكنولوجيا الحديثة ومستجداتها، ولا يكون ذلك بطبيعة الحال، إلا عن طريق الاستفادة من الممارسات الفضلى والتجارب الناجحة وتبادل الخبرات.

يحقق التعاون الدولي بخصوص تبادل الخبرات أهدافا جمة، بعضها يتعلق بالتعرف على أحدث التطورات في مجالات الإجرام وأساليب مكافحتها، والبعض الآخر يرتبط بتقريب وجهات النظر وتوحيد المفاهيم بين الدول لتجنب الاختلاف الذي يمكن أن يقع بينها حول مسائل ذات الصلة بالقانون، عن طرق طرح الموضوعات والمشاكل ودراستها دراسة مشتركة لإيجاد الحلول لها[3]، وهو ما يؤدي في الأخير إلى توحيد الخبرات[4].

كما تساهم الهيئات الدولية المعنية بمكافحة الإجرام في تمكين الدول الأعضاء من الوسائل والتقنيات الفعالة وآخر ما توصلت إليه لتكنولوجيا الحديثة، سواء في مجال ارتكاب الجريمة أو في مجال مكافحتها، كما هو الحال بالنسبة للمنظمة الدولية للشرطة الجنائية التي تعمل على دعم أجهزة الشرطة الوطنية للدول الأعضاء بتوفير المعلومات والبيانات التي يمكن تبادلها وفق قنوات اتصال مأمونة[5] متاحة بنظام 24/7 الذي يعني بأنها متوفرة على مدار كل أيام الأسبوع ولمدة 24 ساعة في اليوم، وهذه البيانات تعتمد على تكنولوجيات متقدمة تتماشى مع المعايير الدولية[6]، بالإضافة إلى تسيير الأبحاث والتحاليل العلمية حول الإجرام، بشكل يفضي إلى فهم الجريمة وتعزيز التعاون الدولي بشأنها، وعقد ندوات لموظفي الشرطة لتبادل الآراء والخبرات[7].

---

[1] – دليل البرامج التعليمية لعام 2021، من إعداد جامعة نايف العربية للعلوم الأمنية، متاح على موقعها: mausse.edu.sa، ص25 وما يليها.

[2] – نصر شومان، المرجع السابق، صفحة 23.

[3] – علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، دراسة للإستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات، إيتراك للنشر والتوزيع، القاهرة مصر، سنة 2000، صفحة 90.

[4] – كمال بويعاية– السعيد برابح، المرجع السابق، صفحة 145.

[5] – Jean Michel LOUBOUTIN, Interpol et la lutte contre la criminalité organisée, ouvrage : La criminalité organisée. Droit français, droit international et droit comparé, LexisNexis, Paris France 2012, page 256.

[6] – قواعد البيانات، النشرة الإعلامية للإنتربول، متاحة على الموقع الرسمي للإنتربول. رمز الوثيقة: COM/FS/2016-03/GI-04

[7] – تحليل بيانات الاستخبار الجنائي، صحيفة وقائع تصدر عن الإنترول، متاحة على نفس الموقع، رمز الوثيقة: COM/FS/2014-05/CAS-01

كما تساهم بعض الهيئات الدولية ذات البعد الإقليمي في تعزيز التعاون بين أعضائها، فبالنسبة لمجلس وزراء الخارجية العرب يساهم في تدعيم الدول الأعضاء بالاستفادة من الخبرات الناجحة في مكافحة الإجرام وفي استخدام وسائل التكنولوجيا الحديثة في ذلك، بعقد العديد من المؤتمرات والاجتماعات منها مؤتمر قادة الشرطة والأمن العربي، مؤتمر رؤساء أجهزة المباحث والأدلة الجنائية ومؤتمر مدراء إدارات التدريب ومعاهد وكليات الشرطة والأمن العربي[1]. كذلك، تعمل جامعة نايف العربية للعلوم الأمنية على إثراء البحث العلمي في مجالات الدراسات الأمنية الإستراتيجية، وتقديم الاستشارات العلمية للدول بما يخدم التعاون الدولي في مكافحة الجريمة[2].

تمهد الاتفاقيات الدولية والمؤتمرات ذات الصلة بمكافحة الإجرام الطريق نحو رفع مستويات التخصص بالنسبة لأجهزة الدولة المعنية بذلك، وبتأطير المساعدة القانونية والتقنية المتبادلة بين الدول التي تشمل أفضل الممارسات العملياتية والبرامج المقررة في هذا المجال[3]. في هذا السياق أبرمت الجزائر عديد الاتفاقيات الثنائية الأطراف كأساس يعتمد عليه في تبادل الخبرات في مجال مكافحة الإجرام، استنادا إلى الاحترام المتبادل لسيادة كل طرف ومبدأ المعاملة بالمثل. منها الاتفاقية المبرمة بين الجزائر واسبانيا في مجال الأمن ومكافحة الإرهاب والإجرام المنظم مجالات التعاون المرتبطة بتبادل الخبرات ذات الصلة بالتكنولوجيا الحديثة، من أهمها:

– تبليغ المعلومات المتعلقة بمناهج الإجرام وأشكاله الجديدة وتبادل نتائج البحث في مجال التحقيق الجنائي وعلم الإجرام وتبادل المعلومات فيما بينهما حول مناهج التحقيق ووسائل مكافحة الإجرام الخاص بهما[4].

– المعلومات المتعلقة بالمناهج والتقنيات الحديثة للوقاية من الإرهاب ومكافحته[5] ونتائج أبحاث علم التحقيق الجنائي وعلم الإجرام التي تم القيام بها في مجالات الاتجار غير المشروع بالمخدرات والمؤثرات العقلية[6].

– تبادل المعلومات والخبرات والتجارب المهنية، نقل التكنولوجيا والمساعدة في مجال التجهيزات الخاصة وتبادل الوثائق المتخصصة[7].

كما تضمن اتفاق التعاون بين الجزائر وايطاليا في مجال الإرهاب والإجرام المنظم والاتجار غير المشروع في المخدرات والمؤثرات العقلية والهجرة غير الشرعية صورا للتعاون التكنولوجي في تبادل الخبرات، منها:

– تبادل المعلومات والتجارب حول الطرق والتقنيات في إطار الوقاية من الإرهاب ومحاربته[8]، في مجال الإجرام الإجرام الدولي المنظم[9] وفي مجال محاربة الاتجار غير المشروع في المخدرات والمؤثرات العقلية[10].

---

[1] – أنشطة المجلس على الصعيد العربي، وثيقة متاحة على الموقع الرسمي لمجلس وزراء الداخلية العرب: https://www.aim-council.org

[2] – نبذة عن الجامعة، الموقع الرسمي لجامعة نايف العربية للعلوم الأمنية: www.nausse.edu.sa

[3] – التعاون الدولي بما في ذلك التعاون على الصعيد الإقليمي لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، ورقة عمل من إعداد الأمانة، مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، الدوحة، من 12 إلى 19 أبريل 2015، رمز الوثيقة: A/conf.222/7

[4] – المطة (ج) و(د) من المادة 2 من الاتفاقية بين الجمهورية الجزائرية الديمقراطية الشعبية والمملكة الاسبانية، المرجع السابق.

[5] – المطة (د) من المادة 3 من نفس المرجع.

[6] – المطة (ب) من المادة 4 من نفس المرجع.

[7] – أنظر المادة 6 من نفس المرجع.

[8] – أنظر الفقرة (أ) من المادة 2 من اتفاق التعاون بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الايطالية، المرجع السابق.

[9] – المطة (3) من الفقرة (ب) من نفس المادة.

[10] – المطة (2) من الفقرة (ج) من نفس المادة.

– تبادل المعلومات حول المعارف واستعمال الوسائل التقنية المستخدمة في مجال محاربة الجريمة المنظمة بكل أشكالها[1].

المبحث الثاني: استخدام التكنولوجيا الحديثة في التعاون الدولي العملياتي في مكافحة الإجرام.

تتحدد سياسة الدول في مكافحة الإجرام من خلال إقرار خطط واستراتيجيات متعددة، بعضها يكون ذا طابع وقائي يهدف إلى الحلول دون وقوع الجرائم، والبعض الآخر ذو طابع ردعي يتجلى في مجموعة الإجراءات التي ينبغي اتخاذها من وقوع الجريمة إلى غاية تنفيذ الحكم الصادر فيها القاضي بالإدانة.

والأصل أن التعاون الدولي المؤسسي يوصف بأنه تعاون وقائي، إذ أنه يهدف إلى بناء قدرات الدول وأجهزتها لمواجهة أي طارئ يحدث، عن طرق التحكم في التكنولوجيا والوسائل التقنية والرفع من كفاءة هذه الأجهزة، لكن قد يطال التعاون الدولي حتى مرحلة ما بعد وقوع الجريمة، بخصوص التحري والتحقيق فيها وكذا التواصل والاتصال، مع اشتراط استخدام التكنولوجيا الحديثة في ذلك بما يحقق الفعالية المرجوة.

المطلب الأول: استخدام التكنولوجيا الحديثة في التعاون الدولي المتعلق بمباشرة البحث والتحري.

تعد مرحلة البحث والتحري من أهم المراحل التي تمر بها الدعوى العمومية، ذلك أنها تؤدي إلى الوصول إلى المعلومة التي تتجسد في تهيئة كل ما يلزم لإعداد القضايا جزائيا[2]، ساهم في ذلك بالدرجة الأولى الاستخدام الاستخدام الأمثل للتكنولوجيا الحديثة، إذ أصبح في متناول المحققين وأعضاء الضبطية القضائية عامة، وسائل تقنية متطورة تساعد بشكل كبير في اكتشاف الأدلة التي يتركها المجرمون، كأجهزة الإعلام الآلي والآلات الكاشفة للبصمات وآلات التصوير الحراري التي تحدد وقت فرار المجرم ومغادرته لمكان وقوع الجريمة ضمن فترة زمنية معقولة تلي ارتكاب الجريمة[3].

لكن، يثبت الواقع أن العديد من المجرمين استطاعوا أن ينفذوا بأنشطتهم الإجرامية دون ضبطهم، بفضل مهاراتهم الفائقة وتحكمهم الكبير في وسائل التكنولوجيا المتطورة، بشكل فاق حتى قدرة أجهزة إنفاذ القانون في ذلك. لذا فإن التعاون الدولي في مجال البحث والتحري ينبغي أن يبنى على معطيات ترتبط بالتكنولوجيا الحديثة وبتسخيرها في كل العمليات المتخذة في هذا الميدان، سواء كانت تتعلق بالبحث والتحقيق المشترك أو بالبحث والتحقيق الانفرادي.

الفرع الأول: استخدام التكنولوجيا الحديثة في الإنابة القضائية الدولية.

استطاع المجرمون تدويل أنشطتهم الإجرامية عبر الدول والقارات بفضل العولمة وما أفرزته من وسائل اتصال ومواصلات متطورة، أدت إلى إزالة القيود والعقبات التي كانت مفروضة نتيجة رسم الحدود السياسية للدول. بهذا المعنى، قد يقع وأن ترتكب جريمة في دولة معينة وتبقى مادياتها السلوك الإجرامي حبيسة إقليمها في حين أن نتائجها تقع قي دولة أخرى، فلا تكون للدولة المتضررة القدرة على لم شتات الجريمة وأدلة الثبات فيها دون تعاون مع الدولة التي وقعت فيها.

---

[1] – الفقرة 2 من المادة 2 من اتفاق التعاون بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الايطالية، المرجع السابق.

[2] – قادري أعمر، التعامل مع الأفعال في القانون الجزائي العام، دار هومة للطباعة والنشر، الجزائر، سنة 2012، صفحة 19.

[3] – نصر شومان، المرجع السابق، صفحة 9.

يتجسد التعاون الدولي في هذه الحالة من خلال نظام الإنابة القضائية الذي يعرف بأنه: " قيام سلطة قضائية تابعة لدولة أجنبية باتخاذ إجراء أو أكثر من إجراءات التحقيق، وذلك لحساب سلطة قضائية مختصة تابعة لدولة أخرى من أجل الوصول إلى كشف الحقيقة في قضايا جنائية"[1].

نظم المشرع الجزائري أحكام الإنابة القضائية الدولية من خلال قانون الإجراءات الجزائية في المادتين 71 و722 منه، وكذلك بموجب نصوص قانونية خاصة معنية بمكافحة بعض صور الإجرام، كما هو الحال في قانون الوقاية من الفساد ومكافحته[2] وقانون الوقاية من تبييض الأموال وتموين الإرهاب ومكافحتهما[3].

تستند الإنابة القضائية على مبدأ المعاملة بالمثل وتتم في إطار اتفاقيات أو ترتيبات ثنائية أو متعددة الأطراف، تقوم على أساس فكرة التعايش المشترك بين النظم القانونية، تبررها ضرورات عملية تتعلق باستحالة اتخاذ كافة إجراءات التحري والتحقيق بشأن الدعوى المرفوعة أمام الجهات القضائية لدولة معينة دون تدخل دولة أخرى[4].

وحتى تتحقق النتائج المرجوة من التعاون الدولي في مكافحة الإجرام ينبغي أن تتحلى الدولة المطلوب منها اتخاذ إجراء من إجراءات البحث والتحري بالإرادة الجادة وباستخدام كل وسائل التكنولوجيا الحديثة في التقصي والكشف للوصول إلى الأدلة الكافية في الإدانة، حتى تستطيع الدولة الطالبة مباشرة اختصاصها بالنظر في الدعوى العمومية. كما أن التعاون الدولي في هذه الحالة يقتضي أن تتبنى الدول أساليب التحري الخاصة في تشريعاتها الوطنية، حتى تكون قادرة على مباشرة هذه الأساليب نيابة عن دولة أخرى.

تساهم العديد من أساليب التحري الخاصة المعتمدة على التكنولوجيا الحديثة، في تفعيل الخطط المنتهجة في مكافحة الإجرام بين الدول، المتخذة في سياق الإنابة القضائية، من أهمها:

<u>أولا:</u> استخدام التكنولوجيا في التعاون الدولي المرتبط بنظام الاختراق.

ظهرت الحاجة الملحة إلى اعتناق أساليب تحر خاصة نتيجة التطور الذي شهده الإجرام، من ذلك نظام الاختراق الذي يقوم على مبدأ التحقيق المسبق دون انتظار وقوع الجريمة[5]، حتى لا يقع أي تضليل للمحققين ورجال العدالة، خصوصا وأن وسائل الإجرام الحديثة بإمكانها أن تؤدي إلى إخفاء الآثار المترتبة عن الجريمة المرتكبة[6].

---

[1] – علي سالم علي سالم النعيمي، المواجهة الجنائية للجريمة المنظمة، دراسة مقارنة، رسالة دكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق بجامعة عين شمس، سنة2011، صفحة 296.

[2] – أنظر المادة 57 من القانون رقم 06-01 مؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية، عدد 14، بتاريخ 08 مارس 2006، معدل ومتمم.

[3] – أنظر المادة 30 من القانون رقم 05-01 مؤرخ في 6 فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية عدد 11، بتاريخ 9 فبراير 2005، المعدل والمتمم.

[4] – بن عودة نبيل– درعي العربي، الإنابات القضائية الدولية في المجال الجزائي، مجلة القانون الدولي والتنمية، مجلة دولية محكمة تصدرها جامعة عبد الحميد بن باديس مستغانم، ISSN : 2353-0111، المجلد 7، العدد 2019/02، صفحة 148.

[5] – شريف سيد كامل، شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة مصر، الطبعة الأولى، سنة 2013، صفحة 235.

[6] – أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، دراسة مقارنة للضمانات النظرية والتطبيقية المقررة للمشتبه فيه في التشريع الجزائري والتشريعات الأجنبية والشريعة الإسلامية ، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية سنة 2011، صفحة 209.

حدد المشرع الجزائري الأحكام المتعلقة بنظام الاختراق تحت تسمية التسرب في المواد من 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية[1]، وكذلك في بعض القوانين الخاصة كما هو الحال في قانون الوقاية من الفساد ومكافحته[2] وكذلك قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3].

ولما كانت أغلبية الجرائم في الوقت الحالي عابرة للحدود، تعتمد على وسائل الاتصال الحديثة، فإن نظام الاختراق المنفذ، تبعا لطلب الإنابة القضائية الدولية، ينبغي أن يقوم على التوغل داخل هذه الوسائل فالمؤسسات الضبطية في عديد الدول تقوم بتجنيد عناصرها أو بالاعتماد على الغير، كمقدمي الخدمات مثلا للدخول إلى العالم الافتراضي، وبالأخص المواقع التي تفتح حلقات للنقاش وقاعات الدردشة، أو الاتصال المباشر، بالاستعانة بأسماء وصفات مستعارة ووهمية، قصد البحث والتحري عن الجريمة المطلوبة[4] وتقديم الأدلة الأدلة الكافية حولها إلى الدولة الطالبة للإنابة من أجل المتابعة الجزائية لمرتكبيها.

<u>– المراقبة الالكترونية:</u>

يشكل الإثبات حجر الزاوية في المسائل الجزائية، يرتبط بكل جهد قضائي متخذ في سبيل إظهار الحقيقة[5] الحقيقة[5] من ذلك المراقبة الالكترونية التي تعد وسيلة ناجحة يمكن أن تؤدي إلى الوصول إلى استقصاء أدلة كافية تزود بها الدولة الطالبة للإنابة لاعتمادها على تقنية الترصد.

يقتضي الإثبات الجزائي عدم قبول أي دليل تم التوصل إليه بطريق غير مشروع[6]، وهو ما دفع العديد من من دول العالم، كما هو الحال بالنسبة للجزائر، إلى التكريس التشريعي لنظام المراقبة الالكترونية في مجال البحث والتحري عن الجرائم، ما يعني أن استعمال هذا الأسلوب قد يؤدي إلى استقصاء الأدلة اللازمة في حالة ما إذا طلب منها اتخاذ هذا الإجراء في إطار الإنابة القضائية الدولية.

يجد نظام المراقبة الالكترونية في الجزائر أساسه القانوني من خلال قانون الإجراءات الجزائية، الذي حدد أحكامه في المواد من 65 مكرر 05 إلى 65 مكرر 10، فتنفيذا للإنابة القضائية الدولية الواردة يمكن لوكيل الجمهورية المختص، إذا اقتضت ضرورات التحري في جرائم معينة، القيام بما يلي:

– اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية،

– وضع ترتيبات تقنية قصد التقاط وتثبيت وتسجيل الكلام أو التقاط الصور[7].

---

[1] – الأمر رقم 66–155، مؤرخ في 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد 48، بتاريخ 10 جوان 1966، المعدل والمتمم.

[2] – أنظر المادة 56 من القانون رقم 06–01، المرجع السابق.

[3] – أنظر المادة 16 من القانون رقم 09–04، المرجع السابق.

[4] – غزالي لخضر، التحريات المستحدثة في جرائم التكنولوجيا الحديثة، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلة دولية محكمة تصدر عن كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة 7684–2661: EISSN المجلد 5، العدد 2020/1، صفحة 975.

[5] – محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان الأردن، سنة 2015، صفحة 21.

[6] – نفس المرجع، صفحة 214.

[7] – أنظر المادة 65 مكرر 05 من قانون الإجراءات الجزائية.

في ذات الاتجاه، تضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها عديد الأساليب التي تصب في مجال المراقبة الالكترونية التي يمكن أن تحقق النجاعة المطلوبة في تنفيذ الإنابات القضائية الدولية، خاصة وأنها تعتمد على استعمال وسائل تكنولوجيا متقدمة، ولعل من أهم هذه الأساليب ما يلي:

– مراقبة الاتصالات الإلكترونية في حالة صعوبة الوصول إلى نتيجة تهم البحث الجاري دون اللجوء إلى ذلك[1].

– تفتيش المنظومات المعلوماتية، ولو كان ذلك عن بعد، مع الاعتماد على نظام المساعدة إذا كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني طبقا للاتفاقيات الوطنية ووفقا لمبدأ المعاملة بالمثل[2].

– حجز المعطيات المعلوماتية إذا كانت المعلومات المخزنة مفيدة في الكشف عن الجرائم أو مرتكبيها[3].

– الحجز هن طريق منع الوصول إلى المعطيات، وذلك باستعمال التقنيات المناسبة لمنع الوصول إلى المعلومات التي تحتويها المنظومة المعلوماتية أو نسخها[4].

<u>الفرع الثاني:</u> استخدام التكنولوجيا الحديثة في التحريات والتحقيقات المشتركة.

تتطلب مكافحة الإجرام في بعض الحالات اتخاذ إجراءات تتجاوز العمل الانفرادي لكل دولة، باللجوء إلى التحريات والتحقيقات المشتركة التي تساهم فيها الأجهزة المكلفة بإنفاذ القانون التابعة لدولتين فأكثر، خاصة إذا كان المجرمون يتنقلون بين الدول بأنفسهم أو بأنشطتهم الإجرامية.

نصت في هذا الاتجاه اتفاقية الأمم المتحد لمكافحة الجريمة المنظمة عبر الوطنية على ضرورة أن تتخذ الدول الأعضاء جميع الوسائل من أجل إنشاء هيئات تحر أو تحقيق مشتركة بينها، بما في ذلك إبرام اتفاقيات أو ترتيبات ثنائية أو متعددة الأطراف، مع اعتبار أن هذا الإجراء جائز اللجوء إليه حتى في حالة عدم وجود أي اتفاقية أو ترتيب شريطة أن يتم الاتفاق على كل حالة على حدة وبالاحترام التام لسيادة الدولة التي سيجري التحقيق أو التحري داخل إقليمها[5].

وفي هذه الحالة ينبغي أن تتخذ التحريات والتحقيقات المشتركة باستخدام وسائل التكنولوجيا الحديثة، التي تعد همزة الوصل بين الأجهزة الأمنية لمختف الدول المشاركة من أجل توحيد الجهود وتنسيقها، بغية تحقيق نتائج ايجابية في تعقب المجرمين والوصول إلى المعلومات في أوانها وتمريرها في وقتها المناسب.

<u>الفرع الثاني:</u> استخدام التكنولوجيا الحديثة في التنسيق بين أجهزة إنفاذ القانون.

غالبا ما يكون الدليل الجرمي ماديا يتألف من أشياء مادية تدرك بالحواس وتكون كافية للدلالة على الإدانة أو البراءة. لكن بعض الجرائم الحديثة تتم في بيئة لا علاقة لها بالماديات، كالأوراق والمحررات الورقية

---

[1] – أنظر المادة 4 من القانون رقم 09-04، المرجع السابق.

[2] – أنظر المادة 5 من نفس المرجع.

[3] – أنظر المادة 6 من نفس المرجع.

[4] – أنظر المادة 7 من نفس المرجع.

[5] – أنظر المادة 19 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المرجع السابق.

حيث تتم في إطار افتراضي يمكن الجاني، وباستغلال نبضات إلكترونية لا تدركها الحواس، من ارتكاب جريمته ثم التلاعب بكل ما يمكن أن يؤدي إلى اكتشافها[1].

إذا كان من السهولة بمكان ضبط المعلومات والأشياء المتعلقة بجريمة ما في السابق، فإن ما وصل إليه حال الإجرام جعل هذه المهمة أمرا صعبا. وهو ما يعني أن القواعد التقليدية المطبقة في مجال التعاون الدولي لن تكون فعالة في أي بحث أو تحر ما لم تدعم بآليات مستحدثة وتسخيرها في ربط أي تنسيق بين الدول.

<u>أولا:</u> استخدام التكنولوجيا الحديثة في الاتصال الدائم بين الأجهزة الوطنية للدول.

أصبح الإجرام في الوقت الحالي يشكل تحديا للقواعد التقليدية نتيجة ما يثيره من مشاكل قانونية وعملية تواجه الجهود المبذولة لمكافحته على الصعيد الإجرائي، وبالأخص ما تعلق منها بسلطات التحري والملاحقة وبضبط الجريمة وإقامة الدليل فيها. فمثلا في مجال الجرائم الالكترونية فإن المسرح المعنوي الذي ارتكبت فيه الجريمة قد يتضمن ما يسمح بالوصول إلى دليل ارتكابها، بتتبع عناصرها، كتحديد العنوان الالكتروني ونوع الجهاز المستخدم والمكان الذي وقعت فيه، لكن الأمر ليس بهذا القدر من البساطة، إذ قد يعمد المجرمون مباشرة بعد ارتكاب الجريمة إلى إخفاء ومحو آثارها، من خلال عدة طرق كمسح الملفات الموجودة على الجهاز المستعمل وإخفاء العناوين الالكترونية وتغيير الأرقام السرية.

ولا تقتصر المشكلات العملية المتعلقة بالبحث والتحري على الجرائم الالكترونية، أو بصفة عامة الجرائم المرتكبة باستخدام التكنولوجيا الحديثة، بل قد ترتبط حتى بالجرائم التقليدية، بفضل تعدد وسائل المواصلات وتقدمها يمكن أن ينتقل المجرم بكل يسر وسهولة بين الدول والقارات، ففي الوقت الذي تبحث عنه دولة ما تجده قد انتقل إلى دولة أخرى، وبمجرد علمها بذلك يكون قد انتقل إلى وجهة أخرى.

لمواجهة هذه المشاكل يعد التواصل الدائم بين الأجهزة الأمنية للدول الأساس في ضمان الحصول على الأدلة في الجريمة المرتكبة وضبط مقترفيها، وذلك بتوفير المعلومات في أوانها واستخدامها في وقتها لمباغتة الجاني ومنع إفلاته تمهيدا لعرضه على السلطات الوطنية المختصة بمحاكمته أو معاقبته على حسب الأحوال.

يقع على عاتق الدول الالتزام بنظام يكفل جمع وتوفير المعلومات وتبادلها فيما بينها، فإذا استطاع المجرمون إقامة علاقات في بيئة اتصال بينهم، لتوفير المعلومات الكافية لارتكاب أنشطتهم الإجرامية، فإنه من باب أولى ينبغي أن تتفاعل الدول من أجل خلق نظام يضمن تدفق المعلومات وإيصالها في حينها.

استطاعت المنظمة الدولية للشرطة الجنائية الوصول إلى ضمان التنسيق بين أجهزة الشرطة الوطنية للدول المنتمية إليها، باستخدام وسائل التكنولوجيا المتطورة، وذلك من خلال ما يلي:

– التعاون المباشر بين المكاتب المركزية الوطنية التابعة للدول الأعضاء في المنظمة[2]، من خلال توفير خدمات اتصالات شرطية عالمية مأمونة، وكذلك خدمات بيانات ميدانية وقواعد بيانات شرطية[3].

---

[1] – نصر شومان، المرجع السابق، صفحة 119 وما يليها.

[2] – عكروم عادل، المنظمة الدولية للشرطة الجنائية كآلية لمكافحة الجريمة المنظمة، دراسة مقارنة، دار الجامعة الجديدة للنشر، الإسكندرية مصر، سنة 2013، صفحة 144.

[3] – لمحة عن منظمة الإنتربول، وثيقة متاحة على الموقع الرسمي للشرطة الجزائرية: www.Algerie police.dz

– التبادل السريع والآني للمعلومات الشرطية والجنائية، وكذلك تجميع المعلومات العملياتية[1].

– تعقب المجرمين والجرائم المرتكبة، وتسهيل وتفعيل عمليات إلقاء القبض عليهم وتسليمهم[2].

– إصدار النشرات الدولية التي تعد بمثابة تنبيهات دولية لتبادل المعلومات والتهديدات الأمنية[3].

كذلك تقوم المنظمة الأوربية للشرطة الجنائية بعدة مهام تصب في تعزيز التعاون بين الدول المنضوية تحتها، لاسيما في المجال التكنولوجي المتعلق بالاستقصاء وتوفير المعلومات، وذلك بخلق نظام متطور لتبادل المعطيات المرتبطة بالبحث والتحري في جرائم معينة وتوزيعها بعد تجميعها داخل جميع أجهزة التعاون الدولي[4].

على المستوى الوطني، نص اتفاق التعاون بين الجزائر وايطاليا في مجال محاربة الإرهاب والإجرام المنظم والاتجار غير المشروع في المخدرات والمؤثرات العقلية والهجرة غير الشرعية على إمكانية الاتصال المباشر بين أجهزة إنفاذ القانون للبلدين لتنفيذ هذا التعاون[5]، لضمان تبادل المعلومات في أوانها، منها التعرف على الهوية والبحث عن الأشخاص الذين ارتكبوا الجنايات المنصوص عليها في التشريعات الوطنية لكلا البلدين، المنظمات الإجرامية الدولية وشبكات التهريب[6].

غير أن الاتفاقيات الأخرى لم تتضمن الإشارة إلى إمكانية التواصل الدائم وتسخير وسائل التكنولوجيا الحديثة في ذلك، فعلى سبيل المثال تضمن اتفاق التعاون بين الجزائر وفرنسا الإشارة إلى أن التعاون يكون وفقا للطرق الدبلوماسية عن طريق الوزراء المعنيين الذين يقومون بتعيين الهيئات المكلفة بتنفيذ مختلف مجالات التعاون[7]، وأن المعطيات الاسمية المتعلقة بالتحري والتحقيق لا ترسل إلا للسلطات المختصة، ولا يمكن إرسالها إلى سلطات أخرى إلا بالموافقة الكتابية للطرف المرسل[8]، وهو ما يعيق التعاون في هذه الحالة.

<u>ثانيا:</u> استخدام التكنولوجيا الحديثة في التواصل بين الأجهزة الوطنية للدول.

يعد التعاون الدولي ضرورة تضاف إلى اعتبار مبدأ تخصص السلطات الوطنية في مكافحة الإجرام الداخلي، يجسد النظام الدولي العام لحماية المصالح المشتركة للمجتمع الدولي[9].

يتم التواصل بين الدول في مجال المساعدة المتبادلة استنادا إلى أحكام الاتفاقيات الثنائية والمتعددة الأطراف القائمة على العلاقات الدولية والوسائل الدبلوماسية[10]، حيث تحدد هذه الاتفاقيات الإجراءات التي ينبغي اعتمادها من تقديم الطلبة من الدولة الطالبة إلى تنفيذه من طرف الدولة المطلوب منها.

---

[1] – لمحة عن منظمة الإنتربول، المرجع السابق.

[2] – أحمد البدري، المرجع السابق، صفحة 332.

[3] – منظومة النشرات الدولية، صحيفة وقائع تصدر عن الإنتربول، رمز الوثيقة: COM/FS/2015-02/GI-02

[4] - Michel QUILLE, Europol, ouvrage : La criminalité organisée, sous la direction de Marcel LECLERC, la documentation Française, Paris 1996, page 265.

[5] – أنظر المادة 10 من اتفاق التعاون بين الجزائر وايطاليا في مجال محاربة الإرهاب والإجرام المنظم والاتجار غير المشروع في المخدرات والمؤثرات العقلية والهجرة غير الشرعية، المرجع السابق.

[6] – أنظر المطة (1) و(02) من الفقرة أ من المادة 1 من نفس المرجع.

[7] – أنظر المادة 8 من نفس المرجع.

[8] – أنظر الفقرة 3 من المادة 9 من نفس المرجع.

[9] – سليمان عبد المنعم، دروس في القانون الجنائي الدولي، دار الجامعة الجديدة، الإسكندرية مصر، سنة 2005، صفحة 79.

[10] – علاء الدين شحاته، المرجع السابق، صفحة 117.

وما يميز الاتفاقيات المتخذة في سياق المساعدة القضائية طول الإجراءات وتعقيدها، مع إضفاء الرسمية على كل إجراء متخذ، فعلى سبيل المثال نصت اتفاقية الرياض العربية للتعاون القضائي على أن المساعدة المطلوبة تتم عن طريق وزارة العدل لدى كل من الدولتين الطالبة والمطلوبة[1]، ونصت اتفاقية التعاون القضائي في المجال الجزائي المبرمة بين الجزائر وايطاليا على أن إرسال الطلبات يتم بواسطة وزارة العدل مع إمكانية أن يتم ذلك عن الطريق الدبلوماسي[2].

غير أن اتخاذ الإجراءات المحددة في الاتفاقيات المذكورة أعلاه قد يؤدي إلى إفراغ التعاون الدولي من محتواه بعدم الحصول على أي نتيجة تذكر، ذلك أن الوصول إلى الأدلة المطلوبة لا يكون إلا في المراحل الأولى من وقوع الجريمة، وأن أي تأخر في اتخاذ الإجراء المناسب سيؤدي إلى طمس كل ما تعلق بالجريمة المرتكبة والتعتيم عليها.

إحساسا بأهمية التواصل الفوري غير المقيد بالإجراءات الشكلية، نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على أنه: "يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي، ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل، بما في ذلك الفاكس أو البريد الالكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك استخدام التشفير) وتأكيد الإرسال حسبما تطلب الدولة الطرف، ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الاتصالات"[3].

لأغراض ذلك، نص قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه: "يمكن، في حالات الاستعجال، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولي أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني"[4].

ولتفعيل إجراءات الاتصال السريع في مجال المساعدة الدولية المتبادلة لابد من تضمين اتفاقيات التعاون في المجال الجزائي هذه الإجراءات، إذ بدونها يبقى ما نصت عليه الاتفاقية العربية لمكافحة جرائم تقنية المعلومات والقانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مجرد نصوص قانونية سوف لن يكتب لها التنفيذ.

---

[1] – أنظر المادة 15 من اتفاقية الرياض العربية للتعاون القضائي الموقعة في الرياض بتاريخ 6 أبريل 1983، المصادق عليها بموجب المرسوم الرئاسي رقم 01-47 مؤرخ في 11 فبراير 2001، الجريدة الرسمية، عدد 11، بتاريخ 12 فبراير 2001.

[2] – أنظر المادة 7 من الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الايطالية، الموقعة بالجزائر بتاريخ 22 جويلية 2003، المصادق عليها بموجب المرسوم الرئاسي رقم 05-73 مؤرخ في 13 فبراير 2005، الجريدة الرسمية عدد 13، بتاريخ 16 فبراير 2005.

[3] – الفقرة 3 من المادة 32 الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[4] – الفقرة 2 من المادة 16 من القانون رقم 09-04، المرجع السابق.

الخاتمة:

من خلال ما سبق تتضح، بما لا يدع مجالا للشك، أهمية التكنولوجيا الحديثة ووسائلها في تدعيم التعاون الدولي في مجال مكافحة الإجرام الذي ما فتئ يغير أسلوبه وصوره في كل مرة، بشكل يتحدى به حتى الأجهزة الأمنية والقضائية الوطنية للدول وقدرتها على مواجهته.

من هذا المنطلق ينبغي على الدول، إذا ما أرادت أن تحقق تعاونا فعليا في مجال مكافحة الإجرام أن تعيد حساباتها في الوسائل المقررة في هذا المجال وأن تعنى في سياستها الداخلية والخارجية بالتكنولوجيا الحديثة باعتبارها حجر الزاوية في اتخاذ الإجراءات اللازمة لمواجهة الأنشطة الإجرامية التي استشرت في وقتنا الحالي بطريقة فظيعة يندى لها الجبين.

كما أن نجاح أي سياسة متخذ من قبل الدول في مجال مكافحة الجريمة يستلزم، بالدرجة الأولى، تقدير الخطورة الإجرامية بقدرها، ثم إيجاد الوسائل الكفيلة لتحقيق الفعالية المرجوة، ولا يكون ذلك إلا من خلال تملك التكنولوجيا الحديثة والتحكم بها، مع تحميل الدول المسؤولية هذا المجال، بالتعاون فيما بينها نقل التكنولوجيا لبعضها البعض وتبسيط استعمالها بتبادل التدريب والخبرات والمسائل التقنية.

إضافة إلى ذلك، لا ينبغي النظر إلى التعاون الدولي على أساس تلك النظرة الضيقة، القائمة على استخدام الوسائل التقليدية في التواصل والاتصال، وإنما ينبغي ضمان المراقبة المستمرة والتواصل الدائم بين أجهزة إنفاذ القانون في الدول، قصد تشديد الخناق على المجرمين وتقييد أنشطتهم الإجرامية، ولا يكون ذلك إلا باستعمال وسائل الاتصال السلكية واللاسلكية الحديثة والرقمنة التي تعد هي السمة البارزة للتواصل في العصر الحالي، وتجسيدها كوسائل للاتصال بينها في طلبات المساعدة المتبادلة في مختلف المجالات التي يقتضيها التعاون.

وفي الأخير يمكن القول أنه ينبغي على الدول أن تتحلى بإرادة جادة في تعاونها مع الدول الأخرى في مكافحة الإجرام، وبإعلاء المصالح المشتركة بينها وعدم التمسك بالنظرة الضيقة لمبدأ السيادة، مع السعي دائما إلى إبرام المزيد من اتفاقيات التعاون وتحيين تلك الموجودة بين الحين والآخر لضمان مسايرة أحكامها للتطور الحاصل في المجتمع.

المراجع:

أولا: المراجع باللغة العربية.

1- المؤلفات:

- أحمد بدري، دور الشرطة في مكافحة جريمة غسل الأموال، الطبعة الأولى، دار النهضة العربية، القاهرة مصر 2012.
- أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، دراسة مقارنة للضمانات النظرية والتطبيقية المقررة للمشتبه فيه في التشريع الجزائري والتشريعات الأجنبية والشريعة الإسلامية، دار هومة للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية 2011.
- سليمان عبد المنعم، دروس في القانون الجنائي الدولي، دار الجامعة الجديدة، الإسكندرية مصر 2005.
- شريف سيد كامل، شرح قانون العقوبات، القسم العام، دار النهضة العربية، القاهرة مصر، الطبعة الأولى 2013.
- عثمانية لخميسي، عولمة التجريم والعقاب، دار هومه للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية 2008.
- عكروم عادل، المنظمة الدولية للشرطة الجنائية كآلية لمكافحة الجريمة المنظمة، دراسة مقارنة، دار الجامعة الجديدة للنشر الإسكندرية مصر 2013.
- علاء الدين شحاته، التعاون الدولي لمكافحة الجريمة، دراسة للإستراتيجية الوطنية للتعاون الدولي لمكافحة المخدرات، إيتراك للنشر والتوزيع، القاهرة مصر 2000.
- علي محمد جعفر، السياسة الجزائية في ظل نظام العولمة، المؤسسة الجامعية للدراسات والنشر لبنان، الطبعة الأولى 2013.
- قادري أعمر، التعامل مع الأفعال في القانون الجزائي العام، دار هومة للطباعة والنشر، الجزائر 2012.
- محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي، دراسة مقارنة، دار الثقافة للنشر والتوزيع، الأردن 2015.
- محمد علي رهف القحطاني، الجريمة المنظمة، مطابع الحميضي، الرياض المملكة العربية السعودية، الطبعة الثالثة 2013.
- مختار شبلي، الإجرام الاقتصادي والمالي الدولي وسبل المكافحة، دار هومه للطباعة والنشر والتوزيع، الجزائر، الطبعة الثانية منقحة ومزيدة 2012.
- نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، بدون دار نشر، الطبعة الأولى 2011.

2- الأطروحات والمقالات العلمية:

- علي سالم علي سالم النعيمي، المواجهة الجنائية للجريمة المنظمة، دراسة مقارنة، رسالة دكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق بجامعة عين شمس، سنة2011.
- بن عودة نبيل- درعي العربي، الإنابات القضائية الدولية في المجال الجزائي، مجلة القانون الدولي والتنمية، مجلة دولية محكمة تصدرها جامعة عبد الحميد بن باديس مستغانم، ISSN : 2353-0111، المجلد 7، العدد 2019/02، صفحة 148.
- سهى حمزاوي، نقل التكنولوجيا إلى الدول النامية بين حتمية مدرسة التبعية ومنطق الخصوصية التاريخية، مجلة العلوم الاجتماعية، جامعة عمار ثليجي الأغواط، عدد 21، نوفمبر 2016.
- غزالي لخضر، التحريات المستحدثة في جرائم التكنولوجيا الحديثة، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، مجلة دولية محكمة تصدر عن كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة EISSN :2661-7684 المجلد 5 العدد 2020/1.
- كمال بوعباية- السعيد برابح، التدريب ودوره في مكافحة الجريمة عبر الوطنية، مجلة الدراسات والبحوث القانونية، مجلة علمية محكمة جامعة المسيلة، CISSN 2676-1688، المجلد السادس، العدد الثاني 2021.

3- الاتفاقيات والوثائق الدولية:

- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتخذة رقم 25، الدورة 55، المؤرخة في تشرين الثاني/نوفمبر 2000، وثيقة رقم A/RES/55/25.

– وثيقة: تقرير عن اجتماع الفريق العامل المعني بالتعاون الدولي، المعقود في فيينا يومي 27 و28 أكتوبر 2015، مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، صفحة 2، رمز الوثيقة CTOC/COP/WG.3/2015/4.
– آليات التعاون الدولي الرسمية، الوحدة التعليمية 7: التعاون الدولي على مكافحة الجريمة الإلكترونية، متاح على موقع مكتب الأمم المتحدة المعني بالمخدرات والجريمة.
– التعاون الدولي بما في ذلك التعاون على الصعيد الإقليمي لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، ورقة عمل من إعداد الأمانة، مؤتمر الأمم المتحدة الثالث عشر لمنع الجريمة والعدالة الجنائية، الدوحة، من 12 إلى 19 أبريل 2015، رمز الوثيقة: A/conf.222/7
– اتفاقية الرياض العربية للتعاون القضائي الموقعة في الرياض بتاريخ 6 أبريل 1983، المصادق عليها بموجب المرسوم الرئاسي رقم 01–47 مؤرخ في 11 فبراير 2001، الجريدة الرسمية، عدد 11، بتاريخ 12 فبراير 2001.
– الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الايطالية، الموقعة بالجزائر بتاريخ 22 جويلية 2003، المصادق عليها بموجب المرسوم الرئاسي رقم 05–73 مؤرخ في 13 فبراير 2005، الجريدة الرسمية عدد 13، بتاريخ 16 فبراير 2005.
– اتفاق التعاون بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الإيطالية في مجال محاربة الإرهاب والإجرام المنظم والاتجار غير المشروع في المخدرات والمؤثرات العقلية والهجرة غير الشرعية، المصادق عليه بموجب المرسوم الرئاسي رقم 07–374 مؤرخ في 01 ديسمبر 2007، الجريدة الرسمية، عدد77، تاريخ 09 ديسمبر 2007.
– اتفاقية بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا في مجال الأمن ومكافحة الإجرام المنظم، المصادق عليها بموجب المرسوم الرئاسي رقم 08–427 مؤرخ في 28 ديسمبر 2008، الجريدة الرسمية، عدد 05، بتاريخ 21 جانفي 2009.
– أنظر المادة 14 من الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، المصادق عليها بموجب المرسوم الرئاسي رقم 14–252 مؤرخ في 8 سبتمبر 2014، الجريدة الرسمية، عدد 57، بتاريخ 28 سبتمبر 2014.

3– النصوص القانونية:

– الأمر رقم 55–166، المؤرخ في 5 جوان 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، عدد 84، بتاريخ 24 ديسمبر 2006، المعدل والمتمم.
– القانون رقم 05–01 مؤرخ في 6 فبراير 2005، يتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، الجريدة الرسمية، عدد 11، بتاريخ 9 فبراير 2005، المعدل والمتمم.
– القانون رقم 06–01 مؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية، عدد 14، بتاريخ 08 مارس 2006، المعدل والمتمم.
– القانون رقم 09–04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، بتاريخ 16 أوت 2009.

ثانيا: المراجع باللغة الفرنسية

- Jean Michel LOUBOUTIN, Interpol et la lutte contre la criminalité organisée, ouvrage : La criminalité organisée. Droit français, droit international et droit comparé, LexisNexis, Paris France, 2012.
- Michel QUILLE, Europol, ouvrage : La criminalité organisée, sous la direction de Marcel LECLERC, la documentation Française, Paris 1996.

المواقع الإلكترونية:

– موقع المنظمة الدولية للشرطة الجنائية: **interpol.int**
– الموقع الرسمي لمجلس وزراء الداخلية العرب: **https://www.aim-council.org**
– موقع جامعة نايف العربية للعلوم الأمنية: **www.nausse.edu.sa**
– الموقع الرسمي للشرطة الجزائرية: **www.Algerie police.dz**

جامعة الجزائر 01

بن يوسف بن خدة

كلية الحقوق و العلوم السياسية

قسم الحقوق

الملتقى الدولي الإفتراضي الموسوم بـــ

" **القانون الجنائي في ظل التطور التكنولوجي – إشكالات و معالجات** – "

المعلومات	**المتدخل**
اللقب و الإسم	قادري نور الهدى
الرتبة	طالبة الدكتوراه قانون إداري متخصص
المؤسسة الجامعية	جامعة سيدي بلعباس – جيلالي اليابس –
كلية	كلية الحقوق و العلوم السياسية
القسم	الحقوق
المخبر البحث	مخبر المرافق العمومية و التنمية
محور المداخلة	**المحور الخامس:** تأثير الوسائل العلمية الحدية على الإثبات الجنائي
عنوان المداخلة	**الأشعة الغير المرئية ودورها في الإثبات الجنائي**
البريد الالكتروني	Inasse223@gmail.com
رقم الهاتف	06.59.57.53.64

ملخص :

تعتبر الأشعة الغير المرئية وسيلة من أهم الوسائل العلمية الحديثة الناتجة عن التطورات التكنولوجية الحديثة التي عرفها العالم في العقود الأخيرة من الزمن ، والتي إتسعت مجال إستخدامتها في محال خدمة العدالة الجنائية، و ذلك نظرا للدور الفعال الذي تلعبه في مجال الإثبات الجنائي من خلال الكشف عن ما تعجز عنه الحواس البشرية عن طريق الكشف العديد عن الجرائم و الأساليب الخفية التي يتبعوها المجرمين لم يكن بإمكان فك ألغازها بوسائل الإثبات التقليدية .

الكلمات المفتاحية : التطور التكنولوجي ، أدلة الإثبات الجنائي ، الأشعة الغير المرئية .

Abstract:

Invisible rays are considered one of the most important modern scientific methods resulting from modern technological developments that the world has known in recent decades, and which have expanded their use in criminal justice services, due to the effective role they play in the field of criminal proof by revealing what The human senses are incapable of revealing many of the crimes and the hidden methods that criminals use that could not be deciphered by traditional means of proof.

Keywords: Technological development, criminal proof evidence, invisible radiation.

مقدمة :

لقد أتاح التطور التكنولوجي الذي أصاب وسائل الإتصال الحديثة الإنتقال من الإثبات التقليدي إلى نوع جديد يتسم بالطابع الإلكتروني . إذ أصبحت عملية تبادل المعلومات و البيانات و إثباتها سهلة وميسرة بفضل التقنية المعلوماتية و التكنولوجيات الحديثة ، التي قد تم إستغلالها في مجال الإثبات الجنائي نظرا للقصور الأجهزة و الوسائل التقليدية خاصة في ظل تطور أنواع الجرائم و أساليب المجرمين فظهرت العديد من وسائل العلمية الحديثة تماشيا و الثورة التكنولوجية القادرة على تحقيق العدالة الجنائية .

وفي هذا الإطار تعتبر أدلة الإثبات الإلكتروني خاصة في مجال الجنائي من بين المواضيع القانونية الجديدة التي أثارت إهتمام جانب من الفقه القانوني وكذا رجال العدالة ، نظرا لما تحتله هذه الأخيرة من أهمية بالغة في الكشف عن ما تعجز عنه الحواس البشرية و الكشف عن الأثار الخفية للجرائم و تحقيق السرعة و الفعالية في التحقيقات الجنائية المطولة و المعقدة ، و من بين الوسائل العلمية الحديثة على غرار جهاز كشف الكذب و كذا البصمة الوراثية .و تعتبر الأشعة الغير المرئية دليل من أدلة الإثبات الجنائي التي إتسعت مجال إستخدامتها في مجال خدمة العدالة، و ذلك نظرا للدور البارز الذي تلعبه في عملية التحقيق الجنائي من خلال الكشف عن ملبسات الجريمة و الأساليب الخفية التي يتبعوها المجرمين.

و عليه تهدف هذه الدراسة إلى تبيان أهمية الدور التي تلعبه الأشعة الغير المرئية التي مكنت المحققين الجنائيين و رجال العدالة في الكشف عن المجرمين و إثبات إرتكابهم لجرائم لم يكن بإمكان فك ألغازها بوسائل الإثبات التقليدية ، فيكون بذلك ضمير القاضي مطمئنا لما يصدر عنه من أحكام ، بما لا يدع لديه مجالا للشك في إمكانية صواب قراره من عدمه ، و بالتالي شعور بالطمأنينة لدى المجني عليه أو ذويه، بأن الجاني الحقيقي هو الذي نال عقابه ، و ليس شخص آخر .

ومن هنا يثيرنا التساؤل حول دور هذه الأخير بإعتبارها كدليل علمي حديث من أدلة الإثبات الجنائي في تحقيق العدالة الجنائية .

و للإجابة عن هذا التساؤل سيتم تقسيم موضوع بحثنا المحورين الآتين هما :

- **المحور الأول :** مفهوم الأشعة الغير المرئية .
- **المحور الثاني :** دور الأشعة الغير المرئية في الإثبات الجنائي .

و سيتم إتباع المنهج التحليلي الوصفي من خلال تبيان مفهوم الأشعة الغير المرئية و إبراز دورها في مجال الإثبات الجنائي بإعتباها دليل من بين الأدلة العلمية الحديثة التي لها دورا بارز في مجال تحقيق العدالة الجنائية .

المحور الأول : مفهوم الأشعة الغير المرئية

إن التطور العلمي الملحوظ في مجال تقنية المعلومات ، و ما استتبعه من تعدد للأدلة العلمية وفقا للظروف كل قضية ووسيلة إرتكابها ، وما يفرزه مسرح الجريمة من أثار تعتمد في إستخراجتها على التقنيات العلمية الحديثة ،و التي لا يمكن تحديدها على سبيل الحصر ، بل تتكاثر مع التقدم العملي و التطور الحديث للحياة في مجال البحث الطبي و الإلكترونيات و غيرها من الوسائل الحديثة التي تخدم البشرية ، غيرها أنها توسع نطاق إستخدامها لتعد بذلك كأدلة علمية تستخدم في مجال الإثبات الجنائي من بينها الأشعة الغير المرئية.

و عليه سوف نحاول من خلال هذا المحور التعرف على هذه الأشعة و أنواعها بإعتبارها كدليل علمي حديث يعتد به في الإثبات الجنائي .

أولا : تعريف الأشعة الغير المرئية

نظرا للتطور أنواع الجرائم وتطور الأساليب التي يتبعوها المجرمين ، كان لا بد من تطور الأدلة البحث و التحري بما يتوافق و التطورات التكنولوجية الحاصلة . الأمر الذي دفعنا الفضول للتعرف على ماهية الأشعة الغير المرئية بإعتبارها دليل علمي حديث من أدلة الإثبات الجنائي نظرا للدور الفعال التي تلعبه هذه الأخير في الكشف عن العديد من الجرائم و ذلك من خلال :

أ- تعريف الأشعة غير المرئية

إن الله تعالى – جل جلاله – قد أعطانا القدرة على رؤية الأوان أشعة الطيف السبعة، و هي الأحمر و البرتقالي ، و الخضر، و الأزرق ، و البنفسجي وهي أشعة مرئية ضوئية (كهرومغناطسية) . غير أن هناك أشعة غير مرئية التي تعد وسيطا لتسجل ما لا تراه العين البشرية ، وقد حاول العلماء الإستفادة منها لخدمة الإنسان ، و لقد إتسعت مجالات إستخدامها إلى مجال العدالة التي أصبحت تعتبر دليلا علميا حديثا يتم الإستعانة للكشف عن ملابسات الجريمة و الكشف عن الأساليب الخفية التي يتبعوها المجرمين في إرتكابها[1].

---

[1] – آمال عبد الرحمن يوسف حسن ، الأدلة العلمية الحديثة و دورها في الإثبات الجنائي ، رسالة قدمت لإستكمال لمتطلبات الحصول على درجة الماجستير في القانون العام ، قسم القانون العام ، كلية الحقوق ، جامعة الشرق الأوسط 2012/2011 ، ص 99 .

فهي عبارة عن أشعة لا يراها الإنسان ، و لكن تأثيرها تظهر على أفلام التصوير الفوتوغرافية الحساسة ، تستخدم هذه الأشعة في إظهار البصمات الغير الواضحة ، بقع الدماء و غيرها من الأشياء الموجودة في مسرح الجريمة ، و قد ساعد إستخدام تلك الأشعة في الكشف عن العديد من الجرائم كالكشف عن التزوير في المستندات و الأعمال الفنية وكذا إظهار البصمات الكامنة، وبقع الدم، ومكان تواجد السائل المنوي، وفي مجالات كثيرة . [1]

ب – أهمية الأشعة غير المرئية :

إن من بين المسؤوليات الملقاة على عاتق خبراء الشرطة العلمية هي البحث و التحري بهدف كشف الجريمة و إزالة الغموض عنها, خاصة في ظل تقدم طرق الإجرام وتفنن المجرمين في ارتكابها من خلال استخدام العلوم والوسائل الحديثة التي تسهل عليهم ارتكابها وتساعدهم في الإفلات من أيدي رجال الشرطة ، ولذلك كان لزاما على خبراء الشرطة العلمية أن تستعين بنفس سلاح المجرم وتطور أسلوبها في مجابهة من خلال استخدام أحدث الأدوات والأساليب والأجهزة العلمية المتطورة حتى يكتشف و يدحض خاصة فيما الأساليب الإجرامية المبتكرة التي ينتهجها المجرمون مهما بلغت من تطور، يتعلق بالآثار الجنائية المتحصل عليها من موقع الجريمة [2] .

تلعب الأشعة الغير المرئية بإعتبارها من بين التقنيات التكنولوجية الحديثة دورا في بارزا في الإثبات الجنائي و مساعدة ضباط الشرطة القضائية و العلمية في الكشف عن العديد من الجرائم و الأدلة الخفية التي تعجز عنها الأدلة الإثبات التقليدية إكتشافها، و الكشف عن الأساليب الحديثة التي يتبعوها المجرمين في ارتكاب العديد الجرائم خاصة في ظل التطور التكنولوجي الذي يعيشه العالم في الأونة الأخيرة و التي تطورت معه أساليب إرتكاب الجرائم التي أصبحت تتميز بنوع من التعقيد و صعوبة إكتشافها ، فكان من الضروري إيجاد في المقابل وسائل علمية حديثة من شأنها المساعدة للوصول إلى الحقيقة و تحقيق العدالة الجنائية ، كفحص المستندات المزورة و المطموسة و المحررة بأحبار متعددة ، و كذا الكشف عن الصور المقلدة و المزورة ، و إظهار الكتابات الخفية .

---

[1] – رياض عبد الفتاح ، تصوير مالا تراه العين بالأشعة الغير المرئية ، د ط ، دار النهضة العربية ، القاهرة ،ص 01 .

[2] – مراد عبد الفتاح ، التحقيق الجنائي التطبيقي ، دار الكتب و الوثائق الرسمية ، مصر ، 1995 ، ص 201 .

ثانيا : مدى مشروعية الأشعة الغير المرئية بإعتبارها دليل علمي حديث في الإثبات الجنائي

لكي يكون الدليل مقبولا في القانون الوضعي ، يجب أن تكون وسيلة الحصول مشروعة ، بمعنى أن تكون الإجراءات التي إتبعت للحصول على الدليل مطابقة للأحكام و القواعد وفقا للإجراءات الواردة في التشريع ، فإذا كان الدليل قد وصل بوسيلة غير مشروعة أصبح لا قيمة له ، فمن الأصول الدستورية الكبرى في نظام الدولة الديمقراطية ما يعرف بمبدأ إلتزام القانون أو سيادة القانون ، و تعتبر قاعدة شرعية الجرائم و العقوبات إحدى الدعائم الأساسية التي ترتكز عليها التشريعات الجنائية منها و التشريعات المعاصرة [1]، و معناها لا جريمة و لا عقوبة إلا بنص وهو ما تبناه المشرع الجزائري ضمن نص المادة الأولى من قانون العقوبات الجزائري .

فمبدأ مشروعية الدليل الجنائي بصفة عامة و الدليل الجنائي العلمي الحديث على وجه الخصوص بما تتضمنه من مخرجات كمبيوتر أو تسجيلات صوتية ومرئية أو الهاتف او التلكس أو وسائل الخبرة العلمية أو غيرها من الأدلة العلمية الحديثة بما فيها الأشعة الغير المرئية ، التي تعني بضرورة إتفاق الإجراء مع القواعد القانونية و الأنظمة الثابتة في وجدان المجتمع المعاصر [2] .

و عليه يمكننا القول أن بمشروعية الدليل المستمد من الوسائل العلمية الحديثة أن إستخدام هذه الأخيرة في الإثبات ، و عدم مشروعية إستخدامها ، تكمن في التنصت و التجسس أو الإعتداء بالإكراه لأخذ الدليل أو شهادة الشهود ، و عليه يقتضي للإضفاء المشروعية على الدليل العلمي المستمد من الوسائل العلمية الحديثة أن تكون الإجراءات التي إتبعت في الحصول على هذا الدليل متطابقة مع أحكام الشريعة و القانون[3]، بما فيها الأشعة الغير المرئية التي تعد بذلك من بين الأدلة العلمية الحديثة التي أصبحت وسيلة من الوسائل العلمية التي تستخدم في المجال خدمة العدالة الجنائية ، نظرا للدور الفعال التي تلعبه في الكشف عن العديد الجرائم و الأساليب المتطورة التي يتبعوها المجرمين في إرتكابها بحيث أصبحت يعتمد عليها قضائيا في الإثبات الجنائي .

---

[1] – أبكر علي عبد المجيد أحمد ، عادل محمد عبد الله عبد الباقي ، مدى حجية الوسائل العلمية الحديثة في الإثبات من منظور التشريعات السودانية،المجلة الأكاديمية للبحوث القانونية و السياسية ، المجلد الثاني ، العدد الرابع ، جامعة عمار ثليجي ، الأغواط ، ص 593 .

[2] – مرجع نفسه ، ص 593 .

[3] – مرجع نفسه ،ص 594 .

المحور الثاني : دور الأشعة الغير المرئية في مجال الإثبات الجنائي

تعد الأشعة الغير المرئية إحدى وسائل الإستدلال التي قد يلجأ إليها ضباط الشرطة القضائية للوصول إلى الحقيقة والكشف عن ملابسات الجريمة و الأساليب الخفية التي يتبعها المجرمين وتأخذ الأشعة الغير المرئية عدة أنواع سوف نحاول التعرف عليها من خلال :

أولا :التصوير بالأشعة فوق البنفسجية والأشعة تحت الحمراء ودورهما في الإثبات في المجال الجنائي

يعد التصوير بالأشعة فوق البنفسجية و الأشعة تحت الحمراء من بين أكثر أنواع الأشعة الغير المرئية إنتشارا و إستعمالا خاصة في مجال الإثبات الجنائي ، و هو ما يدفعنا للتعرف علن الدور الذي اللذان يلعبانه في تحقيق العدالة الجنائية و الكشف عن ملابسات الجريمة . و ذلك من خلال :

أ- الأشعة فوق البنفسجية و دورها في الإثبات الجنائي :

توجد الأشعة فوق البنفسجية في الطبيعة في ضوء الشمس ، و يمكن الحصول عليها عن طريق التحليل الضوئي الطبقي ، و تتراوح أطول موجاتها بين 136 . و 3900 وحدة أنجستروم ، و توجد في الجزء الغير المرئي من الأشعة .[1]

وتعد الأشعة فوق البنفسجية هي نوع من أنواع الأشعة الغير المرئية ، التي لا ترى بالعين المجردة و لا يمكن الحصول عليها بالعين المجردة ،و يمكن الحصول عليها بالطرق العلمية و ذلك للإستفادة منها في العديد من المجالات بما فيها المجال الإثبات الجنائي ، حيث تستخدم هذه التقنية في المعامل الجنائية للكشف و إثبات بعض الجرائم التي يصعب إكتشافها و إثباتها بالطرق العادية[2] .

و تستخدم الأشعة فوق البنفسجية في مجال الإثبات الجنائي خاصة فيما يخص الكشف تزوير المستندات التي قد يكون بالحف (أي يكون بالحذف جزء من المستند) ، أو يكون بالإضافة من خلال إضافة حروف أو أرقام أو يكون بالحذف و الإضافة معا، وكذا تستخدم للكشف عن حالة تزوير الشيكات

---

[1] – آمال عبد الرحمن يوسف حسن ، المرجع السابق ، ص 100 .

[2] – مرجع نفسه ،ص 100 .

لهذا تلجأ معظم ، البنوك إلى فحص الشيكات التي يشتله فيها بواسطة الأشعة فوق البنفسجية قبل صرفها .[1]

كما و تستخدم الأشعة فوق البنفسجية في التأثير على بعض المواد عند تعرضها و تعطي توهجا مميزا على المادة مما يساعد على فحص هذه المواد المتعلقة بالجريمة فحصا دقيقا سواء في المواقع الحادث أو داخل المعمل الجنائي ، كما يساعد في فحص الأثار المادية للجريمة الغير الظاهرة بالعين المجردة، كما و تستخدم هذه الأشعة في جرائم الحرائق و تخريب و الآداب ، إضافة تستخدم في مجال تحليل بقع الدم ، و تساعد على التعرف على إظهار الآثار الناتجة و المسببة للجريمة .[2]

على غرار ما سبق تستخدم الأشعة فوق البنفسجية في البحث عن الحوادث الجنسية إذ تستطيع هذه الأخيرة عن التمييز الحيوانات المنوية عن إفرازات الجسم الآخرى ، كما تتبع عن حوادث الإغتصاب في الكشف عن الأماكن التي تم الضغط عليها من قبل الجاني [3].

ب – الأشعة تحت الحمراء و دورها في مجال الإثبات الجنائي .

تعتبر الأشعة تحت الحمراء نوع من أنواع الأشعة الغير المرئية و المسؤولة عن التأثير الحراري لضوء الشمس ، و تتراوح أطول موجاتها من 7600 إلى 5000.000 وحدة أنجستروم ، و يمكن الحصول عليها عن طريق إمرار الضوء من خلال مرشحات ضوئية خاصة .[4]

و تستخدم الأشعة تحت الحمراء في مجال الإثبات الجنائي خاصة فيما يتعلق بإظهار الكتابة على الأوراق المحترقة جزئيا ، أو إظهار الكتابة بالحبر السري على الورق ، و كذا كشف في حالة التزييف الأوراق المالية (ذلك لأن المزيف للأوراق المالية لا يستخدم واحد للألوان كما الورقة الأصلية بل عدة ألواح كل منها بلون) و من المعروف أن إمتصاص الألوان للأشعة تحت الحمراء يختلف من لون لآخر

---

[1] – رياض عبد الفتاح ، المرجع السابق ، ،ص 100

[2] – فايق عوضن محمد تحفة ، حدود استبعاد أدلة تقنيات الذكاء الاصطناعي الجنائية والعلمية المتحصلة بطرق غير مشروعة "دراسة مقارنة بين النظامين الأنجلوسكسوني واللاتيني" ، مجلة روح القوانين ، العدد 91 ، يوليو 2020 ، ص 785 .

[3] – آمال عبد الرحمن يوسف حسن ، المرجع السابق ، ص 101 .

[4] – مرجع نفسه ، ص 101 .

كما و تستخدم في إكتشاف بقع الدم على الأقمشة السوداء و الكشف عن بقع على الملابس مثل الزيوت و آثار البارود .[1]

كما و تستخدم في مراحل البحث عن آثار البارود في حوادث استخدام للأسلحة النارية وكذلك تحديد المسافة بين القاتل و القتيل ، وبالتالي فهي تفيد في تحديد فيما إذا كان الحادث انتحار من عدمه من خلال الكشف على يد القتيل بواسطة الأشعة تحت الحمراء بحثا عن آثار بارود محترق، كما تستخدم في التمييز بين أنواع الأنسجة المختلفة ذات الألوان المتشابهة التي تظهر للعين المجردة بلون واحد ولو كان لون أبيض[2].

ثانيا : دور أشعة X و أشعة جاما في الإثبات الجنائي .

تعتبر أشعة **X** و أشعة جاما نوعا من أنواع الأشعة الغير المرئية التي أصبحت تستخدم في مجال خدمة العدالة الجنائية، و ذلك نظرا للدور البارز الذي تلعبه في مجال الإثبات الجنائي. و عليه سوف نحاول التعرف عليهما و التعرف على الدور الذي يلعبانه للوصول إلى الحقيقة من خلال :

أ – دور الأشعة X في مجال الإثبات الجنائي .

توجد الأشعة **X** في الجزء الغير المرئي من أشعة الشمس ، يمكن الحصول عليها بإمرار التيار الكهربائي داخل أنبوب مفرغة من الهواء، و تتمتع بقدرتها في إختراق بعض المواد حسب تفاوت وزنها فكلما زاد الوزن النوعي قلت الدرجة النفاذية و الإختراقية. وتستخدم كدليلا في مجال الإثبات الجنائي .[3]

و يتمثل دور الأشعة **X** في مجال الإثبات الجنائي فيما يلي :

– تستخدم أشعة في فحص حالات محو لإستظهار الكتابة التي محيت و التي إستخدم في كتابتها معادن ثقيلة مثل للحديد و النحاس .

– التعرف على الكتابة المدونة على الخطابات داخل ظروفها ، و التي تقع داخل الأوراق الملتصقة مثل الطوابع البريد .

---

[1] – رياض عبد الفتاح ، المرجع السابق ، ص 103 .

[2] – فايق عوضن محمد تحفة ، المرجع السابق ، ص 785 .

[3] – آمال عبد الرحمن يوسف حسن ، المرجع السابق ، ص 104 .

– وفي المستندات المحترقة والكتابات التي حررت بأحبار تحت وي على معادن ثقيلة مثل الرصاص .[1]

ب– الأشعة السينية دورها في مجال الإثبات الجنائي :

وهي كذلك أشعة غير منظورة ذات موجات قصيرة وهي تستخدم من قبل عناصر الشرطة العلمية في الكشف عن القنابل ، إنما في تلك الأماكن أو المناطق التي تواجه تهديدا دائما بالقنابل كالمطارات ومكاتب الخدمات الحكومية و المراكز العسكرية ومراكز الشرطة . كما تستخدم في الكشف عن محتويات الحقائب و الطرود بحثا عن أي دليل في التحقيق الجنائي ، كما تختص هذه الأشعة في الكشف عن الأشياء التي لا يستطيع الميكروسكوب كشفها ، ولها قدرة الاحتراق للأشياء القابلة للبحث عن الرصاص كالجدران ومن باب أول كالأخشاب ، و البحث عن ذرات البارود المتناثرة على المسرح ، وأجسام الكائنات الحية لتحديد سن الجثث من خلال نمو أعضاء جديدة وتحديد كل ما يبتلعه الجاني من أشياء .[2]

كما و تستخدم الأشعة السينية في المجال الجنائي في البحث عن الأجسام الغريبة واختبار المعادن وتسجيل بصمات الأصابع، وفحص الأقمشة والمنسوجات .[3]

و تجدر الإشارة انه لقد لجأت إليه الشرطة الأمريكية ، لا سيما تلك التي تستخدم تقنية التنقيب من خلال الأشعة تحت الحمراء ، و التي تعد هذه التقنية ذات أصل عسكري، وقد عملت الشرطة على تطويرها و إستخدامها لغرض ملاحقة الجناة ، لما تسمح به من إمكانية رؤية ما يحدث خلف الجدران و تحديد مكان الأشخاص المفقودين و الهاربين ، فضلا عن إمكانية إستخدامها في الحياء السكنية للحصول على " صورة حرارية " لبعض المساكن التي يزرع فيها نبات البانجو المخدر[4] .

---

[1] – آمال عبد الرحمن يوسف حسن ، المرجع السابق ، ص 105 .

[2] – علاء الدين سليماني ، دور الشرطة العلمية في إثبات الجريمة ، مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص قانون الجنائي ، قسم الحقوق ، كلية الحقوق و العلوم السياسية ، جامعة محمد خيضر – بسكرة – 2014/2013 ص 21 .

[3] – فايق عوضن محمد تحفة ، المرجع السابق ، ص 785 .

[4] – مرجع نفسه ، ص 786 .

خاتمة :

و عليه يمكننا القول من خلال دراستنا لموضوع الأشعة الغير المرئية ودورها في مجال الإثبات الجنائي أنه يعد موضوعا مهما و جد حيويا ، خاصة في ظل عصر الثور المعلوماتية ، النى تغيرت معها أنواع الجرائم و الأساليب التي يتعبوها المجرمين ، الأمر الذي بات من الضروري تغيير و تطوير وسائل و أساليب البحث و التحري.

و بذلك تعد الأشعة الغير المرئية من بين الأدلة العلمية الحديثة في مجال الإثبات الجنائي التي تلعب دورا بارز في تحقيق العدالة الجنائية من خلال الكشف عن الجرائم و الأساليب الخفية التي يتبعوها المجرمين .

من خلال هذه الدراسة توصلنا إلى مجموعة من **النتائج** يمكن أن نستخلصها فيما يلي :

- لقد لعبت التطورات التكنولوجية الحديثة دورا بارزا في تطوير الوسائل البحث والتحري عن الجرائم و الكشف عن الأساليب الحديثة التي يعتمد عليها المجرمين في إرتكابها.
- تساعد التقنيات التكنولوجية الحديثة في الكشف على أنواع الجرائم و مكان وقوعها ، و التنبؤ بالأماكن التي ستشكل بؤرا للإجرام مستقبلا .
- تعتبر الأشعة الغير المرئية من بين الأدلة الإثبات الحديثة التي يعتد بها أمام القضاء الجنائي.
- تعد الأشعة الغير المرئية من بين الأدلة العلمية الحديثة التي لها دورا بارز في عملية التحقيق الجنائي من الكشف عن الجرائم و الأساليب الخفية التي يتبعوها المجرمين.
- وجود العديد من الأدلة المادية الموجودة في مسرح الجريمة ، و التي لا يمكن رؤيتها بالعين المجردة ، مثل البصمات الكامنة ، و بقع الدم التي تم غسلها و التي لا يمكن إكتشافها إلا عن طريق الأشعة الغير المرئية مثل الأشعة فوق البنفسجية ، و الأشعة تحت الحمراء والأشعة **x** و الأشعة السينية .

و لقد توصلنا من خلال دراستنا لموضوع الأشعة الغير المرئية ودورها في مجال الإثبات الجنائي إلى مجموعة من **التوصيات** التي تتمثل فيما يلي :

- ضرورة مواكبة قانون الإجراءات الجزائية للتطورات التكنولوجية الحديثة نظرا للتطور الهائل الذي مس الجانب الإجرامي .
- على المشرع الجزائري تبني التقنيات التكنولوجية الحديثة التي من شأنها مساعدة ضباط الشرطة القضائية في مجال البحث و التحري عن الجرائم و الكشف عن الأساليب الحديثة التي يتبعوها المجرمين في إرتكابها .
- تنظيم دورات تدريبية للأعوان الشرطة القضائية فيما يخص الإستفادة التقنيات الحديثة والإعتمادة عليها في مجال الإثبات الجنائي .
- ضرورة نشر الثقافة الإلكترونية وسط المجتمع من خلال تنظيم حملات و ندوات علمية حول كيفية إستغلال التكنولوجيات الحديثة في مختلف تصرفاتهم القانونية .

قائمة المراجع :

أولا : **الكتب**

- رياض عبد الفتاح ، تصوير مالا تراه العين بالأشعة الغير المرئية ، د ط ، دار النهضة العربية القاهرة .
- مراد عبد الفتاح ، التحقيق الجنائي التطبيقي، دار الكتب و الوثائق الرسمية، مصر، 1995.

ثانيا : الأطروحات و المذكرات العلمية

1 – مذكرات الماجستير

- آمال عبد الرحمن يوسف حسن ، الأدلة العلمية الحديثة و دورها في الإثبات الجنائي ، رسالة قدمت لإستكمال لمتطلبات الحصول على درجة الماجستير في القانون العام، قسم القانون العام كلية الحقوق ، جامعة الشرق الأوسط ، 2012/2011.

2- **مذكرات الماستر**

- علاء الدين سليماني ، دور الشرطة العلمية في إثبات الجريمة ، مذكرة مقدمة لنيل شهادة الماستر في الحقوق تخصص قانون الجنائي ، قسم الحقوق ، كلية الحقوق و العلوم السياسية جامعة محمد خيضر – بسكرة – 2014/2013 .

ثالثا : المقالات العلمية :

- أبكر علي عبد المجيد أحمد ، عادل محمد عبد الله عبد الباقي ، مدى حجية الوسائل العلمية الحديثة في الإثبات من منظور التشريعات السودانية ، المجلة الأكاديمية للبحوث القانونية و السياسية ، المجلد الثاني ، العدد الرابع ، جامعة عمار ثليجي ، الأغواط .
- فايق عوضن محمد تحفة ، حدود استبعاد أدلة تقنيات الذكاء الاصطناعي الجنائية والعلمية المتحصلة بطرق غير مشروعة "دراسة مقارنة بين النظامين الأنجلوسكسوني واللاتيني" مجلة روح القوانين ، العدد 91 ، يوليو 2020

مداخلة الملتقى الدولي الموسوم ب: القانون الجنائي في ظل التطور التكنولوجي

اشكالات ومعالجات

اللقب: حيمي

الاسم: سيدي مُحَمَّد

الوظيفة: أستاذ جامعي

الرتبة العلمية: أستاذ محاضر« أ »

التخصص: قانون خاص

المؤسسة: جامعة أبو بكر بلقايد – تلمسان –

الهاتف: 0552948609

عنوان البريد الإلكتروني: mohammed.himmi45@gmail.com

محور المداخلة: المحور الخامس: تأثير الوسائل العلمية الحديثة على الاثبات الجنائي

مداخلة بعنوان: "اشكالات استخدام المراقبة الالكترونية في اجراءات التحري والاثبات الجنائيين"

مقدمة:

تعتبر العملية الإثباتية عملية لا تتم بصورة عشوائية، وإنّما هي منهجية منتظمة ترتكز على قواعد أساسية يمكن اعتبارها معطيات تتشابك فيما بينها في مختلف مراحل الدعوى العمومية، منذ ارتكاب الواقعة الجرمية حتى صدور حكم فيها، فالإثبات والتفتيش الجنائيين يعتبران نشاطان إجرائيان موجهان مباشرة للوصول إلى اليقين القضائي طبقاً لمعيار الحقيقة الواقعية[1].

[1] لؤي عبد الله نوح، مدى مشروعية المراقبة الإلكترونية في الإثبات الجنائي، مركز الدراسات العربية للنشر والتوزيع، ط1، 2018، ص.21.

تُثير مسألة الإثبات في نظم الحاسوب والإنترنت صعوبات كبيرة أمام القائمين على التحقيق، وذلك لجملة من الأمور، نذكر منها: التخزين الإلكتروني للمعطيات الذي يجعلها غير مرئية، إضافةً إلى أنّ انعدام الدليل المرئي يُشل عقبة كبيرة أمام كشف هذه الجرائم[1].

كما تتعقد المشكلة عندما يتعلق الأمر بمعلومات أو بيانات تمّ تخزينها في الخارج بواسطة شبكة الاتصال عن بُعد، والقواعد التقليدية في الإثبات لا تكفي لضبط مثل هذه المعلومات بحثاً عن الأدّلة وتحقيقها، فمن الصعب إجراء التفتيش للحصول على الأدّلة في هذه الحالة داخل أدّلة أجنبية باعتبار هذا الإجراء يتعارض مع سيادة الدولة الأخيرة[2].

ولما كانت أدّلة الإثبات المتحصلة من التفتيش على نظم الحاسوب والإنترنت تحتاج إلى خبرة فنيّة ودراسة فائقة في هذا المجال[3]، فإنّ نقص خبرة سلطات جمع الاستدلالات والتحقيق والمحاكمة قد يؤدي إلى ضياع الدليل بل تدميره أحياناً.

لعلّ الوسائل المستحدثة وعلى رأسها المراقبة الإلكترونية قد ساهمت بشكل معتبر في ملاحقة مجرمي المعلومات وكشف جرائمهم، إلاّ أنّها قد أبرزت جانباً خطيراً آخر وهو الاعتداء على حرمة الحياة الخاصة وسرّية الاتصالات والمراسلات[4].

بالإضافة لِما تقدم من صعوبات وإشكالات، يثور التساؤل عمّا إذا كان الدليل المستمّد من التفتيش والإثبات الجنائيين له شرعية قانونية لاكتشاف هذا النوع من الجرائم المستحدثة.

---

[1] لمزيد من المعلومات أنظر، سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، دار النهضة العربية، القاهرة، ط1، 1999، ص.95.

[2] لؤي عبد الله نوح، المرجع السابق، ص.09.

[3] يتردّد الضحايا في الجرائم المعلوماتية عن كشف المعلومات حول ما يقع عليهم أو مؤسساتهم خوفاً من فقدان الثقة أو الإساءة لسمعة مؤسساتهم والتبعات الاقتصادية المترتبة على ذلك. أنظر، الرائد جمال الكركي، جرائم الحاسوب ودور مديرية الأمن في مكافحتها، ورقة بحثية مقدمة إلى ندوة القانون حماية حق المؤلف المنعقدة في عمان بتاريخ 1997/07/05، ص.10 وما يليها.

[4] بن بادة عبد الحليم، المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني بين الحق في الخصوصية ومشروعية الدليل الإلكتروني، المجلة الأكاديمية للبحث القانوني، المجلد 10، العدد 03، 2019، ص.387، 403.

وللإجابة عن مختلف هذه التساؤلات وغيرها اعتمدنا تقسيم هذه الدراسة إلى مجموعة من المحاور الأساسية تُعالج مضمون البحث.

بالإضافة إلى ذلك فقد اتخذنا المراقبة الإلكترونية كنموذج للدراسة باعتبارها أهم آلية يمكن الاعتماد عليها في كشف الجرائم الإلكترونية.

المبحث الاول: ماهية المراقبة الإلكترونية.

لعب التطوّر العلمي الحديث في مجال الاتصالات دوراً مهماً في مجال المحادثات الهاتفية، حيث زوّد الإنسان بأجهزة ووسائل حديثة من شانها اقتحام خلوته وتجريده من كلّ خصوصياته.

فالمراقبة هي الاعتداء على حرية الحديث الذي هو حق من الحقوق اللصيقة بالشخصية الإنسانية ودون خصوصية للحديث والاتصالات يصبح الفرد متردّداً وخائفاً من ممارسة حقّه عبر وسائل الاتصالات الحديثة.

ولقد تبنى المشرّع الجزائري مصطلح المراقبة الإلكترونية كغيره من التشريعات المقارنة الذي استمّدته من نص الاتفاقية المتعلقة بمكافحة الجريمة المنظمة عبر الحدود الوطنية والتي سنتها منظمة الأمم المتحدّة في إطار مكافحة الجريمة المنظمة[1].

المطلب الاول: مفهوم المراقبة الإلكترونية:

لم يتعرض التشريع الجزائري لتعريف مصطلح المراقبة الإلكترونية كدليل رقمي لا في قانون الإجراءات الجزائية ولا في مواد القانون رقم 09-04 المتعلق بالقواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]، وإنّما ترك ذلك للفقه حيث عرفها بعضهم على أنها إجراء يتعمّد فيه الإنصات والتسجيل ومحلها المحادثات الخاصّة سواء أكانت مباشرة أو غير مباشرة.

---

[1] بوخبزة عائشة، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماجستير، كلية الحقوق، جامعة وهران، 2012-2013، ص.124.

[2] القانون رقم 09-04 المؤرخ في 2009/08/05، يتضمن القواعد الخاصّة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ج.ر، رقم 47، المؤرخة في 16 أوت 2009.

أي سواء كانت ممّا يتبادله الناس في مواجهة بعضهم البعض أو عن طريق وسائل الاتصال السلكية واللاّسلكية.

أمّا بخصوص بعض التشريعات المقارنة فنجد أنّ التشريع الأمريكي عرّفها في المادة 2510-04 من قانون الاتصالات الفيدرالي الأمريكي لعام 1968 بأنّها: «عملية الاستماع لمحتويات أسلاك أو أيّ اتصالات شفوية عن طريق استخدام جهاز إلكتروني أو أيّ جهاز آخر»، وطبقا لقانون الاتصالات الأمريكي لعام 1986 أصبح التعريف المذكور يشمل الاتصالات الإلكترونية الأخرى[1].

المطلب الثاني: مميزات نظام المراقبة الإلكترونية:

يمتاز نظام المراقبة الإلكترونية بمجموعة من الخصائص تميّزه عن غيره من البدائل العقابية المقترحة للحدّ من مشكلة العقوبات السالبة للحرية، فهو نظام يخضع لمبدأ الشرعية، إذ لا يقرّر إلاّ بموجب نص قانوني يطبق على هذه الآلية وما هي شروطها والحالات التي يرفض فيها، فالشرعية لا تشمل شرعية التجريم فقط ولكنها تشمل كذلك شرعية الجزاء[2].

إضافةً إلى تلك، فإجراء المراقبة الإلكترونية يتمّ بصورة سريّة دون علم أو رضا صاحب الشأن وعلّة ذلك المحافظة على خصوصية الأحاديث والمراسلات وسرّيتها، وبالتالي يمكن معه تطبيق كلّ الضوابط وضمانات المراقبة والحماية المقرّرة قانوناً لحماية حق الفرد في سريّة مراسلاته واتصالاته[3].

إضافةً إلى ذلك، فنظام المراقبة الإلكترونية يحقق الهدف من الجزاء، حيث سعى إلى إصلاح الجاني وتأهيله لإعادة إدماجه في النسيج الاجتماعي عقب تطبيق هذا النظام، فارتداء أسورة إلكترونية قد يحقق إيلام الجاني وإحساسه أنّه غير عادي بارتدائه هذا السوار[1].

---

[1] ياسر الأمير الفاروق، مراقبة الأحاديث الخاصة في الإجراءات الجزائية، دار المطبوعات الجامعية، مصر، 2009، ص.139.

[2] بلعرابي عبد الكريم، عبد العالي بشير، نظام المراقبة الإلكترونية نحو سياسة جنائية جديدة، مجلة القانون والمجتمع، المجلد 5، العدد 02، ص.08.

[3] رامي متولي القاضي، نظام المراقبة الإلكترونية في القانون الفرنسي والقانون المقارن، مجلة الشريعة والقانون، جامعة الإمارات المتحدّة، العدد 63، يوليو 2015، ص.290.

المبحث الثاني: حجيّة الدليل الإلكتروني الناشئ عن التفتيش و الاثبات الجنائيين

إنّ حجيّة المخرجات المتحصلة من الكمبيوتر هي قوتها الاستدلالية على صدق نسبة الفعل إلى شخص معين أو كذبه، أو هي قيمة ما يتمتع به المخرج المتحصل من الحاسوب بأنواعه المختلفة الورقية والإلكترونية والمصغرات الفيلمية من قوّة استدلالية في كشف الحقيقة[2].

المطلب الاول : حجية الدليل الإلكتروني المستمّد من التفتيش وحالات استعماله

إنّ الأدّلة الإلكترونية إمّا أن تكون مخرجات ورقية يتمّ إنتاجها عن طريق الطابعات أو الراسم، وإمّا أن تكون مخرجات غير ورقية، أو أن تكون إلكترونية كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الإلكترونية غير التقليدية.

الفرع الاول: شروط حجية الدليل الناشئ من التفتيش

الدليل الإلكتروني يجب الحصول عليه بصورة مشروعة غير مخالفة لأحكام الدستور ولا لقانون العقوبات، فجميع المراسلات البريدية والبرقيات والمخاطبات الهاتفية سرّية فهي لا تخضع للمراقبة أو التوثيق إلاّ في الأحوال المنصوص عليها قانوناً[3].

وفي إطار مشروعية الأدّلة الإلكترونية، نجد أنّ قانون الإجراءات الجنائية الفرنسي رغم أنّه لم يتضمن أيّة نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة، إلاّ أنّه كان بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية أو في مجال التنقيب عن جرائم الحاسوب[1].

---

[1] بلعربي عبد الكريم، عبد العالي بشير، المرجع السابق، ص.57.

[2] لؤي عبد الله نوح، المرجع السابق، ص.57.

[3] فهذه النصوص المجسّدة بموجب أحكام الدستور تفرض على المشرّع عند وضع قواعد الإجراءات الجزائية الالتزام بها وعدم الخروج عنها وكذلك فإنّ إجراءات الحصول على الأدّلة الجنائية يجب أن تكون ضمن الإطار العام الذي حدّده الدستور. راجع في هذا الصدد، علي حسن الطوالبة، مشروعية الدليل الإلكتروني المستمّد من التفتيش الجنائي–دراسة مقارنة–، مركز الإعلام الأمني، البحرين، (د.د.ن)، 2009، ص.15.

وبالرجوع إلى القانون الجزائري نجد أنّ المشرّع حدّد ساعات المراقبة في إذن المراقبة لأنّ الإطالة في عملية المراقبة المفتوحة فيها كشف لأسرار المواطنين دون مبرّر وهو ما حدّده المشرّع الجزائري بستة أشهر قابلة للتجديد في المادة 4 من القانون رقم 09-04 في فقرتها السادسة[2].

ومن بين الشروط أيضا نجد أنّ إجراء المراقبة الإلكترونية كدليل رقمي يتمّ بصورة سرّية، أي أنّ هذا الإجراء يتمّ بصورة خفية دون علم رضا المعني بالأمر وعلّة ذلك هي المحافظة على خصوصية الأحاديث والمراسلات وسرّيتها وبالتالي يمكن معه تطبيق كلّ ضوابط وضمانات المراقبة والحماية المقرّرة قانوناً لحماية حق الفرد في سرّية مراسلاته واتصالاته[3]. وبخصوص إذن المراقبة يجب أن تتضمن الأحاديث والمراسلات هوية الأشخاص الخاضعين للمراقبة.

يجب على القائم بالمراقبة القيام بتسجيل ما يرخّص له في إذن المراقبة فقط وما ضبط فوق ذلك يمنع تسجيله ومراقبته، إضافة إلى ضرورة ختم الشرائط لعدم إمكانية تغيير فحواها وذلك عند القيام بأمر المراقبة[4].

الفرع الثاني: حالات استعمال الدليل الرقمي:

نصت المادة 04 من القانون رقم 09-04 على الحالات التي يمكن للضبطية القضائية اللجوء إلى استخدام الدليل الرقمي وهي محدّدة خصوصاً في الوقاية من الجرائم الإرهابية أو التخريب أو الجرائم الماسة بأمن الدولة، إضافةً إلى حالة وجود أنباء عن احتمال اعتداء على منظومة معلوماتية على النحو الذي يهدّد النظام العام، أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني[5].

---

[1] كان يستخدم أعضاء الضابطة القضائية طرقاً معلوماتية في أعمال التصنت على المحادثات الهاتفية ويشير رأي فقهي فرنسي إلى أنّ القضاء قد قبل استخدام الوسائل العلمية الحديثة تحت تحفظ أن يتمّ الحصول على الأدلة الجنائية ومن بين الأدّلة المتحصل عليها من الحاسوب والإنترنت. علي حسن الطوالبة، المرجع السابق، ص.16.

[2] بن بادة عبد الحليم، المرجع السابق، ص.393.

[3] ياسر الأمير فاروق، المرجع السابق، ص.139.

[4] علي حسن مُحَمَّد الطوالبة، المرجع السابق، ص.228.

[5] بن بادة عبد الحليم، المرجع السابق، ص.396.

كذلك مقتضيات التحقيق القضائي تتطلب استخدام الأدّلة الرقمية على غرار المراقبة الإلكترونية في حالة تعذر الوصول إلى نتيجة تعلّم التحقيقات القائمة، وكذلك في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

باستقراء الحالات المذكورة في المادة الرابعة أعلاه، يتبيّن لنا أنّ المشرّع حصر الحالات التي يمكن فيها اللجوء واستعمال الدليل الرقمي مثل اقتصارها على الجرائم التي تمسّ الأمن الوطني وكذلك الجرائم الإرهابية التي تطال المدنيين وعن حق الشخص في الخصوصية، لأنّ المصلحة العامة في خطر، بالإضافة إلى ذلك حالات المساعدة القضائية.

المطلب الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي والمواقف الدولية في حل اشكالاته:

في إطار رصد الدليل الرقمي نرى أنّ الإشكالية لا تقع فقط في طريقة الحصول عليه أو ضبطه أو نقله للعالم الافتراضي إلى العالم المادي، بل تنبثق صعوبة أخرى تتمثل في مدى حجية الدليل الإلكتروني في الإثبات الجنائي ومدى قوته الاستدلالية على نسب الجريمة الإلكترونية إلى المتهم. وأن تصدر سلطة التحقيق– النيابة العامة– أمراً بإحالة الدعوى الجنائية إلى المحكمة، أو أن تصدر أمراً بإخلاء سبيل المتهم بناءًا عليه[1].

الفرع الاول : مدى اعتبار الدليل الرقمي من أدّلة الإثبات الجنائي:

إنّ الإثبات الجنائي نشاط إجرائي موجّه مباشرة للوصول إلى اليقين القضائي طبقاً لمعيار الحقيقة الواقعية، بمعنى إقامة الدليل على وقوع الجرم ونسبته إلى شخص معين فاعلاً كان أم شريكاً. والهدف

[1] محمّد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي–دراسة مقارنة–، دار الجامعة الجديدة، 2018، ص.371.

منه هو إظهار الحقيقة سواء تعلق الأمر بالأفعال المرتكبة أو بشخصية المتهم الذي يكون محل المتابعة الجنائية[1].

كما أنّ الإثبات يتم عن طريق وسائل معينة هي أدّلة الإثبات والأدّلة الجنائية هي عبارة عن الوقائع المادية والمعنوية التي يتم معرفتها أو اكتشافها والتي تؤدي إلى كشف الجريمة وإجلاء الغموض الذي يكتنفها، ما يعني أنّ الدليل هو الواقعة التي يستمدّ القاضي منها البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه[2].

أ-يقينية الدليل الإلكتروني في نظام الإثبات:

اليقين عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، فهي تلك الحالة الذهنية للشخص الذي تجعله يعتقد بحدوث واقعة لم تحدث أمام مرآه، ولتحقيق هذا اليقين بنوعيه من المعرفة الحسّية التي تدركها الحواس والمعرفة العقلية التي يقوم بها العقل عن طريق التحليل والاستنتاج[3].

وحتى يتحقق اليقين لدى سلطة التحقيق أو القاضي الجنائي في الجريمة الإلكترونية يجب أن يكون الدليل الإلكتروني ذو علاقة بموضوع الجريمة، وهذا الشرط يُشار إليه في قانون الإثبات الفيدرالي الأمريكي بمبدأ العلاقة الكاشفة The principal of relevance بين الدليل وبين الواقعة محل الدعوى ويسمى هنا الدليل بالدليل الكاشف The Relevant Evidence .

وبتطبيق هذه الميكانيزمات على الأدّلة الإلكترونية فإنّ المحقق أو القاضي يستطيع تكوين يقينه بحجيّة الدليل الإلكتروني في الإثبات الجنائي، من خلال مطابقة الدليل الإلكتروني المستخرج من

---

[1] إلهام شهرزاد روابح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، العدد العاشر، ص.186.

[2] وذلك إمّا بتحقيق حالة اليقين لديه فيحكم بالإدانة أو ترجيح موقف الشك لديه فيحكم بالبراءة، إلهام شهرزاد روابح، المرجع السابق، ص.186.

[3] هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مكتبة النهضة العربية، ط1، 2009، ص.78 وما بعدها.

الحاسوب للأصل الموجود بداخله، ويتمّ ذلك عن طريق المعاينة الحسّية، كمعاينة وتفتيش مسرح الجريمة الإلكترونية والولوج داخل النظام المعلوماتي[1].

ب- الإشكالات التي تؤثر على تقييم الدليل الإلكتروني في مجال الإثبات:

تتمثل هذه الصعوبات بطبيعة الدليل ذاته وأهمّ الإشكالات الموضوعية نجد مبدأ التعدّي على الخصوصية، حيث أنّ الدليل الإلكتروني دليل غير مرئي عبارة عن سجل كهرومغناطيسي مخزن في نظام حاسوبي في شكل ثنائي وبطريقة غير منظمة وبالتالي قد يؤثر على حرمة وخصوصية المعلومات الشخصية للمستعمل.

كما أنّ غياب الآثار المادية يصعب من مأمورية رجال الضبطية القضائية، حيث أنّ الدليل الإلكتروني في الجرائم المعلوماتية عبارة عن نبضات إلكترونية لا تفصح عن شخصية معيّنة وهذه المشكلة تظهر بصفة جليّة مع شبكة الإنترنت. حيث تسمح لمستخدميها الاتصال دون الكشف عن أسمائهم الحقيقية كإرسال رسائل البريد الإلكتروني مجهولة المصدر[2].

كما أنّ صعوبة تعقب الدليل الإلكتروني وضبطه مسألة عويصة، حيث ينتقل هذا الأخير عبر شبكات الاتصال بسرعة ديناميكية فائقة، بمعنى إمكانية تخزين المعلومات أو البيانات في الخارج بواسطة شبكة الاتصال عن بُعد، ممّا يترتب على ذلك صعوبة تعقب الأدّلة الإلكترونية وضبطها.

أمّا بخصوص الإشكالات الإجرائية للدليل الإلكتروني نجد على رأسها مشكلة الاختصاص في الجرائم المعلوماتية، فالجرائم المعلوماتية من أكبر الجرائم التي تُثير مسألة الاختصاص على المستوى الدولي ولا توجد أيّ مشكلة بالنسبة للاختصاص على المستوى الوطني أو المحلي حيث يتمّ الرجوع إلى

---

[1] مُحَمَّد كمال شاهين، المرجع السابق، ص.374.

[2] بن طالب ليندة، الدليل الإلكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، رسالة دكتوراه علوم، جامعة تيزي وزو- الجزائر، 2019، ص.171.

المعايير المحدّدة قانوناً لذلك، أمّا على المستوى الدولي فإنّ اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المعلوماتية التي تتميز بكونها عابرة[1].

فقد تُثار فكرة تنازع الاختصاص القضائي في حالة تأسيس الاختصاص على مبدأ الإقليمية، كما لو قام الجنائي ببث صور خليعة ذات طابع إباحي من إقليم دولة معيّنة، وتمّ الإطلاع عليها في دولة أخرى، ففي هذه الحالة يثبت الاختصاص وفقاً لمبدأ الإقليمية لكلّ دولة من الدول التي مسّتها الجريمة.

نجد أيضاً من الإشكالات الإجرائية التي تُعيق نظام الإثبات في الجرائم الإلكترونية، مشكلة الخبرة والتدريب في الجرائم المعلوماتية حيث انعكس على عمل جهات التحقيق والمحاكمة، إذ يتطلب الكشف عن هذه الجرائم وإثباتها إتباع إستراتيجيات خاصّة تتعلق باكتسابهم مهارات خاصة على نحو يساعدهم على مواجهة تقنيات الحاسب الآلي وشبكاته.

المطلب الثاني: الموقف الدولي والوطني أمام إشكال الدليل الإلكتروني في مجال الإثبات الجنائي:

إنّ القضاء على إشكاليات الدليل الإلكتروني لا يكون إلاّ بمواجهة الجريمة المعلوماتية، فإنّ البعد الدولي للجريمة المعلوماتية وصعوبة ضبط الأدّلة الإلكترونية الناجمة عنها يفرض على المجتمع الدولي، تقوية وسائل الإثبات الجزائية بِما يتناسب مع الجانب التقني لهذه الجريمة، كما يفرض البحث عن وسائل أكثر ملائمة لطبيعة هذه الجرائم لتصنيف الثغرات القانونية التي برع مرتكبوها في استغلالها للتهرّب من الجزاء ولنشر نشاطهم الإجرامي في مناطق مختلفة من العالم[2].

---

[1] بن طالب ليندة، المرجع السابق، ص.180.

[2] بن طالب ليندة، المرجع السابق، ص.189.

ولقد نص المشرّع الجزائري على المساعدة القضائية الدولية في مجال الإجرام المعلوماتي في المادة 16 من قانون 09-04 حيث يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدّلة الخاصة للجريمة في الشكل الإلكتروني.

خاتمة:

نخلص في نهاية هذا البحث أنّ الخصوصية التي يتميّز بها الدليل الإلكتروني جعل مختلف الدول والهيئات والمنظمات الدولية والإقليمية تتسارع لوضع أساليب وإجراءات حديثة تسهّل عملية البحث عنه واشتقاقه ، ولقد أصبح من الضروري في مجال التفتيش والإثبات الجنائيين في مجال الجريمة الإلكترونية إصدار إذن التفتيش لضبط المعلومات بالرّغم من طبيعتها المعنوية، كما أنّ مجرد الحصول على الدليل الإلكتروني وتقديمه للقضاء لا يكفي لاعتماده كدليل إدانة، إذ أنّ الطبيعة الفنية الخاصّة للدليل تمكن من العبث بمضمونه على نحو يحّرف الحقيقة دون أن يكون في قدرة الشخص غير المتخصص إدراك ذلك العبث.

وكتوصية في الأخير، يمكن القول أنّه من الضروري تعزيز ترسانة قانونية لمكافحة الجريمة المعلوماتية لأنّها غير كافية، إذ يجب إثراؤها للتمكّن من وصف كلّ أنواع الجرائم الإلكترونية.

كما أصبح التعاون الدولي أمر ضروري لمكافحة الجرائم المعلوماتية وتطوير وسائل الإثبات وتتبع المجرمين الذين أصبحوا وراء أجهزة الإعلام الآلي متحكمين في آخر ما أنتجته التكنولوجيا.

عنوان المداخلة

"خصوصية إجراءات الضبط القضائي في ظل التطور التكنولوجي"

المحور الرابع: استخدام التقنيات الحديثة في مجال العدالة الجنائية

1/ التطور التكنولوجي عامل تطور لإجراءات التحري و التحقيق في الجرائم

الأستاذ: درعي العربي "أستاذ محاضر أ"

كلية الحقوق و علوم السياسية

جامعة عبد الحميد بن باديس مستغانم

Larbi.drai@univ-mosta.dz

ملخص:

لقد نالت قواعد القانون الجنائي سواء تلك الموضوعية او الإجرائية حظها الوافر من التطور التكنولوجي الذي عرفته البشرية، و هو ما راعته مختلف التشريعات الجنائية المقارنة و اقرتها في منظوماتها القانونية بغية تعقب المجرمين و التحري عن الجرائم حتى لا يكون الفضاء الالكتروني و العالم الافتراضي وسيلة للجرائم يتخفى المجرمون خلفها بأسماء و ألقاب وهمية أو مستعارة، وعليه اقر المشرع الجزائري إجراءات خاصة تتماشى و التطور التكنولوجي تمكن الضبطية القضائية من البحث و التحري عن الجرائم و كشف مرتكبيها في ظل عجز إجراءات الضبطية العادية.

ولعل من أهم الإجراءات التي نجدها في هذا الصدد هو ما نص عليه المشرع الجزائري في جرائم التمييز وخطاب الكراهية المتمثلة خصوصا في التفتيش الالكتروني و التسرب الالكتروني وتحديد الموقع الجغرافي للجريمة كآليات جديدة للبحث و التحري تساير التطور التكنولوجي الذي عرفته الجريمة .

كلمات مفتاحية: التطور التكنولوجي، إجراءات الضبط، التسرب الالكتروني، المنظومة المعلوماتية ، تحديد الجغرافي.

Summary

The rules of criminal law, whether substantive or procedural,

have gained a great deal of technological development that mankind has known, which is what the various comparative criminal legislation has taken into account and approved in their legal systems, in order to track criminals and investigate crimes and so that cyberspace and the virtual world are not A means of crimes that criminals hide behind with fictitious or pseudonyms, and accordingly the Algerian legislator has approved special procedures in line with technological development that enable judicial police to search and investigate crimes and uncover their perpetrators in light of the inability of normal police .procedures

Perhaps one of the most important measures that we find in this regard is what the Algerian legislator stipulates in the crimes of discrimination and hate speech, especially in electronic leakage and determining the geographical location of the crime as new mechanisms for research and investigation in line .with the technological development that the crime has known

Key words: technological development, control procedures, electronic leakage, information system, geographical identification

مقدمة:

لقد استأثرت جميع نواحي الحياة بالتطور التكنولوجي الذي بلغته البشرية، سواء تلك المتعلقة بالمجال الاقتصادي أو العسكري أو الثقافي أو التجاري وغدت بذلك التكنولوجيا إحدى أهم الوسائل الضرورية في جميع نشاطات الأفراد و الجماعات بما توفره من سرعة و أهمية في التواصل.

كما ساهم التطور التكنولوجي و أثر بطريقة مباشرة على سلوكيات الأفراد ونشاطاتهم بحيث نقلهم من العالم المادي الملموس إلى العالم الافتراضي أو ما يسمى بالبيئة الرقمية والتي أصبحت ميدانا خصبا لكل السلوكيات الفردية.

ومن ضمن تلك السلوكيات التي استأثرت بها التكنولوجيا السلوك الإجرامي الذي يرتكبه الأفراد، فبعد أن كان السلوك الإجرامي هو سلوك مادي أصبح السلوك الإجرامي يرتكب في وسائط البيئة الرقمية والعالم الافتراضي حيث انتقل اسم المجرم من المجرم العادي أو الطبيعي إلى المجرم الالكتروني، ولقد

كان للجرائم الماسة بكيان المجتمع وتركيبته النصيب الأوفر من ذلك النوع من الجرائم والمتمثلة أساسا في جرائم التمييز والخطاب الكراهية[1]، بحيث أصبحت فيها التكنولوجيا حليفا استراتيجيا للمجرمين القائمين بتلك الأفعال المحرمة.

وبذلك أصبحت ضرورة العمل القضائي تستدعي تفعيل آليات تكنولوجيا تتناسب وتلك الأفعال المجرمة في سبيل ترصد المجرمين وضبط جرائمهم لتحقيق العدالة الجنائية، على اعتبار أن المجرمون عادة ما يرجون لتلك الجرائم عبر الفضاء الالكتروني الذي أصبح متاحا للجميع بأسماء مستعارة أو وهمية، وتكون معرفتهم والوصول إليهم صعب بالنظر إلى ما تكتسبه تلك الطرق من حيث سهولة طمس الأدلة وخصوصية بالجرائم الالكترونية بصفة عامة.

وعليه بات من الضروري أن تنال إجراءات الضبط والتحري عن تلك الجرائم حقها مما وصلت إليه التكنولوجيا وذلك ما تبناه المشرع الجزائري في قانون الإجراءات الجزائية والقوانين الملحقة به سواء تعلق الأمر بضبط ومتابعة المجرمين والكشف عن الجرائم أو تعلق الأمر بالإثبات الجنائي، لذلك ارتأينا أن نبحث في هذه المداخلة جزئية مهمة كرسها المشرع الجزائري ضمن قانون مكافحة التمييز و خطاب الكراهية والمتعلقة أساسا بالطرق التكنولوجية المستحدثة لضبط والتحري عن الجرائم المتصلة بها وهي تفتيش المنظومة المعلوماتية او التفتيش الالكتروني و التسرب الالكتروني والتحديد الجغرافي لموقع الجريمة.

أهمية الموضوع:

إن البحث في خصوصية إجراءات ضبط ومتابعة الجرائم المتعلقة بمكافحة التمييز وخطاب الكراهية ينشق من أهمية الملتقى نفسه وهو محاولة الوقوف على تأثير التكنولوجيا على القواعد الإجرائية للقانون الجنائي في البحث والتحري عن الجرائم.

كذلك فان قواعد العدالة الجنائية وتطبيق العقاب على كل مخالف للقانون تقتضي أن يكرس العمل القضائي كل ما من شأنه تحقيق تلك النتيجة ومنها تسخير التكنولوجيا لخدمة القانون الجنائي.

---

[1]– لقد صدر أول قانون بجرم التمييز وخطاب الكراهية في الجزائر بمقتضى القانون رقم 20–05 المؤرخ في28 أفريل 2020 المتعلق بالوقاية من التمييز وخطاب الكراهية و مكافحتها، الجريدة الرسمية العدد 25 الصادر بتاريخ 29 أبريل 2020.

وما يزيد في أهمية هذه المداخلة هو أن الفقه والقضاء الجنائي في جوانبه الإجرائية يسعى إلى تثبيت فكرة مهمة وهي الإجراءات الجزائية الرقمية والذي تختلف قواعدها عن النظام القديم للإجراءات الجزائية سواء ما يتعلق بالضبط القضائي أو الإثبات الجنائي أو حتى في تنفيذ العقوبات.

دواعي اختيار الموضوع:

- من دواعي اختار هذا الموضوع هو الوقوف على المستجدات التي كفلها المشرع الجزائري لضبط ومتابعة الجرائم المتعلقة بمكافحة التمييز وخطاب الكراهية، لاسيما الانتقال من الإجراءات العادية مثل التفتيش المادي المقرر في نص المادة 47 قانون الإجراءات جزائية الى التفتيش الالكتروني و التسرب المقرر في نص المادة 64 وما بعدها في قانون الإجراءات الجزائية الى التسرب الالكتروني، وكذلك التحديد الجغرافي لمكان الجريمة.
- كذلك من دواعي اختيار هذا الموضوع هو استقراء ما أسفرت عنه التكنولوجيا وتفعيلها في ضبط الجرائم.

اشكالية الموضوع:

في إطار منهج يتناسب وأهمية الموضوع نحاول أن نجيب عن إشكالية مفادها: ما هي خصوصية الإجراءات التكنولوجية التي أقرها المشرع في مجال البحث والتحري ضمن نطاق الجرائم المتعلقة بالتمييز وخطاب الكراهية.

منهجية البحث:

بغية تحديد المفاهيم المتعلقة بموضوع المداخلة واستقرائها وتوضيحها اخترنا المنهج الوصفي التحليلي وذلك عن طريق استقراء طرق البحث والتحري – ضبط الجرائم – وفق التكنولوجيا الجديدة والتي كرسها المشرع الجزائري في قانون مكافحة التمييز وخطاب الكراهية.

خطة الدراسة:

في سياق الاشكالية المطروحة ارتأينا أن نضع هذه المداخلة وفق العناصر الاتية:

مفهوم التمييز وخطاب الكراهية

أولا: نبذة عن خطاب الكراهية

ثانيا: تعريف خطاب الكراهية فقها ة شريعا

- تعريف خطاب الكراهية فقا
- تعريف خطاب الكراهية تشريعا

الاليات التكنولوجية الحديثة ومتابعة الجرائم والمجرمين المتعلقة بالتمييز وخطاب الكراهية

اولا: تفتيش المنظومات المعلوماتية

ثانيا: التسرب الالكتروني

ثالثا: التحديد الموقع الجغرافي للجريمة.

مفهوم التمييز و خطاب الكراهية

إن مفهوم خطاب الكراهية من المفاهيم الحديثة التي لم يستقر الفقه أو التشريع في ضبطها، وذلك راجع لعدة عوامل تحول دون الالتفاف حول مفهوم موحد، ونحاول بسط هذا المفهوم وتوضيحه من خلال التعريج إلى نبذة عن خطاب الكراهة، ثم إلقاء الضوء على بعض التعريفات الفقهية والتشريعية لخطاب الكراهة.

أولا: نبذة عن خطاب الكراهية

في ظل البناء الفسيفسائي للمجتمعات البشرية وتنوع طوائفها، سواء كان مرد ذلك التنوع إلى العرق أو الأصل أو اللون أو الدين أو الانتماء تنامت ظاهرة التميز وخطاب الكراهية من فئة اتجاه فئة أخرى، مما أثر ذلك على المجتمعات خاصة عندما يتجسد هذا التمييز والخطاب على أرض الواقع في شكل أفعال من شأنها أن تؤدي إلى نتائج وخيمة على تركيبة المجتمع وعلى كيان الدولة بشكل عام.

وبالتالي يتحول هذا الخطاب إلى الدعوة إلى العنف والتعصب وبغض الآخر لاسيما على المستوى الدولي.

ولقد أدرك المجتمع الدولي حقيقة الأمر وما قد ينجر عن خطاب التمييز والكراهية من نتائج سلبية، وفي غمار ذلك الإدراك اتخذت مجموعة من المبادرات مثل الدعوة إلى حوار الحضارات وحوار الأديان في دعوة من المجتمع الدولي إلى إرساء فكرة التسامح وقبول أفكار

الآخر، كما تجلت تلك الدعوة أيضا في نصوص القانون الدولي ذاته[1]، وفي ذلك نصت المادة 19 من الإعلان العالمي الحقوق الانسان على أنه: "لكل شخص حق التمتع بحرية الرأي والتعبير، ويشمل هذا الحق حريته في اعتناق الآراء دون مضايقة"، كما اعترفت المادة الثانية من العهد الدولي الخاص بالحقوق المدنية والسياسة بتعهد الدول على كفالة جميع الحقوق للأفراد دون تمييز سواء كان على أساس الدين أو العرق أو الأصل القومي أو الاجتماعي أو الرأي السياسي[2]، وعلى المستوى المؤسساتي فقد أنشأ المجلس الأوربي اللجنة الأوربية لمناهضة العنصرية والتعصب.

واذا كانت وسائل الإعلام التقليدية تحمل الوزر الكبير لنشر هذا النوع من التصرفات، فإن الدول قد أدركت تلك الحقيقة، بحيث وضعت مجموعة من الضوابط والقيود لممارسة الحرية الإعلامية، وذلك في شكل ضوابط قانونية أو مهنية، وهو ما جسده المشرع الجزائري فعلا في القانون العضوي رقم 12-05 المتعلق بالإعلام حيث نص في مادته الثانية "يمارس نشاط الاعلام بحرية في إطار أحكام هذا القانون العضوي والتشريع والتنظيم المعمول بهما وفي ظل احترام :

"... 2. الدين الإسلامي وباقي الأديان؛ 3. الطابع التعددي للأفكار؛ كرامة الانسان والحريات الفردية والجماعية..."

كما نص القانون رقم 14-05 المتعلق بالسمعي البصري[3] في مادته 48 المتضمنة قواعد دفتر الشروط المنح رخصة ممارسة نشاط سمعي أو بصري على " يضمن دفتر الشروط العامة لاسيما الالتزامات التي تسمح بـ

- الالتزام بالمرجعية الدينية الوطنية واحترام المرجعيات الدينية الأخرى وعدم المساس بالمقدسات والديانات الأخرى..."

---

[1]– قاسمية جمال، منع التمييز في القانون الدولي لحقوق الانسان وأثاره، دار الجامعة الجديدة، الإسكندرية، مصر، طبعة 2014، ص 92

[2]– العهد الدولي المتعلق بالحقوق المدنية والسياسة 16 ديسمبر 1966 دخل حيز النفاذ في 23 مارس 1976 صادقت عليه الجزائر بموجب المرسوم الرئاسي رقم 89-67 المؤرخ في 16/05/1989، الجريدة الرسمية عدد 20 الصادرة بتاريخ 26/02/1997.

[3]– القانون رقم 14-04 الصادر بتاريخ 24 فبراير سنة 2014 المتضمن النشاط السمعي البصري، جريدة رسمية عدد 16 سنة 2014

وعلى المستوى المني فقد أنشأت سلطتي ضبط الصحافة المكتوبة والسمعي البصري كسلطتين ضابطتين مستقلتين، إلا أن هذه القواعد جاءت مجردة من أي نص تجريمي ماعدا تركيزهما على الضوابط القانونية والمهنية.

وفي ظل تطور وسائل التكنولوجيا والإعلام ازداد انتشار خطاب التمييز والكراهية عبر منصات التواصل الاجتماعي، فرغم كونها وسيلة للتقارب بين المجتمعات والثقافات إلا أن استغلالها جاء من طرف البعض لنشر خطابات الكراهية والتمييز، مما بات لزاما على الدول التعامل مع هذا النوع من التصرفات على أنها أفعال كيدية إجرامية يوجب إدانتها.

وهو ما أدركه المشرع الجزائري ولو بصفة متأخرة، إلا أنه جاء في سياق التعاون الدولي والتوجهات الدولية الرامية إلى مكافحة ومنع التمييز وخطاب الكراهية وذلك ما تجسد في صدور القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها[1].

ثانيا: تعريف خطاب الكراهية فقها وتشريعا

مصطلح خطاب الكراهية يعد من المصطلحات التي أثارت وتثير الجدل حول ضبط تعريف جامع مانع لها، وذلك لاختلاف المعايير والاعتبارات التي تقيد عملية التعريف، كون المصطلح يرتبط بجل مقومات الفئات الإنسانية كالدين والعرق واللغة والجنس واللون وغيرها.

1. تعريف خطاب الكراهية فقها

رغم توظيف مصطلح خطاب الكراهية في الكثير من النصوص الدولية والتشريعات الداخلية، إلا أنها لم تتفق في إعطاء مفهوم موحد ولا على تسمية موحدة سواء على المستوى الدولي أو الوطني أو الفقي، وعرف خطاب الكراهية عدة تسميات مختلفة في مثيل الدعوة إلى الكراهية، التحريض على الكراهية وبعض التسميات الأخرى التي تصب في ذات المعني، حيث ترى الأستاذة "كلاوديا هوبت" أن خطاب الكراهية يعد من بين أكثر المفاهيم اضطرابا وتقلبا في مجال القانون الدولي لحقوق الإنسان إذ يختلف مفهومه بحسب الزمان والمكان، بل وحتى من حيث الأسس التي يقوم عليها، وفي أحسن الأحوال يمكن أن نذكر له مفهوما تقليديا الذي يقوم على أساس الإساءة لجماعات بسبب الدين أو العرق أو الإثن"[2].

---

[1]- القانون رقم 20-05 الصادر بتاريخ 28 افريل سنة 2020 المتضمن الوقائية من التمييز وخطاب الكراهية ومكافحتهما، جريدة رسمية، عدد 25 سنة 2020.

[2]- الأزهر لعبيدي، جرائم التمييز وخطاب الكراهية في التشريع الجزائري، المجلة الدولية للبحوث القانونية والسياسية، جامعة الوادي، المجلد 04 العدد 01، ص 33.

وبالتالي فإن خطاب الكراهية هو مجموعة الأنماط المختلفة من التعبير العام التي تدعو إلى نشر الكراهية أو التمييز أو العداوة أو تحرض عليها أو تروج لهم أو تبررهم من شخص أو مجموعة بناء على الدين أو العرف أو الجنسية أو القومية .. أو أي شيء آخر.

2. التعريف التشريعي لخطاب الكراهية وأشكاله طبقا للقانون 20-05

1.2. تعريف خطاب الكراهية تشريعا (القانون 20-05):

عرفت المادة الثانية من القانون 20-05 المتعلق بالتمييز وخطاب الكراهية ومكافحتهما بأنه جميع أشكال التعبير التي تنشر أو تشجع أو تبرر التمييز، وكذا تلك التي تتضمن أسلوب الازدراء أو الإهانة أو العداء أو البغض أو العنف الموجه إلى شخص أو مجموعة أشخاص على أساس الجنس أو العرق أو اللون أو النسب أو الأصل القانوني أو الإثني أو اللغة أو الانتماء الجغرافي أو الإعاقة أو الحالة الصحية.

ومن خلال التعريف يمكن استخلاص الملاحظات الاتية:

1- إن التعريف نفسه يفتقد إلى الدقة وذلك نتيجة استعمال بعض المصطلحات مثل البغض أو العداوة، ونرى بأن مفهومهما واحد، وما يفرقهما سوى أن البغض حالة نفسية مضمرة في نفس الإنسان أما العداوة فيمكن أن تتجسد في شكل أفعال.

2- إن المشرع الجزائري يستعمل مصطلح أو عبارة " جميع أشكال التعبير التي تنشر أو تشجع" والتي نرى بأن النشر لا يعبر دائما عن الكراهية، حتى أن المرجعية الدولية لهذا القانون وهو العهد الدولي للحقوق المدنية والسياسية ومجموع النصوص ذات الصلة بالموضوع توظف عبارة "أي دعوة إلى الكراهية"[1].

2- كذلك فإن المشرع الجزائري أدمج تعريف خطاب الكراهية في التمييز وذلك بقوله" ..تشجع أو تبرر التمييز..."

وعليه يمكن القول بأن القانون جاء ناقصا من التعريف ببعض المصطلحات المهمة كما أن القانون ورغم أهميته إلا أنه جاء مقتضبا مكونا من 48 مادة فقط

[1]- تنص المادة 20 من العهد الدولي الخاص بالحقوق المدنية والسياسية على "1..... - 2 تحصر بالقانون اية دعوة إلى الكراهية القومية او العنصرية او الدينية التي تشكل تحريضا على التمييز او العداوة أو العنف.

القانون حماية خاصة باعتباره مستودع سر صاحبه، يستوي في ذلك أن يكون هذا المحل جهاز إلكتروني أو نظام على شبكة الإنترنت"[1].

ولكن التفتيش في الجرائم الإلكترونية يختلف اختلاف كبير عن التفتيش في الجرائم التقليدية، لأنه يعتبر كتفتيش في الفضاء الخارجي[2]، فهو كيان مادي ومعنوي، فتتوفر فيه الصفة المعنوية والصفة المادية، ويحتوي على معلومات إلكترونية يحتاج إخراجها وجمعها مهارات وكفاءات عالية جدا، سواء من الناحية الفنية أو من ناحية توفر القانون المناسب والمتطور بشكل دائم الملاحقة مثل هذه الجرائم المتطورة، لذا فهو يحتاج إلى قانون خاص يتناسب مع خطورة هذه الجرائم الإلكترونية التي باتت تهدد جميع مناحي الحياة[3].

❖ الاليات التكنولوجية الحديثة في ضبط ومتابعة الجرائم والمجرمين المتعلقة بالتمييز و خطاب الكراهية

أولا: تفتيش المنظومات المعلوماتية:

قبل التطرق الى تفتيش المنظومات المعلوماتية وجب علينا التطرق أولا الى التفتيش الالكتروني الذي يعتبر الأصل العام لتفتيش المنظومة المعلوماتية، فعلى غرار التفتيش المادي الذي أورده المشرع الجزائري من نص المادة 47 من قانون الاجراءات الجزائية أجاز المشرع الجزائري استخدام تكنولوجيا التفتيش الالكتروني في جرائم التمييز و خطاب الكراهية.

ويقصد بنظام المعلوماتية حسب معاهدة بودابست" الدولية بأنها " كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة التي يمكن أن تقوم بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين، بأداء معالجة ألية للمعلومات.[4]

---

[1]– عبدالله الخثمعي، التفتيش في الجرائم المعلوماتية في النمظام السعودي، رسالة لنيل درجة المجستير، السياسة الجنائية، جامعة نايف للعلوم الأمنية، 2011، ص 47.

[2]– عنان الدحدوح، تفتيش نظم الحاسب الآلي، دراسة وصفية تحليلية، رسالة لنيل درجة الماجستير، القانون والإدارة العامة،2017 م، ص 53.

[3]– ياسركلزي، حقوق الإنسان في مواجهة سلطات الضبط الجنائي، دراسة مقارنة، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، 2007م، ص 62

[4]– معاهدة بودابست صادقت عليها الدول الأوربية في 23 نوفمبر 2001 وذلك لوضع اتفاقية دولية لمكافحة الجريمة الالكترونية

وعرفها قانون الاونيسترال الخاص بالتجارة الالكترونية بانها " النظام الذي يستخدم لإنشاء وسائل البيانات أو إرسالها أو استلامها أو تخزينها أو لتجهيزها على أي وجه آخر".[1]

1- تعريف التفتيش الالكتروني:

عرف بعض الفقهاء بأنه: " البحث عن شيء يتصل بجريمة وقعت، ويفيد في كشف الحقيقة عنها وعن مرتكبيها. وقد يقتضي إجراء البحث في محل له حرمة خاصة"[2]، ومن هنا تظهر أهمية التفتيش؛ كونه من إجراءات التحقيق وتتولاه سلطة مختصة للبحث عن أدلة الجريمة وجمعها؛ للكشف عن الجريمة، في محل خاص يتمتع بالحرمة، دون اعتبار لإرادة صاحبه. وقد أحاطت القوانين هذا التفتيش بضمانات عديدة، ومحل التفتيش إما أن يكون مسكنا أو شخصا، وهو بنوعية قد يكون متعلقا بالمتهم أو بغيره، وهو في كل أحواله جائز مع اختلاف في بعض الشروط.

كما عرفه البعض الآخر على أنه: "عمل من أعمال التحقيق الابتدائي يتم بقصد البحث عن أدلة جريمة وقعت، فيؤدي إلى المساس بحق الشخص في الحفاظ على أسراره عن طريق تحري شخصه أو مكانه الخاص"[3].

أما المشرع الجزائري فقد عرفها في نص المادة 02 فقرة ب من القانون 0904" بأنها أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

وتتجلى هذه الطريقة في حالتين:

الحالة الأولى: وهي المنصوص عليها في نص المادة 22 من القانون 20-05 المتعلق بالتمييز وخطاب الكراهية ومكافحتها ومؤدى هذا الاجراء أن تأمر الجهات القضائية مقدمي الخدمات أو أي شخص آخر بتسليمها أي معطيات أو معلومات تكون مخزنة باستعمال وسائل تكنولوجيا الاعلام والاتصال.

---

[1]- أيمن عبد الله فكري، جرائم نظم المعلومات، الدار الجامعية الجديدة، الاسكندرية، 2007، ص 26.

[2]- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1980 م، ص 449.

[3]- حسن الجوخدار، شرح قانون أصول المحاكمات الجزائية، الجزء الأول، مطبعة جامعة دمشق، دمشق، 1981، ص 154.

ومرد هذه الالتزامات أنه وعلى سبيل المثال في المراسلة بالبريد الالكتروني والتي تم استقبالها بواسطة مقدم الخدمات الخاص بالمرسل إليه والتي لم يطلع عليها بعد فإنها تستقر في حالة تخزين إلكتروني ففي هذه المرحلة تبقى النسخة مخزنة على أساس وسطي في انتظار المرسل إليه من مقدم الخدمة وبمجرد استلام المرسل إليه الرسالة المرسلة عبر البريد الالكتروني فإن مقدم الخدمة له دوران إما مسحها وإما تخزينها وفي حال طلب السلطات لتلك الرسالة فإنه يكون ملزم بحفظها وتخزينها وتقديمها للسلطات القضائية[1].

ويقصد بمقدمي الخدمات أيا كيان عامة أو خاصة يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام الاتصالات[2].

الحالة الثانية: وهي الواردة في نص المادة 23 من القانون 20-05 السالف الذكر والذي يمنح سلطة للجهة القضائية في إصدار أمر إلى مقدمي الخدمات بالتحفظ الفوري على المعطيات المتعلقة بالمحتوى أو بحركة السير المرتبطة بالجرائم المنصوص عليها في هذا القانون، ويعني بذلك التحفظ على كل محتوى إذا كان يشكل تمييزا أو خطاب كراهية، ولقد عرفت الفقرة "ه" من المادة 02 من قانون رقم 09-04 المعطيات المتعلقة بحركة السير على أنها "أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات توضح مصدر الاتصال والوجهة المرسل إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة" وهو نفس التعريف الوارد في اتفاقية بودابست (الفقرة د المادة 01).

ويشكل هذا الإجراء ترصد للمحتويات المتضمنة لجرائم التمييز والكراهية وذلك عن طريق تعقبها وحركة سيرها باعتبار طائفة من البيانات المعلوماتية الخاضعة لنظام قانوني معين تنشا عن طريق الحاسب الآلي في سلسلة اتصالات من المنبع إلى مكان الوصول وهي بذلك من ملحقات الوصول وتتكون حركة السير من عدة طوائف مثل رقم الهاتف أو عنوان بروتوكول الإنترنت وخط السير ومكان

[1]- المادة 02 من القانون 09-04 الفقرة د.

[2]- بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، منشورات الحلبي الحقوقية، بيروت، طبعة أولى، 2012، ص 434

الوصول ووقت الوصول بالإضافة حجم وطول الاتصال، وهذه الطوائف لا تكن متاحة من الناحية الفنية إلا أنه يمكن الحصول عليها من مقدمي الخدمات[1].

كما يمكن للجهات القضائية أن تأمر مقدمي الخدمات بالتدخل الفوري السحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو تشفيرها وجعلها غير قادرة على الدخول إليها، وذلك طبقا لنص المادة 24 من القانون 20-05.

2- التسرب الإلكتروني

نتيجة للخصوصية التي ترتكب بها جرائم التمييز وخطاب الكراهية وذلك باعتمادها في غالب الأحيان على تكنولوجيا الإعلام والاتصال أجاز المشرع الجزائري في نص المادة 26 من القانون 20-05 بإجراء التسرب الإلكتروني[2].

ويعتبر التسرب من الإجراءات المستحدثة للضبط القضائي وذلك في تعديل قانون الإجراءات الجزائية رقم 06-22 بحيث عرفته المادة 65 مكرر 12 با "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

وعلى عكس التسرب المادي السائد في أغلب القضايا، فإن التسرب الإلكتروني كإجراء من إجراءات التحري والتحقيق في جرائم التمييز وخطاب الكراهية يقصد به ولوج المتسرب (ضابط الشرطة القضائية) إلى منظومة معلوماتية أو نظام للاتصالات الإلكترونية واشتراكه في محادثات الدردشة أو حلقات النقاش

[1]- الهام بن خليفة، القواعد الاجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، مقال منشور في الانترنيت موقع www.univ-elared.dz اطلع عليه يوم الخميس 07 جانفي 2021 على الساعة 08:00

[2]- تنص المادة 26 من القانون 20-05 المتعلق بالتمييز وخطاب الكراهية على "مع مراعاة أحكام قانون الاجراءات الجزائية يمكن وكيل الجمهورية أو قاضي التحقيق بعد اخطار وكيل الجمهورية أن يأذن تحت رقابته لضابط الشرطة القائية بالتسرب الالكتروني الى منظومة معلوماتية او نظام للاتصالات الالكترونية أو أكثر قصد مراقبة الأشخاص المشتبه في ارتكابهم لأي جريمة من الجرائم المنصوص عليها في هذا القانون وذلك بايهامهم انه فاعل معهم او شريك لهم.

مستخدما اسم مستعار أو صفات مستعارة لأجل مراقبة الأشخاص المشتبه في ارتكابهم الجرائم المذكورة سالفا مع إيهامهم أنه فاعل معهم أو شريك[1].

وباعتبار إجراء التسرب من الإجراءات الاستثنائية والخاصة للضبط القضائي لما ينطوي عليه من مساس بخصوصية الأفراد فإن المشرع الجزائري قد أحاطه بمجموعة من الشروط وهي: الشروط الشكلية: وتتمثل في:

1. ضرورة صدور إذن قضائي يجيز عملية التسرب.
2. احترام المدة القانونية المقررة للتسرب
3. تسبيب عملية التسرب الشروط الموضوعية: وهو الشرط الخاص الذي نصت عليه المادة 26 من القانون 20-05، المتعلق بموضوع عملية التسرب أو محل التسرب وهو البحث عن المشبه في ارتكابهم لجرائم التمييز وخطاب الكراهية.

3-تحديد الموقع الجغرافي

أجاز القانون 20-05 للسلطات الضبط القضائي في مهمة ضبط الجرائم المتعلقة بالتمييز وخطاب الكراهية استعمال تقنية تكنولوجيا التحديد الجغرافي لمعرفة الأشخاص المشتبه فيهم أو لرصد وسيلة ارتكاب الجريمة وذلك ما نصت عليه المادة 27 بقولها "يمكن وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته لضابط الشرطة القضائية متى توفرت دواع ترجح إرتكاب جريمة من الجرائم المنصوص عليها في هذا القانون بتحديد الموقع الجغرافي للشخص المشتبه فيه أو المتهم أو وسيلة ارتكاب الجريمة أو أي شيء آخر له صلة بالجريمة..."

وعلى خلاق التسرب الالكتروني الذي يجد ضوابطه العامة في قانون الاجراءات الجزائية فإن تحديد الموقع الجغرافي يعتبر إجراء جديد يدخل ضمن منظومة الاجراءات الخاصة بالتحقيق في الجرائم التمييز وخطاب الكراهية، ونظرا لخطورة هذه الوسيلة فان اللجوء اليها لا يكون الا في حالة توفر دواعي ترجح ارتكاب الجريمة هذا بالإضافة إلى شرط وجود الاذن القضائي.

[1]- براهمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، بدون تاريخ نشر، اطلع عليها يوم الخميس 07 جانفي 2021 على الساعة 8:40 البوابة الجزائرية للمجلات العلمية asjp.cerist.dz

الخاتمة:

من خلال هذه الدراسة الموجزة لخصوصية الإجراءات المتبعة في ضبط و تتبع الجرائم و المجرمين ضمن نطاق قانون مكافحة التمييز و خطاب الكراهية نستنتجه أن التكنولوجيا قد اكتسحت المجال القانوني في جميع نواحيه سواء تلك الموضوعية أو الإجرائية المتعلق بضبط و إجراءات متابعة المحرمين والجرائم و ذلك لأجل تحقيق الغاية الاسمي له و هي تحقيق العدالة الجنائية ، فيقظة المجرمين و استعمالهم للطرق التكنولوجية في جرائمهم لا يجب ان يستثنوا من العقاب و المتابعة

-كذلك و مما نستنتجه هو أن المشرع الجزائري قد اقر تلك الالياب التكنولوجية في ضبط الجرائم سواء في قانون الإجراءات الجزائية او في قوانين مستقلة مثل قانون الجرائم المعلوماتية أو القانون محل الدراسة

- و مما نستنتجه كذلك هو الاتجاه الذي يسود حاليا الفقه القانوني في إرساء فرع جديد من القانون و هو قانون الإجراءات الجزائية الرقمي و المخصص أساسا لضبط الجرائم الرقمية

و في هذا الصدد يمكن ان نخرج بالتوصيات الآتية:

1- ضرورة ضبط المفاهيم المتعلقة بالآليات التكنولوجية الحديثة لضبط الجرائم و تتبع المجرمين

2- وضع تلك الآليات و تبيان طرق ممارستها و شروطها لكون العالم الافتراضي و البيئة الرقمية أكثر مساسا بخصوصية الأفراد.

3- كذلك من المهم ان توضع تلك الآليات الجديدة ضمن نصوص خاصة حتى لا يكون هناك تضارب بينها.

قائمة المراجع:

الكتب:

1. قاسمية جمال، منع التمييز في القانون الدولي لحقوق الانسان وآثاره، دار الجامعة الجديدة، الإسكندرية، مصر، طبعة 2014.
2. لحسين بن شيخ ات ملويا، رسالة في جنح الصحافة، الطبعة الثانية، دار هومة، الجزائر، 2014، ص 2012.
3. أيمن عبد الله فكري، جرائم نظم المعلومات، الدار الجامعية الجديدة، الاسكندرية، 2007.

4. محمد حسان محمود لطفي، الإطار القانوني للمعاملات الالكترونية، النسر الذهبي، القاهرة، 2001.
5. بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات، منشورات الحلبي الحقوقية، بيروت، طبعة أولى، 2012.

مقال في مجلة:

1. الازهر لعبيدي، جرائم التمييز وخطاب الكراهية في التشريع الجزائري، المجلة الدولية للبحوث القانونية والسياسية، جامعة الوادي، المجلد 04 العدد 01.
2. الهام بن خليفة، القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيا الاعلام والاتصال، مقال منشور في الانترنيت موقع – www.univ elared.dz اطلع عليه يوم الخميس 07 جانفي 2021 على الساعة 08:00
3. براهمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، بدون تاريخ نشر، اطلع عليها يوم الخميس 07 جانفي 2021 على الساعة 08:40 البوابة الجزائرية للمجلات العلمية asjp.cerist.dz

مواقع الانترنت:

1. موقع ويكيبيديا ar.m.wikipedia.org بتاريخ 07 جانفي 2021 على الساعة 19:30

القوانين:

1. العهد الدولي المتعلق بالحقوق المدنية والسياسة 16 ديسمبر 1966 دخل حيز النفاذ في 23 مارس 1976 صادقت عليه الجزائر بموجب المرسوم الرئاسي رقم 89-67 المؤرخ في 16/05/1989 الجريدة الرسمية عدد 20 الصادرة بتاريخ 26/02/1997.
2. القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، جريدة رسمية عدد 47 المؤرخة في 16 غشت 2009.
3. القانون رقم 14-04 الصادر بتاريخ 24 فبراير سنة 2014 المتضمن النشاط السمعي البصري، جريدة رسمية عدد 16 سنة 2014.

4. القانون رقم 20-05 الصادر بتاريخ 28 افريل سنة 2020 المتضمن الوقائية من التمييز وخطاب الكراهية ومكافحتهما، جريدة رسمية، عدد 25 سنة 2020.

مداخلة المشاركـــــة

الملتقى الدولي الافتراضي الموسوم :

القانون الجنائي في ظل التطور التكنولوجي

-إشكالات ومعالجات-

جامعة الجزائر-1 بن يوسف بن خدة

كلية الحقوق -سعيد حمدين

يومي28-29 سبتمبر 2022

الاسم: نعيمة

اللقب: بوعقبة

الرتبة: أستاذ محاضر –أ-

التخصص: قانون دولي عام

الهيئة المستخدمة: جامعة الشاذلي بن جديد-الطارف

الهاتف: 07 98 93 33 20

البريد الالكتروني:bouakba-naima@univ-eltarf.dz

محور المشاركة:المحور الخامس: تأثير الوسائل العلمية على الاثبات الجنائي

عنوان المداخلة: استخدام البيانات الشخصية في التحقيق الالكتروني بين أولوية مكافحة الجرائم وضمان الحق في الخصوصية

الملخص:

يعترف القانون الدولي بحق الشخص في حماية بياناته الشخصية التي باتت اليوم تمثل جزء من الحق في الخصوصية غير أن هذا الاعتراف يخضع بالمقابل من ذلك إلى جملة من القيود أهمها اعتبارات الأمن الوطني، حيث تسمح غالبية التشريعات والمواثيق الدولية الخاصة بحماية البيانات أو المعطيات الشخصية للأفراد، بالخروج عن مبدأ حظر معالجة البيانات الشخصية، من خلال معالجة هذه البيانات بهدف منع الجرائم والتحقيق فيها الكترونيا لمواجهة النشاط الإجرامي السيبراني.

ولأن التحقيق الجنائي الالكتروني باستخدام هذه البيانات الشخصية قد يؤدي إلى الكشف عن بيانات شخصية للأفراد لاتتعلق بموضوع التحقيق، ولأجل ذلك تم إقرار ضمانات تكفل الحق في حماية البيانات الشخصية للأفراد كحق معترف به مايقيد عمل هيئات التحقيق في البيئة الرقمية.

الكلمات المفتاحية: –التحقيق الجنائي الالكتروني_البيانات الشخصية_الحق في الخصوصية_حماية البيانات الشخصية.

Abstract:

International law recognizes the right of a person to protect his personal data, which today is considered part of the right to privacy, However, this recognition is subject to a number of restrictions, the most important of which are national security considerations, where the majority of international legislation and charters related to the protection of data or personal data of individuals allow a departure from the principle of prohibiting the processing of personal data, by processing this data in order to prevent and investigate crimes electronically to counter cybercriminal activity.

And because an electronic criminal investigation using this personal data may lead to the disclosure of personal data of individuals that are not related to the subject of the investigation, for this reason, guarantees have been established that secure the right to protect the personal data of individuals as a recognized right, which restricts the work of investigation bodies in the digital environment.

Key Words :-Electronic criminal investigation_Personal data_Right to privacy_Personal data protection

مقدمة:

أدى التطور التكنولوجي في مجال الرقمنة إلى اتساع نطاق الحق الفرد في الخصوصية أو الحياة الخاصة، إذ لم يعد هذا الحق يقتصر على ضمان حماية سمعة وأسرة ومسكن الشخص، بل كذلك يعني الحق في حماية البيانات الشخصية للأفراد وحظر معالجتها، الذي بات حقا معترف به ضمن العديد من المواثيق وتشريعات حماية البيانات الشخصية.

غير أن هذا الاعتراف يخضع بالمقابل من ذلك إلى جملة من القيود أهمها اعتبارات الأمن الوطني، حيث تسمح غالبية التشريعات والمواثيق الدولية ذات الصلة بحماية البيانات أو المعطيات الشخصية للأفراد، خروجا عن مبدأ حظر معالجة البيانات الشخصية، بحق آخر للدول في إمكانية معالجة هذه البيانات بهدف منع الجرائم الجنائية والتحقيق فيها وملاحقتها بأي وسيلة كانت بما فيها التحقيق الالكتروني.

يسمح التحقيق الالكتروني بجمع الأدلة الرقمية لمواجهة النشاط الإجرامي السيبراني على وجه الخصوص؛ وذلك عن طريق استخراج تتبع وجمع وتحليل البيانات الشخصية للأفراد المخزنة في الأجهزة الرقمية؛ كبيانات الهاتف المحمول ورسائل البريد الالكتروني والبيانات المخزنة على خوادم الكومبيوتر والبريد الصوتي والصور الرقمية وجداول البيانات، كما قد يشمل التحقيق الالكتروني كذلك عمليات نقل هذه البيانات إلى دول ثالثة أو منظمات دولية كمنظمة الشرطة الدولية (الانتربول) في إطار التعاون القضائي الدولي.

لا شك أن اللجوء إلى التحقيق الالكتروني من قبل الهيئات المخولة ذلك قانونا على المستوى الوطني أو الدولي، قد يساعد على مكافحة الجرائم السيبرانية التي تتطلب جمع أدلة رقمية تتماشى والطبيعة الخاصة لهذه الجرائم، غير أنه يثير أيضا إشكالات أخرى تتعلق بحق الأفراد في حماية بياناتهم الشخصية وفي خصوصية هذه البيانات، خاصة وأن التحقيق الجنائي الالكتروني باستخدام هذه البيانات الشخصية قد يؤدي إلى الكشف عن معلومات خاصة لا تتعلق بموضوع التحقيق عند نقل البيانات الشخصية مثلا عبر الحدود أو إرسالها أو استقبال هذه البيانات الشخصية.

هذا ما يطرح التساؤل عن الحدود المسموح بها في معالجة البيانات الشخصية للأفراد في سياق التحقيق الجنائي الالكتروني من جهة؟ وعن الضمانات المقررة لحماية الحق في خصوصية البيانات الشخصية في مرحلة التحقيق الجنائي الالكتروني من جهة أخرى؟

1. حماية البيانات الشخصية كحق أساسي إلى جانب الحق في الخصوصية:

انعكس التطور التكنولوجي على الحق في الخصوصية، على نحو أدى إلى اتساع مضمون هذا الحق ليشمل كذلك حق جديد ألا وهو حق في الفرد في حماية بياناته الشخصية، ولفهم مضمون هذا الحق ومدى ارتباطه بالحق في الحياة الخصوصية، سنحاول التعرف أولا على المقصود بالبيانات الشخصية ثم تبيان طبيعة الحق في حماية البيانات الشخصية وارتباطه بالحق في الخصوصية وثالثا التطرق إلى مضمون الحق في حماية البيانات الشخصية.

1.1. تعريف البيانات الشخصية:

تعرف الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010 البيانات على أنها:" كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات مثل الأرقام والحروف والرموز وما إلى ذلك".[1]

أما اتفاقية الاتحاد الأفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية لسنة 2014، فتعرف البيانات الشخصية بأنها:" أي معلومات متصلة بشخص طبيعي محدد أو قابل للتحديد بشكل مباشر أو غير مباشر بالإشارة الى رقم هويته أو إلى عامل واحد أو أكثر محدد لهويته الطبيعية او السيكولوجية أو الذهنية أو الاقتصادية أو الاجتماعية أو الثقافية.[2]

وتعرفهاالمبادئ التوجيهية لمنظمة التعاون الاقتصادي والتنمية (OECD) المعدلة (2013) البيانات الشخصية على أنها:" تعني أي معلومات تتعلق بمعرف أو فرد يمكن التعرف عليه."

كما تعرفها اتفاقية مجلس أوروبا الخاصة بحماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية المعتمدة في 1981/1/28(اتفاقية 108) بأنها تعني:" أي معلومات تتعلق بفرد محدد الهوية أو يمكن التعرف عليه"[3].

أما في إطار التوجيهات الأوربية الخاصة بحماية بيانات الأفراد وحرية انتقالها لا سيما منها اللائحة العامة لحماية البيانات الشخصية GDPR رقم 2016/679 فتعرف المادة 4 فقرة 1 منها البيانات الشخصية بأنها:" تعني أي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه ويعتبر شخصا طبيعيا يمكن التعرف عليه؛ شخصا طبيعيا يمكن تحديده، بشكل مباشر أو غير مباشر على وجه الخصوص بالرجوع إلى معرف مثل الاسم ورقم التعريف، بيانات الموقع أو المعرّف عبر الإنترنت أو عنصرا محددا أو أكثر خاص بهويته الجسدية أو الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.[4]

وعلى صعيد التشريعات الوطنيةفنجد المشرع الجزائري على سبيل المثاليعرف البيانات الشخصية بموجب القانون 07/18 المؤرخ في 2018/6/10 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي بأنها:" كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه بالشخص المعني بصفة مباشرة أو غير مباشرة لا سيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومتريةأو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية".[5]

أماالمشرع الفرنسي فنجده يعرف البيانات الشخصية بموجب القانون رقم 801 لعام 2004 الخاص بحماية البيانات الشخصية نجده ضمن المادة 2 منه بأنها:" أي معلومة تتعلق بشخص طبيعي محددة هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة سواء تم تحديد هويته بالرجوع إلى رقمه الشخصي أو بالرجوع إلى أي شيء يخصه"[6].

وعليه استنادا لما تقدم يمكننا القول بأن:

-البيانات الشخصية بصورة عامة تعني المعلومات التي يمكن عن طريقها الاستدلال على هوية شخص ما، سواء صرحت تلك البيانات بهوية ذلك الشخص، أو احتوت في مجموعها على بيانات يمكن عن طريق معالجتها تحديد هوية هذا الشخص.

- قد تشمل هذه البيانات أو المعلومات التي تحدد هوية الشخص بشكل مباشر مثل الاسم واللقب العنوان الشخصي، كما قد تشمل أيضا المعلومات التي تحدد الشخص بشكل غير مباشر والتي ترتبط في الغالب بالتقنيات الحديثة مثل رقم الهاتف، عنوان البريد الالكتروني، رقم السيارة، رقم بطاقة الائتمان، بيانات شخصية مثل الصورة، الصوت، بصمات الأصابع، الحمض النووي، البيانات البيومترية.[7]

وتعد من قبيل البيانات الشخصية كذلك فئة البيانات الشخصية ذات الطبيعة الخاصة أو ما تعرف بالبيانات الحساسة وهي البيانات التي تكشف عن الآراء السياسية والمعتقدات الدينية للشخصوالبيانات البيومترية، البيانات المتعلقة بالعرق والأصل العرقي، البيانات المتعلقة بالآراء الفلسفية والعضوية في النقابات، البيانات الصحية، البيانات الجينية البيانات المتعلقة بالحياة الجنسية والتوجه الجنسي.

-أن البيانات الشخصية ترتبط بالشخص موضوع البيانات وهو كل شخص طبيعي تكون المعطيات الحساسة المتعلقة به موضوع معالجة، ويشترط أن يكون الشخص الطبيعي محل الحماية محدد أو قابل للتحديد ويشير مصطلح **محدد** إلى شخص معروف أو متميز عن مجموعة من الأشخاص، أما مصطلح **قابل للتحديد** فهو شخص لم يتم تحديده بعد لكنه ممكن التعريف.[8]

وعموما يتم التعرف على الشخص أو تحديده بشكل أكثر شيوعًا عن طريق الإشارة إلى الاسم بالاقتران مع معلومات إضافية إذا لم يكن الاسم فريداكرقم الهاتف، السيارة أو رقم الضمان الاجتماعي، أو جواز السفر، العنوان، العمر، المهنة والوظيفة.[9]

وينبغي الإشارة هنا إلى أن البيانات التي تحذف عناصر التعريف الشخصية منها كالبيانات المجهولة البيانات المستعارة، البيانات المشفرة، تخرج من دائرة الحماية القانونية.[10]

2.1. الاعتراف بالحق في حماية البيانات الشخصية وباعتباره جانب من الحق في الخصوصية

1.2.1. حماية البيانات الشخصية كجزء من الحق في الخصوصية:

يعد الحق في الخصوصية أو الحق في الحياة الخاصة أحد الحقوق الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية، ويرد الاعتراف بهذا الحقضمن العديد من الصكوك الدولية لحقوق الأسان العالمية منها والإقليمية وكدا ضمن غالبية الدساتير الوطنية للدول، وفي هذا السياق تنص المادة 12 من الإعلان العالمي لحقوق الإنسان لسنة 1948 على أنه:"لا يجوز تعريض أحد لتدخل في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته ولا لحملات تمس شرفه وسمعته ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات".

من جهته يكرس العهد الدولي الخاص بالحقوق المدنية والسياسية الحق في الخصوصية بنفس مضمون الإعلان العالمي لحقوق الإنسان حيث جاء في نص المادة 17 من العهد على أن:" لكل شخص الحق في عدم التعرض على نحو تعسفي أو غير مشروع لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته ولا لأي حملات لا قانونية تمس بشرفه أو سمعته".

كما تعترف الاتفاقية الأوربية لحقوق الإنسان وحرياته الأساسية لسنة 1950 بالحق في الخصوصية مستعملة مصطلح الحياة الخاصة بنفس المعنى الوارد عليه في الإعلان الدولي والعهد الدولي للحقوق المدنية والسياسية حيث جاء في نص المادة 8 الفقرة الأولى منها بأن:" لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته."

يتضح من مجملأحكام اتفاقيات حقوق الإنسان العالمية والإقليمية المشار اليها أعلاه، بأن الحق في الخصوصية ينصرف في مضمونه إلى الحق في الحياة الخاصة للشخص في منزله ومراسلاته وأسرته.

2.2.1. تكريس الحق في حماية البيانات الشخصية كحق من حقوق الانسان:

غير أن الحق في الخصوصية ونتيجة التطور التكنولوجي قد طرأ عليه تغيير أدى إلى اتساع نطاقه ليشمل زيادة على المجالات التقليدية المتمثلة في حرمة المنزل وسرية المراسلاتالحق حماية البيانات الشخصية للأفراد.

وبالتالي أصبحت البيانات الشخصية وحمايتها تندرج ضمن حدود الحياة الخاصة للأفراد وتتطلب حماية مماثلة لحماية الحق في الخصوصية، وهذا ما جاء في حكمالمحكمة الأوربية لحقوق الإنسان بمناسبة نظرها في قضية روتار **Rotaru** عندما أعلنت صراحة بأن:" المعلومات المتعلقة بالإدانة الجزائية –والتي تمثل فئة من فئات البيانات الشخصية ذات الطبيعة الخاصة–جزءا من الحياة الخاصة للشخص".[11]

كما يجد هذا الاعتراف تأكيدا له في التعليق العام رقم 16 (1988) للجنة المعنية بالحقوق المدنية والسياسية حيث اعتبرت اللجنة عند تحديد مضمون التزامات الدول في حماية الحق في الخصوصية بأن البيانات الشخصية جزء من الحق في الخصوصية وتفترض حماية مماثلة للحماية الممنوحة للحق في الخصوصية وفي هذا تقول اللجنة بأنه:"يجب أن ينظم القانون عمليات جمع وحفظ المعلومات الشخصية باستخدام الحاسوب ومصارف البيانات وغيرها من الوسائل سواء أكانت تجريها السلطات العامة أم الأفراد العاديون أو الهيئات الخاصة ويتعين أن تتخذ الدول تدابير فعالة لكفالة عدم وقوع المعلومات المتعلقة بالحياة الخاصة للشخص في أيدي الأشخاص الذين لا يجيز لهم القانون الحصول عليها أو تجهيزها أو استخدامها وعدم استخدامها على الإطلاق في أغراض تتنافى مع العهد.[12]

غير أنه وبالنظر للتباين في أطر الحماية المقررة لمجالات الحق في الخصوصية كما هو مبين في اتفاقيات حقوق الإنسان العالمية والإقليمية على نحو ما سبق بيانه، كان من الصعوبة بمكان أن مجرد حظر تبادل المعلومات الشخصية وفقا للقواعد التقليدية لحماية الخصوصية لم يعد قابلا للتطبيق، ولأجل ذلك ظهرت العديد منواللوائح والتوجيهات الإقليمية والتشريعات الداخلية إلى جانب عدد محدود من الاتفاقيات الرامية لحماية البيانات الشخصية للأفراد.

كانت البداية سنة 1980 عن طريق منظمة التعاون الاقتصادي والتنمية الأوربية والتي أصدرت توصيات بشأن المبادئ التوجيهية التي تحكم حماية الخصوصية والتدفقات عبر الحدود للبيانات الشخصية، ثم سنة 1981 من خلال اتفاقية مجلس أوروبا الخاصة بحماية الأفراد فيما يتعلق بالمعالجة التلقائية للبيانات الشخصية المعدلة سنة 2013أين تم الاعتراف صراحة بالحق في حماية البيانات كحق فردي قائم بذاته لكنه وفي نفس الوقت يرتبط بخصوصية الشخص حيث جاء في ديباجتها :" بأن الدول

الأعضاء في منظمة التعاون والتنمية في الميدان الاقتصادي لديها مصلحة مشتركة في تعزيز وحماية القيم الأساسية للخصوصية والحريات الفردية والتدفق العالمي الحر للمعلومات."

كما يرد الاعتراف بهذا الحق كذلك في ميثاق الحقوق الأساسية للاتحاد الأوروبي لسنة 2000 والذي جاء فيه بأن:" لكل فرد الحق في حماية البيانات الشخصية المتعلقة به".[13]

وقد اتسع نطاق قوانين ولوائح حماية البيانات الشخصية للأفراد باعتبارها حق منفصل أملتها اعتبارات حماية الحق في الخصوصية، كما هو الشأن مع التوجيه الأوربي EC 95/46 والذي تم تعديله عن طريق اللائحة العامة الأوربية لحماية البيانات الشخصية GDPR2016/679 واتفاقية الاتحاد الإفريقي بشأن أمن الفضاء الالكتروني وحماية البيانات ذات الطابع الشخصي لسنة 2014 إلى جانب العديد من التشريعات الداخلية.

3.1. مضمون الحق في حماية البيانات الشخصية:

على الرغم من إقرار غالبية المواثيق الدولية والقوانين ذات الصلة بالحق في حماية البيانات الشخصية كحق أساسي انطلاقا من خصوصية هذه البيانات، لكنها في الوقت نفسه تسمح لجهات محددة بإمكانية معالجة هذه البيانات.

وتعني معالجة البيانات الشخصية؛ مجموعة العمليات المنجزة على البيانات الشخصية كالجمع والتسجيل التنظيم التعديل والاسترجاع، المعاينة الحفظ الكشف بواسطة النقل الضبط الإفشاء بشكل عام، العرض علانية الدمج المحو منع الوصول أو الإلغاء، ويستوي خضوع البيانات الشخصية للمعالجة بصرف النظر عن الطريقة المتبعة في المعالجة سواء أكانت المعالجة آلية تمت الكترونيا بواسطة استخدام الحاسوب[14]، أو معالجة يدوية لكون الوظائف والأهداف هي نفسها وإن اختلف أسلوب المعالجة من الجهة التقنية[15]،فمعالجة البيانات لا يقتصر فقط على الطرق الالكترونية بل يمكن أن يتم أيضا من خلال الطرق العادية.[16]

على ضوء ما تقدم يمكننا أن نستشف بوضوح بأن الحق في حماية البيانات الشخصية، يعني حماية خصوصية هذه البيانات عند خضوعها للمعالجة سواء بصورتها اليدوية أو الالكترونية وللوصول إلى هذه الغاية، حرصت مختلف الصكوك العالمية والإقليمية وتشريعات حماية البيانات الشخصية الوطنية، على إقرار جملة من المبادئ الذي يستلزم الخضوع لها عند معالجة هذه البيانات الشخصية من قبل الهيئات العامة أو الخاصة لتفادي استغلال معالجة البيانات الشخصية وسوء استخدامها ويمكن اجمال هذه المبادئ فيما يلي:

1.3.1. المشروعية:

إذ يجب أن يكون الوصول إلى هذه البيانات الشخصية بالوسائل القانونية والعادلة وذلك من خلال الحصول عليها من قبل السلطة القانونية المختصة، أو بموافقة الشخص موضوع البيانات.

2.3.1. تقييد الاستخدام:

عدم استخدام البيانات الشخصية لأغراض أخرى غير تلك المحددة إلا بموافقة صاحب البيانات أو بسلطة قانونية، وهذا ما يتوقف على شرط سابق هو تحديد الأغراض التي من أجلها يتم جمع البيانات الشخصية.

3.3.1.الآمان:

وجب أن يتم معالجة البيانات الشخصية بطريقة تضمن الأمان المناسب لهذه البيانات بما في ذلك الحماية من الكشف غير المقصود أو غير المصرح به، والحماية من الفقد أو التلف أو التلف العرضي، أو التدمير أو التعديل باستخدام التدابير التقنية أو التنظيمية المناسبة.[17]

4.3.1. تحديد الغرض:

يجب أن يقتصر مقدار البيانات الشخصية التي يتم جمعها على ما هو ضروري لتحقيق غرض وعدم جواز الاحتفاظ بها وتخزينها لفترات تتجاوز قدر ما سيتم معالجة البيانات الشخصية، باستثناء الحالات الذي يرتبط فيها التخزين بأغراض الأرشفة فقط للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو الأغراض الإحصائية.[18]

–حق الشخص المعني موضوع البيانات في الاطلاع على البيانات وطلب تصحيحها أو محوها أو منع الدخول إلى البيانات المتعلقة به لا سيما إذا كانت البيانات غير كاملة أو غير صحيحة.[19]

2.تجاوز التحقيق الجنائي لخصوصية البيانات الشخصية تبعا لاعتبارات الأمن الوطني:

رعاية لبعض المصالح العليا للدول كصيانة أمنها الوطني وملاحقة الجرائم الجنائية بمختلف أشكالها بما فيهاالجرائم السيبرانية وإجراءات التحقيق الجنائي التي تخضع لها، أجازت غالبية اللوائح والتوجيهات والاتفاقيات الدولية، إلى جانب التشريعات الوطنية ذات الصلة بحماية البيانات الشخصية للدول بتجاوز أطر تنظيم هذه البيانات ومنح الأولوية لاعتبارات الأمن الوطني ومكافحة الجريمة في البيئة الرقمية.

1.2. تعريف التحقيق الجنائي الإلكتروني باستخدام البيانات الشخصية:

يقصد بالتحقيق الجنائي الالكتروني أو الرقمي؛ التحقيق الذي يرتكز في مختلف مراحله وعملياته على استخدام تقنيات التكنولوجية قصد الوصول إلى الأدلة الرقمية بصدد جريمة من الجرائم وتوثيق مكان وجود هذه الأدلة، وذلك عن طريق فحص هذا الدليل الذي قد يكون عبارة عن قرص صلب سجلات النظام، وسائط التخزين الخارجية، سجلات الموجة رسائل البريد الالكتروني، سجلات المحادثات، أجهزة الهاتف، شريحة الهاتف، سجلات قواعد البيانات، ثم تحليلها، أو استرجاع البيانات أو الملفات المحذوفة، والتي من شأنها أن تساهم في تقدم عملية التحقيق.[20]

وتحدد العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010 بوضوح جملة الإجراءات والعمليات التي تخضع لها البيانات الشخصية في إطار التحقيق الجنائي الالكتروني والتي تتمثل فيما يلي:

–تتبع المستخدمين الذي قد تكون لهم صلة مباشرة أو غير مباشرة بالجريمة الكترونيا

– تفتيش المعلومات المخزنة

– ضبط المعلومات المخزنة ونسخها والاحتفاظ بها

– جمع وتسجيل المعلومات وإلزام مزود الخدمة بالتعاون والمساعدة

– اعتراض معلومات المحتوى[21]

– نقل البيانات عبر الحدود وتداولها وتبادلها، بما فيها تلك المتعلقة بالحمض النووي وبصمات الأصابع وتسجيل المركبات.[22]

2.2. استثناء البيانات المتعلقة بالجرائم والأمن الوطني من نطاق الحماية المقررة للبيانات الشخصية:

على الرغم من أن غالبية اللوائح والتوجيهات والاتفاقيات الدولية، إلى جانب التشريعات الوطنية ذات الصلة بحماية البيانات الشخصية جعلت البيانات الشخصية للأفراد مشمولة بالحماية، غير أنها كذلك وفي نفس الوقت استبعدت من نطاق هذه الحماية البيانات الشخصية بما فيها البيانات ذات الطبيعة الخاصة أو الحساسة،والمرتبطة بالتحقيق الجنائي الالكتروني، بالنظر للأولوية التي تحوزها اعتبارات مكافحة الجريمة على حق الأفراد في حماية بياناتهم.

ويبرز هذا الاستثناء ضمن غالبية نصوص اللوائح والتوجيهات والاتفاقيات الدولية والتشريعات الوطنية الخاصة بحماية البيانات الشخصية، ويمكننا أن نورد في ذلك على سبيل المثال ما جاء ضمن المبادئ التوجيهية للأمم المتحدة لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الالكترونية لعام 1990 حيث جاء فيه:" لا يجوز السماح باستثناءات للمبادئ من 1 إلى 4 إلا إذا كانت ضرورية لحماية الأمن الوطني أو النظام العام."[23].

وأيضا في نص المادة 2 فقرة د من اللائحة العامة لحماية البيانات الشخصية GDPR2016/679الذي جاء فيه: " لا نطبق اللائحة على المعالجة التي تقوم السلطات المختصة لأغراض منع الجرائم أو التحقيق فيها أو كشفها أو مقاضاة مرتكبيها أو تنفيذ عقوبات جنائية بما في ذلك الحماية من الأخطار التي تهدد الامن العام ومنع مثل هذه التهديدات".

نجد استثناء مماثل كذلك ضمن أحكام اتفاقية الاتحاد الافريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية، حيث جاء في نص المادة 14 منها بأن:" 1-تتعهد الدول الأطراف بحظر أي جمع للبيانات ومعالجتها تكشف عن الأصل العرقي والاثني الإقليمي أو البنوة أو الآراء السياسية أو المعتقدات الدينية...

2-لا يسري الحظر المنصوص عليه في المادة 14 فقرة 1 على الفئات التالي:

هـ-عند إقامة اجراء قضائي أو التحقيق الجنائي".

من جهتها تتبنى الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010 التوجه ذاته حيث أحالت بشكل صريح للدول باتخاذ الإجراءات والتدابير الضرورية انطلاقا من قانونها الداخلية لتحديد الصلاحيات والإجراءات المتعلقة بالتحقيق الجنائي في الجرائم لا سيما الالكترونية منها.[24]

3.2. القيود والضمانات المقررة لحماية البيانات الشخصية في التحقيق الجنائي الرقمي:

يتضح مما ذكر أعلاه بأن اتفاقيات وتشريعات حماية البيانات الشخصيةتسمح للجهات والسلطات المختصة بمعالجة البيانات الشخصية كلما تعلق الأمر بالتحقيق والكشفعن الجرائموأن هذا الجواز يمتد للحظر الوارد على البيانات الشخصية ذات الطبيعة الخاصة (فئات البيانات الحساسة).

لا شك أن عمليات التحقيق الجنائي الالكتروني باستخدام بالبيانات الشخصيةوعلى الرغم من أنه يركز عادة على جمع المعلومات والأدلة المتعلقة بالجريمة محل التحقيق، غير أنه قد يؤدي أحيانا أو في الكثير من الأحيان إلى احتمال الكشف عن بيانات شخصية وحتى حساسة لا تتعلق بالجريمة محل التحقيق، ومراعاة لخصوصية البيانات الشخصية وحماية هذه الخصوصية.[25]

وبالرجوع إلى تشريعات ومواثيق حماية البيانات الشخصية نجدها في حقيقة الأمر وفي غالبيتها لا تعالج هذه النقطة، بل تتركها محل حماية التشريعات الوطنية للدول التي بدورها لم توفر قيود استثنائية خاصة بحماية البيانات الشخصية أثناء التحقيق الجنائي لاستخلاص الدليل الالكتروني باستثناء ما هو مكرس ضمن التوجيه الصادر عن البرلمان ومجلس الاتحاد الأوروبي رقم 680/2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية من قبل السلطات المختصة لأغراض منع

الجرائم الجنائية أو التحقيق فيها أو الكشف عنها أو تنفيذ العقوبات الجنائية وحرية نقل هذه البيانات، لا يحمي هذا التوجيه البيانات الشخصية للأفراد التي تتم معالجتها لأغراض منع الجرائم الجنائية أو التحقيق فيها أو الكشف عنها فحسب، بل يضمن أيضا مستوى عال من الأمان عند التدفق الحر لهذه البيانات بين السلطات المختصة.[26]

تضمن توجيه الشرطة رقم 2016/680 المشار إليه أعلاه جملة من الضمانات التي تكفل حماية البيانات الشخصية في مختلف مراحل التحقيق الجنائي الالكتروني والتي يتوجب على السلطات المختصة بالتحقيق مراعاتها وهي:

1.3.2.المشروعية:

يشترط أولا وقبل أي استخدام للبيانات الشخصية ومعالجتها في سياق التحقيق الجنائي الالكتروني أن تكون هذه المعالجة مشروعة، ومفاد ذلك أن تتم من قبل السلطة المختصة والمخولة قانونا بذلك

2.3.2. الضرورة والتناسب والغرض:

تفرض هذه الضمانة على السلطات المختصة بالتحقيق الجنائي أن تمتثل أثناء اجراء التحقيق وفي جميع مراحله لمبادئ الضرورة والتناسب والغرض، ومعنى ذلك أن يتم معالجة البيانات الشخصية عند التحقيق الجنائي وللأغراض وبالقدر الذي تقتضيه متطلبات التحقيق.[27]

3.3.2. الرقابة:

يقيد هذا المبدأ عمل السلطات المختصة بإجراء التحقيق الجنائي الالكتروني بالخضوع لرقابة سلطة مستقلة تتولى مهمة مراقبة مدى امتثال الجهات المعنية بالتحقيق الجنائي، وذلك بالإخطار المسبق لجهة الرقابة بعمليات التحقيق الجنائي على البيانات الشخصية واستخلاص الدليل الرقمي.[28]

4.2. الإشكالات التي يطرحها التحقيق الجنائي الالكتروني باستخدام البيانات الشخصية

على الرغم من أن الدول تقيد التحقيق الجنائي الالكتروني عند استخدام البيانات الشخصية في التحري عن الجرائم بجملة من القيود والتي تمثل في حقيقتها ضمانات لمصلحة الشخص موضوع البيانات على النحو المشار إليه أعلاه، إلا أن هذا لم يمنع من وجود إشكالات تعتري المحافظة أو ضمان خصوصية البيانات الشخصية للأفراد والتي يمكن إجماله فيما يلي:

-يلاحظ في الاجمال أن غالبية المواثيق العالمية والإقليمية المتعلقة بحماية البيانات الشخصية تحيل إلى التشريعات الوطنية للدول بيان الضمانات المتاحة لفائدة البيانات الشخصية عند استخدامها في سياق التحقيقات الجنائية الالكترونية، هذا ما يجعل معالجة البيانات الشخصية عند التحقيقات الجنائية خاضع لهامش تقدير كل دولة خاصة، وهذا ما من شأنه أن يؤدي إلى تباين واختلاف الحماية المقررة لهذه البيانات من دولة إلى أخرى.

-يلاحظ كذلك بأن غالبية المواثيق العالمية والإقليمية المتعلقة بحماية البيانات الشخصية تسمح للدول وفي إطار تشريعاتها الوطنية ذات الصلة بحماية هذه البيانات الشخصية، بمعالجة البيانات الشخصية في سياق التحقيق الجنائي، بل حتى لو تعلق الأمر بالبيانات الشخصية الحساسة ذات الطبيعة الخاصة التي تخضع لمبدأ حظر معالجتها، وبالتالي فليس هناك أية تفرقة أو تمييز بين فئات البيانات غير الحساسة والبيانات الشخصية الحساسة عند استخدامها في التحقيقات الجنائية

-الإشكال الآخر الذي يطرح بخصوص البيانات الشخصية عند التحقيق الجنائي الالكتروني ينصب حول ما اذا كانت البيانات الشخصية التي تم استخدامها عند التحقيق قابلة للاستخدام في تحقيق جنائي آخر أما لا، خاصة وأن غالبية المواثيق العالمية والإقليمية المتعلقة بحماية البيانات الشخصية أكدت على أن البيانات الشخصية الخاضعة للمعالجة يجب أن تكون ذات صلة بالغرض الذي تم تخزينها من أجله، غير أنها كذلك عبرت صراحة على إمكانية عدم التقيد بهذه الضمانة إلا في حال وجود نص في القانون الوطني لكل دولة أو في حال الاجراء كان لضرورة أملتها اعتبارات الأمن أو قمع الجريمة.[29]

الخاتمة:

في ختام هذه الورقة البحثية يمكننا القول، أن تكريس الحق في حماية البيانات الشخصية وخصوصية هذه البيانات، وبقدر ما أدى إلى ضمان حماية هذه البيانات انطلاقا من حق الفرد في الحياة الخاصة وعدم الكشف عنها لعموم الناس، لكنه كذلك اصطدم أولوية أسمى وهي اعتبارات الأمن الوطني للدولة، في مكافحة الجرائم عن طريق التحقيق الجنائي في هذه الجرائم ذات الطبيعة الخاصة التي كانت محل بحث هذه الدراسة التي تم من خلالها التوصل للنتائج الآتية:

-أن الحق في حماية البيانات الشخصية وإن كان حقا قائما بذاته، لكنه يرتبط ارتباطا وثيقا بالحق في الخصوصية، بل ويعتبر جزء منه.

-بسبب الطبيعة الدولية للجرائم الالكترونية المرتكبة في الفضاء الرقمي، تجيز المواثيق الدولية والتشريعات الوطنية المعنية بحماية البيانات الشخصية، بمعالجة هذه البيانات في سياق التحقيق الجنائي الالكتروني والبحث عن الأدلة.

-أن التحقيق الجنائي الالكتروني باستخدام البيانات الشخصية ومراعاة للأمن الوطني للدولة لا يقتصر في نطاقه على فئة البيانات الشخصية العادية فحسب، بل يمتد ويشمل كذلك فئات البيانات الشخصية ذات الطبيعة الخاصة أو الحساسة المتمثلة في البيانات الصحية، الجينية، البيانات المتعلقة بالعرق والتقاليد والآراء والمعتقدات الدينية والسياسية، البيانات المتعلقة بالعضوية النقابية، وهي البيانات التي يحظر معالجتها كقاعدة عامة.

-أن معالجة البيانات الشخصية في سياق التحقيق الجنائي الالكتروني، غير مطلق بل يخضع لقيود تعد بمثابة ضمانات لمصلحة الشخص موضوع البيانات محل التحقيق الجنائي، وتستهدف بالدرجة الأولى ضمان خصوصية هذه البيانات عند معالجتها، وتشمل هذه القيود: مشروعية المعالجة عند التحقيق الجنائي الضرورة والتناسب والغرض، والرقابة

لكن وعلى الرغم من إقرار هذه الضمانات حماية لخصوصية البيانات الشخصية للفرد، غير أن التحقيق الجنائي من شأنه كما لاحظنا أن يجعل بيانات الافراد عرضة لمخاطر، كما أنه من جهة أخرى يثير إشكالات تتعلق على وجه الخصوص بالبيانات الحساسة التي تختلف في طبيعتها عن بقية البيانات وتستدعي التعامل معها بحرص أكبر، وعليه فإننا من وجهة نظرنا نقترح لتجاوز هذه الإشكالات ما يلي:

-بخصوص فئات البيانات الشخصية عند التحقيق فهنا وجب التمييز بين البيانات الشخصية الحساسة والبيانات الشخصية الأقل حساسية إذ وجب أن تعامل البيانات الشخصية الحساسة بطريقة أكثر حرص لا سيما وأنها ترتبط بحقوق وحريات الأفراد.

-إقرار مبادئ أكثر صرامة تحمي فئات البيانات الحساسة، وعدم اخضاعها لذات المبادئ والقيود التي تسري على كافة البيانات الشخصية

-استبعاد البيانات الشخصية التي لا تتعلق بموضوع التحقيق أثناء عمليات التحقيق قدر الإمكان

-وجوب مراعاة توحيد وتوضيح مبادئ حماية البيانات الشخصية عند مباشرة إجراءات التحقيق الالكتروني خاصة أثناء نقل هذه البيانات عبر الحدود بين الدول.

الهوامش:

[1]المادة 1 من الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات المعدلة، جامعة الدول العربية، المعتمدة في 21 ديسمبر 2011، على الرابط التالي: https://www.courts.gov.ps › userfiles › file

[2]المادة 1 من اتفاقية الاتحاد الأفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية، المعتمدة في 27 جوان 2014، دخلت حيز النفاذ في 11 ماي 2020، على الرابط التالي:

https://au.int/sites/default/files/treaties/29560-treaty-0048__african_union_convention_on_cyber_security_and_personal_data_protection_a.pdf

[3]Lifrange, M, Protection des données à caractère personnel .(diplôme master), Faculté de Droit, de Science Politique, Belgique, 2018, pp 11-12.

[4]Journal officiel de l'Union européenne.(2016). 27 avril .Règlement (UE) 2016/679 du Parlement Européen et du Conseil. Sur le site : eur-lex.europa.eu consultè le 2/7/2020.

[5]المادة 2 من القانون رقم 07/18 المؤرخ 2018/6/10، المتعلق بحماية الاشخاص الطبيعين في مجال المعطيات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، المؤرخة في10 يونيو2018، العدد 34.

[6]عثمان بكر عثمان، المسؤولية عن الاعتداء على البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، مجلة جامعة طنطا، دون تاريخ نشر، ص 8.

[7]أحمد محمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي دراسة مقارنة مجلة كلية الشريعة والقانون، مصر، 2018،العدد 33، صص 1946، 1947.

[8]إرشادات الإسكوا للتشريعات السيبرانية، الإرشاد الرابع المتعلق بمعالجة وحماية المعطيات ذات الطابع الشخصي، بيروت 2012، ص 98، على الرابط التالي: https://www.unescwa.org

[9]أحمد محمد المعداوي، المرجع السابق، ص 1950.

[10]Wang. M, Jiang. Z,The Defining Approaches and Practical Paradox of Sensitive Data , I J C, N.11, 2017, P 5.

[11] راجع حيثيات حكم المحكمة الأوربية لحقوق الانسان وحرياته الأساسية على الرابط التالي:

https://rm.coe.int/t-pd-2018-15-case-law-on-data-protection-may2018-en/16808b2d36

[12]البند رقم 10 من التعليق العام رقم 16/ 1988: **الحق في حرمة الحياة الخاصة. المادة 17 من العهد الدولي الخاص بالحقوق المدنية والسياسية**، اللجنة المعنية بالحقوق الاقتصادية والاجتماعية والثقافية، الدورة 34 (1988).

[13]المادة 8 من ميثاق الحقوق الأساسية للاتحاد الأوربي، ديسمبر 2000، على الرابط التالي:

http://hrlibrary.umn.edu/arab/eu-rights-charter.html#:

[14]محمد علي سالم، عبيد هجيج، الجريمة المعلوماتية، مجلة جامعة بابل العلوم الإنسانية، العدد 39. المجلد 14، 2007ص 93.

[15]إرشادات الإسكوا للتشريعات السيبرانية، الإرشاد الرابع المتعلق بمعالجة وحماية المعطيات ذات الطابع الشخصي، المرجع السابق، ص 93.

[16]أحمد محمد المعداوي، المرجع السابق، تهميش رقم 1، ص 1950.

[17]Art 5 Règlement (UE) 2016/679 du Parlement Européen et du Conseil, op.cit.

[18]المادة 22 من اتفاقية الاتحاد الأفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية، المرجع السابق.

[19]إرشادات الإسكوا للتشريعات السيبرانية، الإرشاد الرابع المتعلق بمعالجة وحماية المعطيات ذات الطابع الشخصي، المرجع السابق، ص 95.

[20]رضوان أسخيطة، التحقيق الجنائي الرقمي في ضوء قوانين حماية البيانات الشخصية، مجلة العلوم السياسية والقانون المركز الديمقراطي العربي، برلين، المانيا، المجلد 3، العدد 17، سبتمبر 2019، ص ص 41، 43.

[21]أنظر المواد 24، 26، 27، 28، 29 من الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات المعدلة، جامعة الدول العربية، المرجع السابق.

[22]معاهدة بروم الموقعة في 25 ماي 2005 بشأن تبادل البيانات الشخصية من قبل الشرطة على الحدود،الاتحاد الأوربي الموقعة في 25 ماي 2005، دخلت حيز النفاذ في 4 افريل 2007، على الرابط التالي:

https://edps.europa.eu/data-protection/our-work/publications/opinions/cross-border-cooperation-pr%25C3%25BCm-treaty_en

[23] المبدأ رقم 6 من المبادئ التوجيهية للأمم المتحدة، (1990)، تنظيم ملفات البيانات الشخصية المعدة بالحاسبة الالكترونية. الجمعية العامة. القرار 95/ 45 على الرابط التالي:http://hrlibrary.umn.edu.

[24]تنص المادة 22 من الاتفاقية العربية لمكافحة جرائم تكنولوجيا المعلومات لعام 2010 بأن تلتزم كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والإجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث من هذه الاتفاقية.

[25]Rob van den Hoven ,van Genderen, Cybercrime investigation and the protection of personal data and privacy, Council of Europe, Economic Crime Division Directorate General of Human Rights and Legal Affairs Strasbourg, France, 25/3/2008, P 5.

[26]Journal officiel de l'Union européenne.(2016). 27 avril .Règlement (UE) 2016/680 du Parlement Européen et du Conseil. sur le site : eur-lex.europa.eu consultè le 2/7/2020.

[27]Art 8 ,Ibed.

[28]Art 4 ,Ibed.

[29]Rob van den Hoven ,vanGenderen, op.cit, p 26.

جامعة الجزائر 1
كلية الحقوق سعيد حمدين
الملتقى الدولي: القانون الجنائي في ظل التطور التكنولوجي – إشكالات ومعالجات
عنوان المداخلة: حق المشتبه فيه في المساواة في الأسلحة في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال
المحور الخامس: تحديات استعمال الدليل العلمي بالنسبة لحقوق الإنسان
الأستاذ صيدي عبد الرحمان أستاذ محاضر أ بكلية الحقوق جامعة الجزائر 1
a.sidi@univ-alger.dz – sidiabderrahmane2014@gmail.com

مقدمة

لا جدال في أن العصر الحالي هو عصر التطور التكنولوجي وعصر المعلومات لأهميتها في كل مجالات الحياة، لكن صاحب هذا التطور ظواهر إجرامية مستحدثة استغل مرتكبوها التطور الهائل في تكنولوجيات الإعلام والاتصال من اجل تسهيل أعمالهم الإجرامية والإفلات من المسؤولية، لذلك لجأت جل التشريعات لانتهاج سياسات جنائية من اجل حماية المصالح التي يوفرها هذا التطور التكنولوجي في مجال الإعلام والاتصال من جهة، وتفادي الآثار السلبية الناتجة عنه من جهة أخرى.

وانعكس تأثير هذه الوسائل الالكترونية على القوانين الموضوعية والإجرائية خاصة فيما يتعلق بإثبات هذا النوع من الإجرام الناتج عن تطور تكنولوجيات الإعلام والاتصال، وتحتم اللجوء الى طرق جديدة للإثبات في هذا المجال، كالتفتيش والحجز الالكتروني، الترصد والمراقبة الالكترونية، والتي تتطلب تخصصا تقني عال، ما حتم وضع مؤسسات متخصصة للوقاية من هذه الجرائم ومكافحتها متمثلة في الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال، والقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ونظرا لخطورة هذا النوع من الإجرام وصعوبة الكشف عنه وإثباته فقد خرج المشرع عن القواعد العامة التي تحكم البحث عن الدليل، ووضع أساليب تحري خاصة لاسيما في مرحلة جمع الاستدلالات والتي تعتبر نواة الدعوى العمومية التي تحدد مصير المتهم.

ومن جهة أخرى يضمن الدستور وقانون الإجراءات الجزائية محاكمة عادلة لكل متهم، ومن ضمن مبادئ المحاكمة العادلة أن تقوم على المساواة بين الخصوم في جميع مراحل الدعوى العمومية لاسيما المساواة في منح الأسلحة للأطراف للدفاع عن أنفسهم وتمكينهم من تقديمها على قدم المساواة.

ونظرا للتخصص العالي للهيئات والأشخاص التي تقوم بإجراءات البحث والتحري في هذه الجرائم فإنه يطرح التساؤل حول حق المتهم في الدفاع عن نفسه وعن الخلل الذي يحدثه هذا التخصص بين طرفي الدعوى العمومية لاسيما من حيث المساواة في تقديم الأسلحة في هذه المرحلة الحاسمة من مراحل الدعوى العمومية.

ويطرح موضوع المداخلة إشكالية **مدى ضمان حق المشتبه فيه في المساواة في تقديم الأسلحة في مرحلة البحث والتحري في الجرائم المتصلة بتكنولوجيات الإعلام والإتصال؟**

ولمعالجة هذه الإشكالية إرتئينا تقسيم الموضوع الى مبحثين، نتناول في المبحث الأول البحث والتحري في جرائم تكنولوجيات الإعلام والاتصال، في المطلب الأول المتخصصين في البحث والتحري والمطلب الثاني أساليب التحري الخاصة. أما المبحث الثاني فيتناول الحق في المساواة في الأسلحة في مرحلة البحث والتحري ضمن مطلبين، في المطلب الأول: حق المشتبه فيه في المساواة في الأسلحة في مرحلة البحث والتحري، وفي المطلب الثاني: مدى احترام المشرع للحق في المساواة في الأسلحة في مرحلة البحث والتحري.

المبحث الأول: البحث والتحري في جرائم تكنولوجيات الإعلام والاتصال

الاستدلال هو مجموعة من الإجراءات التمهيدية السابقة على تحريك الدعوى العمومية تهدف إلى جمع المعلومات بشأن جريمة ارتكبت وتقديمها للنيابة لتتخذ بناء عليها قرار تحريك الدعوى العمومية من عدمه تمثل مرحلة الاستقصاء أو جمع الأدلة مرحلة تمهيدية في الدعوى العمومية، حيث تكون الجريمة الواقعة مازالت غامضة وتنقصها الأدلة اللازمة لإدانة الفاعل لذلك من مهام الشرطة القضائية كشف غموض

الجريمة والإحاطة بمختلف ملابساتها، والبحث عن الأدلة وتعقب فاعليها والربط بين مختلف عناصرها[1] وبالنسبة للبحث والتحري في جرائم تكنولوجيات الإعلام والاتصال فيقوم بها متخصصون ويمكن اللجوء فيها الى أساليب التحري الخاصة.

المطلب الأول: المتخصصين في البحث والتحري في جرائم تكنولوجيات الإعلام والاتصال

نصت المادة 11من ق إ ج على انه "تكون إجراءات التحري سرية، ما لم ينص القانون على خلاف ذلك ودون إضرار بحقوق الدفاع"

ونصت المادة 12 يقوم بمهمة الشرطة القضائية القضاة والضباط والأعوان والموظفون المبينون في هذا الفصل ... ويناط بالشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها مادام لم يبدأ فيها تحقيق قضائي." كما نصت المادة 13 على أنه إذا ما فتح التحقيق فإن على الضبط القضائي تنفيذ تفويضات جهات التحقيق وتلبية طلباتها"

المادة 17 يباشر ضباط الشرطة القضائية السلطات الموضحة في المادتين 12 و 13 ويتلقون الشكاوى والبلاغات ويقومون بجمع الاستدلالت واجراء التحقيقات الابتدائية.

ونصت المادة 35 ق إ ج على أنه يمكن للنيابة العامة الاستعانة في مسائل فنية بمساعدة متخصصين، يساهم المساعدون المتخصصون في مختلف مراحل الإجراءات تحت مسؤولية النيابة العامة التي يمكنها ان تطلعهم على ملف الإجراءات لانجاز المهام المسندة إليهم ... تنجز الأعمال التي يقوم بها المساعدون المتخصصون في شكل تقارير تلخيصية أو تحليلية يمكن ان ترفق بالتماسات النيابة العامة.

لقد نص المشرع في القانون رقم 09-04 المؤرخ في 05 غشت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في المواد 13 و14 منه على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفية سيرها، وحدد المرسوم الرئاسي رقم 19-172 المؤرخ في 06-01- 2019 [2] تشكيلة هذه الهيئة، والتي تعتبر بحسب المادة الثانية منه مؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني.

وتنص المادة 11 منه على أن تكلف المديرية التقنية بمهمة المراقبة الوقائية للاتصالات الالكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة، وتتولى هذه المديرية بحسب المادة 12، مساعدة السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التي تتطلب اللجوء الى أساليب التحري الخاصة للهيئة.

جمع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها وتتبعها بغرض استعمالها في الإجراءات القضائية. ونصت المادة 13 على ان تمارس المديرية التقنية مهامها المرتبطة بالشرطة القضائية وفقا لأحكام قانون الإجراءات الجزائية.

أما المادة 65 مكرر 8 فنصت على أنه يجوز لوكيل الجمهورية او ضابط الشرطة القضائية الذي إذن له ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه ان يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية او خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5 .

ويحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري.[3]

---

[1] جلال ثروت، سليمان عبد المؤمن، اصول المحاكمات الجزائية، المؤسسة الجامعية للدراسات والنشر والتوزيع، الطبعة الاولى، بيروت لبنان ، 1996، ص 394.

[2] المنشور في الجريدة الرسمية رقم 37 المنشورة في 9 يونيو 2019

[3] المادة 65 مكرر 09 من ق إ ج

ويصف أو ينسخ ضابط الشرطة القضائية المأذون له أو المناب المراسلات أو الصور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة في محضر يودع بالملف.[1]
إذن يقوم بعملية البحث والتحري في جرائم تكنولوجيات الإعلام والاتصال فئة خاصة تتمثل في المديرية التقنية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

المطلب الثاني: أساليب التحري الخاصة.

لم تعد الطرق التقليدية المتبعة في البحث عن الأدلة والوصول إليها تصلح أو تكفي للوصول الى الأدلة المتحصلة من الوسائل الالكترونية، بل وجب إتباع طرق جديدة تتناسب مع هذه الأدلة، ويمكن بإتباعها إثبات الجرائم التي تقع على العمليات الالكترونية بواسطة تدخل مباشر من طرف محققين مؤهلين ومختصين وخبراء في تقنية وعلوم الكمبيوتر.[2]
لقد نصت المادة 65 مكرر 5من قانون الإجراءات الجزائية على أنه إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو في التحقيق الابتدائي في جرائم المخدرات أو في الجرائم المنظمة العابرة للحدود الوطنية، أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، أو جرائم تبييض الأموال أو الإرهاب، أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:
-اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية
-وضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص. ....
وتنص المادة 65 مكرر 11 " عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة أدناه.
تعتبر جرائم تكنولوجيات الإعلام والاتصال من الجرائم التي أجاز المشرع اللجوء فيها الى أساليب التحري الخاصة، وهي أساليب تعطي سلطة استثنائية للشرطة القضائية تخرج عن القواعد العامة التي تحكم الاستدلال وتمس أكثر بحقوق وحريات المشتبه فيه، وتتمثل أساليب التحري الخاصة في:

أولا: الخبرة القضائية

إن اللجوء للمختصين في مجال المعلوماتية لا ينحصر فقط في الخبرة المنصوص عليها في المادة 143 وما بعدها من قانون الإجراءات الجزائية بالرغم من كونها الأكثر تطبيقا أمام المحاكم. هذه المهمة تترجم في تدبير يتخذ من طرف القاضي لتعيين تقني لمعالجة وضعية واقعة تتطلب إنارتها وإعطاء رأي تقني بحت حول الأسئلة التي يطرحها، لذلك فإن قانون الإجراءات الجزائية دقق في أن الخبرة يمكن أن تلتمس عندما يطرح سؤال تقني،[3] فهي تشكل فكرة آنية للعدالة الجزائية تقدم في كثير من الأحيان في شكل تقرير في وقت معين.
ونظم المشرع تدخل التقنيين في مرحلة البحث والتحري من خلال مخابر الفحص التقني التابعة للضبطية القضائية كمعهد الأدلة الجنائية وعلم الإجرام التابع لقيادة الدرك الوطني، ومخابر الشرطة العلمية، بحيث يمكن اللجوء لهذه المخابر في مرحلة البحث والتحري ويمكن أن تعتبر كشبه خبرة.
ويشكل الفحص التقني في مادة تكنولوجيات الإعلام والاتصال أثناء مرحلة البحث أهمية كبيرة، لأنه يسمح برفع الأدلة الأولية حول الجريمة، كما أن مرحلة البحث تشكل نقطة تحول للمتابعة فهذه البداية هي النبض الأساسي للإجراءات اللاحقة.

---

[1] المادة 65 مكرر 10 من ق إ ج
[2] مناصرية يوسف، الدليل الالكتروني في القانون الجزائي، الطريق الى تحول ادلة الاثبات في المادة الجزائية، دراسة مقارنة، دار الخلدونية، 2018، ص 299.
([3])-المادة 143 و146 من قانون الإجراءات الجزائية

وإلى جانب الخبراء هناك نوع آخر من المتخصصين لهم وجود دائم في العدالة الجنائية، ويتعلق الأمر بمساعدين مختصين تلجأ إليهم النيابة على طول طريق الإجراءات. جاء بهم تعديل قانون الإجراءات الجزائية بموجب الأمر 15-02 لمساعدة النيابة في معالجة القضايا المعقدة يدعون المساعدين المتخصصين، يساهمون في مختلف مراحل البحث والتحري تحت مسؤولية النيابة العامة والتي يمكنها أن تطلعهم على ملف الإجراءات لانجاز المهام المسندة إليهم. في كامل طريق الإجراءات الجزائية عن طريق القيام بعملية التحليل والتلخيص وتحرير تقارير تقدم للنيابة العامة للاستعانة بها في اتخاذ القرارات الملائمة في شأن المتابعة وتقديم الطلبات. ويمكن بحسب المادة 35 مكرر من قانون الإجراءات الجزائية أن ترفق هذه التقارير بالتماسات النيابة العامة وهي ليست ملزمة بوضع هذه التقارير في الملف ليطلع عليه الخصم ويقوم بمناقشته، ثم ما مصير المحادثات والملاحظات والتوجيهات الشفوية التي يقدمها هذا المختص ولا توضع في الملف، فهذه الوضعية تشكل إخلال واضح بمبادئ المحاكمة العادلة المنصوص عليها في المادة الأولى من قانون الإجراءات الجزائية لاسيما مبدأي التوازن في الأسلحة والوجاهية.
ونظرا لما تلعبه الخبرة من دور مركزي في الدعوى الجزائية لأن من شأنها أن تغير مسار الدعوى عندما يتعلق الأمر بتحقيقات تقنية وجب على القاضي الذي يلجأ إلى الخبرة أن يراعى التوازن بين الأطراف، وهو المبدأ الذي يحكم الإجراءات الجزائية، وتكون المحافظة على التوازن بين الأطراف في الدعوى الجزائية عبر منح إمكانية لكل طرف باسم المساواة في الأسلحة إجازة الخبرة، وكذلك مناقشة الخبرة الغير المناسبة ودحضها تحقيقا لمبدأ الوجاهية.

وفيما يتعلق بتعيين الخبير فإن اللجوء إلى خبير معلوماتي ليس ممكن بالنسبة للمشتبه فيه بالرغم من أن الضبطية القضائية في إطار البحث والتحري وتحت إشراف وكيل الجمهورية يمكن لهم اللجوء إلى أشخاص مؤهلين ومخابر أدلة، إلا أن الشخص المتابع لا يمنح له أي دور قانوني موازن، لذلك فإن الخلل في المساواة يكمن في هذه المرحلة من الإجراءات.
وتعتبر هذه الوضعية غير ملائمة بالنسبة للشخص محل المتابعة في الجرائم المتصلة بتكنولوجات الاعلام والاتصال التي تجريها السلطات القضائية ومنها تحقيقات الضبطية القضائية التي تعتبر تحقيقات أولية جد واسعة ومعمقة،

التفتيش الالكتروني

نصت المادة 05 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد الى
أ-منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.
ب-منظومة تخزين معلوماتية ...
ويمكن تمديد التفتيش الى منظومة معلوماتية أخرى مخزنة فيها معطيات أو الى منظومة معلوماتية تقع خارج الإقليم الوطني، كما يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها.
ويكون التفتيش بحسب المادة 03من القانون 09-04 مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، وتكون وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية.

ثانيا: الحجز الالكتروني

نصت المادة 06 من القانون 09-04 على أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية...
ويجوز للسلطة التي تقوم بالتفتيش والحجز استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل

هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، بشرط أن لا يؤدي ذلك الى المساس بمحتوى المعطيات.
ونصت المادة 07 على أنه إذا استحال إجراء الحجز وفقا لأحكام المادة 6 لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول الى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.
ويمكن بحسب المادة 8 للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة.
وتتضمن الإجراءات الواجب اتخاذها حجز عتاد ودعائم التخزين للإعلام الآلي وعندما تكون المعطيات مخزنة بنظام التشغيل ولا تسمح خصائصه القيام بإجراء نسخة للمعطيات تحجز دعامة التخزين ذاتها. [1]

ثالثا: التنصت والمراقبة الالكترونية

يمكن اللجوء للمراقبة الالكترونية للحفاظ على النظام العام والوقاية من الجرائم الخطيرة مثل الجرائم الإرهابية والجرائم الماسة بأمن الدولة، فيجيز القانون وضع ترتيبات تقنية وبرامج معلوماتية على مستوى متعاملى الانترنت من أجل القيام بعمليات الرقابة على الاتصالات الالكترونية مع جمع وتسجيل محتواها في الوقت الحقيقيين، فهي مراقبة موجهة ووقتية يأذن بها القضاء بترخيص مكتوب.[2]
ونصت المادة 11 من المرسوم الرئاسي رقم 19-172 [3] على أنه تكلف المديرية التقنية بمهمة المراقبة الوقائية للاتصالات الالكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة.
ونصت المادة 12 على أن تتولى المديرية التقنية ... مساعدة السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها ، بما في ذلك في مجال الخبرات القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التي تتطلب اللجوء الى أساليب التحري الخاصة للهيئة.
المراقبة بالفيدو: اعتمد المشرع تقنية المراقبة بالفيديو سنة 2009 بإنشائه مؤسسة إنجاز أنظمة المراقبة بواسطة الفيديو [4] وهي تقنية للاطلاع والاستباق تساهم في مكافحة الإرهاب والوقاية من الأعمال الإجرامية وحماية الأشخاص والممتلكات، وكذا الحفاظ على النظام العام، وضبط حركة السير عبر الطرق ومعاينة المخالفات لقواعد حركة المرور عبر الطرق وكذا تامين البنايات والمواقع الحساسة، وتسيير وضعيات الأزمة والكوارث الطبيعية او غيرها.
وحدد المشرع الأماكن المعنية بالمراقبة بواسطة الفيديو وحصرها في اربع حالات متعلقة بأماكن عامة مفتوحة للجمهور، وهي التجمعات الحضرية الكبرى وأماكن ضواحي المدن، ومحاور الطرق الكبرى لاسيما مقاطع الطرق ذات الحركة الكثيفة، والأماكن المفتوحة للجمهور كالموانئ والمطارات والمنشآت الرياضية الكبرى، والمؤسسات الاقتصادية الكبرى.
وتكون المراقبة بالفيديو في هذه الأماكن محصورة في يد السلطات العمومية فقط

رابعا: الاعتراض والالتقاط الالكتروني

بالرجوع الى المادة 65 مكرر 05 من ق إ ج ينفذ هاذين الإجرائين بموجب إذن من وكيل الجمهورية في التحري في الجريمة المنظمة العابرة للحدود الوطنية وجرائم المخدرات والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد، عندما تقتضي دواعي التحريات اللجوء لهذا الإجراء.
ويسمح هذا الإذن لضابط الشرطة القضائية بالدخول الى المحلات السكنية أو غيرها حتى خارج المواقيت القانونية وبغير علم أو رضى الأشخاص الذين لهم الحق على تلك الأماكن، ويمكن لوكيل الجمهورية أو

---

[1] مناصرة يوسف، المرجع السابق، ص 413.
[2] المادة 04 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
[3] يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها، الصادر بتاريخ 06 يونيو 2019 المنشور في الجريدة الرسمية عدد 37 المنشورة بتاريخ 9 يونيو 2019 ص 05
[4] المادة 65 مكرر 08 من ق إ ج

ضابط الشرطة القضائية الحاصل على الإذن أن يسخر كل عون مؤهل لدى هيئة أو مصلحة مكلفة بالمواصلات السلكية واللاسلكية كمتعاملي الهاتف النقال أو مقدموا خدمة الانترنت للتكفل بالجوانب التقنية للعمليات المذكورة أعلاه.[1]

وعلى ضابط الشرطة القضائية تحرير محضر عن أي عملية اعتراض أو تسجيل أو وضع ترتيبات تقنية وعمليات الإلتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري ويذكر بداية هذه العمليات والانتهاء منها، كما يودع أي تسجيل او اعتراض أو نسخ تم أثناء عملية المراقبة بالملف.[2]

ويهدف الالتقاط الالكتروني للسماح بمعرفة النصوص المسجلة والمحفوظة على دعامة كالمفتاح أو القرص المضغوط أو على الحاسوب المستهدف.

وتمكن هذه الإجراءات من التعرف على المبحوث عليهم عن طريق معطيات الاتصالات الهاتفية والمعلوماتية والمعلومات التقنية عن الأجهزة الالكترونية والمعلوماتية المستخدمة في الاتصالات السلكية واللاسلكية بتحديدها لرقم المتعامل، الأرقام الهاتفية العناوين، البريد الالكتروني للمتصلين والمتصل بهم، وتمكن من إسناد الوقائع إلى أصحابها.[3]

ويقوم بهذه المهمة بحسب المادة12 من المرسوم رقم 19-172 المديرية التقنية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

خامسا: التسرب الالكتروني

عرف المشرع التسرب في المادة 65 مكرر 12 بأنه " قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو مخفي.

ونص المشرع في المادة 56 من القانون 06-01 المتعلق بالوقاية من الفساد ومكافحته على إمكانية اللجوء لأساليب التحري الخاصة المتمثلة في الترصد الالكتروني والاختراق دون أن تعرفهما، كما نصت المادة 40 من الأمر 05-06 المتعلق بمكافحة التهريب إذ نص في المادة 33 منه على إمكانية اللجوء الى أساليب تحري خاصة.

لا يمكن الجزم بان النصوص المذكورة أعلاه تجيز صراحة اللجوء إلى التسرب الالكتروني بصريح العبارة.

سادسا: تحديد التموقع الالكتروني

تحديد الموقع الجغرافي هو تقنية معرفة مكان وجود شخص بشكل دقيق الى حد ما، إما باستخدام عنوان IP، وإما عبر اتصال الشبكة اللاسلكية، أو عبر برج التغطية الخلوية الذي يتصل به الهاتف النقال، أو عبر شريحة GPS التي تحسب مكانك نسبة الى خطوط الطول والعرض من المعلومات التي ترسلها الأقمار الصناعية من السماء، وينطوي هذا النظام على معطيات ذات طابع شخصي كرقم الهاتف ولوحة الترقيم، وهي تشكل معالجة آلية لمعطيات شخصية.[4]

ولا يوجد في التشريع الجزائري نص يجيز اللجوء لتقنية تحديد التموقع الجغرافي مع أن الضبطية القضائية تقوم في الواقع بوضع معدات تتبع بمركبات المشتبه فيهم، وهي تسمح بمراقبة الأشخاص بدقة وتوقيفهم في التوقيت المناسب متلبسين بالجريمة، لكن ومع غياب النص القانوني المجيز لعمليات تحديد التموقع الجغرافي لا يسمح للضبطية بتسجيل تحركات المشتبه فيهم على محاضر رسمية وتقديمها كدليل إثبات الكتروني في الملف الجزائي.[5]

---

[1] مناصرة يوسف، المرجع السابق، ص 413.

[2] المادة 65 مكرر 09 من ق إ ج

[3] مناصرة يوسف، المرجع السابق، ص 463.

[4] مناصرة يوسف، المرجع السابق، ص 486 هامش رقم 2.

[5] المرجع السابق، ص 487.

لقد استعمل المشرع هذه التقنية بواسطة السوار الالكتروني كآلية للرقابة القضائية، ويتمثل الوضع في المراقبة الالكترونية في إجبار أو تكليف شخص موضوع تحت يد العدالة بالالتزام بمكان محدد وفي مواقيت زمنية مبينة.[1]

واستعمل المشرع في قانون تنظيم السجون المراقبة الالكترونية عن طريق السوار الالكتروني كبديل للعقوبات السالبة للحرية القصيرة المدة.

المبحث الثاني: الحق في المساواة في الأسلحة في مرحلة البحث والتحري

وفقا لمبدأ الشرعية الإجرائية، يجب أن يعني التحقيق الابتدائي بالموازنة بين حق الدولة في العقاب وأصل البراءة، وهو ما يقتضي التوفيق بين مقتضيات فعالية الإجراءات وضمان الحقوق والحريات.

ويتوقف تقييم التنظيم الإجرائي في بلد ما على مدى التوفيق الذي يحققه القانون بين مقتضيات فعالية الإجراءات وعدم تقييد حقوق المتهم وحرياته وخاصة حقوقه في الدفاع[2] لذلك سنتطرق لمصدر هذا الحق ومقتضياته ثم ننظر مدى ضمانه للمشتبه فيه في قانون الإجراءات الجزائية.

المطلب الأول: حق المشتبه فيه في المساواة في الأسلحة في مرحلة البحث والتحري

لم يتم الإعلان صراحة عن مبدأ تكافؤ وسائل الدفاع في المواثيق الدولية لحماية حقوق الإنسان، ولكن تم تكريسه من خلال السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان وأصبح ركيزة أساسية ضمن الحق في محاكمة عادلة.

ويندرج هذا المبدأ ضمن المبادئ الدستورية المتعلقة بالمساواة أمام القانون والقضاء والحق في محاكمة عادلة وتساوي الأسلحة بين أطراف الخصومة المنصوص عليها في المواد 37 التي تنص على أن " كل المواطنين سواسية أمام القانون، ولهم الحق في حماية متساوية ..." والمادة 41 على " كل شخص يعتبر بريئا حتى تثبت جهة قضائية إدانته، في إطار محاكمة عادلة" والمادة 165 التي تنص على أن " يقوم القضاء على أساس مبادئ الشرعية والمساواة" ونصت المادة 175 على أن " الحق في الدفاع معترف به" الحق في الدفاع مضمون في القضايا الجزائية" والمادة 177 يحق للمتقاضي المطالبة بحقوقه أمام الجهات القضائية، ويمكنه أن يستعين بمحام خلال كل الإجراءات القضائية."

ونصت المادة 11 من الإعلان العالمي لحقوق الإنسان، والمادة 14 من العهد الدولي الخاص بالحقوق المدنية والسياسية، والمادة 13 من الميثاق العربي لحقوق الإنسان، والمادة 03 من الميثاق الأفريقي لحقوق الإنسان والشعوب.

إن مبدأ المساواة أمام القضاء هو وسيلة لتقرير الحماية القانونية المتكافئة للحقوق والحريات، وأن حقوق الإنسان مترابطة لا تقبل التجزئة فإن الإخلال بحق المساواة أمام القانون يؤثر على الحق في محاكمة عادلة التي يعتبر حق الدفاع فيها الركيزة الجوهرية والإخلال به يفقد المحاكمة العادلة قيمتها، ومن بين المساواة الفعلية بين أطراف الخصومة دون تمييز بينها، المساواة في القواعد الإجرائية التي تستلزم تكافؤ الفرص بين الدفاع والنيابة ويجب أن تكون لهما نفس الحقوق.

يتطلب مبدأ تكافؤ وسائل الدفاع في المسائل الجزائية أن يكون كل طرف في المحاكمة قادر على عرض قضيته في ظل ظروف لا تضعه في وضع غير موات بشكل واضح مقارنة بخصمه، ويعني ضمنيا المساواة بين الأطراف في الوصول إلى المعلومات ولاسيما الحق في الاطلاع على الملف.

المطلب الثاني: مدى احترام المشرع للحق في التوازن في الأسلحة بين المشتبه فيه والنيابة.

بعدما تناولنا في المبحث الأول القائمين بالبحث والتحري في الجرائم الماسة بتكنولوجيات الإعلام والاتصال من الشرطة القضائية والمخابر التابعة لها، وكذا المديرية التقنية التابعة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وإمكانية اللجوء لأساليب التحري الخاصة. ورئينا في المطلب الاول من المبحث الثاني معنى الحق في المساواة في الأسلحة كأحد ركائز الحق في المحاكمة العادلة ومصادره القانونية الدولية والداخلية نبحث في هذا المطلب مدى احترام هذا الحق في قانون

---

[1] انظر المادة 125 مكرر 1 من ق ا ج .

[2] احمد فتحي سرور، الوسيط في قانون الإجراءات الجزائية، الكتاب الأول، دار النهضة العربية، الطبعة الرابعة، 2014، ص 825

الإجراءات الجزائية الجزائري من خلال فرعين في الفرع الأول الحق في الدفاع في مرحلة البحث والتحري، وفي الفرع الثاني الاطلاع على أدلة النيابة العامة ومناقشتها في مرحلة البحث والتحري.

الفرع الأول: حق الدفاع في مرحلة البحث والتحري

لقد نصت المادة 51 مكرر 1 من قانون الإجراءات الجزائية على انه يجب على ضابط الشرطة القضائية ان يضع تحت تصرف الشخص الموقوف للنظر كل وسيلة تمكنه من الاتصال فورا بأحد أصوله او فروعه او اخوته او زوجه حسب اختياره ومن تلقي زيارته، أو الاتصال بمحاميه وذلك مع مراعاة سرية التحقيق وحسن سيرها،... إذا تم تمديد التوقيف للنظر يمكن الشخص الموقوف ان يتلقى زيارة محاميه، وإذا كانت التحريات تتعلق بجرائم المتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف والفساد، فإن الشخص الموقوف تحت النظر لا يمكن أن يتلقى زيارة محاميه إلا بعد انقضاء نصف المدة القصوى المنصوص عليها في المادة 51

فالمشرع وبدلا من تعزيز حق الدفاع في هذه المرحلة اقتصر فقط على تمكين الموقوف تحت النظر من تلقى زيارة محاميه وفي حالة تمديد مدة التوقيف للنظر فقط. أما الغريب في هذا التعديل -الذي تعتبره السلطة التنفيذية تقدما في مجال حقوق المشتبه فيه- هو أنه وفي حالة كون التحريات تتعلق بجرائم المتاجرة بالمخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف والفساد، فإن الشخص الموقوف تحت النظر لا يمكن أن يتلقى زيارة محاميه إلا بعد انقضاء نصف المدة القصوى المنصوص عليها في المادة 51 من قانون الإجراءات الجزائية، أي بعد انتهاء التحريات، أما الزيارة فتتم في غرفة خاصة على مرأى من ضابط الشرطة القضائية ولمدة لا تتجاوز 30 دقيقة.

على المشرع تعزيز حقوق المشتبه فيه أيضا أثناء البحث والتحري من خلال توسيع الحق في الاستعانة بالدفاع في هذه المرحلة، وليس الاكتفاء بحق زيارة المحامي عند تمديد التوقيف للنظر مثلما جاء في المادة 51 مكرر1 من الأمر 02-15.[1]

فالمشرع وبعدما تنتهي الضبطية القضائية المتخصصة من جمع الأدلة في هذه القضايا المعقدة ومنها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، يمكن الموقوف للنظر من تلقى زيارة محاميه، وهنا تقتصر الزيارة على مقابلة المشتبه فيه فقط دون الاطلاع على الملف أو حضوره أثناء سماعه،[2] أو تمكين الدفاع من مناقشة الأدلة أو الاستعانة بخبراء أو تقديم طلبات، وهذا في رأيينا يمس بمبدأ المساواة في الأسلحة بين الأطراف، لاسيما في الجرائم المعقدة ومنها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي تلعب فيها مرحلة جمع الأدلة دور كبير في تقرير مصير المشتبه فيه أمام المحكمة، لذلك ندعو إلى إصلاح هذا الخلل من خلال تمكين المشتبه فيه في هذه الجرائم من حق الاستعانة بالدفاع وكذا المختصين وتمكينهم من دور فعال في تكوين أدلة النفي تحقيقا لمبدأ المساواة في الأسلحة.[3]

الفرع الثاني: مناقشة أدلة الإثبات وخطر تحويل الوظيفة القضائية

من مبادئ المحاكمة العادلة المنصوص عليها في المادة الأولى من قانون الإجراءات الجزائية المعدل والمتمم بالأمر 07-17 المؤرخ في 27 مارس 2017 احترام التوازن بين حقوق المتهم وجهة الاتهام أثناء المحاكمة الجنائية.

أولا: مناقشة أدلة الإثبات

1-مناقشة الخبرة

([1])-المادة 51 مكرر من الأمر رقم 02-15 المعدل والمتمم لقانون الاجراءات الجزائية

([2])-الفقرة 05 من المادة 51 مكرر من قانون الاجراءات الجزائية

([3]) صيدي عبد الرحمان، السياسة الجنائية في مواجهة الجريمة الاقتصادية، اطروحة دكتوراه، نوقشت في كلية الحقوق بجامعة الجزائر 1 سنة 2018، 278

ونظرا لما تلعبه الخبرة من دور مركزي في الدعوى الجزائية لأن من شأنها أن تغير مسار الدعوى عندما يتعلق الأمر بتحقيقات تقنية وجب على القاضي الذي يلجأ إلى الخبرة أن يراعى التوازن بين الأطراف، وهو المبدأ الذي يحكم الإجراءات الجزائية، وتكون المحافظة على التوازن بين الأطراف في الدعوى الجزائية عبر منح إمكانية لكل طرف باسم المساواة في الأسلحة إجازة الخبرة، وكذلك مناقشة الخبرة الغير المناسبة ودحضها تحقيقا لمبدأ الوجاهية.

وفيما يتعلق بتعيين الخبير فإن اللجوء إلى خبير في تكنولوجيات الاعلام والاتصال ليس ممكن دائما بالنسبة للمتهم بالرغم من أن الضبطية القضائية في إطار البحث والتحري وتحت إشراف وكيل الجمهورية يمكن لهم اللجوء إلى أشخاص مؤهلين ومخابر أدلة كما رئينا، إلا أن الشخص المتابع لا يمنح له أي دور قانوني موازن، لذلك فإن الخلل في المساواة يكمن في هذه المرحلة من الإجراءات.

وتعتبر هذه الوضعية غير ملائمة بالنسبة للشخص محل المتابعة في الجرائم المتصلة بتكنولوجيات الاعلام والاتصال التي تجريها السلطات القضائية ومنها تحقيقات الضبطية القضائية، والمديرية التقنية بالهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال وهي تحقيقات أولية جد واسعة ومعمقة.

وتكمن مخاطر غياب الوجاهية فيما يتعلق بالخبرة في أن الخبير المعين من طرف القاضي يكون مساعد لجهة الاتهام وحريص على دعم الجهة المكلفة بالمتابعة،[1]

2- مناقشة المساعد المتخصص

إن الخلل الملاحظ في مبدأ الوجاهية في الإجراءات فيما يتعلق بالاستعانة بالخبرة ومناقشتها أمام الضبطية القضائية والنيابة العامة لاسيما في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يتفاقم بالنسبة للمساعدين المتخصصين المنصوص عليهم في المادة 35 مكرر من تعديل قانون الإجراءات الجزائية لسنة 2017، فالمساعد المتخصص يشارك مع النيابة في كامل الإجراءات، ويمكنهم دراسة الوقائع المحتمل تكييفها جزائيا، والاطلاع على الوثائق ومعالجتها واستغلالها ثم تحليلها وتلخيصها، لا يدل على وجود أي ضمان لاحترام الوجاهية في موضوع مناقشة التقارير والأعمال التي يقدمها هؤلاء المساعدين، خاصة وأن المادة 35 مكرر سالفة الذكر تنص على إمكانية أن ترفق هذه التقارير بالتماسات النيابة العامة، وهي ليست ملزمة بوضع هذا التقرير في الملف ليطلع عليه الخصم ويقوم بمناقشته، ومن جهة أخرى ما مصير المحادثات والملاحظات والتوجيهات الشفوية التي يقدمها هذا المختص ولا توضع في الملف، لذلك يكون من الضروري استدراك الوضع فيما يتعلق بمهام المساعدين المتخصصين وتعديل المادة 35 مكرر والنص على ضرورة إدراج أعمالهم في ملف الدعوى بصفة آلية على الأقل تجسيدا لمبدأ الوجاهية، وبذلك تكون مهام هؤلاء المساعدين مفيدة وفعالة في الإجراءات الجزائية الاقتصادية والمالية وتحترم حقوق الشخص المتابع وفق آليات المحاكمة العادلة المنصوص عليها في المادة الأولى من قانون الإجراءات الجزائية.[2]

إذا كان تخصص جهات البحث والتحري يسمح بالدراسة العميقة للأفعال التي تشكل جرائم متصلة بتكنولوجيات الاعلام والاتصال فإن ذلك قد يؤدي إلى المساس بالتوازن الضروري بين حقوق الأطراف، في هذا الإطار اعتبر المجلس الأوروبي لحقوق الإنسان أن تطور جهة البحث والتحري قد يخل بالمساواة في الأسلحة الذي يحكم المحاكمة العادلة المنصوص عليه في المادة 6 S 1 من الاتفاقية الأوروبية لحقوق الإنسان[3]، وفي ذلك رأى قضاة ستراسبورغ في القرار الصادر في 27/11/1993 [4] بشأن قضية Dombo Beheer، أن هذا المبدأ يقتضي أن كل طرف يجب أن تتاح له إمكانية معقولة لتقديم قضيته في ظروف لا يكون في وضعية سيئة بالمقارنة مع خصمه.

ثانيا: خطر تحويل الوظيفة القضائية

([1])-R.Merle et A.Vitu traité de droit criminel, t II op cit, n 203 P 259

([2]) صيدي عبد الرحمان، السياسة الجنائية في مواجهة الجريمة الاقتصادية، المرجع السابق، ص

([3])-CEDH,24 fevr 1997, De Haes et Gijsels C/ Belgique Rec 1997-I ,RSC 1998P 394 et s

([4])-CEDH,27oct 1993 Dombo Beheer c/ Pays-Bas. Serit A N 274.

القاضي الذي يتجه إليه المجتمع عندما يتعلق الأمر بإظهار الحقيقة، يلجأ هو الآخر إلى سلطة أخرى لتوضيح مفهوم قانوني وهذا من الصعب قبوله لأن عملية شرح القاعدة القانونية وإعطاء تكييف قانوني للأفعال تكون أيضا موضوع إحالة لطلب رأي المتخصص أو الخبير، وفي هذا تجريد للقاضي من سلطته القضائية التي هي محور وظيفته.

لكن وبالرغم من هذا الخطر يرى بعض الكتاب أن هذا التحول للسلطة القضائية لصالح متخصص في القانون هو الأقل سوء خاصة مع ظاهرة التعقد المتزايد للقانون،[1] لذلك فإن الأخصائي قادر على تزويد القاضي بقراءة للقاعدة القانونية مما يجيز سلب بعض السلطات القضائية منه، وفي ذلك فائدة في الإحالة لرأى الخبراء المتخصصين.

إن تحويل الوظيفة القضائية لصالح مختص في الوقائع يمكن أن تنشأ عنه علاقة متناقضة بين القاضي والخبير، بحيث يصبح الخبير قاضي في مكان القاضي، ولتفادي هذا الارتباط يكفي أن يكتفي التقني بشرح الوقائع وليس القانون، ويعمل التقني وفق هذا الشرط ضمن المكونات الثلاث للنزاع والتي هي الوقائع، التقنية، والقاعدة القانونية.[2]

إن تحويل الوظيفة القضائية لصالح تقنى الوقائع فيه خطر كبير عندما يغزو هذا الأخير مهمة قول القانون التي هي من اختصاص القاضي، وتصبح هذه الخطورة حقيقية عندما يتخلى القاضي عن وظيفته لصالح الخبير أو المختص، لذلك يكون من الضروري رفض كل الوظائف المعيارية لتقني الوقائع وحصر مهمته في مساعدة أجهزة الدعوى فقط.[3]

وكثيرا ما يلجأ القاضي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للمختصين والخبراء وينتهي في حكمه إلى تأييد الاستنتاجات التي يتوصل إليها الخبير، بينما مهمة الخبير أو المساعد التقني تقتصر على الإجابة على سؤال حول الوقائع من أجل تسهيل الوصول إلى الحقيقة في نزاع معين.

إن تقرير الخبرة في تكنولوجيات الاعلام والاتصال كما في جميع المواد الجنائية الأخرى لا يكون إلا كمؤشر بالنسبة للقاضي وليس خلاصة للقرار الذي سيتخذه، فقرار القاضي لابد من تطعيمه بمنطق المختص وتبيين عمله، وكما يقول البعض أن القاضي يجب أن يكون تفكيره كتفكير المختص، يفكر كالمهندس مع المهندس وكطبيب مع الطبيب وكذلك يجب أن يكون معلوماتي مع مهندسي الإعلام والاتصال.[4]

خاتمة

لقد قمنا في هذه المداخلة بدراسة تأثير تكنولوجيات الإعلام والاتصال على الحق في محاكمة عادلة وركزنا فيها على مرحلة مهمة ومصيرية من مراحل الدعوى العمومية وهي مرحلة البحث والتحري أين يكون مركز المشتبه فيه هش وضعيف، كما ركزنا على صورة أساسية من صور المحاكمة العادلة وهي الحق في المساواة في الأسلحة بين خصوم الدعوى العمومية وتوصلنا الى النتائج التالية.

أن مرحلة البحث والتحري مرحلة حاسمة في الدعوى العمومية بحيث يتقرر مصيره بحسب الأدلة المستقاة في هذه المرحلة.

يقوم بالبحث والتحري في جرائم تكنولوجيات الإعلام والاتصال شرطة قضائية متخصصة، وتكلف المديرية التقنية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بمهمة المراقبة الوقائية للاتصالات الالكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية والتخريبية والاعتداء على أمن الدولة، وتتولى هذه المديرية بحسب المادة 12، مساعدة السلطات القضائية ومصالح الشرطة القضائية بناء على طلبها بما في ذلك في مجال الخبرات القضائية في إطار مكافحة

([1])-B.Oppetit, la résurgence du rescrit, D 1991 chron, p 109.

([2])-A.Lorieux, L'expertise et le jugement, Dalloz, 1995 p 123 et s, spéc p 127.

([3])-O.Leclerc.Le juge et l'expert Contribution a l'étude des rapports entre le droit et science, LGDJ, 2005, spéc n 16.

([4])-A.Lorieux, op cit, p 128.

الجريمة المتصلة بتكنولوجيات الإعلام والاتصال والجرائم التي تتطلب اللجوء الى أساليب التحري الخاصة للهيئة.
تعتبر جرائم تكنولوجيات الإعلام والاتصال من الجرائم التي أجاز المشرع اللجوء فيها الى أساليب التحري الخاصة، وهي أساليب تعطي سلطة استثنائية للشرطة القضائية تخرج عن القواعد العامة التي تحكم الاستدلال وتمس أكثر بحقوق وحريات المشتبه فيه، وتتمثل أساليب التحري الخاصة في الخبرة والتفتيش والحجز الإلكترونين، والتسرب الالكتروني، والمراقبة الالكترونية والترصد الالكتروني وتحديد الموقع.
توصلنا أيضا الى أن الحق في المساواة في الأسلحة تم تكريسه من خلال السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان وأصبح ركيزة أساسية ضمن الحق في محاكمة عادلة.
ويندرج هذا المبدأ ضمن المبادئ الدستورية المتعلقة بالمساواة أمام القانون والقضاء والحق في محاكمة عادلة وتساوي الأسلحة بين أطراف الخصومة. المضمونة في المادة الأولى من قانون الإجراءات الجزائية.
توصلنا أيضا الى أن هذا المبدأ يتطلب تكافؤ وسائل الدفاع في المسائل الجزائية وأن يكون كل طرف في المحاكمة قادر على عرض قضيته في ظل ظروف لا تضعه في وضع غير موات بشكل واضح مقارنة بخصمه، ويعني ضمنيا المساواة بين الأطراف في الوصول إلى المعلومات ولاسيما الحق في الاطلاع على الملف.
لق رئينا انه من مقتضيات المحاكمة العادة والمساواة في الاسلحة ضمان حق الدفاع في جميع مراحل الدعوى العمومية، لكن المشرع الجزائري وان كان قد نص على تمكين المشتبه فيه الموقوف للنظر من زيارة محاميه الا ان ذلك يكون بعدما تنتهي الضبطية القضائية المتخصصة من جمع الأدلة في هذه القضايا المعقدة ومنها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتقتصر الزيارة على مقابلة المشتبه فيه فقط دون الاطلاع على الملف أو حضوره أثناء سماعه، أو تمكين الدفاع من مناقشة الأدلة أو الاستعانة بخبراء أو تقديم طلبات، وهذا في رأيينا يمس بمبدأ المساواة في الأسلحة بين الأطراف، لاسيما في الجرائم المعقدة ومنها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال التي تلعب فيها مرحلة جمع الأدلة دور كبير في تقرير مصير المشتبه فيه أمام المحكمة، لذلك ندعو إلى إصلاح هذا الخلل من خلال تمكين المشتبه فيه في هذه الجرائم من حق الاستعانة بالدفاع وكذا المختصين وتمكينهم من دور فعال في تكوين أدلة النفي تحقيقا لمبدأ المساواة في الأسلحة.
لقد رئينا ان الخبرة لها دور مركزي في الدعوى الجزائية لأن من شأنها أن تغير مسار الدعوى عندما يتعلق الأمر بتحقيقات تقنية وجب على القاضي الذي يلجأ إلى الخبرة أن يراعى التوازن بين الأطراف، وهو المبدأ الذي يحكم الإجراءات الجزائية، وتكون المحافظة على التوازن بين الأطراف في الدعوى الجزائية عبر منح إمكانية لكل طرف باسم المساواة في الأسلحة إجازة الخبرة، وكذلك مناقشة الخبرة الغير المناسبة ودحضها تحقيقا لمبدأ الوجاهية. وهذا ما لم يتسنى للمشتبه فيه في مرحلة البحث والتحري ما يشكل إخلال بحق المساواة في الأسلحة.
لقد رئينا ان المشرع مكن النيابة العامة من الاستعانة بمساعدين متخصصين، يشاركون مع النيابة في كامل الإجراءات، ويمكنهم دراسة الوقائع المحتمل تكييفها جزائيا، والاطلاع على الوثائق ومعالجتها واستغلالها ثم تحليلها وتلخيصها، ولا يمكن للمشتبه فيه تلقى المساعدة من أي متخصص او خبير او حتى الدفاع، وفي ذلك إهدار لمبدأ المساواة ومبدأ الوجاهية في موضوع مناقشة التقارير والأعمال التي يقدمها هؤلاء المساعدين.
لقد رئينا أيضا اللجوء المحتوم للمتخصصين والخبراء في مجال تكنولوجيات الإعلام والاتصال من شأنه أن يؤدي الى تحويل الوظيفة القضائية لصالح مختص في الوقائع، يمكن أن تنشأ عنه علاقة متناقضة بين القاضي والخبير، بحيث يصبح الخبير قاضي في مكان القاضي.
لقد رئينا انه كثيرا ما يلجأ القاضي في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للمختصين والخبراء وينتهي في حكمه إلى تأييد الاستنتاجات التي يتوصل إليها الخبير، بينما مهمة الخبير أو المساعد التقني تقتصر على الإجابة على سؤال حول الوقائع من أجل تسهيل الوصول إلى الحقيقة في نزاع معين.

لقد توصلنا الى أنه فيه اختلال واضح في التوازن في الأسلحة بين المشتبه فيه والنيابة العامة في مرحلة البحث والتحري لا سيما في الجرائم الخطيرة والمعقدة ومنها الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إحدى مفرزات التطور التكنولوجي.

مخبر الدراسات القانونية التطبيقية
فرقة البحث دراسات مستحدثة في التشريعات العقابية
وبالتعاون مع فرقة بحث التكوين الجامعي prfu
المحاكمة عن بعد: سرعة الإجراءات أم إهدار للضمانات
يوم 20 جوان 2022

//////////////////////////////
ر ت م د ...../ر ت م د إ : ...../ .....
دريهمي عبد الحكيمجامعة الجزائر 1
عنوان المداخلة :تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية

Remotecriminaltrailtechnology as a mechanism to ensure the speed of criminalprocrdures

الملخص:

سعيا لتحقيق المحاكمة العادلة كرست القوانين الجزائية المعاصرة نظام المحاكمة الجزائية عن بعد استجابة لمسايرة متطلبات التطور العلمي في مكافحة الإجرام ، و قد سار المشرع الجزائري على نهج الأنظمة الجزائرية المقارنة في تبني المحاكمة الجزائية عن بعد من خلال النص عليها بموجب القانون رقم 15-03 المؤرخ في 01 فبراير 2015 و المتعلق بعصرنة العدالة ، وبموجب الأمر رقم 20- 04 المؤرخ في 30 أوت 2020 الذي فعل سريانها في قانون الإجراءات الجزائية ، حيث تعد المحاكمة الجزائية عن بعد أحد الوسائل المستحدثة كضمانة لتعزيز سرعة الإجراءات الجزائية من جهة ، و هذا ما لا يتحقق إلا من خلال تجسيد فكرة تبسيط إجراءات التقاضي عند كل مرحلة من مراحل سير الخصومة الجنائية من جهة أخرى .

و لمعالجة هذا الموضوع ارتأينا طرح الاشكالية التالية : ما هي الأهمية التي تبرر اللجوء إلى استخدام تقنية المحادثة المرئية في نظام المحاكمة الجزائية عن بعد كوسيلة لتبسيط إجراءات التقاضي في ظل احترام مبادئ المحاكمة العادلة ؟ .

و سوف تتم الإجابة على هذا الاشكال ضمن مطلبين على النحو التالي:

المطلب الأول : أهمية استخدام نظام المحاكمة عن بعد .

المطلبالثاني : أثر استخدام تقنية المحاكمة عن بعد على متطلبات المحاكمة العادلة .

و على هذا الأساس سنحاول الوصول إلى نتيجة مفادها بيان مدى تأثير استخدام تقنية المحادثة المرئية و المسموعة عن بعد على الضمانات المقررة لأطراف الخصومة الجنائية .

الكلمات المفتاحية : التحاضر المرئي ، السرعة الإجرائية ، المحاكمة ، الضمانات.

////////////////////////////////
ر ت م د ...../ر ت م د إ : ...../ .....
دريهمي عبد الحكيمجامعة الجزائر 1
عنوان المداخلة :تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية

Remotecriminaltrailtechnology as a mechanism to ensure the speed of criminalprocrdures

استمـــــــــارة المشـــاركـــــة في اليـــوم الدراســـــــي حـــــول:

المحاكمـــــة عن بعـــــد : ســـرعـــــة الإجـــــراءات أم إهـــــدار للضمانـــــــات .

عنوان المداخلة : تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الإجراءات الجزائية

الإسم: عبـــد الحكيـــــم

اللقب: دريـــــــهمـــــــي

الدرجة العلمية : دكتـــــوراه

جامعـــــة الجزائـــــــر 1 بن يوسف بن خـــــدة

البريد الإلكتروني :drihmi.hakim01@gmail.com

////////////////////////////////
ر ت م د ...../ر ت م د إ : ...../ .....
دريهمي عبد الحكيمجامعة الجزائر 1
عنوان المداخلة :تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية

Remotecriminaltrailtechnology as a mechanism to ensure the speed of criminalprocrdures

المقدمة :

إن التطور الحاصل في المجال التكنولوجي خاصة في مجال المعلوماتية و الاتصالات ، ستهم بشكل فعال في تقليص الحدود و قصر المسافات لاسيما استخدام الوسائل التكنولوجية الحديثة في المعاملات ، أو في ما استغلته الجماعات الاجرامية من هذا التطور الذي ساهم في تكيف تمطها الاجرامي في شكل منظم عابر للحدود الوطنية و الدولية ،الأمر الذي دفع الدول سواء مجمعة أو منفردة في ضرورة تطوير منظومتها القانونية لمواكبة هذا التطور بهدف مواجهة هذا النوع من الإجرام المستحدث هذا من جهة ،كما أن الحق في سرعة الإجراءات الجزائية الذي يقتضي لضمانه وجوب الفصل في الخصومة الجنائية خلال أجل معقول باعتباره أحد مقتضيات المحاكمة العادلة ، و هي الأهمية التي تبرر ضرورة اللجوء لاستعمال الوسائل التكنولوجية الحديثة لتحقيق ذلك و التي يجسدها نظام المحاكمة عن بعد من خلال استخدام تقنية المحادثة المرئية و المسموعة عن بعد ، بهدف تحقيق سرعة الإجراءات وفقا لما تقتضيه مبادئ المحاكمة العادلة .

و لمعالجة هذا الموضوع ارتأينا طرح الإشكالية التالية : ماهي الأهمية التي تبرر اللجوء إلى استخدام تقنية المحادثة المرئية في نظام المحاكمة الجزائية عن بعد كوسيلة لتبسيط إجراءات التقاضي في ظل احترام مبادئ المحاكمة العادلة ؟ .

و سوف تتم الإجابة على هذه الإشكالية ضمن مطلبين ، يتضمن الأول أهمية استخدام نظام المحاكمة عن بعد ، أما الثاني فيتضمن أثر استخدام المحاكمة عن بعد على مبادئ المحاكمة العادلة .

المطلب الأول : أهمية استخدام نظام المحاكمة عن بعد

تعد المحاكمة عبر تقنية المحادثة المرئية **Visioconférence**أو التحاضر المرئي من الآليات المستحدثة في الإجراءات التي يمكن اتخاذها أمام القضاء الجزائي باعتبارها نت الوسائل التي تتطلبها عصرنة العدالة و ما تقتضيه من تيسير إجراءات التقاضي لضمان سرعة إجراءات الفصل في الدعوى الجزائية دون

الإخلال بمتطلبات المحاكمة العادلة على النحو الذي يضمن مصلحة العدالة و المتهم على حد سواء دون الاخلال بمصلحة على حساب مصلحة اخرى ، و هذا ما سنحاول تبيانه من خلال ما يأتي :

الفرع الأول : مدى ضمان تقنية المحادثة المرئية لمصلحة العدالة و مصلحة المتهم

الفرع الثاني : مدى ضمان تقنية المحادثة المرئية على سرعة سير الإجراءات

الفرع الأول : مدى ضمان تقنية المحادثة المرئية لمصلحة العدالة و مصلحة المتهم

يوفر استخدام تقنية التحاضر عن بعد في المسائل القضائية خاصة ذات الطابع الجزائي أهمية بالغة بالنسبة لكل من المتهم و العدالة ، و هذا ما يفسر لجوء العديد من الأنظمة القانونية إلى الأخذ بها و تكثيف اللجوء إلى استخدامها على الرغم مما لهذه التقنية من تأثير على شروط إجراء المحاكمة وفقا للقواعد التقليدية ، و هذا ما يجعل الأمر لا يستوي بالنظر للمختصين خصوصا الفقهاء الأوروبيين منهم ، حيث يشترطون ضرورة ضمان كل الظروف لاستخدام تقنية المحادثة المرئية و المسموعة عن بعد بالشكل اللازم الذي يتوافق مع متطلبات المحاكمة العادلة ، خاصة من حيث تعزيز مراقبة هذه التقنية عند استخدامها في كل مرحلة من مراحل سير الخصومة الجزائية لاسيما وأن مصالح المتهم تختلف حسب كل مرحلة إجرائية لذلك و بالرجوع إلى الأساس القانوني للمحاكمة عن بعد باستخدام تقنية المحادثة المرئية و المسموعة و هو القانون رقم 15-03 المتعلق بعصرنة العدالة قد أقر شروطها و ضمانات لإجراء التحقيق و المحاكمة الجزائية عن بعد و هذا بهدف ضمان حقوق المتهم دون الإخلال بمصلحة العدالة و ما يقتضيها حسن سيرها .

ففي مرحلة إجراءات تحقيق المحاكمة الجزائية عن بعد و على الرغم من اعتبار أنهما يتمان افتراضيا في نطاق جغرافي واحد يتمثل في مكتب غرفة التحقيق أو جلسة المحاكمة عن طريق الحضور الالكتروني ، و هو الإجراء الذي يوفر مجموعة من الضمانات من بينها ضمان سرعة سير إجراءات الخصومة الجزائية و الفصل فيها دون إطالة غالبا ما تتميز بطول إجراءات الدعوى الجزائية وتعقيدها ، لأن مصلحة المتهم تقتضي ضرورة الفصل في مصيره سواء بتقرير الإدانة أو البراءة ، و لتفادي ما يتكبده من عناء و طول

الإجراءات التي تنتهي في نهاية الأمر إلى مصادرة حقه في الحياة أو حقه في الحرية [1]، لأن الإجراءات الجزائية من مبررات تشريعها أنها وجدت لحماية المتهم لذلك يطلق الفقه على قانة الإجراءات الجزائية بدستور الحريات ، و بالتالي فإن استخدام تقنية المحاكمة المرئية و المسموعة عن بعد في المحاكمة من شأنه ضمان سرعة الإجراءات التي يترتب على ضمانها حماية حقوق المتهم عند كل مرحلة إجرائية خاصة عند مرحلة التحقيق و المحاكمة ، و خلاصة ذلك ما عبرت عليه المحكمة الدستورية في مصر بقولها : إن سرعة الفصل في الدعوى يعد جزء من الحق في محاكمة جزائية منصفة فلا يجوز أن يكون الاتهام متراخيا أو معلقا أمدا طويلا بما يثير قلق المتهم و يعوق بالضرورة مباشرته للحقوق و الحريات التي كفلها الدستور .

و نظرا لأهمية ضمان حقوق المتهم في نظام المحاكمة عن بعد تثير في نفي الوقت جملة من الإشكالات الإجرائية في استخدام تقنية المحاكمة المرئية و المسموعة عن بعد مرتبط ارتباطا وثيقا بمبادئ سير إجراءات المحاكمة العادلة تتمثل أساسا في مسألة الاختصاص و الحضورية و الشفوية و الوجاهية و التدوين ، و لضمان ذلك أوجب المشرع قيام جملة من الشروط الأساسية لأجل استخدام هذه التقنية و مراعاة الاحترام للحقوق و القواعد المنصوص عليها في قانون الإجراءات الجزائية ، و باستقراء هذه الشروط يتبين لنا من خلال مدلولها أن المشرع الجزائري قد اعتبر اللجوء إلى استعمال المحادثة المرئية و المسموعة عن بعد اثناء الإجراءات القضائية إجراءاجوازيا مؤكدا أن الأصل في المحاكمة تكون عادية في ظل الحضور الفعلي للمتهمين و استجوابهم و سماع الأطراف المدنية و الشهود و الخبراء و إجراءات الاستجواب و المواجهة بين عدة أشخاص ، حيث لم يجز المشرع الجزائري استعمال المحادثة المرئية و المسموعة عن بعد من طرف جهة الحكم في القضايا الجنحية شريطة موافقة المتهم و النيابة العامة على ذلك ، و إذا كان المتهم غير محبوس فإن جهتي التحقيق و المحاكمة يمكنهما استعمال آلية المحادثة المرئية عن بعد في إجراء الاستجواب أو السماع أو المواجهة بمقر المحكمة الأقرب إلى مكان إقامة الشخص المطلوب تلقي تصريحاته بحضور وكيل الجمهورية المختص إقليميا و أمين الضبط مع وجوب تسجيل التصريحات على دعامة الكترونية وتأمين سلامتها و ترفق بملف الإجراءات و وجوب تدوين التصريحات كاملة و حرفيا على محضر يوقع من طرف القاضي المكلف بالملف و أمين الضبط [2]، وبالتالي فإن استخدام تقنية المحادثة عن بعد في ظل القانون رقم 15-03 المتعلق بعصرنة العدالة لاسيما في مرحلتي التحقيق و

////////////////////////////////
ر ت م د ...../ر ت م د إ : ...../ .....
دريهمي عبد الحكيمجامعة الجزائر 1
عنوان المداخلة :تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية
Remotecriminaltrailtechnology as a mechanism to ensure the speed of criminalprocrdures

المحاكمة الجزائية عن بعد يعد إجراء مستحدث من شأنه أن يوفر ضمانة إجرائية تتعلق بحسن سير العدالة و هي المصلحة المنشودة متى تم تنفيذه على الوجه الأكمل و بالطرق و الوسائل الممكنة التي تقر حقوق الخصوم بوجه عام و حق المتهم على وجه الخصوص باعتباره طرفا أساسيا في الخصومة الجزائية و الذي بناء على حضوره القانوني يتحقق انعقاد الخصومة الجزائية فعلا و يترتب عنه ضمان تحقيق أهم شروط و متطلبات المحاكمة العادلة .

الفرع الثاني : مدى ضمان المحادثة المرئية عن بعد الحق في سرعة الإجراءات

يعد اللجوء إلى استخدام التقنيات و منها تقنية المحادثة المرئية عن بعد في قطاع العدالة بوجه عام من أهم التطورات الفكرية التي أثرت بشكل فعال في سير إجراءات التقاضي خاصة بالنسبة للإجراءات الجزائية التي لها علاقة وطيدة و تأثير مباشر على الحقوق و الحريات العامة للأفراد في المجتمع .

و لعل ما يبرر اللجوء إلى استخدام هذه التقنيات هي الأهمية البالغة لها و التي تعود لعدة اعتبارات منها ما يتعلق بفكرة تبسيط إجراءات التقاضي و ترشيدها على النحو الذي يضمن سرعة سريان الفصل في الخصومة الجزائية دون إطالة غير مبررة و ما يترتب عليها من أضرار تلحق بأطراف الخصومة الجزائية على حد سواء الأمر الذي يبرر استخدام تقنية المحادثة المرئية عن بعد لتعزيز ضمان أحد متطلبات المحاكمة العادلة و هو الحق في إجراء المحاكمة الجزائية في أجل معقول ، حيث كان اللجوء إلى هذه التقنية من اجل مواكبة التطور التكنولوجي و عصرنة قطاع العدالة من خلال تحقيق السرعة و تبسيط إجراءات الدعوى الجزائية ، ففي حالات عديدة يتم تأجيل الجلسات بسبب البعد الجغرافي بين مكان توقيف المتهم و قاعات التحقيق أو المحاكمة ، أو لأسباب تتعلق بسماع شهادة أحد الشهود بناء على طلب المحكمة أو أحد أطراف الخصومة نظرا لبعد مكان إقامته ، هذه الأسباب و غيرها من الأسباب الإجرائية التي من شأنها أن تؤدي إلى إطالة سير الدعوى الجزائية ، وبالتالي يمكن من خلال استخدام تقنية المحادثة عن بعد المرئية اختزال كل ذلك في ظرف زمني وجيز .

و لقد كرس المشرع الجزائري بموجب الأمر رقم 02-04 استخدام تقنية المحادثة المرئية عن بعد و اعتمادها كآلية لتبسيط الإجراءات عند كل مرحلة من مراحل الخصومة الجزائية – مرحلة التحقيق

الابتدائي ، مرحلة المحاكمة - ، و ذلك من خلال نص المادة 441 مكرر 01 متى تتحقق الحالات المنصوص عليها في المادة 441 مكرر من الأمر السالف الذكر ، و هو ما يؤكد حرص المشرع على سير إجراءات التقاضي عن بعد في الإجراءات الجزائية بذات الإجراءات و الضمانات المكفولة قانونا في ظل الإجراءات العادية لاسيما ما تعلق منها بحق الدفاع و مبدأ المواجهة و التدوين و الحضورية .

كما يظهر جليا أن استخدام تقنية المحادثة المرئية عن بعد لا يقتصر فقط على مرحلة أو إجراء معين بل وسع المشرع الجزائري اللجوء إليه في مرحلة التحقيق و المحاكمة كما وسع استخدامه لمباشرة عدة إجراءات ذات صلة بمرحلة التحقيق أو المحاكمة ضمانا لتحقيق سرعة الإجراءات و تجنب كل ما من شأنه أن يعيق السير الحسن للعدالة ، فبنسبة لمرحلة التحقيق الابتدائي أجاز المشرع الجزائري استخدام تقنية المحادثة المرئية عن بعد في إجراءات محددة و هذا حسب حالات الشخص المراد سمعه كما يلي :

فبالنسبة لمرحلة التحقيق الابتدائي وكان الشخص غير موقوف ومقيما بدائرة اختصاص محكمة اخرى في هذه الحالة تقوم جهة التحقيق المختصة بتوجيه طلب الى وكيل الجمهورية للمحكمة الاقرب لمحل اقامته قصد استدعائه للتاريخ المحدد للقيام بالإجراء ، وفي هذه الحالة لا يجوز سماع المتهم أو المدعي المدني أو اجراء مواجهة بينهما الا بحضور محاميه أو دعوته قانونا مالم يتنازل صراحة عن ذلك ، بحيث يجب وضع ملف الاجراءات تحت طلب محامي المتهم قبل استجوابه بأربعة وعشرين ساعة على الاقل كما يجب ان يوضع تحت طلب محامي المدعي المدني قبل سماع أقواله بأربع وعشرين ساعة على الأقل وفقا لما نصت عليه المادة 105 من قانون الاجراءات الجزائية [3].

أما في حالة ما تعذر استخراج المحبوس او تحويل المتهم او الشخص المحبوس لاحد الاسباب المنصوص عليها في المادة 441 مكرر ، يمكن لجهة التحقيق بعد اخطار مدير المؤسسة العقابية سماعه بها عن طريق اجراء المحادثة المرئية والمسموعة عن بعد بحضور امين ضبط المؤسسة الذي يقوم بتحرير محضرا عن سير عملية استعمال هذه التقنية و يوقعه ثم يرسله بمعرفة مدير المؤسسة العقابية إلى الجهة القضائية المختصة لإلحاقه بملف الإجراءات ، و يحق للمحامي في هذه الحالة الاختيار بين أن يكون إلى جانب موكله بمكان سماعه أو أمام الجهة القضائية المختصة بالتحقيق عملا بنص المادة 441 مكرر 04 من قانون

الإجراءات الجزائية ، و من بين الضمانات الإجرائية التي أقرها المشرع في ظل استخدام المحادثة المرئية عن بعد و ضمانة التدوين كتابة ، حيث أوجب تواجد أمين الضبط أمام الجهة القضائية أو المؤسسة العقابية التي يتم أمامها عملية سير المحادثة المرئية عن بعد ، حيث يتولى تحرير محضر الاستجواب أو المواجهة وفقا لأحكام المادة 108 من قانون الإجراءات الجزائية ، كما نستنتج من خلال النصوص السالفة الذكر حرض المشرع على احترام الحقوق المنصوص عليها في قانون الإجراءات الجزائية و من بينها الحق في الدفاع الذي هو جق مكفول في جميع مراحل الدعوى الجزائية لاعتباره من أهم الركائز التي تضمن المحاكمة العادلة ، كما حرص المشرع كذلك على وجوب أن تتم إجراءات التحقيق بصورة سرية ما لم ينص القانون على خلاف ذلك ، و في حالة قرر قاضي التحقيق إصدار أمر بوضع المتهم المسموع عن طريق تقنية المحادثة المرئية عن بعد رهم الحبس المؤقت وجب عليه تبليغه هذا الأمر شفاهة عن طريف نفس التقنية مع إحاطته علما بأن له 03 أيام من تاريخ التبليغ للاستئناف [4].

أما بالنسبة لاستخدام المحادثة المرئية عن بعد في مرحلة المحاكمة الجزائية من طرف جهات الحكم بعد استطلاع رأي النيابة العامة و إعلام باقي الخصوم الذين لهم الحق في الاعتراض لتبرير رفض الامتثال لهذا الإجراء و رأت جهة الحكم عدم جدية هذا الاعتراض أو الدفوع تصدر فورا قرارا غير قابل لأي طعن باستمرار المحاكمة ، كما يمكن لأطراف الدعوى أو دفاعهم تقديم طلب للجهة القضائية المختصة لاستقدام تقنية المحادثة المرئية عن بعد ، و لهذه الجهة القضائية سلطة تقدير قبول الطلب أو رفضه بعد استطلاع رأي باقي الطراف او دفاعهم أو النيابة العامة ، و في حالة استخدام هذه التقنية عن بعد بعتبر الحكم حضوري في حالة رفض المتهم الإجابة أو قرر التخلف عن الحضور تطبيقا لأحكام المادة 347 من قانون الإجراءات الجزائية ، حيث اعتبر المشرع الجزائري النطق بالحكم باستخدام هذه التقنية حضوريا للمحاكمة ، فالمحاكمة الالكترونية عن بعد متى توافرت شروطها فهي تخضع لنفس أحكام المحاكمة العادية عملا بمضمون نص المادة 441 مكرر 10 من قانون الإجراءات الجزائية[5] .

المطلب الثاني : أثر استخدام تقنية المحادثة المرئية عن بعد على متطلبات المحاكمة العادلة

////////////////////////////////
ر ت م د ...../ر ت م د إ : ...../ .....
دريهمي عبد الحكيمجامعة الجزائر 1
عنوان المداخلة :تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية
Remotecriminaltrailtechnology as a mechanism to ensure the speed of criminalprocrdures

إن تبني المشرع الجزائري لنظام المحادثة عن بعد كان وفقا لمعايير موضوعية و إجرائية كفيلة بضمان متطلبات المحاكمة العادلة و ما تتطلبه من مقتضيات ، و تأسيسا على اعتبار الحق في المحاكمة العادلة من اهم حقوق الإنسان في الدعوى الجزائية بما يقره من حماية لحقوق الإنسان الأخرى المكرسة عند مراحل سير إجراءات الخصومة الجزائية ، و حيث تكون المحاكمة منصفة يجب أن ترتكز على وسائل قانونية ثقيلة لحماية هذه الحقوق لأن توفير محاكمة عادلة هو ضروري ليس فقط من منظور حماية حقوق المتهم أو الضحية لكن لضمان حسن سير العدالة ، كذلك بما فيها من إجراءات ضمان سرعة الفصل في القضايا خلال مدة معقولة و هذا دون أن يشكل استخدام تقنية المحادثة عن بعد بمبرر ضمان سرعة الإجراءات إخلالا بأهم المبادئ التي ترتبط ارتباطا مباشرا بمرحلة المحاكمة مثل مبدأ الحضورية و الشفوية و العلنية .

الفرع الأول : أثر استخدام تقنية المحادثة المرئية عن بعد بالحق في الحضور الشخصي ومبدأ العلنية

يعد الحضور الشخصي بالنسبة للمتهم ضمانة في التحقيق النهائي تجسيدا لمبدأ شفوية المرافعات ، حيث يمكن لجهة الحكم و الخصوم مناقشة الأدلة المقدمة فلا يكفي صحة الدليل لاقتناع المحكمة به ،بل لا بد أن يكون هذا الدليل قد تمت مناقشته في الجلسة و هذا ما أكدت عليه المادة 212 ف 02 من قانون الإجراءات الجزائية بنصها : و لا يسوغ للقاضي أو يبني قراره إلا على الأدلة المقدمة في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه و بالتالي فإن هذا المبدأ يقتضي ضرورة تمكين الخصوم من حضور الجلسة و إعلامهم بموعدها قبل انعقادها ، و عليه فإن إبعاد المتهم عن الحضور بعد إجراءات التحقيق النهائي يترتب عنه البطلان المتعلق بالنظام العام[6].

و بعد أن كانت هذه التقنية مقتصرة على مرحلة التحقيق للأجل الاستجواب أو إجراء سماع الشهود ضمانا للحق في سرعة الإجراءات و الفصل السريع في الخصومة الجزائية ، انتشرت كذلك بشكل ملفت للانتباه خصوصا في الآونة الأخيرة بسبب انتشار جائحة كوفيد 19 ، أين لجأ قطاع العدالة إلى اعتماد هذه التقنية تفاديا لانتشار العدوى و حسن سير مرفق العدالة الذي عرف تذبذبا كبيرا بسبب الحجر الصحي و بالتالي أدخل المشرع تعديلات على قانون الإجراءات الجزائية معتمدا الحضور عبر تقنية المحادثة المرئية

عن بعد أثناء المحاكمة كبديل للحضور الشخصي من خلال قانون 20-04 المعدل و المتمم لقانون الإجراءات الجزائية في المواد من 441 مكرر 07 إلى غاية 441 مكرر 10 ، حيث أجازت هذه المواد لجهات الحكم استخدام هذه التقنية من تلقاء نفسها أو بناء على طلب النيابة العامة أو أحد الخصوم أثناء الاستجواب أو إجراء المواجهة ، و ما يمكن استقراءه من خلال النصوص القانونية التي اقرها المشرع بموجب الأمر 20-04 أن سلطة القاضي التقديرية تكون في الحالات التي يحددها القانون متى رآها مبررا و الاعتراض عليه يجب أن يكون مبينا على دفوع جدية ، وقرار المحكمة في هذه الحالة غير قابل لأي طعن ، حيث قضت محكمة النقض الفرنسية في قرار لها و بشكل صريح بأن اللجوء إلى تقنية التحاضر المرئي عن بعد أو المحادثة المرئية يكون غير مسبب .

و مما لا شك فيه أن استخدام هذه التقنية يقوض عمليا جودة استماع القاضي بسبب الحاجز و المسافة التي تخلقها الشاشة بين القاضي و المتقاضين و عدم قدرة إدراك المحكمة لأهم النقاط المرتبطة بنفسية المتهم أو الضحية كعلامات الانزعاج أو عدم الارتياح و معرفة متى يمكن التحدث و متى يمكن التمسك بحق الصمت ، كل هذه البديهيات الضرورية تختفي أثناء المرافعة من خلال استخدام تقنية المحادثة المرئية عن بعد ، بالإضافة إلى الأعطال الفنية في الاتصال مثل انقطاع الصورة و الصوت ، كل هذا يشكل في وجهة نظرنا مساسا بحق المتهم في أن تناقش قضيته مناقشة بطريقة وجاهية من جهة ، كما أن على الرغم من أنه إجراء يضمن تحقيق سرعة إجراءات الدعوى الجزائية [7].

الفرع الثاني : أثر استخدام تقنية المحادثة عن بعد على مبدا العلانية و الحق في الدفاع

ان العلانية تعد ضمانة هامة للمحاكمة العادلة ضد اي عدالة سرية حيث تعد الرقيب على عدالة الاجرات ومن ابرز مظاهرها السماح لجمهور الناس بالدخول الى القاعة التي تجرى فيها المحاكمة , وتمكينهم من الاطلاع على ما يجرى فيها من اجراءات و ما يدور خلالها من مناقشات و اقوال علما ان المحكمة ليست ملزمة باستدعاء الجمهور فلا تنتفي العلانية ما لم يحضر الجمهور حيث يكفي ان المحكمة اتاحت له ذلك مادامت ابواب القاعة مفتوحة وتوصف جلسة المحاكمة العلنية بانها احد

النقاط الاساسية و الاكثر رمزية للعدالة باعتبارها تجسيدا لمبدا قانوني اساسي كما انها ممارسة مهنية تبرز من خلالها خبرة و اهلية الفاعلين في الساحة القضائية من محامين و قضاة وكتاب ضبط و خبراء وبالتالي تعد العلنية النتيجة الطبيعية للمحاكمة العادلة , فعندما تجرى المرافعات على شبكة اتصالات عن طريق تقنية المحادثة المرئية و المسموعة عن بعد وليس بقاعة الجلسات هو ما يثير اشكال بالنسبة لمبدا علنية المرافعات الذي يصبح محل استفهام على الرغم من ان العلنية ليست قاعدة مطلقة فله عدة استثناءات في حالات معينة معروفة قانونا ولقد لاحظنا اخيرا كيف اصبحت قاعات المحاكم شبه مهجورة بسبب اجراءات الحجر الصحي التي تبعت جائحة كوفيد 19 فهناك من التشريعات من اعتبرت الجائحة سببا للاستثناء كما فعل المشرع الفرنسي من خلال المادة السابعة من الامر 20- 303 المؤرخ في 25 مارس 2020 المتعلق بتكييف قواعد الاجرات الجنائية على اساس قانون الطوارئ رقم 2020-290 المؤرخ في 20 مارس 2020 بتعامل مع وباء كوفيد 19 محاولا تبرير هذا الاستثناء الذي يحد من العلانية وذلك من حلال النص صراحة على امكانية السماح بحضور الصحفيين للجالسات حتى في الحالة التي يأمر فيها القاضي بعقد الجلسة سرية في ضل ظروف الامن الصحي التي يتعين على القاضي تحديدها وبالتالي فان حضور الصحفيين يعد ضمان الدعاية للجمهور و تخصيص مقعد لهم اثناء الجلسة يعد في نظرهم دليل كافي لمراقبة الجمهور [8].

كما ان علانية المحاكمة وفق استخدام تقنية التحضر المرئي عن بعد لا يحقق الفائدة المرجوة و المطلوبة في اجراءات التقاضي كما هو الحال عند ممارستها بالشكل العادي وجاهة امام القضاة لأسباب منها ان بعض المحامين قد يترافعون في قضاياهم من مكاتبهم او من بعض الاماكن خاصة , وهو ما يترتب عليه عدم فعالية علانية المحاكمة بالشكل الالكتروني لأنه يؤدي الى نتيجة مفادها ضعف القناعة الشخصية لدى العامة في التقاضي الالكتروني بالإضافة الى ذلك فان حق الخصوم في الوصول الملموس و الفعال الى القاضي يكون ضعيفا لعدم ممارسته وضيفته بشكل صحيح فالحكم وهو ما يخل بمبدا الاقتناع الذاتي للقاضي الجزائي الذي يكونه كاصل عام من خلال ما يدور في معرض المناقشات العلنية بسبب ان التبادلات المشفرة التي يتطلبها استخدام تقنية المحادثة المرئية عن بعد وبالتالي هو ما يؤدي الى خطورة هذه التقنية على الصفة الانسانية للعدالة الجزائية حيث ان هذه الاخيرة ليست خدمة عامة مثل

////////////////////////////////
ر ت م د ...../ر ت م د إ : ...../ .....
دريهمي عبد الحكيمجامعة الجزائر 1
عنوان المداخلة :تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية
Remotecriminaltrailtechnology as a mechanism to ensure the speed of criminalprocrdures

الخدمات الاخرى ولا ينبغي النظر الى لاجراء على انه مجرد تقنية بسيطة لتنظيم المحاكمة بهدف تحقيق سرعة الفصل في الخصومة خلال اجل معقول من جهة وتحسين الاداء و الربح و الفعالية في سير الاجراءات الجزائية من جهة اخرى بل يجب ان تتخذ هذه التقنية ضمن ادارة الخدمة العامة للعدالة ويجب ان لا يترتب على استخدامها ضرر بنوعية و جودة الاحكام القضائية و بعدها الانساني ومع ذالك فان هذه التكنولوجيا المستحدثة ونضرا لمدى توغلها في النشاط القضائي جعل هذا الاخير قابلا للقياس الكمي وفي ذالك خطر يؤدي الى الانحراف الاداري و تقويض مبدا استقلالية القاضي على الرغم من كون استخدام هذه التقنية يوفر العديد من المزايا للمتقاضين كتوفير الوقت الازم و الضروري لاقتضاء الحقوق و حماية الحريات العامة عن طريق تحسين عملية الوصول الى تطبيق القانون وهو ما يجعل الامر مربوط بضرورة توفر الوسائل المادية الذكية للوصول اغلى هذه التكنو لوجيا التي تمكن الخصوم بوجه عام من الحفاض على حقهم في الوصول الحقيقي الى القاضي[9].

كما يشكل الحق في الدفاع ضمانة اساسية لاطراف الدعوى الجزائية عند استخدام تقنية المحادثة المرئية عن بعد وما نلاحظه من خلال استقرائنا من القانون رقم 05-03 المتعلق بعصرنة العدالة السالف الذكر لم يعطي اهمية قصوى للحق في الدفاع عند اجراء المحاكمة الالكترونية وهو ما يثير فعلا عدة اشكالات اجرائية في هذا الشان سيم ما تعلق في حرية اتصال المحامي بالمتهم مباشرة في أي وقت علما ان الواقع العملي اثبت عدم السماح للمحامي بالاتصال المباشر بالمتهم , وان التهويل الى استخدام تقنية الاتصال المرئي اثناء المحاكمة لا يوفر على الاطلاق للمتهم حرية كاملة من الاستفادة من الحق في الدفاع عن نفسه و اعداد دفاعه و اختيار الاسلوب و الكيفية الازمة لتقديم الرد على الاتهام بالدليل المناسب لدحض ادلة الاثبات التي تدفع بها النيابة العامة او الضحايا في مواجهته اثناء جلسة المحاكمة او التحقيق النهائي فالمتهم الذي يختار المحاكمة الجزائية عن بعد مكن خلال استخدام تقنية الاتصال المرئي المسموع يكون تحت رقابة قاضي الحكم اثناء استجوابه او مواجهته بغيره من الخصوم و الشهود حيث لا يسمح له بعد ذلك او قبل ذلك بالاتصال بمحاميه عبر الهاتف او أي وسيلة من وسائل الاتصال الافتراضي الحديث علما ان تمكين المتهم من الاتصال بمحاميه عبر الهاتف لا يوفر له الضمانات الكافية لحفض اسراره و خبايا نفسه من استراق السمع و التنصت عليه خاصة في القضايا الحساسة و الخطرة التي لا تخلو من

////////////////////////////////
ر ت م د ...../ر ت م د إ : ...../ .....
دريهمي عبد الحكيمجامعة الجزائر 1
عنوان المداخلة :تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية
Remotecriminaltrailtechnology as a mechanism to ensure the speed of criminalprocrdures

اية مخاطرة ينتج عنها الاختراق لدوائر الاتصال فيما بينها في مجال التصنت على المحادثات التي ترجع علي بالضرر الذي يهدد حريته و يكشف اسراره و اخباره لذلك فان اقتصار استخدام تقنية الاتصال المرئي المسموع في نضام المحاكمة عن بعد بين المتهم و محاميه عند اجراء المحاكمة الجزائية التي تكون تحت اشراف رقابة القضاة فقط يعد في الواقع انتهاك و اعتداء على حرية الاتصال بين المتهم و محاميه في أي وقت يتعين فتح المجال لاتصال المحامي بالمتهم عبر تقنية الاتصال امرئي المسموع عن بعد وفق الشروط القانونية المطلوبة لان منع المتهم من حقه في الاتصال بمحاميه و تقديمه للاستجواب او المواجهة امام قاضي الحكم دون تمكينه من الوقت الازم و الضروري لحرية الاتصال ب محامي قبل ذلك او بعد ذلك و في حرية تامة يعد انتهاك صارخا لضمانة الحق في الدفاع الكمرس دستوريا طبقا لاحكام المادة 170 من الدستور التي تنص على (يستفيد المحامي من الضمانات القانونية التي تكفل له الحماية من كل اشكال الضغوط وتمكنه منم ممارسة مهنته بكل حرية في اطار القانون) [10].

الخاتمة :

نستنسج من خلال ما تقدم ان استخدام تقنية المحادثة المرئية و المسموعة عن بعد في نظام المحاكمة عن بعد قد ضهر نتيجة التطور الحاصل في مجال تكنولوجيا الاتصالات هذه الاخيرة التي فرضت على مختلف الانظمة القانونية في العالم ضرورة تحيين منضوماتها و قوانينها بما يتماشى و متطلبات العصر الحالي خاصة مع ما توفره من مزايا كبيرة للعدالة كاتحقيق سرعة الإجراءات الجزائية حيث تعد هذه الأخيرة ضمانة هامة للحقوق الخصوم في كل مراحل الدعوى الجزائية واحد أهم ركائز المحاكمة الجزائية العادلة.

الإحالة والتهميش:

1- ليندة مبروك، 2022، ضمانات المحاكمة العادلة ، مجلة الحقوق والعلوم الانسانية، المجلد15، العدد 01. ص642.
2- حاتم محمد فتحي أحمد البكري، مبدأ الشفوية والتقنيات الحديثة في المحاكمات الجنائية ، جامعة المنصورة مصر، دون ذكر سنة النشر، ص 152.

3- عادل يحيا، التحقيق والمحاكمة الجنائية عن بعد، دراسة تحليلية تأصيلية لتنقية فيديو كونفرانس، دار النهضة العربية، مصر، 2006، ص202.

قائمة المراجع :

أولا : الكتب بالغة العربية

1- حاتم محمد فتحي أحمد البكري، مبدأ الشفوية والتقنيات الحديثة قي المحاكمات الجنائية ، جامعة المنصورة مصر، دون ذكر سنة النشر.
2- رمضان غسمون، الحق في المحاكمة العادلة من خلال التشريع الوطني الجزائري والتشريع الدولي، دار المعية للنشر والتوزيع، الجزائر 2010.
3- عادل يحيا، التحقيق والمحاكمة الجنائية عن بعد، دراسة تحليلية تأصيلية لتنقية فيديو كونفرانس، دار النهضة العربية، مصر، 2006.
4- عمارة عبد الحميد ، 2018 ، استخدام تقنية المحادثة المرئية عن بعد في التحقيق والمحاكمة الجزائية ،المجلة العربية في العلوم الإنسانية والاجتماعية، مجلد10 عدد 03 ، الجزائر ،ص 1065.
5- دريهمي عبد الحكيم، 2021، حق إجراء المحاكمة الجزائية خلال أجل معقول، أطروحة دكتوراه، الجزائر، جامعة الجزائر 1، كلية الحقوق، قسم القانون العام ، تخصص القانون الجنائي والعلوم الجنائية، اشراف عبد الحميد عمارة، ص 254.
6- أنظر المادة 212 من قانون الإجراءات الجزائية الجزائري.
7- عمارة عبد الحميد ، المرجع السابق، ص 1067.
8- عمارة عبد الحميد، نفس المرجع، ص 1069.
9- عبد الحكيم دريهمي، الأطروحة السابقة، ص 262.
10- عادل يحيا، المرجع السابق، ص 184.

////////////////////////////////
ر ت م د ...../ر ت م د إ : ...../ .....
دريهمي عبد الحكيمجامعة الجزائر 1
عنوان المداخلة :تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية
Remotecriminaltrailtechnology as a mechanism to ensure the speed of criminalprocrdures

ثانيا: المقلات

1 – عمارة عبد الحميد ، 2018 ، استخدام تقنية المحادثة المرئية عن بعد في التحقيق والمحاكمة الجزائية ،المجلة العربية في العلوم الإنسانية والاجتماعية، مجلد10 عدد 03 ، الجزائر.

2 – دريهمي عبد الحكيم، 2021، حق إجراء المحاكمة الجزائية خلال أجل معقول، أطروحة دكتوراه، الجزائر، جامعة الجزائر 1، كلية الحقوق، قسم القانون العام ، تخصص القانون الجنائي والعلوم الجنائية، اشراف عبد الحميد عمارة.

3 –ليندة مبروك، 2022، ضمانات المحاكمة العادلة ، مجلة الحقوق والعلوم الانسانية، المجلد15، العدد 01.الجزائر.

مخبر الدراسات القانونية التطبيقية
فرقة البحث دراسات مستحدثة في التشريعات العقابية

وبالتعاون مع فرقة بحث التكوين الجامعي prfu

المحاكمة عن بعد: سرعة الإجراءات أم إهدار للضمانات

يوم 20 جوان 2022

//////////////////////////////////

ر ت م د ...../ر ت م د إ : ...../ .....

دريهمي عبد الحكيمجامعة الجزائر 1

عنوان المداخلة :تقنية المحاكمة الجزائية عن بعد كآلية لضمان سرعة الاجراءات الجزائية

Remotecriminaltrailtechnology as a mechanism to ensure the speed of criminalprocrdures

الاسم:نصيرة
اللقب:نهاري
أستاذة محاضرة قسم أ بكلية الحقوق والعلوم السياسية
بجامعة وهران 2 محمد بن أحمد –الجزائر-
رقم الهاتف:002137-91-50-68-06
الاميل:nehari_n@hotmail.fr
الاسم:هداية
اللقب:بوعزة
أستاذة محاضرة قسم أ بكلية الحقوق والعلوم السياسية
بجامعة وهران 2 محمد بن أحمد–الجزائر-
رقم الهاتف:002135-56-14-34-83
الاميل:hidayetb@ymail.com

عنوان المداخلة: وسائل المراقبة الإلكترونية في الإثبات الجنائي

المحورالخامس:تأثير الوسائل العلمية الحديثة على الإثبات الجنائي

الملخص:

يعد نظام المراقبة الإلكترونية من أهم ما أقرته وسائل التقدم العلمي التكنولوجي، والذي ينعكس بدوره على السياسة العقابية في معظم الأنظمة الجنائية المعاصرة، والتي أخذت به في مجال الإثبات الجنائي.

فالمراقبة هي الصورة الحية والمرئية التي تمثل الواقع الفعلي للحدث الإجرامي، والتي من خلالها يستطيع رجال الشرطة القضائية تقييم صحة استخباراتهم وتحرياتهم، حيث هناك طائفة من الوسائل العلمية الحديثة والتي يتم الاستعانة بها في عملية التحري،والتي اعتمدها المشرع الجزائري في قانون العقوبات كإعتراض المراسلات،تسجيل الأصوات وإلتقاط الصور.

الكلمات المفتاحية:القانون،العقوبات،الجنائي،المراقبة،الإلكترونية.

Abstract:

The electronic monitoring system is one of the most important things approved by the means of scientific and technological progress, which in turn is reflected in the punitive policy in most contemporary criminal systems, which have been adopted in the field of criminal proof.
Surveillance is the live and visual image that represents the actual reality of the criminal event, through which the judicial police can assess the validity of their intelligence and investigations, as there are a range of modern scientific methods that are used in the investigation process, and which were adopted by the Algerian legislator in the Penal Code such as intercepting correspondence, recording Sounds and take pictures.

Keywords: Law, Penalties, Criminal, Monitoring, Electronic.

مقدمة:

إزاء تطور أساليب ارتكاب الجريمة أصبح اكتشاف الجاني أمراً عسيراً ومن ثَمَّ كان لزاماً على المجتمع أن يستخدم نفس السلاح (سلاح العلم والتكنولوجيا)، باستخدام وسائل المراقبة بالأجهزة الحديثة لكشف الجريمة واثباتها، وهذا مايسمى بالمراقبة الإلكترونية والتي يقصد بها ذلك العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية، لجمع البيانات والمعلومات عن المشتبه به، سواء كان شخصا أو مكانا أو شيئا حسب طبيعته، وبالتالي فمن خلال هذا التعريف يتضح لنا أن المراقبة الإلكترونية هي وسيلة حديثة تخص فقط الجريمة المعلوماتية دون غيرها، وأيضا هي من وسائل جمع البيانات والمعلومات عن المشتبه فيه.

وقد عرفت المادة 03 من قانون 09-04 مراقبة الاتصالات الإلكترونية، حيث تشمل الاتصالات السلكية واللاسلكية، والخلوية كالفاكس والبريد الإلكتروني، ومواقع الدردشة حتى المنتديات وساحات الرأي والنقاش التي تسمح بنقل الأفكار والمعلومات.

ومن هذا كان لابد من الأخذ بنظام المراقبة الإلكترونية في مجال الإثبات الجنائي، مما يعزز من نتائج البحث والتحري وخاصة عندما لا تتعارض نتائجها العلمية مع الضمانات الشرعية والطبيعية للحقوق الإنسانية.

ومن هنا نتساءل عن الوسائل المتبعة في المراقبة الإلكترونية ؟وفيما تتمثل أهم شروطها وضوابطها القانونية؟هذا ماسنجيب عنه إتباعا لمايليّ:

المبحث الأول: إجراء اعتراض المراسلات

يعتبر إجراء اعتراض المراسلات مكسبا هاما لسلطات البحث والتحري في الكشف عن بعض الجرائم المحددة على سبيل الحصر ومنها الجرائم الإلكترونية، وهذا بالرغم ما قد يشكله من مساس بحرمة الحياة الخاصة المكفولة قانونا، لذلك لا بد من الوقوف على المقصود بإجراء اعتراض المراسلات(المطلب الأول)، ومن ثم بيان خصائصه(المطلب الثاني).

المطلب الأول: مفهوم إجراء اعتراض المراسلات

يعد اعتراض المراسلات من الإجراءات التي جاءت وليدة الحاجة، لتمكن رجال الشرطة القضائية من مواجهة الصعاب التي قد تعترضهم في كشف الجرائم ومرتكبيها ويشمل هذا الإجراء على نسخ أو تسجيل المراسلات.

واعتبارا لما يستلزمه هذا الإجراء من سرية وحيطة حتى لا يمس بخصوصيات الأشخاص، فإننا سنخصص الفرع الأول لتعريف اعتراض المراسلات باعتبار أن هذا الأسلوب حديث في القانون الجزائري ونظرا للخصائص التي يحض بها هذا الإجراء سنتعرض لدراستها في فرع ثان.

الفرع الأول

تعريف إجراء اعتراض المراسلات

يقصد بالمراسلات قانونا جميع الخطابات والرسائل والطرود والمكالمات الهاتفية، لكونها لا تعدوا أن تكون من قبيل الرسائل الشفوية، والمشرع الجزائري في المادة 65 مكرر 5 من ق.ا.ج حصر تعريف المراسلات في تلك التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية فقط [1].

كما يعتبر إجراء اعتراض المراسلات اختراق المكالمة الهاتفية والاستماع إليها دون رضا صاحبها[2]، وهاته المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين والاستقبال والعرض[3].

كما يمكن اعتبار اعتراض المراسلات أيضا على أنه: تلك العملية التي تهدف إلى كل تلقي للمراسلة مهما كان نوعها مكتوبة أو مسموعة بغض النظر عن وسيلة إرسالها وتلقيها سلكية أو لاسلكية[4].

إضافة إلى أنه إجراء تحقيق يباشر خلسة وخفية، وينتهك سرية الأحاديث الخاصة، وتأمر به السلطة القضائية في الشكل المحدد قانونا [5].

الفرع الثاني

خصائص اعتراض المراسلات

يتضمن أسلوب اعتراض المراسلات خصائص معينة تساعد على تحديد مفهومه، وطبيعة العمل به، وهذه الخصائص تتمثل في اعتراض المراسلات الذي تتم خلسة دون علم أو رضا صاحب الشأن، اعتراض المراسلات إجراء يمس بحق الشخص في سرية الحديث، اعتراض المراسلات عملية تستهدف الحصول على دليل غير مادي ، استخدام أجهزة قادرة على التقاط الأحاديث.

1-عبد العالي حاحة، الآليات القانونية لمكافحة الفساد الإداري في الجزائر، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق، ص 260.

2- محمد خريط، مذكرات في قانون الإجراءات الجزائية الجزائري، ط 6، دار هومة للطباعة والنشر والتوزيع ط6، الجزائر 1، 2001، ص 67.

3- عبد القادر دحدوح، أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية العدد 03، المركز الجامعي تيسمسيلت، الجزائر، 2017، ص 40.

4- عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، ، دار هومةط1، الجزائر، 2013، ص 62.

5-سميرة طالب ، إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في التشريع الجزائري وضمانات احترام حقوق وحريات المشتبه فيهم، مذكرة لنيل شهادة الماستر في الحقوق والعلوم السياسية، جامعة أكلي محند أو لحاج، 2016 ص 09.

أولا

اعتراض المراسلات خلسة

هو إجراء يتم دون رضا وعلم صاحب الشأن فلو كان صاحب الشأن عالم بالإجراء المطبق عليه لا تطبق بذلك خاصية الاعتراض، وكنا عندها أمام وسيلة وضع الخط الهاتفي تحت المراقبة، وبالتالي لا يمكننا القول بأننا أمام إجراء الاعتراض، لهذا فهو إجراء سري[6].

ثانيا

اعتراض المراسلات إجراء يمس بحق الشخص في سرية الحديث

هو إجراء يمس بحق الإنسان في سرية حديثه رغم أن نص المادة 39 من الدستور الجزائري[7]، تنص على حرية الحياة الخاصة، وتحمي سرية المراسلات والاتصالات الخاصة دون أي قيود، إلا أن إجراء اعتراض المراسلات ينتهك هذه الحرمة ويسترق السمع على المكالمات السلكية واللاسلكية.[8] التي عدّلت بنص المادة 46 من الدستور الجزائري والتي تنص على :" لا يجوز انتهاك حرمة حياة المواطن الخاصة ويحميها القانون، سريّة المواصلات والإتصالات الخاصة بكل أشكالها مضمونة. لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية ويعاقب القانون على انتهاك هذا الحكم حماية للأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه".

ثالثا

اعتراض المراسلات بهدف الحصول على دليل مادي

تعتبر تقنية التصنت على الأحاديث الهاتفية، دليل غير مادي ينبعث من عناصر شخصية، ما يصدر عن الغير من أقوال وأحاديث تقنع القاضي بطريقة غير مباشرة وتفيد في الكشف عن الجريمة، فتعتبر الأحاديث دليل معنوي لا مادي، فهدف هذا الإجراء هو التقاط الأدلة المعنوية بغية تأكيد الاتهام.

6- نصر الدين مروك ، محاضرات في الإثبات الجنائي، ج 1، ، دار هومة للطباعة والنشر والتوزيع ط3، الجزائر، 2009، ص 132.

7- تنص المادة 39 من الدستور الجزائري على أنه : " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها."

8- نلاحظ من نص المادة 65 مكرر 5 أن :" يمكن أن ينصب اعتراض المراسلات على مسألتين : التصنت على المكالمات الهاتفية تتمثل في التصنت المباشر والتصنت الغير المباشر، أما المسألة الثانية فتتمثل في الضبط والإطلاع على وسائل الاتصال السلكية واللاسلكية الأخرى.

رابعا

الأجهزة القادرة على التقاط الأحاديث

لقد ظهرت مع تطور عهد التكنولوجيا الحديثة تقنيات جديدة ذات فعالية كبيرة لاقتحام خصوصيات الأشخاص المشتبه بهم، لهذا فان عملية اعتراض المراسلات تستلزم أجهزة ذات تقنية واسعة قادرة على التقاط الأحاديث الصوتية بدقة [9].

المطلب الثاني: إجراءات اعتراض المراسلات

تعتبر عملية اجراء اعتراض المراسلات من أهم الإجراءات الأدلة الجنائية الرقمية، حيث عمل المشرع وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها[10]، والقيام أيضا بعملية التفتيش والحجز داخل منظومة معلوماتية[11].

الفرع الأول

تحديد مجال اعتراض المراسلات والجهة القضائية المختصة

عند القيام باجراء اعتراض المراسلات،يعتبر من الضروري تحديد مجال هذا الإعتراض وذلك بتحديد أنواع الجرائم التي يشملها هذا الإجراء،كما أنه من المهم كذلك تعيين الجهة القضائية المختصة في منح إذن القيام به.

أولا

تحديد مجال اعتراض المراسلات

نصت المادة (65 مكرر 5) من (ق.ا.ج.ج) على الجرائم التي يجوز القيام فيها بهذه العملية وهي: جرائم المخدرات، الجريمة المنظمة العبرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، وجرائم تبيض الأموال.

ثانيا

الجهة القضائية التي يجوز لها بمنح الإذن للقيام بهذه العملية

حسب ما ورد في نص المادة (65 مكرر 5) فان منح الإذن للقيام بهذه العمليات مقتصر على كل من :

1- وكيل الجمهورية: يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفيذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة له.

9- خداوي مختاري، إجراءات البحث والتحري الخاصة في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق والعلوم السياسية جامعة طاهري مولاي سعيدة 2015_2016، ص 32.

10- المادة 03 من القانون رقم: 09_04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

11- المرجع نفسه من 05 _09.

2-قاضي التحقيق: في حالة فتح تحقيق قضائي فان العمليات المذكورة في المادة 65 مكرر 5 تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة 65 مكرر 6/5 من ق. إ.ج.ج.

الفرع الثاني

الأماكن التي يسمح فيها بالاعتراض ومضمون الإذن ومدته

من أبرز الأمور التي يجب مراعتها عند القيام بإجراء إعتراض المراسلات ،هي تحديد الأماكن التي تقام فيها هذه العملية،كما أن معرفة مضمون الإذن بإجراء اعتراض المراسلات وتقدير مدته القانونية شيئين لا يمكن الإستغناء عنهما عند إجراء اعتراض المراسلات.

أولا

الأماكن التي يسمح فيها بالاعتراض

لم يحدد المشرع الجزائري بدقة الأماكن التي ستتم فيها عملية الاعتراض، بل جاء النص على عمومه، حيث نصت المادة 65 مكرر 05على:"... في أماكن خاصة أو عمومية... " دون استثناء فقد يكون منزلا أو مقهى للانترنت أو شركة...الخ مخالفا في ذلك المشرع الفرنسي الذي أورد استثناءات في هذا الشأن بموجب المادة 706-96 من (ق. إ.ج.الفرنسي) مثل: المحلات التي تحتوي على مؤسسات إعلامية والمحلات ذات الطابع المهني للأطباء وسيارات النواب والمحامين[12].

ثانيا

مضمون الإذن و مدته

يتضمن الإذن المذكور في المادة 65 مكرر 5 الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سواء كانت سكنية أو غيرها، وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، حيث تنص المادة 65 مكرر 7 على : " يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه كل العناصر التي

[12]- "Article 706 – 96 du (CPPF) : lorsque les nécessités de l inforation concernant un crime ou un délit entrant dans le chap d applications des articles 706 -73 et 706 -73 l exigent le juge d instructions peut, après avis du = procureur de la république autoriser par ordonnance otivée les officiers et agents de police judiciaire technique ayant pour objet sans le consenteent des intéressés , la captation la fixation al transission et l enregistreent de paroles prononcées par une ou plusieurs personnes a titre privé ou confidentiel, dans des lieux ou véhicules privés ou publics , ou de l iage d une ou plusieurs personnes se trouvant dans un lieu privé . Ces opérations sont effectuées sous l autorité et le contrôle du juge d instructions…
La ise en place du dispositif technique entionné au preier alinéa ne peut concerner les lieux visés aux articles 56-1.56 -2 et 56-3 ni être ise en œuvre dans le véhicule le bureau ou le doicile des personnes visées a l article 100 – 7... "

تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن السكنية المقصودة أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، يسلم الإذن مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية ".

من خلال هذه المادة يمكن أن نستكشف الشروط الشكلية والزمنية للإذن وهي :

1- أن يكون الإذن مكتوبا.

2- ذكر جميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصود، وذلك بالتحديد الدقيق للاتصال المراد مراقبته أو المراسلة التي سيتم اعتراضها وكذا المكان الذي يتم فيه وضع الترتيبات التقنية.

3- ذكر الجريمة التي تبرر اللجوء إلى هذه العملية وهي إحدى الجرائم المذكورة على سبيل الحصر في نص المادة 56 مكرر 5 من ق.ا.ج.ج.

المبحث الثاني

إجرائي تسجيل الصوت وإلتقاط الصور

إن نظام المراقبة الإلكترونية من أهم ما أقرته وسائل التقدم العلمي التكنولوجي، والذي ينعكس بدوره على السياسة العقابية في معظم الأنظمة العقابية المعاصرة التي أخذت به، حيث أصبح من الممكن رصد المحكوم عليه في أي مكان يتواجد فيه عن طريق متابعته الكترونيا[13]،وقد تم تطبيق هذا النظام تقريبا في أغلب دول قارة أوربا وأمريكا وبعض دول آسيا، حيث أصبح جزءا أساسيا في نظام العدالة الجنائية بها وهذا ما شجع المشرع الجزائري على إقراره ضمن سياسته الجنائية الحديثة.

ولعل من أهم هذه الإجراءات الحديثة المتبعة في نظام المراقبة الإلكترونية هي إجرائي تسجيل الأصوات (المطلب الأول) وإلتقاط الصور (المطلب الثاني).

13-أمنة أمحمد بوزينة، بدائل العقوبات السلبة للحرية في التشريع الجزائري، جامعة غرداية، مجلة أفاق علمية، المجلد 11، العدد 03، 2019، ص 126.

المطلب الأول

إجراء تسجيل الأصوات

حرص المشرع الجزائري على الحياة الخاصة للأفراد، ضد وسائل التجسس ومحاولة كشفها على غرار التشريعات المقارنة، فوضع نصوصا خاصة بذلك في قانون العقوبات، وبالرجوع إلى نص المادة 303 مكرر من ق.ع [14]، يمكن تحديد الأركان الواجب توفيرها في جريمة التقاط أو تسجيل أو نقل المكالمات أو الأحاديث الخاصة أو السرية ، ومن خلال استقراء النص القانوني المجرم والمعاقب على إتيانها أين أوجب المشرع ضرورة توفر الشروط المحددة بالمادة 303 مكرر، بأن يتم الاعتداء بالمساس بحرمة الحياة الخاصة للأشخاص عن طريق إتيان أحد الأفعال المادية المحددة بالتقاط تسجيل أو نقل المكالمات أو حديث خاص أو سري، أو أي تقنية كانت وهو ما سنتطرق فيه إلى تحديد مفهوم تسجيل الأصوات في (الفرع الأول)، ثم سنتناول إجراءات تسجيل الأصوات في (الفرع الثاني).

الفرع الأول

مفهوم تسجيل الأصوات

إن التسجيلات الصوتية يقصد بها جميع المكالمات الهاتفية من أحد الأطراف دون إذن ورضا الطرف الثاني أو دون علمه، وتتم ذلك عن طريق وضع رقابة على الهواتف وتسجيل الأحاديث التي تتم طريقتها.

مما لا شك فيه حظر الاعتداء بواسطة تسجيل الأصوات لا يقتصر على منع التصنت على المحادثات التليفزيونية بل يتعدى ليشمل حظر مراقبة وتسجيل الأحاديث الخاصة، فتسجيل الصوتي بقدر ما يساعد السلطات المختصة على كشف الجريمة، فانه يمثل تعديا على الحريات الشخصية وانتهاك للكثير من الحقوق الإنسانية لذا نتناول تعريف تسجيل الأصوات، ثم نتطرق إلى تسجيل الأصوات.

أولا

تعريف تسجيل الأصوات

يقصد به تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية، أوخاصة في مكان عام أو خاص[15]، فالتسجيل الصوتي هو الذي يجربه رجال الشرطة القضائية للإستعانة به في مجال

---

[14]– المادة 303 مكرر ق.ع، تنص :" يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 50000 دج إلى 300000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك :1 بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أ، رضاه ...» 2 بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه...".

15– سامية بولافة، مبروك ساسي، الأساليب المستحدثة في التحريات الجزائية محلة الباحث للدراسات الأكاديمية، العدد التاسع، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، ص 396.

الإثبات الجنائي، ولهذا فان التسجيلات التي يقوم به الأفراد فيما بينهم لا تعد من قبيل الإجراءات الجنائية نظرا لأنها لم تصدر في شأن دعوى جنائية حولتها السلطات القضائية بقصد الحصول على الحقيقة، كما يخرج من نطاق البحث تسجيل الأحداث التي لا تتضمن اعتداء على حق من يتم تسجيل حديثه[16]، كما

يعني به أيضا : تسجيل أحاديث المتهم وشركائه عن واقعة معينة من الوقائع، المنصوص عليها في المادة 65 مكرر 5 من قانون الإجراءات الجزائية [17].

ثانيا

طرق تسجيل الأصوات

يجب علينا الإشارة إلى طريقة سير الأجهزة المعدة لإجراء هذه العملية، والتي تتمثل في التسجيل الآلي والتسجيل المغناطيسي والتي سنتعرض إليها فيما يلي :

1_ التسجيل الآلي :

يتم التسجيل الآلي بواسطة استخدام آلة خاصة تترجم موجات الصوت إلى اهتزازت خاصة، عن طريق إبرة تعمل على سطح من الشمع أعد خصيصا لذلك، وتتفق هده الاهتزازات مع الأصوات التي تحدثها بالضبط لكي يمكن إعادة الصوت، بحيث تؤثر العلامات على سطح الشمع في الإبرة التي تترجم ذلك أليا أو كهربائيا إلى أصوات متشابهة مع الأصوات الأولى التي سجلت، ولقد وصل الأمر بالفنيين والأخصائيين بالتسجيل إلى إمكانية حذف حرف واحد أو كلمة واحدة بمهارة فائقة، مما يؤدي إلى تغيير محتوى الكلام وهذا ما يجعل مجالا للشك في القيمة العلمية لهذا التسجيل، وبالتالي مدى مشروعية الاعتداء بنتائجه[18].

2_ التسجيل المغناطيسي :

إن في تسجيل الشريط المغناطيسي تسبب الموجات الصوتية اهتزاز الميكروفون ويتم تحويلها إلى تيار كهربائي متغير، والذي يتحول بعد ذلك إلى مجال مغناطيسي متغير مما يؤدي إلى إنشاء تمثيل

16- خولة عباسي، الوسائل الحديثة في الإثبات الجنائي في القانون الجنائي مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية جامعة محمد خيضر، بسكرة، 2013_2014، ص 22.

17- فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، العدد 33، كلية الحقوق والعلوم السياسية، جامعة منتوري قسنطينة، جوان، 2019، ص 237.

18- وسام عواس، مشروعية وسائل البحث الجنائي الحديثة، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر، 2013_2014، ص 105.

للصوت وتكون إعادة إنتاج الصوت تناظرية هي عملية المعالجة العلمية، مع وجود طبقة مكبر صوت أكبر مما تؤدي إلى حدوث تغيرات في الضغط الجوي لتكوين موجات صوتية مسموعة [19].

تعتبر طريقة الصوت على الشرائط الممغنطة من أهم التسجيلات الصوتية حيث نجد أن معظم التسجيلات الصوتية تعتمد على التسجيل المغناطيسي، غير أن التسجيلات الصوتية التي تهمنا هي تلك التي يقوم بها رجال الشرطة القضائية، والتي تتم بناء على أمر تصدرها لسلطة القضائية المختصة، قصد استحداثها في مجال الإثبات الجنائي.

وبالتالي فان التسجيلات الصوتية التي يقوم به الأفراد فيما بينهم لا تدخل ضمن الإجراءات الجنائية، كما يخرج من هذا النطاق أيضا التسجيلات التي تمس بحقوق وحريات الشخص الخاضع حديثه للتسجيل، كما هو الشأن بالنسبة لتسجيل الأحاديث التليفزيونية، أو الإذاعية أو الصحفية، متى يتم ذلك بمعرفة صاحب الشأن.

الفرع الثاني

إجراءات تسجيل الأصوات

يعتبر إجراء تسجيل الأصوات من الإجراءات الخفية مثل اعتراض المراسلات، الهدف منه تمكين أجهزة البحث والتحري من اكتشاف الحقيقة، لذلك سنتطرق لذكر أهم إجراءاته.

أولا

تحديد مجال تسجيل الأصوات

نصت المادة (65 مكرر 5) على الجرائم التي يجوز القيام فيها بهذه العملية وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية.

ثانيا

منح الإذن للقيام بهذه العملية

حسب ماورد في نص المادة 6 (مكرر 5) فان منح الإذن للقيام بهذه العمليات مقتصر على كل من :

1_ وكيل الجمهورية:

يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها تحت مراقبته المباشرة.

2_ قاضي التحقيق:

19- تسجيل الصوت المغناطيسي، مقالة منشورة على الموقع الإلكتروني التالي : تاريخ الإطلاع 2019/06/20 على الساعة 11:21 **http://ohaedsiswet.Ahlaontada**.

في حالة فتح تحقيق قضائي فان العمليات المذكورة في المادة 65 مكرر 5 تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة 65 مكرر 6/5 من ق.ا.ج.ج.

3_ أماكن تسجيل الأصوات :

لم يحدد المشرع الجزائري بدقة الأماكن التي ستتم فيها عملية تسجيل الأصوات، بل جاء النص على عمومه، حيث نصت المادة (65 مكرر 5) على:"... في أماكن خاصة أو عمومية..." [20]، حيث سمح المشرع الجزائري بالدخول إلى تلك الأماكن و وضع الوسائل اللازمة لتسجيل الأصوات كتركيب الميكروفونات حتى بغير علم وموافقة أصحابها وحتى خارج الآجال المنصوص عليها في المادة (47)من (ق.ا.ج.ج) .

1- كيف تتم العملية :

تتم عملية تسجيل الأصوات بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65 مكرر 8)[21]. كما يلزم ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بتحرير محضر عن كل عملية تسجيل الأصوات وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط، ويحدد بالضبط تاريخ وساعة بداية هذه العمليات والانتهاء منها.

إن التسجيلات الصوتية الحديثة لها حجية كبيرة في الإثبات الجنائي، لأن التقنيات الإلكترونية المتطورة للتسجيل لا تحتمل الخطأ، وبإمكان الخبراء كشف أي تعديل أو تلاعب بواسطة تقنية عالية الكفاءة، كما يجب على القاضي قبل ترسيخ قناعته التأكد من أن الصوت المسجل يخص المتهم عن طريق ما يعرف ببصمة الصوت، وأن لا يكون قد حدث تعجيل أو مونتاج على التسجيل، كما يجب أن يكون التسجيل واضحا.

20- عبد الفتاح بيومي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية _ دراسة مقارنة، في ضوء القواعد العامة للإجراءات الجنائية، دار النهضة العربيةط1 مصر، 2009. ص 781.

21- حيث تنص المادة 65 مكرر 5 من ق.ا.ج.ج على : "يجوز لوكيل الجمهورية أ، ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أ، ضابط الشرطة القضائية الذي ينيبه، أن سيخر كل عون مؤهل لدى مصلحة أ، وحدة أ، هيئة عمومية أ، خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالعمليات التقنية للعمليات المذكورة في المادة 65 مكرر 5 أعلاه ".

المطلب الثاني

إجراء التقاط الصور

إن عملية التقاط الصور باعتبارها إحدى وسائل البحث والتحري الحديثة، هي استثناء عن المبدأ العام الذي يمنع التقاط الصور دون رضا صاحبها لما فيها من مساس بحرمة الحياة الخاصة المحمية قانونا، سنتناول في مفهوم التقاط الصور في (الفرع الأول)، ثم نتناول إجراءاته في (الفرع الثاني).

الفرع الأول

مفهوم التقاط الصور

لا تطبق المادة 303 مكرر من ق.ع [22] سوى إذا كان هناك التقاط صور، ذلك أنه يتم بفضل إتباع تقنية معينة، تتمثل في استعمال وسيلة تكنولوجيا، كما يتأكد ذلك أن الصورة يتم تسجيلها أو نقلها بعد ذلك، حيث لا يمكن سوى هذه الوسيلة التقنية أن تقوم بهذه العملية [23].

لهذا سنتعرض إلى تعريف التقاط الصور وإلى الوسائل التي تباشر بواسطتها.

أولا

تعريف التقاط الصور

تعتبر الصورة رسم للملامح المادية والجسدية لشخص وانعكاس لما يدور في عقله من أفكار وما يعتبره من انفعالات وما يخفيه من مشاعر ورغبات، فهي ترتبط ارتباطا وثيقا باعتبارها المرأة العاكسة التي تكشف عن ذاته [24].

أما فيما يخص التقاط الصور ونقلها فهو يعد من الانتهاكات التي قد تمس الحق في الحياة الخاصة، لأن صورة الإنسان تعد من مظاهر الخصوصية التي يحظر على الغير التقاطها دون إذن صاحبها ونقلها إلى الغير، وتداولها بصورة غير مشروعة [25]، فمواثيق حقوق الإنسان والدستور الجزائري نص عن هذا الحق في نص المادة 39 " لا يجوز انتهاك حرمة حياة المواطن الخاصة و حرمة شرفه يحميها القانون "[26].

22- المادة 303 مكرر من ق. ع .ج

23- عبد العزيز نويري، الحماية الجزائية للحياة الخاصة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة 2010_2011، ص 129.

24- فضيلة عاقلي، الحماية القانونية للحق في حرمة الحياة الخاصة، رسالة دكتوراه، تخصص القانون الخاص كلية الحقوق، جامعة الإخوة منتوري قسنطينة 2، 2011_2012، ص 233.

25- نهلاء عبد القادر المر مني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، د " الأردن ، 2008، ص 179.

26- سالم العكلوك، الوسائل الحديثة للإثبات الجنائي في قانون الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أمة البواقي، 2017_2018، ص 21.

ثانيا

وسائل التقاط الصور

تقوم عملية التقاط الصور أساسا على استخدام الكاميرات، أو أجهزة خاصة تلتقط الصور والصوت لوضعية شخص أو عدة أشخاص مشتبه في أمرهم، على الحالة التي كانوا عليها وقت التصدير.

فالتقاط الصور يستبعد الأشكال البسيطة لتجسس البصري، كما يتطلب وسائل تقنية التي سيتم شرحها بالتفصيل فيما يلي :

1_ وسائل الرؤيا و المشاهدة :

تفيد العبارة الواردة في نص المادة 65 مكرر 5 " وضع الترتيبات التقنية "، على استخدام كل أنواع أجهزة التصوير ووسائل الرؤيا والمشاهدة التي تسهل عملية فالتقاط، إذ أدى تطور الجريمة خلال أواخر القرن الماضي، وبداية هذا القرن استخدام المجرمين لأحدث الأساليب العلمية في ارتكاب الجرائم إلى اختراع الدوائر التليفزيونية المغلقة التي تسمح بمراقبة مكان ما، ومعرفة ما يدور بداخله دون علم الحاضرين.

2_ وسائل تسجيل الصورة :

في السنوات الأخيرة ظهرت آلات التصوير عن بعد، والتي تلغي حاجز المسافة، والتي تتيح اقتحام المجال الشخصي للأفراد ليلا، بقدرتها على التقاط صور دقيقة، كما تعد أساسا لأجهزة تسجيل الصورة، نقد أحدث التطور التقني نقلة نوعية لهذه الأجهزة، إذ جرى تصغير حجم هذه الآلات، بحيث أصبح من السهل وضعها في المباني، أو على جسم الشخص الذي يستعمله بطريقة تجعل اكتشافها صعبا[27] .

الفرع الثاني

إجراءات التقاط الصور

تعتبر عملية التقاط الصور الفوتوغرافية من الإجراءات الجديدة التي جاء بها المشرع الجزائري لمكافحة الجرائم المستحدثة ومنها الجرائم الإلكترونية، حيث نص على مجال تطبيقه و توضيح الإجراءات القيام بذلك.

نتطرق إليها كما يأتي :

27- رمزي بوشالة، التصنت على المكالمات والتقاط الصور بين التحريم والإباحة، مذكرة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهدي، أم البواقي، 2014_2015، ص 61.

أولا

تحديد مجال التقاط الصور:

نصت المادة 65 مكرر 5 سالفة الذكر على الجرائم التي يجوز القيام فيها بهذه العملية وهي :

1- جرائم المخدرات.

2- الجريمة المنظمة العابرة للحدود الوطنية .

3- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

4- جرائم تبيض الأموال.

5- الجرائم المتعلقة بالتشريع الخاص بالصرف.

6- جرائم الفساد.

ثانيا

منح الإذن للقيام بهذه العملية

حسب ما ورد في نص المادة 65 مكرر5 فان منح الإذن للقيام بهذه العمليات مقتصر على كل من :

1- وكيل الجمهورية :

يقوم وكيل الجمهورية المختص بمنح الإذن، وتنفذ العمليات المأذون بها على هذا الأساس وتحت المراقبة المباشرة له.

2- قاضي التحقيق :

في حالة فتح تحقيق قضائي فان العمليات المذكورة في المادة 65 مكرر 5تتم بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة وفق نص المادة 65 مكرر 6/5.

3- أماكن التقاط الصور:

على خلاف تسجيل الأصوات التي تتم في أماكن عمومية أو خاصة استثنى المشرع الجزائري التقاط الصور في الأماكن العمومية، غير أنه سمح بهذا التدبير في بعض القوانين الخاصة كالترصد الإلكتروني والاختراق بموجب المادة (56) من القانون 06_01 المتعلق بالوقاية من الفساد ومكافحته [28].

28- تنص المادة 56 من القانون رقم : 06_01 المؤرخ في : 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته على : " من أجل تسهيل جميع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلى التسليم المراقب أو إتباع أساليب خاصة كالترصد الإلكتروني والاختراق، على النحو المناسب وبإذن من السلطة القضائية المختصة "، (ج.ر) رقم : 14 المؤرخة في : 2006/03/08 ص 12.

ثالثا

مضمون الإذن و مدته

ويتضمن الإذن المذكور في المادة 65 مكرر 5 الممنوح سواء من طرف وكيل الجمهورية أو قاضي التحقيق على كل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط الصور لهم والأماكن المقصودة سواء كانت عامة أو خاصة، وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، حيث تنص المادة 65 مكرر7 على :"... يسلم الإذن مكتوبا لمدة أقصاها أربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية ".

رابعا

كيف تتم العملية

تتم عملية التقاط الصور بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة 65 مكرر 8. كما يلزم ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بتحرير محضر عن كل عملية التقاط الصور، وكذا عن عمليات وضع الترتيبات التقنية وعمليات الالتقاط، ويحدد بالضبط تاريخ وسلعة بداية هذه العمليات والانتهاء منها، وهذا بموجب المادتين 9_10 من (ق.ا.ج.ج) بعد دراستنا لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وما تمثله هّذه الإجراءات الجديدة في مكافحة الجرائم المستحدثة ومنها الجرائم الإلكترونية، إلا أنه يمكن ملاحظة بعض الإشكالات القانونية والعملية في تطبيقها [29] نلخصها كما يأتي :

1- الإشكالات القانونية : تتمثل في :

أ_ لم تبين النصوص القانونية الوسائل القانونية التي يمكن من خلالها استعمال الوسائل التقنية التكنولوجية للقيام بهذه العمليات.

ب_ عدم تحديد نوع المؤسسات المسخرة وكذا المصاريف والأتعاب.

2- الإشكالات العملية : تتمثل في :

أ_ مدى توافر الوسائل التقنية لاعتراض المراسلات و تثبيتها، وهي عادة ما تكون وسائل تقنية ذات كفاءة عالية.

ب_ مدى توافر التعداد البشري الكافي والمؤهل.

29- عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012 ص 67_68.

ت_ إمكانية التلاعب وإتلاف المراسلات والأصوات المثبتة على دعامات الكترونية أو مغناطيسية، لذا لا بد من إيجاد احتياطات خاصة لتخزينها.

خاتمة:

من خلال ما تقدم يتضح لنا بأن استخدام الأساليب العلمية الحديثة يجعل عملية الإثبات قابلة للتجديد والتطور وفقا للإنجازات الإنسانية المستمرة في كافة المجالات، نأخذ منها ما يفيد من نتائج، وخاصة عندما لا تتعارض نتائجها العلمية مع الضمانات الشرعية والطبيعية للحقوق الإنسانية، لهذا يجب الأخذ بالأساليب العلمية في الإثبات مع توفر الضمانات الكافية التي تحقق حرية وإرادة الإنسان.

فمسألة الدليل الإلكتروني تعتبر من المواضيع التي لا يستهان بها،إذ فرض هذا الدليل نفسه في مجال الإثبات الجنائي،باعتبار أنه ضروري لإثبات نوع مستحدث من الجرائم،وهي الجرائم الإلكترونية،فالدليل الإلكتروني يتمتع بقوة ثبوتية وحجية كافية،وهذا في مجال الإثبات الجنائي،إذ يجب عل القضاء والقانون الأخذ به،وفي ختام مداخلتنا توصلنا إلى مجموعة من **النتائج** إستلزمت مجموعة من **التوصيات:**

النتائج

-إن الوسائل التي تباشر خفية مثل إعتراض المراسلات،وتسجيل الأصوات،والتقاط الصور ،ورغم ضرورة إستخدامها في الإثبات الجنائي في العصر الحاضر ،إلا أن معظم التشريعات ومنها التشريع الجزائري لا يجيز استعمالها إلا إذا دعت ضرورات الصالح العام لذلك،وبصورة إستثنائية ووفق ضوابط معينة يحددها القانون،وذلك من أجل تحقيق نوع من التوازن بين تلك الضرورات من جهة وحماية تلك الحقوق من جهة أخرى.

-إن الدليل الناتج عن إستخدام هذه الطرق العلمية الحديثة مثله مثل بقية الأدلة الأخرى يخضع لمبدأ الإقتناع الشخصي للقاضي مهما كانت قيمته العلمية.

-إن مناط مشروعية استخدام الطرق العلمية الحديثة في الإثبات الجنائي هو عدم مساسها بالحقوق الفردية أو الكرامة الإنسانية دون أي إعتبار لما يمكن أن تحظى به النتائج المتحصلة بواسطتها من قيمة علمية،فالغاية لا يمكن أن تبرر طريق الوصول إليها.

-قصور أغلب التشريعات الإجرائية،فيما يخص إجراءات الحصول على الدليل الإلكتروني واقتصارها على القواعد العامة،فمازال الكثير منها يخضع هذه الجرائم للنصوص التقليدية وهو ما قد يترتب عليه الإعتداء على مبدأ شرعية الجرائم والعقوبات وإفلات الكثير من الجناة من العقاب.

-نقص الثقافة المعلوماتية فيما يتعلق بالدليل الإلكتروني،لدى رجال الضبط القضائي المكلفين بجمع هذا النوع من الأدلة،وكذلك القضاة الجنائيين،مما يصعب التعامل مع هذا الدليل،وقد يؤدي هذا الأمر إلى إتلافه ونقص قوته الثبوتية.

-إن الإثبات الجنائي مهما تطور بالنسبة للجرائم الإلكترونية وعلى شأن الأدلة العلمية الفنية في هذا الإثبات، فإنه يجب أن نبقي على سلطة القاضي التقديرية في تقديره واقتناعه بالدليل الإلكتروني،لأنه من خلال سلطته التقديرية يستطيع أن يفسر الشك لصالح المتهم،وأن يستبعد الأدلة التي يتم الحصول عليها بطريقة غير مشروعة.

التوصيات:

-التكوين الدوري والمستمر لضباط الشرطة القضائية سواء من الناحية القانونية أو التقنية بغية إكسابهم المهارات المطلوبة في التعامل مع الأدلة الإلكترونية.

-توفير الوسائل الحديثة في مجال تكنولوجيا الإعلام والاتصال للسلطات القضائية المكلفة بالبحث والتحري والعمل على تحديثها دوريا لتتماشى والتطور المستمر لتقنية المعلومات.

-استحداث جهة مختصة في مكافحة الجريمة المعلوماتية تتبع بجهاز الشرطة يتمخض عنها محققون إلكترونيون ذو معرفة ودراية بالناحية القانونية، وأن يتم تأهيل أفرادها للتعامل مع النظام المعلوماتي بما يمكنهم من تفتيش الوسط الإفتراضي وضبط محتوياته.

-.ضرورة التعاون الدولي في المجال الجنائي وخاصة فيما يتعلق بالجرائم الإلكترونية وبجمع الأدلة الإلكترونية،ووضع تشريع دولي خاص بالأدلة الإلكترونية، لأن الدليل الإلكتروني لا يقف عند حدود دولة،باعتبار أن الجرائم الإلكترونية من الجرائم العابرة للحدود،مما يحتم أن يكون هذا التعاون لتسهيل إجراءات تحصيل هذا النوع من الأدلة.

قائمة المراجع:

أولا-الكتب:

1-عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012.

2- نهلاء عبد القادر المرمني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن ، 2008.

3-عبد الفتاح بيومي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية ،دراسة مقارنة، في ضوء القواعد العامة للإجراءات الجنائية، دار النهضة العربية، ط1، مصر، 2009.

4- أمنة أمحمد بوزينة، بدائل العقوبات السلبة للحرية في التشريع الجزائري، جامعة غرداية، مجلة أفاق علمية، المجلد 11، العدد 03، 2019.

5–نصر الدين مروك ، محاضرات في الإثبات الجنائي، ج 1، دار هومة للطباعة والنشر والتوزيع ط3، الجزائر، 2009.

6– محمد خريط، مذكرات في قانون الإجراءات الجزائية الجزائري، ط 6، دار هومة للطباعة والنشر والتوزيع ،الجزائر 1، 2001.

7– عبد المجيد جباري، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، ، دار هومةط1، الجزائر، 2013.

ثانيا: المقالات العلمية:

1–فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، العدد 33، كلية الحقوق والعلوم السياسية، جامعة منتوري قسنطينة، جوان، 2019.

2–سامية بولافة، مبروك ساسي، الأساليب المستحدثة في التحريات الجزائية مجلة الباحث للدراسات الأكاديمية، العدد التاسع، كلية الحقوق والعلوم السياسية، جامعة باتنة 1.

3–عبد القادر دحدوح، أساليب البحث والتحري الخاصة وحجيتها في الإثبات الجنائي، المجلة الجزائرية للحقوق والعلوم السياسية العدد 03، المركز الجامعي تيسمسيلت، الجزائر، 2017.

ثالثا: الرسائل الجامعية:

أ–أطروحات الدكتوراه:

1–عبد العالي حاحة، الآليات القانونية لمكافحة الفساد الإداري في الجزائر، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق.

2–عبد العزيز نويري، الحماية الجزائية للحياة الخاصة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة 2010_2011.

3–فضيلة عاقلي، الحماية القانونية للحق في حرمة الحياة الخاصة، رسالة دكتوراه، تخصص القانون الخاص كلية الحقوق، جامعة الإخوة منتوري قسنطينة 2، 2011_2012.

4–عبد العالي حاحة، الآليات القانونية لمكافحة الفساد الإداري في الجزائر، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق،جامعة محمد خيضر ببسكرة،2012–2013.

ب–مذكرات الماجستير:

–وسام عواس، مشروعية وسائل البحث الجنائي الحديثة، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر، 2013_2014.

ج–مذكرات الماستر:

–رمزي بوشالة، التصنت على المكالمات والتقاط الصور بين التحريم والإباحة، مذكرة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهدي، أم البواقي، 2014_2015.

–سالم العكلوك، الوسائل الحديثة للإثبات الجنائي في قانون الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي أمة البواقي، 2017_2018.

– خولة عباسي، الوسائل الحديثة في الإثبات الجنائي في القانون الجنائي مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية جامعة محمد خيضر، بسكرة، 2013_2014.

– خداوي مختاري، إجراءات البحث والتحري الخاصة في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق والعلوم السياسية جامعة طاهري مولاي سعيدة 2015_2016.–

سميرة طالب ، إجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في التشريع الجزائري وضمانات احترام حقوق وحريات المشتبه فيهم، مذكرة لنيل شهادة الماستر في الحقوق والعلوم السياسية، جامعة أكلي محند أو لحاج، 2016.

رابعا:النصوص القانونية:

–القانون رقم : 06_01 المؤرخ في : 2006/02/20 المتعلق بالوقاية من الفساد ومكافحته.

خامسا:المواقع الإلكترونية:

.-http://ohaedsiswet.Ahlaontada

الأستاذة/ مبروك حورية
أستاذة محاضرة أ جامعة الجزائر -1-

استخدام التكنولوجية في مرحلة البحث والتحري
(مرحلة الاستدلال)

مقدمة

أثبتت التكنولوجيات الرقمية أنها قادرة كسر الحواجز الثقافية والجغرافية، مكنت من تحقيق النمو الاقتصادي ووسعت من نطاق الاستفادة من الخدمات، ولكنها أيضاً هيأت فرصاً جديدة للأنشطة الإجرامية، فكان المجرمون المستفيد الأول من التكنولوجية لجديدة لأن فالتطورات ساعدتهم في توسيع أنشطتهم الإجرامية عبر المنصات الرقمية التي قللت من مخاطر اكتشافهم، ومن ناحية أخرى أتاحت التكنولوجيات فرصاً جديدة لتطيق القانون والتحقيق الجنائي والملاحقة القضائية لتحقيق الأمن وتمكين أجهزة العدالة الجنائية من منع الجريمة ومكافحتها، إلا أن أجهزة العدالة الجنائية تقف الآن في مفترق الطرق في ساحة التكنولوجيا، فالابتكارات التكنولوجية السريعة قد لا تؤدي فحسب إلى حفظ الأمن بفعالية ومعالجة القصور في تطبيق القانون، بل قد تكون عرضة أيضاً للاستغلال الإجرامي في مجالات مختلفة، فهناك العديد من الأمثلة على تكنولوجيات رقمية تستخدم لانتهاك الحقوق، وتقويض الخصوصية.

ولا شك أن قطاع العدالة قد استفاد بشكل ملموس خصوصا في السنوات الأخيرة من هذه التكنولوجية فكانت لها الأهمية البالغة في المساهمة في تسهيل متابعة و محاكمة وتنفيذ الأحكام ضد مرتكبي الجرائم الخطيرة ذات الأبعاد الدولية التي تتجاوز حدود الدولة الواحدة، كجرائم المخدرات والإرهاب والمتاجرة بالأسلحة وغيرها ...حيث سمحت التشريعات في قوانينها بإمكانية استخدام الوسائل التكنولوجيا الحديثة في مجال القضاء بتسهيل الاتصال بين الفاعلين فيه، فمن التلكس الى الفاكس والتليفون الثابت إلى عصر الأجهزة المحمولة والأقمار الصناعية نتاج الثورة الصناعية الثالثة و الرابعة المتمثلة تكنولوجيات الذكاء الاصطناعي التي تستند إلى البيانات الضخمة.

وإذ نركز في دراستنا هذه على استعمال هذه التكنولوجيا خدمة للعدالة من خلال استعمالها في إجراءات ، الدعوى الجزائية التي تتميز عن غيرها من الدعاوى بمراحلها الثلاثة مرحلة الاستدلال ومرحلة التحقيق ومرحلة المحاكمة، ونظر لأن لكل رحلة خصوصيتها فإننا نركز في دراستها هذه على مرحلة الاستدلال التي ترتبط ارتباطا وثيقا بحقوق الأطراف وضماناتها وهذا من خلال **الإشكالية** تتمحور أساسا حول التساؤل عن نطاق استخدام التكنولوجية في مرحلة البحث والتحري وهل حسنت من مستوى فعالية ونجاعة قطاع العدالة من غير المساس بالحقوق والحريات. وللإجابة على هذه الإشكالية نحاول من خلال هذه

المداخلة أن نتعرف على كيفية استخدام التكنولوجية في مرحلة البحث والتحري و الإشكالات التي تواجه الفاعلين القانونيين، من خلال عناصر الخطة التالية :

المبحث الأول / **استخدام التكنولوجية للتحري عن الجريمة ومرتكبيها**

المطلب الأول /**اعتراض المراسلات التقاط الصور وتسجيل الأصوات**

المطلب الثاني / **مراقبة الاتصالات الالكترونية**

المبحث الثاني/ استخدام التكنولوجية أثناء سماع المشتبه فيهم(الموقوف للنظر)

المطلب الأول / **التسجيل السمعي البصري**

المطلب الثاني / **التحاضر المرئي عن بعد**

المبحث الأول / استخدام التكنولوجية للتحري عن الجريمة ومرتكبيها

في إطار مكافحة الإجرام الخطير أصبحت الأساليب التقليدية في البحث والتحري عاجزة وعديمة الجدوى بسبب استغلال منفذي الإجرام التقنيات العلمية الحديثة في تنفيذ جرائمهم. فبات من الضروري مواكبة التطور واللجوء إلى وسائل تقنية حديثة للكشف عن الجريمة والبحث عن مرتكبيها، حيث منح قانون الإجراءات الجزائية الجزائري لوكيل الجمهورية وقاضي التحقيق، ولضباط الشرطة القضائية تحت رقابة هؤلاء صلاحية استخدام هذه الأساليب لتتناسب مع خطورة هذا النوع من الإجرام، موافقا بذلك توصيات الأمم المتحدة في الاتفاقيات المصادق عليها في هذا المجال، وحصرها في إجراءات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بمناسبة التحقيق التمهيدي وحالة التلبس و التحقيق الابتدائي، وهي وسائل أخذ بها المشرّع الجزائري وأخضعها لمجموعة من الضوابط ضمانا لعدم المساس بحقوق الأشخاص وحرياتهم وفي جرائم على سبيل الحصر هي: جرائم المخدرات و الجريمة المنظمة العابرة للحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و جرائم الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد وفقا لأحكام المادة 65 مكرر5 إلى المادة 65 مكرر 10 من قانون الإجراءات الجزائية [1]. كما أجاز المشرع أيضا صورة أخرى خاصة للتحريات عن الجريمة وهي مراقبة الاتصالات الالكترونية من خلال القانون 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المطلب الأول/ اعتراض المراسلات التقاط الصور وتسجيل الأصوات

أجاز المشرع الجـزائري بموجب المـادة 65 مكرر5 من قانون الإجراءات الجزائية لضابط الشرطة القضائية اعتراض المراسلات التقاط الصور وتسجيل الأصوات في مرحلة البحث التمهيدي أو التحقيق الأولي وفي حالة التلبس وفي حالة التحقيق الابتدائي التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية بناء على إذن من وكيل الجمهورية أو قاضي التحقيق.

---

(1)- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون الإجراءات الجزائية.

الفرع الأول/ اعتراض المراسلات

المراسلات بالمفهوم العام هي الرسائل البريدية المكتوبة والمطبوعات و الطرود و البرقيات التي توجد لدى مكاتب البريد و البرق، ومن خلال النص السابق نلاحظ أن المشرع قصد من هذه المراسلات الاتصالات السلكية واللاسلكية فقط ويقصد بالاتصالات السلكية واللاسلكية كما ورد في المادة 08 /21 من القانون 03/2000 [2] تحت عنوان المواصلات السلكية واللاسلكية : " كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية"، واعتبر البرق أيضا شكلا من أشكال المواصلات السلكية واللاسلكية طبقا للمادة 22/8 من نفس القانون.

فهذا النوع من الاتصالات هو الذي يتطلب عند اعتراضه تقنيات من طرف ذوي الاختصاص. وعلى خلاف المشرع الجزائري الذي جمع كل هذه الأساليب في مادة واحدة، فإن المشرع الفرنسي فرق بين هذه الأساليب في قانون الإجراءات الجنائية حيث نص في المادة 706-95 على أسلوب اعتراض المراسلات السلكية واللاسلكية، ونص في المادة 706-96 على تسجيل الأصوات والتقاط الصور بتخصيص مادة لكل منها. وهذا بالنسبة للجرائم الخطيرة المذكور في المادة 706-73 والمادة 706-73 -1 من قانون الإجراءات الجنائية الفرنسي. وتشكل هذه الإجراءات خطورة واعتداء على الحق في سرية المراسلات والاتصالات[3]المضمون دستوريا طبقا للمادة 2/47 والحق في حرمة المسكن المضمون بالمادة 1/48 من الدستور ورغم هذه الحماية الدستورية فان قانون الإجراءات الجزائية قررت لضباط الشرطة القضائية إمكانية التعرض للحياة الخاصة بأمر معلل من السلطة القضائية من وكيل الجمهورية أو قاضي التحقيق عند فتح التحقيق..

الفرع الثاني/ تسجيل الأصوات : التسجيل الصوتي معناه حفظ الأصوات والمحادثات التي جرت بين أشخاص في أجهزة خاصة معدة لهذا الغرض للاستماع إليها مرة أخرى باعتبارها دليل على ما ورد فيها و كان قديما يستعمل لسماع المكالمات الهاتفية الذي كانت أية موظفة اتصالات بإمكانها القيام بها حيث يكفي فقط ربط خط المتنصت عليه بخط المتنصت، ويسمى أيضا التنصت وهو مصطلح قديم يعني استراق السمع على الأحاديث الخاصة والمحادثات التليفونية خلسة دون علم صاحبها بواسطة أجهزة الكترونية أسفر عنها النشاط العلمي حديثا، في حين عرفه البعض بأنه " حفظ الأحاديث الخاصة على المادة المخصصة لإعادة الاستماع اليه مرة أخرى. فتغير إذا ليصبح في ظل التكنولوجية الحديثة اعتراض الاتصالات الالكترونية ليواكب التطور الحاصل في مجال تكنولوجيا الاتصالات عن طريق

---

(2)- القانون رقم 2000-03 المؤرخ في 2000/08/05 المحدد للقواعد المتعلقة بالبريد و المواصلات السلكية و اللاسلكية، الجريدة الرسمية عدد 48.

(3)- أوهايبية عبدالله شرح قانون الإجراءات الجزائية، الجزء الأول، بيت الأفكار، طبعة 2022 ، ص 424.

الهواتف الذكية المحمولة التي بإمكانها تسجيل الصوت والصورة وإرسال البيانات المختلفة وتسجيلها وتخزينه.

ولقد أجاز المشرع هذا الأسلوب من التحريات بوضع الترتيبات التقنية دون موافقة المعنيين من أجل تسجيل الحديث المتفوه به في أماكن خاصة كالمنازل المسكونة وكل توابعها أو عامة كالمعدة لاستقبال العامة كالمحلات التجارية وغيرها حيث تعد طبيعة الحديث أساس الحماية الجنائية بغض النظر عن المكان، ويعني به عبارة عن تسجيل الكلام المتفوه به من طرف المشتبه فيه ومحاوريه عن واقعة معينة من الوقائع خلسة وهو العملية المنصوص عليها في المادة 65 مكرر مكرر5 من ق. إ. ج. ففي الوقت الذي كرس فيه القانون الوطني والقوانين الدولية الحق في الحياة الخاصة ، فإننا نجد تسجيل صوت الشخص بموجب المادة 65 مكرر 5 السالفة الذكر والذي قد يكون اعترافا ضد نفسه ودون رضاه وموافقته عن طريق تسجيل كل ما يتفوه به من كلام بصفة سرية وفي أماكن خاصة أو عامة بمثابة خرق لهذه الخصوصية، وبغض النظر عن مكان التسجيل الذي قد يكون عاما كالشارع أو خاصا كالمسكن أو المكتب، أو التنصت على الهواتف النقالة أو غيرها، فالمهم هو الكلام المعبر عنه الذي قد يشكل دليلا يساعد في إظهار الحقيقة.

-**الفرع الثالث/ التقاط الصور** : لم يكتف المشرع بالسماح لضابط الشرطة القضائية تحت إشراف ورقابة وكيل الجمهورية بتسجيل الأصوات فقط، بل مكنه أيضا من إمكانية التقاط الصور فأجاز التقاط الصور لشخص أو عدة أشخاص يتواجدون في مكان خاص، باستخدام أساليب علمية حديثة مبررا ذلك بالتصدي لتفاقم معدلات الجريمة لما للصورة من نقل حي وكامل وصادق لمكان أو لواقعة معينة تساعد في خدمة القضاء وكشف الحقيقة. أما أجهزة المراقبة فمتعددة ومتنوعة منها ما يتعلق بالرؤية، المشاهدة وتسجيل الصورة وفي كل الأحوال تمثل انتهاكا خطيرا لحياة الأفراد الخاصة سواء في الأماكن الخاصة أو العامة .

فبموجب المادة 65 مكرر5 السالفة الذكر سمح قانون الإجراءات الجزائية الجزائري لضباط الشرطة القضائية أثناء التحريات أو في حالة التلبس من استخدام التصوير في الأماكن الخاصة التي تعد مستودعات أسرار المعنيين حتى وإن كان المشرع أصبغ طابع المشروعية على الدليل المستمد من تسجيل الأصوات والتقاط الصور، إلا أن هذا الأسلوب من الناحية الفنية والتقنية كان محل جدل، خاصة مع التطور التكنولوجي لعمليات التركيب المونتاج، ولهذا من المفروض أن تخضع مثلها مثل أي دليل آخر للسلطة التقديرية للقاضي.

خلاصة القول إنه بالنظر لطبيعة اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كإجراءات غير عادية، فإن المشرع في الوقت الذي غلب فيه المصلحة العامة على الخاصة المتمثلة في حماية خصوصية وأسرار الأشخاص أقر هذه الإجراءات مراعيا عدة شروط مما يحول دون التعسف في اللجوء إليها على نطاق واسع وتعميمها على كل الجرائم وهي كالتالي :

الفرع الرابع/ شروط اعتراض المراسلات تسجيل الأصوات(التصنت) و التقاط الصور : إن اعتراض المراسلات وتسجيل الأصوات والتقاط الصور إجراءات تمس بحرمة الحياة الخاصة للفرد التي أقرتها التشريعات الدولية والداخلية، مما استوجب على المشرع إجازتها ضمن مجموعة من الضوابط القانونية ورتب جزاءات على عدم احترامها، **حيث نصت المادة 65** مكرر 5 من قانون الإجراءات الجزائية الجزائري على أنه يشترط لمشروعية هذه الوسائل الشروط التالية " :

أولا/ ضرورات البحث والتحرّي و في الجريمة المتلبس بها، وفي التحقيق الابتدائي في جرائم المخدرات والجريمة المنظمة العابرة للحدود الوطنية وغيرها ممن عددتهم المادة 65 مكرر 5 السابقة الذكر.

ثانيا/ الحصول على إذن من وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق. والمشرع الفرنسي حماية للحقوق والحريات أوكل مهمة إعطاء الإذن وفقا لنص المادة 706-95 /1 من ق.إ.ف لقاضي من القضاء الجالس سواء في مرحلة التحريات أو التحقيق الابتدائي هو قاضي الحريات والحجز لما يتمع به من استقلالية اعتبارا أن القضاء المستقل حارس للحقوق والحريات، فلقد قضت المحكمة الأوروبية لحقوق الإنسان في هذا الصدد بقرارها MEDVEDEYEV بتاريخ 29 مارس 2010 بعدم اعترافها لوكيل الجمهورية الفرنسي بصفة القاضي[4]نظرا لخضوعه وتبعيته للسلطة التنفيذية وهذا ما اعتبرته المحكمة الأوروبية خرقا للمادة 6 من الاتفاقية الأوروبية لحقوق الإنسان والمتعلقة بالمحاكمة العادلة.

ثالثا/ أن يتضمن الإذن المعلومات اللازمة عن الاتصالات والأماكن المطلوب التسجيل أو التقاط الصور فيها وأن يكون مكتوبا وموقعا وممهورا بختم وكيل الجمهورية. أن يتضمن المدة التي يجب أن لا تتجاوز مدة أربعة أشهر قابلة للتجديد مرة واحدة طبقا للمادة 25 مكرر7 فقرة 2، والتي حددها المشرع الفرنسي بشهر واحد قابل للتجديد المادة 706-95 /1 من ق.إ.ف

-**رابعا/** يسمح الإذن بغرض وضع الترتيبات الخاصة بالتسجيلات بالدخول في الأماكن الخاصة أو العامة مساكن ومحلات أو غيرها دون علم لا رضا لا موافقة صاحب المكان، ويمكن الدخول عنوة وفي أي وقت من أوقات الليل والنهار خلافا لما هو وارد في المادة 47 ق.إ.ج، وهو المستخلص من نص المادة 65 مكرر 5 ق. ا.ج السابقة الذكر. مع الحفاظ على السر المهني المنصوص عليه في المادة 45 ق.إ.ج. وفقا للمادة 65 مكرر 6. ولقد نص المشرع على بعض الشروط الخاصة عند وضع ترتيبات الاعتراض على المراسلات والاتصالات بالنسبة لعضو البرلمان بغرفتيه بحيث من غير الممكن اتخاذ هذه

---

(4)-**المادة 303 مكرر** : " يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص، بأية تقنية كانت وذلك

1 – بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه،

2 – بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.

ويضع صفح الضحية حدا للمتابعة الجزائية.

الإجراءات إلا بعد إخطار رئيس البرلمان بذلك من طرف قاضي التحقيق، نفس الشيء بالنسبة لمساكن أو مكاتب المحامين يخطر النقيب ،بالنسبة لمساكن القضاة ومكاتبهم يخطر الرئيس الأول أو النائب العام للجهة القضائية التي يتبعها طبقا للمادة في 100-7 ق.إ. ف.

ولقد توسعت الغرفة الجنائية لمحكمة النقض الفرنسية في الأماكن الخاصة والعامة المراد وضع ترتيبات الاعتراض على التسجيلات والتقاط الصور فيها ليشمل المحادثات داخل المركبات حيث أباحت تسجيل. الكلام المتفوه به فيها، وأكدت أيضا في قرار لها بتاريخ 1 مارس 2006 على مشروعية التصنت على محادثات الموقوفين في المؤسسات العقابية مع زوّارهم.

خامسا/ تسخير الأعوان المؤهلين في مجال وضع الترتيبات الخاصة بالتسجيل والتقاط الصور **من القطاعات العمومية** أو الخاصة.

سادسا/ تحرير محضرين الأول بكل العمليات التي قام بها الضابط طبقا للمادة 65 مكرر 9 يتضمن تاريخ وساعة بداية ونهاية هذه العمليات، **والمحضر الثاني** يضم نسخ من التسجيلات والصور التي تفيد إجلاء الحقيقة يضمه إلى ملف القضية طبقا للمادة 65 مكرر 10.

المطلب الثاني / المراقبة الالكترونية للاتصالات

في ظل التطور التكنولوجي الحديث فلم تعد المراسلات و الاتصالات مقتصرة على الهاتف الثابث أو المحمول فقط، بل على كل أنواع الاتصال والتواصل التي تتم عن طريق وسائل الاتصال الحديثة من خلال الشبكة العنكبوتية، التي ساهمت بشكل كبير في تسهيل ارتكاب الجرائم المنظمة سواء عن طريق المكالمات الهاتفية أو المراسلات الإلكترونية المتبادلة عبر الشبكة المعلوماتية، وقد أجازت اتفاقية بودابست للجرائم الالكترونية الاعتراض الشرعي لكل أشكال النقل الالكتروني للبيانات سواء تم عبر التليفون أو الفاكس أو البريد الالكتروني...وتشمل الاتصالات محل الاعتراض محتوى غير مشروع أو دليل على الأفعال الإجرامية الخطيرة التي يعرفها القانون الداخلي لكل دولة طرف في الاتفاقية ، مما يستوجب ضرورة اعتراض المراسلات الالكترونية المتبادلة عبر الحاسب الآلي أيضا لدرء خطر الجريمة وملاحقة الجناة، وهذا ما قصده المشرع الجزائري من خلال اعتراض المراسلات السلكية واللاسلكية و ما اتجه إليه المشرع من خلال أحكام القانون 09-04 [5]المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ،حيث أجاز المشرع وضع الترتيبات التقنية لمراقبة الاتصالات الكترونية والقيام بإجراء التفتيش والحجز داخل منظومة معلوماتية في إطار إذن من السلطة القضائية.

(5)- القانون 09-04 المؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية عدد 47

الفرع الأول/ مفهوم مراقبة الاتصالات الالكترونية : لم يتطرق المشرع الجزائري إلى تحديد المقصود بمراقبة الاتصالات الالكترونية بل اكتفى فقط بتحديد مفهوم الاتصالات الالكترونية حيث أن إجراء المراقبة ينصب عليها فوفقا لما نص عليه القانون 09-04 السابق الذكر يقصد بالاتصالات الالكترونية في مفهوم هذا القانون ووفقا لما ذهبت إليه المادة 2 بند(و): "كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية ". وتعرف الاتصالات الالكترونية فقها بأنها الاتصالات التي تتم عن طريق جهاز الحاسب الآلي وأجهزة الهواتف المحمولة العادية و الذكية، والتي تتخذ شكل البريد الالكتروني أو شكل المحادثات الفورية التي تتم عن طريق شبكة الانترنت(كالفايسبوك، وغرف الدردشة وغيرها كل التطبيقات الذكية) وتبعا لذلك تأخذ الاتصالات الالكترونية شكل مراسلات مكتوبة أو محادثات شفوية أو صور ملتقطة وهي تشكل بذلك أهم العناصر الأساسية التي يقوم عليها الحق في حماية الحياة الخاصة، وهذا ما يجعل الإجراء من أخطر الإجراءات التي تمس بحق الإنسان في الخصوصية المنصوص عليه في المادة 303 مكرر إلى 303 مكرر 3 من قانون العقوبات الجزائري أين أضفى المشرع حماية خاصة على للحياة الخاصة في مواجهة الاعتداء عليها بأية تقنية كانت.

مشروعية المراقبة الالكترونية لقد أجاز المشرع الجزائري بنص المادة 65 مكرر 5 إجراءات جزائية السابقة الذكر وبنص المادة 3 من قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما المراقبة الالكترونية فنصت المادة 03 مع مراعاة الأحكام الخاصة التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتسجيل محتواها في حينها والقيام باجراءات التفتيش والحجز داخل منظومة معلوماتية".

الحالات التي يسمح فيها بالمراقبة الالكترونية

نصت المادة 4 من القانون 09-04 السابق الذكر على الحالات التي نلخصها فيما يلي :

- للوقاية الجرائم الإرهابية والجرائم الماسة بأمن الدولة
- في حالة وجود معلومات تكشف عن احتمال التعدي على منظومة معلوماتية تهدد مؤسسات الدولة في نظامها واقتصادها ودفاعها.
- لمقتضيات التحري والتحقيق عندما تكون المراقبة الكترونية هي الوحيد للوصول إلى نتيجة.
- في إطار طلب المساعدة القضائية الدولية ولا يتم ذلك الا بإذن السلطة القضائية
- عندما يتعلق الأمر بالجرائم المذكورة في الفقرة أ من هذه المادة (جرائم الإرهاب وأمن الدولة) يختص النائب العام لمجلس قضاء الجزائر بإعطاء ضابط الشرطة التابع للهيئة المذكورة في

المادة 13 من هذا القانون[6] إذن لمدة 6 أشهر قابلة للتجديد على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها.

بالإضافة إلى المراقبة الالكترونية نجد المشرع نص على التفتيش الالكتروني والتسرب الالكتروني فمثلا لم يكتف بالتسرب المادي في قانون الإجراءات الجزائية بل نظم التسرب لأي منظومة معلوماتية[7] . وكذا عملية تحديد الموقع الجغرافي للمشتبه فيه[8].la geolocalisation

خلاصة

إن تعديل قانون الإجراءات الجزائية بموجب القانون 2006-22 وكذا القانون 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. أثار جدلا كبيرا في مشروعية اللجوء إلى هذه الأساليب من بينها مراقبة الاتصالات الإلكترونية، لأن اللجوء إليها يتعارض مع مبادئ الحرية التي كفلتها الدساتير، والمواثيق الدولية، ويتعارض مع حق الفرد في خصوصيات حياته. حيث أن هذه الوسائل تستعمل خفية دون علم من تباشر عليه، لكنها تستمد مشروعيتها في ظل التطورات الخطيرة التي يشهدها الإجرام المنظم، وارتباطها بجرائم محددة وخطيرة منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات من جهة ومن جهة أخرى إخضاعها لمجموعة من الضمانات، يرى المختصين أن المشرع الجزائري في المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفيان سير الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال قد خرق المشروعية الإجرائية المنصوص عليها في المادة الأولى من قانون الإجراءات الجزائية، بوضع بعض الأحكام تسمح للسلطة الإدارية ممثلة

---

(6)- انظر المادة 13 من القانون 09-04 المؤرخ في 14 شعبان 1430 الموافق ل 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. وانظر المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفيان سير الهيئة الوطنية للوقاية من تلك الجرائم.

(7)- المادة 26 من القانون رقم 20-05 المتضمن الوقاية من التمييز وخطاب الكراهية ومكافحتاهما مع مراعاة أحكام قانون الإجراءات الجزائية، يمكن لوكيل الجمهورية او قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته لضابط الشرطة القضائية بالتسرب الالكتروني إلى منظومة معلوماتية أو نظام الاتصالات الالكترونية أو أكثر قصد مراقبة الأشخاص المشتبه في ارتكابهم لأي جريمة من الجرائم المنصوص عليها في هذا القانون، وذلك بإيهامهم انه فاعل معهم أو شريك لهم . يمنع على ضابط الشرطة القضائية تحت طائلة بطلان الإجراءات إتيان أي فعل أو تصرف بأي شكل من الأشكال من شانه تحريض المشتبه فيهم على ارتكاب الجريمة بغرض الحصول على دليل ضدهم.

(8)- المادة 77 من القانون رقم 20-05 السابق الذكر يمكن أن يأذن وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية لضابط الشرطة القضائية باستعمال أي وسيلة من وسائل تكنولوجيات الإعلام والاتصال أو وضع ترتيبات تقنية بغرض تحديد الموقع الجغرافي للمشتبه فيه أو المتهم أو لتحديد وسيلة ارتكاب الجريمة او كل ما له صلة بالجريمة وكذلك الأمر رقم 20-03 المتعلق بالوقاية من عصابات الأحياء ومكافحتها في مادته 20 التي تنص على أنه يمكن اللجوء إلى أساليب التحري الخاصة.

في الهيئة المذكورة بغرض الكشف عن الجرائم الإرهابية والجرائم المتصلة بتكنولوجيا الإعلام والاتصال مما يسمح لها باتخاذ بعض الإجراءات التي تمس الحقوق والحريات وتمس بالحق في الخصوصية المقرر للفرد في مرحلة تسبق مرحلة البحث والتحري تحت غطاء العمل الوقائي وهذا ما جاءت به المادة 4 من المرسوم الرئاسي[9].

المبحث الثاني/ استخدام التكنولوجية لسماع المشتبه فيه(الموقوف للنظر)

نعالج من خلال في هذا المبحث مجال استخدام التكنولوجية أثناء التوقيف للنظر من خلال مطلبين، الأول نتعرض فيه لاستعمال تقنية التسجيل السمعي البصري و في المطلب الثاني تقنية التحادث المرئي عن بعد.

المطلب الأول/ التسجيل السمعي البصري أثناء سماع الموقوف

يعتبر التسجيل السمعي البصري للموقوف للنظر في التشريعات المقارنة من أهم الضمانات الممنوحة للشخص الموقوف للنظر، على الرغم من أن المشرع الجزائري قد خص إجراءات التوقيف للنظر ببعض الضمانات التي احتوت عليها نصوص قانون الإجراءات الجزائية التي خضعت للتعديل في العديد من المناسبات، إلا أن مسالة التسجيل السمعي البصري لم يوليها المشرع الجزائري الاهتمام اللازم بالرغم من أهميتها أثناء التوقيف للنظر.

سواء تعلق الأمر بالأحداث أو البالغين ولكن نص على التسجيل السمعي البصري للحدث الضحية فقط[10]، ولأهمية الموضوع نحاول أن نتعرض بالشرح لهذه التقنية في القانون الفرنسي في ظل غيابها في القانون الجزائري ونركز على مزاياها وأهميتها في ضمان حقوق الموقوف للنظر.

الفرع الأول/ التسجيل السمعي البصري للحدث الموقوف للنظر في القانون الفرنسي

لأن فئة الأحداث تعتبر الفئة الأكثر حساسية في المجتمع بالنظر لسنها وحالتها النفسية الضعيفة، هذا الذي جعل التشريعات تولي الحدث محل التوقيف للنظر عناية خاصة سواء من حيث المعاملة أو من

---

(9)– انظر أوهايبية عبد الله، المرجع السابق ، ص 429.

(10)– لقد استحدث المشرع الجزائري وسيلة أخرى للإثبات بموجب قانون "15–12 "المتعلق بحماية الطفل، يمكن للقاضي الاستعانة بها، تتمثل في سماع شهادة الطفل الضحية عن طريق التسجيل السمعي البصري. تنص الفقرة الأولى من المادة 46 من قانون حماية الطفل على أن :" يتم خلال التحري و التحقيق، التسجيل السمعي البصري لسماع الطفل ضحية الاعتداءات الجنسية". وهذا ما ذهب إليه المشرع الفرنسي حيث وسع من دائرة الجرائم التي يتم التحقي فيها عن طريق التسجيل السمعي البصري ولم يحصرها في الجرائم الجنسية فقط ، إلا أنه اعتبر أنه إذا تعلق الأمر بهذه الجرائم فيكون التسجيل السمعي البصري إجباري

حيث الإجراء في حد ذاته، مثلا كالاستعانة بمحام و زيارة ومرافقة الأهل للحدث أثناء هذه المرحلة ومدة التوقيف وتمديدها التي تختلف عن مدة البالغ فغالبا ما تكون نصف المدة المقررة للبالغ.

التسجيل السمعي البصري ليس حديثا في القانون الفرنسي فلقد نص عليه المشرع الفرنسي بالقانون رقم رقم 2000/ 516 الصادر في 16 جوان سنة 2000 حيث أصبح التسجيل السمعي البصري للحدث إلزامي من تاريخ صدور هذا القانون من خلال تعديله للمادة 4-6 من الأمر رقم 45-174 المؤرخ 2 فبراير 1945 في فقرتها الأولى على إجبارية التسجيل اسمعي البصري enregistrement audiovisuel للأحداث الموقوفين لدى الشرطة يتم استعمال التسجيل السمعي البصري كأسلوب تقني لسماع الحدث الموقوف بدون موافقة القاصر أو الإشارة إلى عدم موافقته.

أما بعد إلغاء الأمر السابق المؤرخ في 1945 أصبحت الأحكام المتعلقة بالأحداث يحكمها القانون الجنائي للأحداث، ومسألة التسجيل السمعي البصري أصبحت منصوص عليها في المواد من (L413-9 إلى المادة 15-413 L) وهي النصوص المستحدثة بموجب الأمر رقم 2019-950 المؤرخ في 11 سبتمبر 2019 والمتعلق بقانون العدالة الجنائية للأحداث.

ولقد نص المشرع الفرنسي على التسجيل السمعي البصري للحدث الموقوف في المادة 12-413 L من قانون العدالة الجنائية للأحداث بقولة يخضع الحدث الموقوف للنظر للتسجيل السمعي البصري أثناء استجوابه من طرف ضابط الشرطة القضائية، وفي حالة تعذر التسجيل واستحالته لأسباب تقنية يخطر ضابط الشرطة القضائية وكيل الجمهورية أو قاضي التحقيق فورا و يدون ذلك في محضر مع تحديد طبيعة استحالة التسجيل. وفي حالة انعدام التسجيل لا يمكن الحكم بالإدانة بناءً على تصريحات الحدث وحدها المعترض عليها.

و لا يجوز الاطلاع على التسجيل المذكور في المادة 12-413.L ، إلا في حالة الخلاف على محتوى محضر الاستجواب أثناء التحقيق أو أمام جهة الحكم ، وذلك بقرار من قاضي التحقيق أو جهة الحكم.بقوة القانون أو بناءً على طلب وكيل الجمهورية أو أحد الخصوم. لا يمكن تسليم أي نسخة من التسجيل إلى الأطراف أو محاميهم.

ويتعرض أي شخص يقوم ببث التسجيل السمعي البصري الذي تم إجراؤه وفقًا للمادة 12-413.L نسخة منه بعقوبة الحبس لمدة سنة غرامة قدرها 15000 يورو وهذا طبقا للمادة 14-413.L

بعد مرور خمس سنوات على انقضاء الدعوى العمومية، يتم إتلاف التسجيل السمعي البصري ونسخته خلال مدة شهر. طبقا للمادة 14-413.L من قانون العدالة للجنائية للأحداث السابق الذكر.

التسجيل يلعب دورا في ضمان احترام حقوق الفرد الموقوف للنظر كما يعتبر وسيلة يطلع عليها لمراقبة صحة الإجراءات من طرف القائمين بالرقابة.

الفرع الثاني/ التسجيل السمعي البصري للموقوفين للنظر البالغين في مواد الجنايات

حرصا من المشرع على العدل و الإنصاف في النسخ الكتابي لجلسات السماع، التي تجرى في إطار التوقيف للنظر، فإنه جعل مسألة التسجيل السمعي البصري لهذه الجلسات، إلزامية في مواد الجنايات بموجب القانون رقم 2007-291 المؤرخ في 5 مارس 2007.

ومع أن المشرع جعل التسجيل السمعي البصري إلزامي إلا أنه فرق بين ما يجب تسجيله وما يستثنى من التسجيل، حيث تنص الفقرة 1 من المادة 64-1 من قانون الإجراءات الجنائية على ما يلي: "إن جلسات الاستماع للموقوفين لدى الشرطة بتهمة ارتكاب جناية، التي تتم في مقر وحدة الشرطة أو الدرك الموكلة إليها مهمة الضبطية القضائية تكون محل تسجيل سمعي بصري. وتطبق أحكام هذا النص على جميع القضايا الجنائية في مرحلة التحقيق التمهيدي أو في حالة التلبس".

في حالة القانون الحالية، يجب عدم إدراج الإخطار بحقوق الشخص الموقوف المنصوص عليها في المادة 63-1 من قانون الإجراءات الجنائية في التسجيل السمعي البصري لجلسات الاستماع في التوقيف للنظر في مواد الجنايات. ومع ذلك فإن المرسوم رقم 2019-1421 المؤرخ 20 ديسمبر 2019 نظم عملية التسجيل السمعي البصري للإبلاغ عن الحقوق أثناء التوقيف للنظر كتجربة في بعض مصالح أو وحدات معينة للشرطة القضائية المعينة بموجب قرار.

لكن في بعض الحالات قد لا يتم التسجيل السمعي البصري، وهذا لأسباب فنية على وجه الخصوص.

مثلا في الحالة التي تُجرى فيها جلسات الاستماع في إطار التوقيف للنظر لكنها تتم خارج مقر الشرطة أو الدرك. في الواقع أن التسجيل السمعي البصري للأشخاص الموقوفين لدى الشرطة لارتكاب جناية لا يكون إلزامي إلا عندما يتم في مقر مصلحة الشرطة أو الدرك.

أيضا تستثنى من التسجيل الحالات التي يستحيل تسجيلها تقنيا، على أن يذكر السبب في محضر السماع مع تحديد طبيعة استحالة التسجيل، ويجب إخطار وكيل الجمهورية بذلك فورا.

أيضا الحالات التي يقف فيها عدد الموقوفين عائقا أمام تسجيلهم كلهم في وقت واحد أو في أوقات مختلفة. أثناء نفس الإجراء أو في إجراءات منفصلة، في هذه الحالة يحيل ضابط الشرطة القضائية دون تأخير الملف إلى وكيل الجمهورية الذي يحدد بقرار مكتوب الأشخاص المستبعدين من التسجيل السمعي البصري وهذا بالنظر إلى ضرورات التحريات.

تنص المادة 64-1 من قانون الإجراءات الجنائية على ما يلي: "لا يجوز الرجوع إلى التسجيل أثناء التحقيق أو أمام جهة الحكم، إلا في حالة الاعتراض على محتوى محضر السماع ، وبقرار من قاضي التحقيق أو جهة الحكم، بناءً على طلب وكيل الجمهورية أو أحد الخصوم ".

ويمكن لمحامي المتهم أو المشتبه فيه أثناء المحاكمة أن يطلب من جهة الحكم بث تسجيل جلسة سماع الموقوف لدى الشرطة من أجل تقديم حج دفاعه".

يغلق التسجيل الأصلي و يختم توضع نسخة منه في الملف

يحتفظ بالتسجيل مدة خمس سنوات من تاريخ انقضاء الدعوى العامة. ويتم إتلافه على أقصى تقدير في غضون شهر واحد من انتهاء تلك المدة.

يجوز الاحتفاظ بنسخة ثانية من التسجيل لدى مصالح الضبط القضائي أو الوحدة المكلفة بالإجراء بحيث يجوز لها الرجوع إليها لأغراض التحريات. يتم إتلاف هذه النسخة في موعد لا يتجاوز خمس سنوات بعد آخر وثيقة إجرائية وضعها المحققون ، ويعاقب على نشر هذه التسجيلات بالسجن لمدة عام وغرامة قدرها 15000 يورو .

المطلب الثاني / استخدام تقنية التحاضر المرئي لاشك أن اقتحام التكنولوجيا لقطاع العدالة في السنوات الأخيرة أصبح حقيقة لابد منها، خصوصا في المسائل الإجرائية مما أدى إلى عدد من التعديلات في القوانين وبالتالي في أساليب عمل القاضي وكذلك في حقوق أطراف الدعوى، وعلى رأسها الحق في محاكمة عادلة وما يتطلبه من مفترضات كحق الدفاع مثلا. ومن أهم الاستعمالات التكنولوجية الحديثة في المحاكمة الجنائية تقنية التحاضر المرئي في مرحلة الاشتباه وخصوصا أثناء التوقيف للنظر باعتباره من أخطر الإجراءات الماسة بالحرية في مرحلة الاشتباه، ولقد أحاطه المشرع ببعض الضمانات التي تظل غير كافية لحماية حقوق و حريات الأفراد والتي لا تجعل الشخص في منأى عن التجاوزات الخطيرة التي يتعرض لها في مرحلة تكون فيها رقابة القضاء ضعيفة بعض الشيء إذ الإجراء سلطة مقررة لضابط الشرطة القضائية، مما يستوجب إحاطته بضمانات أوسع لحقوق الدفاع.

الفرع الأول/ تعريف تقنية التحاضر المرئي عن بعد ومرجعيتها القانونية

تعتبر تقنية التحاضر المرئي من أهم المستحدثات التكنولوجية التي أتاحت بعداً جديداً من أبعاد التقاضي عن بعد، لقدرتها على إقامة اتصال شخصي ومباشر بالصورة والصوت بين أعضاء هيئة الحكم المتواجدين مثلا في مقر الجهة القضائية وباقي أطراف الدعوى الذين تفصل بينهم مسافات شاسعة فيتفاعل كل منهم مع الآخر بيسر وسهولة كما لو كانوا في قاعة المحاكمة التقليدية،

أولا/ تعريف تقنية التحاضر المرئي عن بعد تعرف تقنية التحاضر المرئي بأنها عبارة عن "اتصال سمعي مرئي يجري في وقت واحد بين أطراف متفاعلة معاً في مواقع مختلفة حيث يمكن من خلال تلك المواقع استعمال شبكة الإنترنت في التحاور معاً أو مع الموقع الرئيس من خلال إمكانيات أجهزة الكمبيوتر السمعية والمرئية وكاميرات الفيديو الرقمية، ويمكن للمتحاورين في المواقع المختلفة توجيه الأسئلة والاستفسارات والتعليقات إلى الموقع الرئيس واستقبال الإجابات والاستفسارات الخاصة بها"[(11)]

ثانيا/ المرجع القانوني لتقنية التحاضر المرئي عن بعد

---

(11)- انظر مبروك ليندة، "ضمانات المحاكمة العادلة من خلال استخدام تقنية المحادثة المرئية " مقال منشور بمجلة الحقوق والعلوم الإنسانية، كلية الحقوق، جامعة زيان عاشور – الجلفة – (المجلد 15 ، العدد 01، الترقيم الدولي : 5086-26026 ، بتاريخ 27 أفريل 2022.

إن من أهم القوانين التي شرعت استخدام هذه التقنية في الجزائر، القانون رقم 15-03 المتعلق بعصرنة العدالة[12] نصت المادة 14 على أنه:" إذا استدعى بعد المسافة أو تطلب ذلك حسن سير العدالة يمكن استجواب وسماع الأطراف عن طريق المحادثة المرئية عن بعد."

أما أحكام المادة 15، فحددت نطاق استخدام هذه التقنية، في فقراتها الثلاث، حيث جاءت كما يلي:"يمكن قاضي التحقيق أن يستعمل المحادثة المرئية عن بعد في استجواب أو سماع شخص وفي إجراء مواجهات بين عدة أشخاص، يمكن لجهة الحكم أيضا أن تستعمل المحادثة المرئية عن بعد لسماع الشهود والأطراف المدنية والخبراء. ويمكن جهة الحكم أن تنظر في قضايا الجنح أن تلجأ إلى نفس الآلية لتلقي تصريحات متهم محبوس إذا وافق المعني والنيابة العامة على ذلك." ونص المشرع أيضا على استخدام هذه التقنية في الأمر رقم 15-02، المعدل والمتمم لقانون الإجراءات الجزائية [13] المادة 65 مكرر 27 بنصها: "يجوز لجهة الحكم، تلقائيا أو بطلب من الأطراف، سماع الشاهد مخفي الهوية عن طريق وضع وسائل تقنية تسمح بكتمان هويته، بما في ذلك السماع عن طريق المحادثة المرئية عن بعد واستعمال الأساليب التي لا تسمح بمعرفة الشخص وصوته..."

وعلى اثر انتشار جائحة كوفيد 19 وحفاظا على المجتمع صدر الأمر 20-04 المعدل والمتمم لقانون الإجراءات الجزائية[14]الذي سمح فضلا عن استخدام هذه التقنية باستعمال وسائل الاتصالات السمعية والمرئية في التحقيق وفقا للمادة 441 مكرر 02 نص أيضا المشرع على استخدامها ة في مرحلة المحاكمة المادة 441 مكرر 07.

استنادا للمرجع القانوني السابق نلاحظ أن المشرع الجزائري قد أجاز إجراءات الاتصال عن بعد تكنولوجيا في مراحل الإجراءات الجزائية بدءً من مرحلة التحري أو الاستدلال ثم التحقيق فالمحاكمة، وهي سلطة مقررة لهذه الجهات المختصة في طلب أطراف الدعوى عبر التكنولوجيا المسموعة والمرئية عندما يرى ضابط الشرطة أو قاضي التحقيق أو جهة الحكم ضرورة لذلك طبعا من خلال النصوص السابقة ونشير فيما يلي إلى كيفية استعمال هذه التقنية أثناء التوقيف للنظر.

---

(12) – القانون رقم 15-03 المتعلق بعصرنة العدالة، المؤرخ في 02/01/ 2015، المنشور بتاريخ 10=/02/ 2015، الجريدة الرسمية، عدد 06.

(13)- الأمر رقم 15-02، ، المتضمن قانون الإجراءات الجزائية المعدل والمتمم الأمر رقم 66-155، المؤرخ في 08 جوان 1966، المؤرخ في 23 جويلية 2015، الجريدة الرسمية الصادرة بتاريخ 23 جويلية 2015، العدد 40، ص 28.

(14)- أمر رقم 20-04 مؤرخ في 30أوت 2020 ، يعدل و يتمم الأمر رقم 66-155 المؤرخ في 08-06-1966 والمتضمن قانون الإجراءات الجزائية، جريدة رسمية عدد 51.

الفرع الثاني/ استخدام التحاضر المرئي أثناء التوقيف للنظر

نحاول من خلال هذا المطلب أن نبحث في نصوص القانون الجزائري ونصوص القانون الفرنسي باعتباره القانون الذي يتأثر به المشرع الجزائري أكثر من غيره في وضع بعض الأحكام خصوصا وأن المشرع الفرنسي كانت له الأسبقية في مجال استخدام هذه التقنية.

أولا / بالنسبة للمشرع الجزائري لا شك إن المتصفح لقانون الإجراءات الجزائية الجزائري، وبالضبط النصوص المتعلقة بالتوقيف للنظر من المادة 41- إلى المادة 65 والمادة 141 وما يليها وتعديلاتها المتكررة وكذا القانون رقم 15-03 المتعلق بعصرنة العدالة[15] السابق الذكر والذي يعتبر من أهم القوانين التي شرعت استخدام هذه التقنية في الجزائر يلاحظ أنه لا يوجد أي ذكر لاستعمال هذه التقنية بالذات أثناء التوقيف للنظر سواء لسماع الشهود أو الضحية أو محامي الدفاع من طرف ضباط الشرطة القضائية، على الرغم من أهميتها القسوى في تأمين التوقيف للنظر وتعزيز أدوات البحث والتحري، فلا توجد نصوص صريحة تتعلق بهذه التقنية وكيفية استخدامها أثناء التوقيف للنظر، لكن وفي ظل انتشار جائحة كوفيد 19 وبصدور الأمر 20-04 المعدل والمتمم لقانون الإجراءات الجزائية المشرع أولى هذه المرحلة أهمية خاصة بالنص صراحة على استخدام تقنية التحاضر المرئي أثناء التوقيف للنظر وهذا من خلال الفقرة الرابعة من المادة 441 مكرر 1 بنصه : " ... كما يمكن لوكيل الجمهورية أو قاضي التحقيق اللجوء إلى المحادثة المرئية **عن بعد في حالة تمديد التوقيف للنظر** وكذا في حالة القبض على المتهم خارج دائرة اختصاص قاضي التحقيق الذي أصدر الأمر بالقبض، ويشار إلى ذلك في المحاضر المحررة في الحالتين." وهي الحالة الوحيدة التي نص فيها على استخدام تقنية التحاضر المرئي عن بعد أثناء التوقيف للنظر. دون أي تفصيل يذكر في كيفية استخدام هذه التقنية فهل يتعلق الأمر هنا بحقوق الدفاع زيارة المحامي للموقوف أم القصد هنا عرض الموقوف على وكيل الجمهورية قبل التمديد حفاظا على فعالية التوقيف للنظر. **و التي نفهم منها أن زيارة المحامي للموقوف تكون شخصية خلال المدة الأصلية وقبل التمديد...**

ثانيا/ بالنسبة للمشرع الفرنسي

المتصفح لنصوص القانون الفرنسي وبالضبط المادة 706-71 في فقرتها الأولى من قانون الإجراءات الجنائية ، يلاحظ أن المشرع الفرنسي قد نص صراحة على إمكانية استخدام تقنية التحادث المرئي لحسن إدارة العدالة بحيث يمكن اللجوء إليها في كافة مراحل الدعوى، مع بعض الاستثناءات.

---

(15) – القانون رقم 15-03 المتعلق بعصرنة العدالة، المؤرخ في 02/01/ 2015، المنشور بتاريخ 10 /02/ 2015، الجريدة الرسمية للجمهورية الجزائرية، عدد 06.

أولا/ استخدام الوسائل التقنية لعرض الموقوف على وكيل الجمهورية : نص المشرع الفرنسي صراحة في المادة 63 فقرة 5 من قانون الإجراءات الجنائية على إمكانية استخدام وسائل الاتصالات السمعية البصرية من طرف وكيل الجمهورية لعرض الموقوف عليه بدلا من الحضور الشخصي.

ثانيا/ التحاضر المرئي عن بعد لتدخل المحامي عن بعد

إن الحق في الاستعانة بمحام مقرر منذ بدء التوقيف للنظر لدى الشرطة ومعناه الحضور الجسدي لأن هذا الحضور يسمح للمحامي بمساعدة موكله مساعدة فعلية حقيقة فيكون إلى جانبه أثناء عدم فهمه أو تردده أو عدم ارتياحه للأسئلة المطروحة، ويشكل وجوده أيضًا دعما له، وفي إطار الظروف الاستثنائية للحد من انتشار جائحة كوفيد 19 من خلال قانون الطوارئ الصحية رقم 290 المؤرخ في 23 مارس 2020 منح للحكومة سلطة اتخاذ أي إجراء بموجب مرسوم لتكييف القواعد المتعلقة بإجراء التوقيف للنظر لدى الشرطة مع حالة الوضعية الوبائية والسماح للمحامي بالتدخل عن بُعد، وبالفعل صدر الأمر رقم 2020-303 المؤرخ 25 مارس 2020 بعد يومين من القانون السابق الذكر معدلا في أحكام التوقيف للنظر بنصه في المادة 13 منه على أنه: "... خلافا لأحكام المادتين 63-4 و63-4-2 من قانون الإجراءات الجنائية، فإن مقابلة المحامي للشخص الموقوف لدى الشرطة أو المحتجز في الحجز الجمركي ومساعدته أثناء جلسات الاستماع ، يمكن أن تتم من خلال وسيط من وسائل الاتصال الإلكترونية، بما في ذلك الهاتف مع مراعاة ضمان سرية المحادثات". طبعا هذا الإجراء قابل للتطبيق مثل جميع التدابير الأخرى لفترة محدودة تنتهي بعد شهر واحد من انتهاء حالة الطوارئ الصحية. باستثناء التمديد أو الإنهاء المبكر لها.

الفرع الثالث/ موقف المحكمة الأوروبية من مساعدة المحامي عن بعد أثناء التوقيف للنظر

يرى المدافعين عن حقوق الإنسان بأنه بموجب هذا الأمر الذي يسمح بمساعدة المحامي للموقوف عن بعد، قد تم انتهاك حقين أساسيين للشخص الموقوف لدى الشرطة، وهما الحق في التحدث مع محام لمدة ثلاثين دقيقة، والحق في الاستعانة بمحام أثناء جلسات الاستماع، على الرغم من أن المحكمة الأوروبية لحقوق الإنسان في قرار سابق لها بريسكو *Brusco* الصادر في 14 أكتوبر 2010 قد أدانت فرنسا لرفضها حضور المحامي منذ بدء التوقيف لدى الشرطة على أساس أن هذا الرفض ينتهك الحق في عدم تجريم الذات والحق في التزام الصمت، وكلاهما تحميهما المادة 6 من الاتفاقية الأوروبية لحقوق الإنسان. على اعتبار أن أولئك المشتبه في ارتكابهم جريمة عندما يتم تقديمهم لأول مرة إلى الشرطة وتوقيفهم قسرا يكونوا الأكثر عرضة للخطر، إلا أن هذا القانون قد وفي إطار حالة الطوارئ الصحية أعاد الحالة إلى ما كانت عليه من قبل.

أولا/ مواءمة الحق في الاستعانة بمحام أثناء التوقيف للنظر مع حالة الطوارئ الصحية

بالرغم من أن حضور المحامي حضورا جسديا إلى جانب الموقوف قد أكدت عليه المحكمة الأوروبية لحقوق الإنسان مرارا وتكرارا ، إلا أنه و في سياق حالة الطوارئ الصحية لم يُلغَ الحق في الاتصال

بمحام، لكنه لم يعد حقًا "وجهاً لوجه"، بل مجرد مساعدة "عن بُعد". وذلك بإجراء المقابلة مع المحامي ومساعدة الموقوف أثناء جلسات الاستماع عن طريق الاتصالات السلكية واللاسلكية بسبب الحالة الصحية الطارئة، وبطبيعة الحال أن الحاجة إلى إبقاء مساعدة المحامي عن بعد هو من أجل التوفيق بين مكافحة انتشار الوباء وضمان استمرارية العمل القضائي الجنائي حفاظا على الأمن العام. وكانت نقابة المحامين في باريس قد صوتت بالإجماع في 24 مارس 2020 على وقف التعيين التلقائي للمحامين أثناء التوقيف للنظر، بسبب الظروف الصحية غير المرضية في مراكز الشرطة، وفي تعليمة وزارية من وزير العدل بتاريخ 14 مار 2020 دعا فيها النيابة العامة إلى إعطاء الأولوية للتحقيقات "التي تمثل مصلحة قوية فيما يتعلق بالنظام العام وتتطلب استجابة قضائية سريعة.

ثانيا / شروط الاستعانة بمحام عن بعد يرى بعض رجال القانون أن مساعدة المحامي عن بُعد يجب تكييفها وتنظيمها تحت طائلة تقويض الفعالية والطبيعة الملموسة للحق التقليدي في الاستعانة بمحام أثناء التوقيف للنظر، و من بين شروط أو طرق تكييف هذا الحق الأساسي ما يلي :

أ- **الحصول على موافقة الشخص المعني** أو محاميه على وجه التحديد، وجاء ذلك في نص تقرير حافظ الأختام الموجه لرئيس الجمهورية المنشور في الجريدة الرسمية بتاريخ 26 مارس صراحة على أن المادة 13 جعلت مساعدة المحامي ممكنة عن طريق الاتصالات مثل الهاتف إذا قبل محامي الشخص الموقوف أو طلب ذلك، لكن نص المادة 13 من المرسوم السابق ذكره، لم يذكر موافقة المحامي وإنما تذكر المادة 13 إمكانية أي (يجوز) أن تتم المقابلة ومساعدة المحامي من خلال وسيلة اتصال إلكترونية بما في ذلك الهاتف.

ب- **توافر الشروط المادية** يذكر التقرير أيضا أن اللجوء إلى هذه الوسيلة الاستثنائية تكون في الحالة التي يراها ضابط الشرطة ممكنة ماديا، هذا القيد المرتبط بتوافر الشروط المادية لتركيب الاتصال عن بعد في مكاتب الشرطة القضائية قد اختفى أيضًا من نص المادة 13. لكنه عاد عبر التعليمة الصادر في 26 مارس التي تحدد بأن "ضابط الشرطة القضائية وحده الذي بإمكانه تقييم ما إذا كان المحادثة والمساعدة أثناء جلسات الاستماع الهاتفية أو عبر تقنية التحادث المرئي ممكنًة ماديًا. بحيث تتم في ظروف تضمن فيها سرية المحادثة المتبادلة.

تساءل بعض المختصين عن المادة 13 وهل تمنح المحامي إمكانية إجراء المقابلة بسرية ومساعدة موكله بشكل فعال؟. في ظل غياب المقابلة الجسدية التي عادة ما تكون في غرفة دون حضور ضباط الشرطة القضائية، يرى البعض أن أن الحفاظ على السرية غير أكيد خصوصا أن معظم مكاتب الشرطة القضائية غير مجهزة بنظام آمن للتحاضر المرئي عن بعد حيث يضطر المحامي في هذه الحالة اللجوء إلى المقابلة الهاتفية والتي ستكون بواسطة "مكبر الصوت" والتي لا تضمن سرية المحادثات.

فالمحامي عبر الهاتف. لايستطيع التحقق من الإخطار بالحقوق أو تقديم مذكرات مكتوبة في نفس الوقت، أيضا الهاتف لا يضمن أن محضر الجلسة يعكس بدقة إجابات الشخص وأسئلة المحامي، سيكون

المحامي قادرًا على أساس كل حالة على حدة إسماع صوته وطلب قراءة المحضر مرة أخرى. لكن التعميم الصادر في 26 مارس لا يقدم إجابة موحدة على هذه الأسئلة، ويذكر فقط المقابلة والمساعدة يجب أن تتم "في ظل ظروف تضمن سرية المحادثات.

خاتمة

من خلال عرضنا تبين لنا أن التكنولوجيا سلاح ذو حدين، فكما يمكن أن تساعد على ارتكاب الجرائم، تسهم أيضاً في منعها وكشفها وقمعها. وبناءً على هذه الازدواجية فإننا لاحظنا أن للتكنولوجيا الدور الفعال في إيجاد الحلول التي تساعد على حفظ الأمن والملاحقة القضائية للمجرمين والنجاح في تطبيق العدالة الجنائية. وذلك بتحسينها لعمليات الاستدلال العلمي الجنائي على نحو يفيد التحقيقات. إلا أنه ينبغي أن يُراعى في تطبيق التقنيات التي تستخدمها تكنولوجيا المعلومات ضرورة إبلاء الاعتبار الواجب للمسائل الأخلاقية وضمانات حقوق الإنسان أثناء التصدي للجريمة وعدم تجاوز الحدود التي تحميها. وحتى تتحقق هذه المعادلة الصعبة لابد من إعطاء أهمية كبرى لتدريب القائمين على هذه التكنولوجية أهمية توفير التدريب وإتباع نُهج متعددة التخصصات وتحقيق التعاون والتآزر في العمل بين أصحاب المصلحة المعنيين من أجل التوصل إلى فهم للفوائد الحالية للتكنولوجيات وما تنطوي عليه من إمكانات يمكن الاستفادة منها في التصدي لمخاطر الجريمة في المستقبل.

وعلى ضوء ما سبق ومن أجل التوازن بين أثر التكنولوجية على الحقوق والحريات، وضرورة استعمالها في عالم ثغت عليه هو الأخر الجريمة بأشكالها المختلفة والتكنولوجية، فإننا نحاول أن نقدم بعض التصورات والمقترحات نوجزها كما يلي :

– بالنسبة للمشرع الجزائري يجب تحري الدقة الوضوح في النصوص القانونية والابتعاد عن العمومية حفاظا على الشرعية.

– استقدام المهارات الفردية في مجال التكنولوجية لاستخدامها في مجال العدالة الجنائية حتى لا يبقى مجالا للخطأ قد يؤدي إلى بطلان الإجراءات.

– مواكبة التطور الحاصل في مجال التكنولوجية والمضي به قدما ليتماشى مع حجم التطور المطرد للجريمة المرتكبة عن طريق وسائل التكنولوجيا.

د / عيشاوي أمال
كلية الحقوق و العلوم السياسية
جامعة البليدة2

أستاذة محاضرة أ

Amelaichaoui2@gmail.com

التفتيش الالكتروني كإجراء للتحقيق في ظل التطور التكنولوجي

Electronic inspection as investigation procedure in light of technological development

الملخص:

يعتبر التفتيش عن الجريمة في ظل التطور التكنولوجي و البيئة الرقمية من أصعب أنواع التفتيش , و يرجع ذلك إلى التطور الحاصل في مجالتكنولوجياالاعلام والاتصال و هذا راجع لكون الأدلة التي يتم البحث عنها هي أدلة تتميز بخصوصية معينة فهي أدلة تتمثل في بيانات مخزنة في أجهزة الالكترونيةو حواسيب متواجدة في أماكن عديدة و مختلفة دخل و خارج الوطن فان البحثعنها و اكتشافها مسالة وعملية صعبةو معقدة تتطلب مهارة و كفاءة من أصحاب الاختصاص.

الكلمات المفتاحية : التفتيشالالكتروني , تكنولوجيا , التطور , التحقيق

Abstract : The search for crime in light of the technological development and the digital environment is one of the most difficult types of inspection, and this is due to the development taking place in the field of public and communication technology, and this is due to the fact that the evidence that is being searched for are evidence characterized by a certain privacy, as evidence is represented in data stored in electronic devices And computers are

located in many different places, inside and outside the country, so searching for and discovering them is a difficult and complex issue that requires skill and competence from the specialists.

Keywords : Electronic inspection, technology, développement, investigation

مقدمة:

إنالتقدم العلمي و التطورات الحديثة ساهمت في إحداثوظهور أشكال و أساليب جديدة منصورالجرائم الالكترونية ,بحيث اصح مفهوم الجريمة الالكترونية يرتبطارتباطا "وثيقا" بالتطور التكنولوجيو تقنية المعلومات، كما انه كلما تطور و اتسعنطاق التجريم ،أحدث ذلك تغيرات مستمرة.ويعتبر التفتيش من الإجراءاتالتي تهدف إلى البحث عنالحقيقة ، وضبط الأدلة على ارتكاب الجريمة و صحةإسنادهاإلىالجاني, لذلك فقد أحاطه المشرع بعدة إجراءات ومعالتطور التكنولوجي من الإجرام وهو ما يسمى بالجرائمالمعلوماتيةو ظهور هذا النوع التي تختلف عنغيرها من الجرائم التقليدية في وسائلارتكابها و الأشخاص الذين يقومونبهافالإشكالية التي يمكنطرحها حول هذا الموضوع **ماالمقصودبالتفتيش الالكتروني و كيف يتم في ظلتطور الجرائم عن طريق استخدام التكنولوجياالحديثة** ؟و للإجابة علىهذهالإشكالية لابدأن نتطرق إلىمفاهيم عامة حول التفتيش الالكتروني و تتمثل فيتعريفه وخصائصهو محله و تطبيقاته و أهميتهزيادةإلى دراسةالشروط الشكلية و الموضوعية للتفتيش الالكترونيو هذا من خلال التطرق إلىقانون رقم 09-04 المتضمن القواعد المتعلقةبالوقاية من الجرائمالمتعلقة بتكنولوجيا الاعلام و الاتصال و مكافحتها زيادةإلىأحكام قانون الإجراءات الجزائية.

و عليه قسمنا هذهالمداخلة إلى محورين, المحور الأول يتعلقبمفاهيم عامة حول التفتيش الالكتروني،أما المحورالثاني نتطرق فيه للضوابط الشكلية و الموضوعية للتفتيش الالكتروني.

المحور الأول/مفاهيم عامة حول التفتيش عامة و التفتيش الالكتروني خاصة:

نتعرض في هذا المحور الى المفهوم التفتيش في المجال التكنولوجي أوألمعلوماتي و إلى الشروط إجرائه و خصائصهو أهميته ونطاقه.

أولا / مفهوم التفتيش :

يقصد بالتفتيش قانونا " المعاينة و البحث في خبايا الأشخاص عن الآثار المؤدية إلى اكتشاف الجريمة في ذاتهم أو مساكنهم ومحلاتهم مع احترام أحكام القانونو مبادئ حقوق الإنسان و أصول اللباقة و حسن المعاملة [1].

أ- **تعريف عامة حول التفتيش/** نتطرق إلى التعريف اللغوي و الاصطلاحي :

1- التعريف اللغوي للتفتيش :

يمكن تعريف التفتيش من الناحية اللغويةبأنه اشتق من فعل فتش ، و فتش الشيء أي تصفحه ، و فتش عنه سأل و استقصى في الطلب. [2]

2- التعريف الاصطلاحي للتفتيش:

[1] د/علي جروة ، الموسوعة في الإجراءات الجزائية, المجلد الأول في المتابعة قضائية ,2006 ,ص378

[2] الكفوي أبو البقاء أيوب موسى الحسني، معجم في المصطلحات و الفروق اللغوية ، ط2 ، مؤسسة الرسالة , بيروت 1998 ص88.

و المقصود به السؤال عن الشيء و الاستقصاء في طلبه، بالسعي و البحث و هو بهذا المعنى يتطرق إلى البحث يجرية الإنسان.[1]

كما لم تتضمن مختلف التشريعات تعريف التفتيش مما تركالمجال للفقه و القضاء التطرق إلى هذه النقطة. فقد وضع الفقه عدة تعريفات لعملية التفتيش.

عرفه البعض بأنه : هو إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية او جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه.[2]

كما عرفه البعض الآخربأنه : الانتقال إلى أماكن وقوع الجرائم للقيام بتفتيشها والى جميع الأماكن اتي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة [3].

قبل الحديث عن مفهوم التفتيش الالكتروني يجدر بنا الإشارة إلىأن المشرع الجزائري لم يضع تعريفا " تشريعيا" للتفتيش الالكتروني في القانون 09-04 و إنما اكتفى فقط بتنظيم أحكامه و ضوابطه تاركا ذلك للفقه ، و بالرجوع إلى التعريفات الفقهية نجد إن التفتيش الالكتروني أو تفتيش الأنظمة المعلوماتية ، عرفها بعض الفقهاء بأنه البحث في مستودع سر المتهم عن أشياء مادية او معنوية تفيد في كشف الحقيقة و نسبتها إليهأو هو البحث الدقيق و الاطلاع على كل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه سواء كان مسكنا أو جهاز حاسوب أو أنظمة او انترنت[4].

---

[1] محمد عبد الله العربي , نظام الحكم في الإسلام , دار الفكر , بيروت 1968 ص21 .

[2] سامي حسن حسني , النظرية العامة للتفتيش , دار النهضة العربية ، القاهرة 1972 ص36.

[3] محمد خريط , أصول الإجراءات الجزائية في القانون الجزائري على ضوء آخر تعديلات لقانون الإجراءات الجزائية و الاجتهاد القضائي , ط2 دار هومة للنشر , الجزائر 2019 ص278.

[4] رضا هميسي , تفتيش المنظومات المعلوماتية في القانون الجزائري , مجلة العلوم القانونية و السياسية , العدد5 , جوان 2012 ص160.

كما أن تفتيش النظم المعلوماتية هو إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني ،و يستهدف ضبط أداة الجريمة مثل البرامج الغير مشروعة و الملفات المخزنة في الحواسيب ، و المعطيات المعلوماتية و الاتصالات الالكترونية.

و يقصد بالمنظومة المعلوماتية في التشريع الجزائري أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أوالمرتبطة، يقومواحد منها أوأكثر بمعالجة آلية للمعطيات تنفيذ برنامج معين [1].

كما أنتفتيش نظم الحواسيب هو تفتيش للفضاء الافتراضي و أوعية التخزين و تفتيش للبيانات التي يحفظها جهاز الكمبيوتر إن كان مزود بحافظات الكترونية للعمليات المنجزة منخلاله و هو أمر يتعلق بالقدرة على تحقيق المطلوب سلفا ، و ليس مجردفحص نظام المعلومات الالكترونية لان التعامل وفق المسلك الأخير قد يكون له عواقب قانونية أهمها بطلان الإجراءات.[2]

و على العموم إن التفتيش سواء كان في شكله التقليدي أو الحديث ، هو إجراء منإجراءاتالتحقيق التي تهدف إلى ضبط الأدلة موضوع الجريمة ، و كل ما يفيد في كشف الحقيقة.

ب-خصائص التفتيش الالكتروني:

يتميزالتفتيش الالكتروني أو النظم المعلوماتية عن غيره من إجراءات التي تهدف أيضا الى إثبات الجريمة" بعدة خصائصأهمها : [3]

---

[1]راجع المادة 2 من القانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق لـ 05 غشت سنة 2009, المتضمن القواعد الخاصة للرقابة من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ,ج ر ج العدد 47.

[2]عبد الله احمد الهلالي , تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي , ط1 , دار النهضة العربية 1997ص73 .

[3]رضا هميسي , تفتيش المنظومات المعلوماتية في القانون الجزائري , مجلة العلوم القانونية و السياسية , العدد5 , جوان 2012ص161.

1- إن التفتيش الالكتروني مثله مثل التفتيش بشكل عام،هذا لأنه يتم فيهتعرض قانوني لحرية المتهم الشخصية أو لحرمة مسكنه بغير إرادته و رغما عنه و هذا فيه اعتداء على إسراره و حياته.

2- يعتبر التفتيش الالكتروني وسيلة من وسائل البحث و التحري عن مختلف الأدلة بهدف الوصول و الكشف عن الحقيقة عن طريق الوصول إلى الدليل الحاسم الذي لا يدان الشخص و لا يعاقب دونه.

3- اعتبار التفتيش قيد على حرمة الشخص لأنه فيه اعتداء على أسراره الموجودة على مستوى نظامه المعلوماتيأو حاسوبه أو بريده الالكتروني،و عليه يترتب خروج كل إجراء لا يمس بسر احد عن إجراء التفتيش لأنه يمس بشيء مكشوف للجميع.[1]

4- يمكن التفتيش أو البحث في الشبكات الالكترونية عن الجرائم المعلوماتية، من استخدام قواعد و أساليب التحقيق الجنائي الفني المعروفة بتقنيات خاصة وفريدة غير معروفة. لكن التفتيش التقليدي فهو لا يتطلب الانتقال إلى مساكن الأشخاص المشتبه فيهم ، و إنما قد يتم عن بعد أو ما يسمى بالتفتيش على الخط.[2]

5- يتميز التفتيش الالكتروني بان المحتوى المعلوماتي يتميز بطابعه اللامادي وانه يتجاوز الحدود الوطنية كما انه سهل إتلافهأو مسحه أو تغييره في زمن قصير.[3]

6- التفتيش الالكتروني هو إجراء معقد يتوجب على القائمين بهان يكونوا على دراية واسعة و كفاءة عالية في البحث.[4]

---

[1] عمر الحاج الخضيري ، إجراءات التفتيش و تطبيقاته في الإدارة الأمنية , المركز العربي للدراسات الأمنية و التدريب الرياض , 1987 ص19

[2] رضا هميسي , المرجع السابق 162

[3] عبد الله بن عبد العزيز عبد الله الخشعمي , التفتيش في الجرائم المعلوماتية دراسة تطبيقية , رسالة ماجستير في العدالة الجنائية , جامعة نايف للعلوم الأمنية , الرياض ,2011 ص35

[4] رضا هميسي، المرجع السابق ، 163

7- إن التفتيش الالكتروني فيه مساس خطير بالحياة الخاصة، لما يترتب عليه من اعتداءات بسبب الترتيبات التقنية لمراقبة الاتصالاتالالكترونية.

ثانيا / محل التفتيش الالكتروني و أهميته :

إن محل التفتيش في الجرائم الالكترونية هوجهاز الكمبيوتر و الأجهزة المتصلة به و الشبكة التي تشمل في مكوناته مقدم الخدمة ، و للتفتيش الالكترونيأهمية بالغة لأنه يساعد على كشف أسرار وخبايا من شانها أن تساهم في التحقيق من اجل الوصول إلى الحقيقة و عليه سوفنتطرق الى محل التفتيش ثمأهميته فيمايلي :

أ- **محل التفتيش الالكتروني** : ينصب التفتيش على نوعين من المكونات الأولى مادية و الثانية التفتيش الخاص بالشبكات الخاصة أو المتصلة بالكمبيوتر.

1- **تفتيش المكونات المادية لجهاز الكمبيوتر** : و يشمل نوعين من القطع الصلبة و أخرى تسمى بالمكونات المنطقية أي البرمجيات.[1]

1-1 **تفتيش المكونات المادية** : إن المراد من تفتيشها هو الكشف عن الحقيقة و عن مرتكبها الذي يخضع للإجراءات القانونية الخاصة بالتفتيش ، و يتوقف ذلك على طبيعة المكان الموجودة فيه تلك المكونات من أماكن عامة او خاصة ، لان صفة المكان و طبيعته مهمة في عملية التفتيش حيث يطبق عليها الإجراءات و الضمانات المقررة في التشريعات المختلفة.[2]

2-1 **تفتيش المكونات المنطقية** : ان تفتيش هذه المكونات أثار جدلا "فقهيا" ، فذهب رأيإلى جواز تفتيش و ضبط البيانات الالكترونية بمختلف أشكالها و يستند هذا الرأي على أنإصدارالإذن بضبط أي شيء خاص بالكمبيوتر يشمل بيانات الكمبيوتر المحسوسة و الغير محسوسة .

---

[1] القطع الصلبة هي hardware اما المكونات المنطقية هي software البرمجيات.

[2] الله احمد الهلالي , تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي , ط1 , دار النهضة العربية 1997 ص73.

أماالرأيالآخر فيرى أن التفتيش حسب الواقع العملي يتطلب أن يقع على البيانات التي اتخذت شكلا ماديا [1]. و عليهلا يمكن إخضاعها للنصوص التقليدية المتعلقة بالتفتيش و عليه فان طبيعة هذه المكونات تتطلب استحداث أسس تفتيش جديدة خاصة بها ،أو تعديل الأسس التقليدية المعروفة لتفتيش بشكل يجعلها تتلاءم مع هذه التقنية الجديدة .

ومن هنا فقد استحدث المشرع الجزائري نصوص قانونية جديدة سمح من خلالهابتفتيش المكونات المعنوية و المنظومات المعلوماتية للحاسب ، و ميز في هذا الشأن بين ما إذا كانت المنظومة متصلة بنظام آخر داخل التراب الوطني ،أو متصلة بمنظومة معلوماتية تقع خارج الإقليم الوطني ،ففي الحالة الأولى أجاز المشرع تمديد التفتيش إلى المنظومة المعلوماتية الموجودة على جهاز آخر المتصل بالجهاز الأول بعد إعلام السلطة القضائية المختصة مسبقا بذلك .

أما الحالة الثانية و التي تكون فيها المعطيات المبحوث عنها يمكن الدخول إليها انطلاقا من المنظومة الأولى و لكنها في منظومة معلوماتية موجودة في بلد أجنبي،أوجبت المادة 5 الفقرة 3 من القانون رقم 09-04 خضوع عملية التفتيش بشأنها للاتفاقيات الدولية المبرمة بين البلدين و هذا عن طريق مساعدة السلطات الأجنبية المختصة و هذا ما يؤكد على ضرورة التعاون الدولي في مجال مكافحة الجرائم الرقمية[2].

2- تفتيش الشبكات المتصلة بالكمبيوتر:

[1] عبد الله احمد الهلالي , نفس المرجع ص84 .

[2] راجع الفقرة3 من المادة 5 من القانون رقم 09-04 2009المتعلق بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

إن التكنولوجيا الرقمية قد عادت بالسلب على التفتيش و الضبط لان البيانات التي قد تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مختلفة و مجهولة بعيدة تماما عن الموقع المادي للتفتيش ، كما قد يكون الموقع الفعلي للبيانات داخل اختصاص قضائيآخرأو حتى في بلد آخر و هذا ما يلزم التعاون القضائي من اجل حل مشاكل الجريمة الالكترونية العابرة للحدود.[1]

ب-**أهمية التفتيش الالكتروني :**

تتعلق أهمية التفتيش بالواقعة و أطرافها و هذا ما سوف نوضحه فيما يلي:[2]

1-بالنسبة للواقعة : يكشف التفتيش الالكتروني الجوانب التالية :

1-1 **ثبوت الواقعة :** أي هنا يبين حدوث الواقعة من عدم حدوثها .

2-1 **وقت و مكان الواقعة :** يساعد في الكشف و تحديد وقت الحادث في حالة عثوره على اثار تدل على زمان الجريمة ، كما يفيد أيضا تحديد المكان حتى و لو كانت الجريمة الالكترونية عابرة للحدود.

2-بالنسبة لأطراف الخصومة: يساعد التفتيش بالنسبةللأطراف عدة مسائل أهمها نوردها فيما يلي:

2-1تحديد الباعث والدافع : قديكشف التفتيش كراهية الجاني للمجني عليه و الرغبة في الانتقام منه.

---

[1] إن الشبكات المتصلة بالكمبيوتر تأخذ 3 أشكال الأولى يكون اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة ، الثاني اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة ، الثالث و يكون التفتيش و المراقبة الالكترونية لشبكات الحاسب الآلي نقلا عن محمد أبو العلا عقيدة ، التحقيق و جمع الأدلة في مجال الجرائم الالكترونية ،ج1، دار النهضة العربية، 1996، ص35.

[2]عبد الله بن عبد العزيز عبد الله الخشعمي ، التفتيش في الجرائم المعلوماتية دراسة تطبيقية , رسالة ماجستير في العدالة الجنائية ، جامعة نايف العلمية الأمنية ، الرياض ,201، ص40 و 41 .

2- 2تحديد شخصية الجاني: قد يجد المحقق صورة شخصية أو أي مستند خاص بالجاني مما يساعد في تحديد هويته.

2-3 تحديد درجة خطورة الجاني : و هذا من خلال ما يجده المحقق من برامج فيروسات أو برامج لفكشفرات أوشهادات عملية تدل على أن هذا المتهم متخصص و محترف في مجال الكمبيوتر و الشبكات.

2-4تحديد عدد الجناة و علاقتهم بالمجني عليه : إن التفتيش من شانه معرفة عدد الجناة إذاكانواأكثر من شخص واحد و هذا من خلال إجراء التفتيش للنظام المعلوماتي وما قد يكشف عنه من العثور على أدوات و أجهزة الكترونية استخدمت في ارتكاب الواقعة.

المحور الثاني : الضوابط الشكلية و الموضوعية للتفتيش الالكتروني

نظرا لخطورة التفتيش الالكتروني و مساسه بالحرية الشخصية للفرد ، فقد حرصت كافة التشريعات الإجرائية بما فيهاالتشريع الجزائري على ضرورة إحاطته بمجموعة من الضوابط الشكلية و الموضوعية التي من شانها العمل على إقامة نوع من التوازن بين الحرية الفردية و حرمة الحياة الخاصة للأفراد. وعلى هذا الأساس سوف نتناول ضوابط التفتيش الالكتروني فيما يلي :

أولا : الضوابط الموضوعية للتفتيش الالكتروني :

ينبغي أن يجرى التفتيش وفقا للشروط الموضوعية اللازمة لصحة التفتيش و يمكن حصرها في ثلاثة شروط أساسية تتمثل في سبب التفتيش , المحل المراد تفتيشه ،و السلطة المختصة بالتفتيش.[1]

[1] عبد الفتاح بيومي حجازي , جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي , دار الكتب القانونية , القاهرة 2007 ص36.

أ- سبب تفتيش نظم المعلوماتية :

إن التفتيش بوصفه إجراء من إجراءات التحقيق يكوون عادة عند وقوع جريمة من الجرائم و إسنادهاإلى شخص معين سواء كان فاعلا مباشرا ا و شريكا فيها و عليه يفترض ان التفتيش يجب ان يستند عند إجرائهإلى مبررات توضح السبب و الهدف منه و تتمثل فيما يلي :

1 **وقوع جريمة معلوماتية** : يشترط كقاعدة عامة لمباشرة إجراء التفتيش الالكتروني أن تكون هناك جريمة معلوماتية قد وقعت فعلا سواء تم تكييفها بأنها جناية أو جنحة ومن ثم تستبعد المخالفة من نطاق هذا الإجراء ، و عليه لا يمكن إجراء التفتيش من اجل جريمة محتملة الوقوع حتى و لو كانت هناك مؤشرات جدية على احتمال وقوعها.[1]

كما تجدر الإشارة إلىأن المشرع الجزائري خرج من هذه القاعدة حيث أجاز المشرع الجزائري بمقتضى المادة 05 من القانون رقم 09-04 اللجوء إلى التفتيش الالكتروني للوقاية من الجرائم أو في حالة توفر معلومات عن احتمال وقوع جرائم معينةذكرتها المادة 04 من نفس القانون.

2 **توجيه التهمة إلى شخص و إسنادهاإليه** : يتعين للقيام بإجراء التفتيش بالإضافة إلى وقوع الجريمة أن يكون هناك اتهام موجه إلى شخص أو عدة أشخاص سواء بصفته فاعلا أو شريكا أو حائزا لأشياء لها علاقة بالجريمة ، كما يجب أن يكون الاتهام جديا و مبنيا على أدلة و قرائن قانونية.[2]

و لا يكفي مجرد الظن أو الاشتباه بل ينبغي توافر الأدلة و القرائن المعقولة و الجدية التي تحمل على الاعتقاد بوقوع جريمة معلوماتيةو نسبتها إلى المتهم المراد تفتيش منظومته المعلوماتية.

ب-محل التفتيش الالكتروني :

---

[1] رضا هميسي , المرجع السابق ص164.

[2] سامي حسني الحسيني , المرجع السابق، ص98.

يقصد بمحل التفتيش الالكتروني ذلك المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سره، وينصب هذا المجال في الجريمة المعلوماتية على جهاز نظام المعالجة الآلية بمكوناته المادية و المعنوية و شبكات الاتصال الخاصة به. أو المتعلقة بالوسائل المعلوماتية بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش , و الأماكن التي توجد بها تلك الأشياء.[1]

و المحل في الجرائم المعلوماتية لا يكون قائما بذاته بل مقترنا بمكان معين كمسكن المتهم أو بشخص معين بصفته مالك أو حائز مثلما هو الشأن في الحاسب المحمول ،أو الهاتف النقال ، لذلك فانه يتعين قبل مباشرة إجراء التفتيش مراعاة طبيعة المكان الذي تتواجد فيه الوسائل المعلوماتية المراد تفتيشها وكذا الضمانات القانونية المحاطة به ، لان حكم تفتيش هذه الوسائل يتوقف غالبا على طبيعة المكان الذي تتواجد فيه.[2]

ج-السلطة المختصة بالتفتيش :

كما هو معروف لا يعتبر التفتيش صحيحا و منتجا لآثارهإلاإذا تم القيام به من طرف الأشخاص أو الجهات المخول لها قانونا صلاحيات إجرائه، و لقد اختلفتالتشريعاتالإجرائية في هذا الشأن ، فمنها من أسندهاإلى المدعي العام و هناك من منحها إلى قاضي التحقيق أو ضابط الشرطة القضائية ،أما بالنسبة للمشرع الجزائري فقد أوكل صلاحية إجراء التفتيش إلى السلطات القضائية المتمثلة في النيابة او التحقيق و كذا ضابط الشرطة القضائية وفقا لأحكام المادة 05 من قانون رقم 09-04.

[1] عبد الفتاح بيومي حجازي , جرائم الكمبيوتر و الانترنت , دار الكتب القانونية , القاهرة 2005 ص39

[2] فهد بن عبد الله اللحيدان , الانترنت شبكة المعلومات العالمية , ط1 , بدون ناشر (دار النشر) 1996 ص99

و نظرا إلى المهارات الفنية التي تتطلبها الجريمة المعلوماتية فقد أجاز المشرع الجزائري للسلطات المكلفة بالتفتيش الاستعانة بخبير له دراية بالمعلوماتية محل البحث بهدف المساعدة و تزويدها بكل المعلومات الضرورية لإنجاز المهمة.[1]

و تتمثل مهمته أو دور الخبير في تقديم التوضيحات الكافية حول كيفية تشغيل هذه الأنظمة و طريقة النفاذ إليهاأوإلىالمعطيات المخزنة أو المعالجة ،أو المنقولة في شكل يمكنفهمه أوإدراكه.[2]

ثانيا / الضوابط الشكلية للتفتيش الالكتروني :

زيادة على الضوابط الموضوعية للتفتيش الالكتروني يتطلب القانون توافر مجموعة من الشروط الأخرى ذاتطابع شكلي،يتعين الالتزام بها عند القيام بعملية التفتيش وذلك حماية للحقوق والحريات الفردية من أي تعسف أو انحراف أواستغلاللسلطة و تتمثل هذه الضوابط فيما يلي :

أ- **إجراء التفتيش بحضور أشخاص يحددهم القانون :** نظرا لاعتبار التفتيش يشكل اعتداء على حرمةأو حرية الأشخاص و الاطلاع على أسرارهم، فقد أوجبتبعض التشريعات حضور المشتبه فيه او من ينوب عنه أو الشهود في عملية التفتيش و ذلك لضمان سلامة هذا الإجراء و الحيلولة دون تعسف الجهة القائمة بالتفتيش.

أما بالنسبة للمشرع الجزائري فقد اشترط في المادة 1/45 من قانون الإجراءات الجزائية ضرورة حصول إجراء التفتيش المتعلق بالمساكن و ملحقاتها بحضور المشتبه فيه عندما يتم تفتيش مسكنه ،وإذا تعذر الحضور وقت إجراء التفتيش تعين على ضابط الشرطة القضائية حضور هذا الإجراء شاهدين.[3]

---

[1] راجع الفقرة الأخيرة للمادة 5 من القانون 09-04

[2] فهد بن عبد الله اللحيدان , المرجع السابق ص 110.

[3] راجع المادة 45 من قانون الإجراءات الجزائية الجزائري.

و عليه نجد المشرع الجزائري فقد اشترط لإجراء عملية التفتيش في المعطيات المخزنة في المنظومة المعلوماتية إعمال قاعدة الحضور تطبيقا لأحكام المادة 5 من القانون 09-04 التي تحيل إلىالأحكام العامة المنصوص عليها في قانون الإجراءات الجزائية ، كما سبق ذكر ذلك.

لكن و نظرا لخصوصية الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات، و ما يتطلبه التحقيق بشأنها من سرية أثناء جمع الدليل الالكتروني زيادة إلىالإسراع في استخلاصه قبل فقدانه ، فقد أورد المشرع الجزائري إسناد في الفقرة الأخيرة من المادة 45 سالفة الذكر[1] على استبعاد هذه الشروط عن إجراء التفتيش الالكتروني و بالتالي يمكن للجهات المختصة إجراء التفتيش دون التقيد بحضور المشتبه فيه أو من ينوب عنه أو حتى الشهود.

ب-**تحرير محضر التفتيش :**

يعتبر التفتيش عملا من أعمال التحقيق ، فانه يجب تحرير محضر يثبت فيه كل ما تم من إجراءات و ما أسفر عن التفتيش من أدلة، و لا يتطلب القانون شكلا معينا" و إنما لابد أن يستوفيعلى أسس عامة في تحرير المحاضر بشكل عام ، و هي ضرورة أن تكون مكتوبة باللغة الرسمية و أن يحمل المحضر تاريخ تحريره و توقيع الشخص أو الجهة التي قامت بتحريره وان يتضمن كافة البيانات المتعلقة بالتفتيش.[2]

كما يختلفالأمر بالنسبة للتفتيش الذي تم من طرف ضابط شرطة قضائية الذي يخضع للقواعد العامة التي يجب أن تتضمنها المحاضر المحررة من قبل الضبطية القضائية، أماعن محاضر التفتيش التي يقوم بإجرائها قاضي التحقيق الذي يكون مصحوب بكاتب يتولى مهمة تحرير المحضر و تدوين ما يتم من

[1] المادة45 الفقرة الأخيرة " لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم المخدرات و الجريمة المنظمة عبر الحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبييض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالعرف , باستثناء الأحكام المتعلقة بالحفاظ على السر المهني و كذا جرد الأشياء و حجز المستندات المذكورة أعلاه"

[2] رضا هميسي , المرجع السابق ص170.

إجراءات[1]و التأشير عليه . كما أن محضر التفتيش الالكتروني يتطلب إحاطة القائم بالتفتيش في الجرائم المعلوماتية الاستعانة بأهل الخبرة الفنية والاختصاص من اجل المساعدة في صياغة وتحرير المحضر الذي يغطي كافة الجوانب الفنية للتفتيش.

ج-الإذن بالتفتيش :

طبقا " للمبادئ العامة للتفتيش" نجد نص المادة 44 من قانون الإجراءات الجزائية لا يجوز إجراء التفتيش إلا بعد الحصول على إذن مكتوب من السلطة القضائية المختصة. لكن بالرجوع إلى القانون رقم 09-04 و البحث في مدى التقيد بهذا الضابط من عدمه عند إجراء التفتيش الالكتروني فإننا نجد نص المادة5 من نفس القانون لا تنص صراحة على وجوب استصدار إذن بالتفتيش الخاص بتفتيش المنظومات المعلوماتية من طرف ضابط الشرطة القضائية ، كما هو الحال بالنسبة للمراقبة الاتصالات المعلوماتية المنصوص عليها في المادة 4 من قانون رقم 09-04.

د-الميعاد الزمني لإجراء التفتيش الالكتروني :

يقصد بهذا الشرط أن يتعين على الشخص القائم بالتفتيش أن يتقيد بالوقت المحدد قانونا لمباشرة هذا الإجراء،,و قد حدد المشرع الجزائري الميعاد القانوني الذي يجوز فيه الدخول إلى المساكن و تفتيشها و ذلك بموجب أحكام المادة 1/47 من قانون الإجراءات الجزائية التي نصت على انه لا يجوز البدء في تفتيش المساكن و معاينتها قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة ليلا . وهذا يعني

[1]راجع المادة 79 من ق.إ.ج.ج التي تنص على وجوب اصطحاب قاضي التحقيق كاتب من اجل تحرير محضر يمضى من طرفه ومن طرف الكاتب.

انه لا يجوز كقاعدة عامة تفتيش المساكن بعد الساعة الثامنة ليلا و قبل الساعة الخامسةصباحا, وهذا من اجل صون الحريات الفردية و حرمة المسكن.[1]

لكن هذه القاعدة أورد عليها المشرع استثناء بحيث أجاز إجراء التفتيش في كل ساعة من ساعات الليل أو النهار و ذلك عندما يتعلق التحقيق بنوع من الجرائم، ومن بينها جرائم المعلوماتية.[2]

و عليه إن التفتيش الالكتروني في الجرائم المعلوماتية يجوز مباشرته في أي وقت، فلا يتقيد الشخص القائم به بالميعاد الزمني و هذا نظرا للطبيعة الخاصة لهذه الجرائم التي تتميز بسهولة محو الأدلة أو تعديلها أوإتلافها.

وتباعا لما سبق ،فانه يترتب على عدم مراعاة الضوابط الموضوعية و الشكلية التي سبق شرحها بطلان إجراء التفتيش الالكتروني و بالتالي فقدان الدليل المستمد منه ولا يجوزالأخذ به سواء من طرف جهات التحقيق أو جهات الحكم.

الخاتمة:

تعتبر الجريمة المعلوماتية من الجرائم المستحدثة التي برزت في الوقت الحالي نتيجة تطور تقنية المعلومات واستغلالها . و نظرا لخصوصية هذه الجريمة كونها ترتكب في بيئة افتراضية رقمية، فانه أصبح من الضروري تطوير أساليب التحقيق الجنائي و إجراءاتهبصورة تتلاءم مع هذه الخصوصية لكي

[1] محمد خريط , المرجع السابق ص281

[2] راجع الفقرة 3 من المادة44 من قانون الإجراءات الجزائية.

تمكن جهات التحقيق من كشف الجريمة و التعرف على مرتكبيها وهوى الأمر الذي سعى إليه المشرع الجزائري من خلال استحداث نصوص قانونية جديدة أوجدتها قواعد إجرائية تتفق مع طبيعة الجريمة ، و يعتبر التفتيش الالكتروني إحدى هذه الإجراءات التي جاء بها القانون رقم 09-04 المؤرخ في 05 أوت 2009 , المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

أما بخصوص الاستنتاجات التي يمكن إبداؤها هي :

1- ان تفتيش المنظومات المعلوماتية هو من أصعب إجراءات البحث و التحري ، كما يتطلب خبرة واسعة و كفاءة عالية من القائمين به.

2- التفتيش الالكتروني يتطلب تعاونا دوليا لمحاصرة هذه الجرائم و ملاحقة مرتكبيها.

3- اختلاف التفتيش الرقمي عن التفتيش الكلاسيكي رغمانه في بعض الأحيان تحكمه قواعد قانون الإجراءات الجزائية مثل تفتيش المساكن التي توجد بها أجهزة الإعلامالآلي .

و في الأخير يمكننا أن نقدم بعض الاقتراحات :

1- إدماج جميعالقواعد و الإجراءات الخاصةبالجريمة الالكترونية في قانون الإجراءات الجزائية بدلا من القوانين الخاصة.

2- إعطاء الأهمية القصوى للخصوصية أثناء تفتيشالمنظومات المعلوماتية ،و الالتزام بمبادئ حماية الحياة الخاصة ، من حيث عدم نشر و توزيع المعلومة و عدم إفشائها.

3- انضمام الاتفاقيات الجماعية ذات العلاقة بالجرائم الالكترونية أو اتفاقيات خاصة بالمساعدة القضائية في هذا المجال .

قائمة المراجع :

أ- **المعاجم :**

1- الكفوي أبو البقاء أيوب موسى الحسني، معجم في المصطلحات و الفروق اللغوية ،ط2 مؤسسة الرسالة ،بيروت 1998.

ب-**الكتب :**

1- هشام محمد فريد رستم ، الجوانب الإجرائية التي تثيرها الجريمة المعلوماتية ، دراسة مقارنة ، مكتبة الآلات الحديثة 1994.

2- محمد حزيط ، أصول الإجراءات الجزائية في القانون الجزائري على ضوء آخر تعديلات لقانون الإجراءات الجزائية و الاجتهادالقضائي ، ط2 دار هومة للنشر ،الجزائر 2019.

3- محمد عبد الله العربي ، نظام الحكم في الإسلام ،دار الفكر، بيروت 1968.

4- سامي حسن حسني ،النظرية العامة للتفتيش ، دار النهضة العربية القاهرة، 1972.

5- عبد الله احمد الهلالي ، تفتيش نظم الحاسب الآلي و ضمانات المتهم المعلوماتي ، ط1 ، دار النهضة العربية، القاهرة ،1997.

6- عبد الفتاح بيومي حجازي , جرائم الكمبيوتر و الانترنت , دار الكتب القانونية , القاهرة 2005

7- عبد الفتاح بيومي حجازي ، جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي ، دار الكتب القانونية ،القاهرة 2007.

8- علي جروة ،الموسوعة في الإجراءات الجزائية , المجلد الأول، في المتابعة القضائية، 2006 .

9- فهد بن عبد الله اللحيدان ، الانترنت شبكة المعلومات العالمية، ط1 ، بدون ناشر (دار النشر) 1996.

ت-**المقالات** :

1- رضا هميسي ، تفتيش المنظومات المعلوماتية في القانون الجزائري ، مجلة العلوم القانونية و السياسية ، العدد5 ، جوان 2012.

ث-**الرسائل** :

1- عبد الله بن عبد العزيز عبد الله الخشعمي , التفتيش في الجرائم المعلوماتية دراسة تطبيقية , رسالة ماجستير في العدالة الجنائية , جامعة نايف العلمية الأمنية , الرياض ,2011.

2- عمر الحاج الخضيري ،إجراءات التفتيش و تطبيقاته في الإدارة الأمنية ، المركز العربي للدراسات الأمنية و التدريب الرياض ،1987.

ج- **القوانين** :

1- الأمر رقم 66-155 مؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية.

2- القانون رقم 09-04 المؤرخ في 14 شعبان 1430هـ الموافق لـ 05 غشت سنة 2009, المتضمن القواعد الخاصة للرقابة من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ,ج ر ج العدد 47.

ملتقى دولي افتراضي

موسوم بـ" القانون الجنائي في ظل التطورات التكنولوجيا"

-إشكالات ومعالجات-

اللقب: زروقي

الاسم: أم كلثوم

الدرجة العلمية: طالبة دكتوراه

المؤسسة: جامعة يحي فارس – المدية- كلية الحقوق .

البريد الالكتروني: zerroukioum1994@gmail.com

عنوان المحور:استخدام التقنيات الحديثة في مجال العدالة الجنائية

عنوان المداخلة: استخدام تقنية المحادثة المرئية عن بعد كآلية لتطوير مرفق القضاء

ملخص:

إن التغيرات التي عرفتها بلادنا في شتى المجلات بفضل الثورة العلمية واستجابة للضرورات العملية التي اقتضت الاستعانة بتكنولوجيات الحديثة لتطوير وتسريع أداء مرفق القضاء، استحدث المشرع بموجب القانون رقم 15-03 والمتعلق بعصرنة العدالة " المحادثة المرئية عن بعد أثناء الإجراءات القضائية" والتي فعلت الحضور الإلكتروني عوضا عن الحضور الفعلي للشخص. غيرأن هذا القانون وإن كان موجودا إلى أنه من الناحية التطبيقية لم يتجسد فعليا إلا بعد تفشي جائحة كورونا التي ظهرت في أواخر شهر ديسمبر 2019 والتي خلفت آثار مست جميع المستويات بما فيها مرفق القضاء والذي ظهرت من خلال توقف العمل القضائي ومن ثم أصبحت الحاجة إلى تفعيل آليات جديدة تتماشى مع أي تعطيل أو مساس بالمراكز القانونية للمتقاضين. مما أدى بالمشرع الجزائري إلى تعديل قانون الإجراءات الجزائية بموجب القانون رقم 20-04 والذي استحدث بموجبه " كتاب 2 مكرر" والمعنون بـ " استعمال وسائل الاتصالات المسموعة والمرئية أثناء الإجراءات" حيث تم توسيع العمل بهذه الالية.

الكلمات المفتاحية: تقنية، المحادثة المرئية، التحقيق، المحاكمة، عصرنة العدالة، جائحة كورونا.

Abstract :

The changes that our country has experienced in various journals thanks to the scientific revolution and in response to the practical imperatives that have necessitated the use of modern technologies to develop and accelerate the functioning of the judicial facility, the legislature introduced, under the 15-03 law on the modernization of justice, the "video conferencing during judicial procedures", which did the electronic presence instead of the actual presence of the person. However, this law, although in practice, did not materialize until the outbreak of the coronapandemic in late December 2019, which left behind the effects of all levels, including the judicial facility, which emerged through the cessation of judicialwork,As a result, the Algerian legislature has amended the Code of Criminal Procedure by Act No : 20-04, by which it introduced a "Book 2 bis", entitled "Use of audio-visual means of communication during procedures".This mechanism has been expanded.

Key words: technical, video conferencing, investigation, trial, modernization of justice, corona pandemic .

مقدمة:

لقد أثر التطور العلمي والتكنولوجي في كافة مرافق الحياة دون استثناء الأمر الذي أدى بالمنحرفين لاستغلال هذا التطور الحاصل في أنشطتهم الإجرامية مما نتج عنه تطور أساليبهم في ارتكاب الجريمة فبعدما كانت تقليدية أصبحت أساليبهم متطورة تعتمد مثلا على أجهزة الكمبيوتر مستغلين أيضا ضعف وقصور بعض الدول التي لازالت تعتمد على الطابع التقليدي لمكافحة ومواجهة مختلف أنواع الجرائم مما جعل بعض الدول تحاول إعادة النظر في المبادئ القانونية المستقرة واستحداث قوانين لمواكبة هذه التطورات[1].

إذ عملت الجزائر على معالجة وتطوير نظامها القانوني عن طريق إصدار قانون رقم 15-03 المتعلق بعصرنة قطاع العدالة[2] والذي يمكن اعتباره خطوة إيجابية نحو عالم التقنية أو ما أصبح يعرف بنظام الادرة الإلكترونية ومن أهم هذه التقنيات " تقنية المحادثة المرئية عن بعد" التي تستعمل في المحاكمة وذلك باستعمال أجهزة متطورة تعتمد على الإنترنت ووسائل المعلوماتية ووسائل الاتصال المسموعة والمرئية.والملاحظ أنه بعد تفشي جائحة كورونا وحفاظا على الأمن والصحة العمومية وكذلك ضمانا لحقوق ومصالح المتقاضين تم توسيع اللجوء لهذه التقنية وذلك إثر تعديل قانون الإجراءات الجزائية وتفعيل استعمال المحادثة المرئية عن بعد من خلال الأمر رقم 20-04[3].

ومن ثم تعتبر تقنية المحادثة المرئية عن بعد خروجا عن الطابع التقليدي في ميدان التحقيق والمحاكمة الذي اتسم به مرفق العدالة الجزائية إلى طابع أكثر ليونة ووافر للجهد وأقل وقتا، حيث يترتب على تطبيقها امتداد النطاق الجغرافي للجلسات وبالتالي يتحقق بموجبها مبدأ المواجهة بين أطراف الدعوى الجزائية وذلك دون الحاجة إلى تواجدهم في مكان واحد، ويتم بواسطتها نقل كافة مجريات التحقيق والمحاكمة[4].

وعليه؛ يمكن طرح التساؤل الآتي : كيف نظم المشرع الجزائري استعمال تقنية المحادثة المرئية ؟

وللإجابة على التساؤل سنتطرق إلى:

الإطار المفاهيمي لاستعمال تقنية المحادثة المرئية عن بعد كمحور أول،نطاق استعمال تقنية المحادثة المرئية عن بعد كمحور ثاني.

<u>المحور الأول: الإطار المفاهيمي لاستعمال تقنية المحادثة المرئية عن بعد</u>

ان استعمال تقنية المحادثة المرئية عن بعد أثناء الإجراءات القضائية تعد قفزة نوعية وجديدة نحو إصلاح وعصرنة قطاع العدالة هذا من جهة وكما تضمن السرعة في التحقيق والمحاكمة من جهة أخرى.

ومن ثم ارتأينا التطرق أولا إلى مفهوم تقنية المحادثة المرئية عن بعد وثانيا إلى شروط استعمالها.

---

[1] صفوان محمد شديفات، التحقيق والمحاكمة الجزائية عن بعد عبر تقنية vidéo conférence، دراسات " علوم الشريعة والقانون"، المجلد 42، العدد 1، سنة 2015، ص353.

[2] القانون رقم 15-03 المؤرخ في 01 فبراير 2015 والمتعلق بعصرنة قطاع العدالة، الجريدة الرسمية، الجمهورية الجزائرية، العدد 06، الصادرة بتاريخ 10 فبراير 2015.

[3] امر رقم 20-04 المؤرخ في 30 غشت 2020 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية ، العدد 51، الصادرة بتاريخ 31 غشت 2020.

[4] رامي متوي القاضي، إجراءات التحقيق والمحاكمة عن بعد – دراسة تحليلية مقارنة- مجلة جامعة الشارقة للعلوم القانونية، المجلد 19، العدد 2، سنة 2022، ص364.

أولا: مفهوم استعمال تقنية المحادثة المرئية عن بعد

1- تعريف استعمال تقنية المحادثة المرئية عن بعد

يعتبر مصطلح تقنية المحادثة المرئية عن بعد مصطلح مستحدث إذ يرجع أصله إلى اللغة الفرنسية والإنجليزية والمعبر عنه بمصطلح "vidéo conférence"، " videoconferencing". والملاحظ أن هذا المصطلح يتكون من كلمتين؛ الأولى"vidéo" والتي تعني باللغة العربية " تلفزيوني" ويقصد بها " جهاز لاستقبال الصور والأصوات المذاعة بالأمواج الكهرومغناطيسية" [5]،أما الكلمة الثانية تتمثل في "conférence" والتي تعني تجمع عدد من الأفراد لإجراء مناقشة أو حوار أو مؤتمر في موضوع معين وحدد[6].

ومن ثم يمكن تعريف تقنية المحادثة المرئية عن بعد بأنها: " وسيلة أو آلية حديثة لمباشرة إجراءات التحقيق أو المحاكمة الجزائية عن بعد، تتم الاستعانة بها في بعض الحالات،لسماعشهادة الشهود والمتعاونين مع العدالة لكشف غموض الجرائم الخطيرة لا سيما المنظم منها. بل كذلك محاكمة المتهمين رغم تواجدهم داخل المؤسسة العقابية، أمام محكمة قد تبتعد عن هذه المؤسسة أو تلك المؤسسة مئات الأميال[7]".

وعليه يمكن القول؛ بأن تقنية المحادثة المرئية عن بعد تعد آلية مستحدثة تقوم على الاتصال المرئي والمسموع وذلك بغرض إجراء تحقيق أو محاكمة جزائية عن بعد في نطاق محدد ومعين.

2- الأساس القانوني لاعتماد استعمال تقنية المحادثة المرئية عن بعد

تجد تقنية المحادثة المرئية عن بعد أساسها القانوني في الاتفاقية الأوروبية للمساعدة القضائية المتبادلة بين دول الاتحاد الأوروبي في المسائل الجزائية لسنة 2000 والتي حصرت مجال استعمالها في التحقيق القضائي عن بعد ولاسيما في مجال سماع الشهود وإفادات الخبراء[8]. وأيضا في حالة الضرورة وذلك إذا ثبت عدم ملائمة أو استحالة انتقال الشاهد أو الخبير إلى الدولة التي تطلب حضورهما أمام سلطتها القضائية. كما اشترطت موافقة المتهم لاستجوابه ووجود اتفاقية خاصة بين الدولتين مع مراعاة قوانينهم الجزائية الداخلية التي تسمح باللجوء لهذه التقنية[9]. كما تجد أساسها أيضا في الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية والتي تنص في المادة 36\3 بند – ب- منها على أنه: " إتاحة الإدلاء بالشهادة على نحو يكفل سلامة الشهود والخبراء والضحايا. ويجوز استخدام التقنيات الحديثة في هذا المجال[10]".إذ يفهم من ذلك أنها أقرت استعمال تقنية المحادثة المرئية عن بعد على نحو يكفل سلامة الشهود والخبراء والضحايا.

وبالرجوع للتشريع الجزائري نلاحظأنه؛ تم استحداث القانون رقم 15- 03 والذي أقر استعمال المحادثة المرئية عن بعد أثناء الإجراءات القضائية والتي اقتصرت في إجراء التحقيق وسماع الشهود والأطراف المدنية والخبراء أو إجراء مواجهة بين عدة اشخاص أو تلقي تصريحات المتهمين داخل المؤسسات العقابية.ولكن المشرع لم يكتف بهذا القانون وإنما قام

---

[5] www.almaany.com

[6] عمارة عبد الحميد، استخدام تقنية المحادثة المرئية عن بعد في التحقيق والمحاكمة الجزائية، مجلة دراسات وابحاث، مجلد 10، العدد 3، سنة 2018، ص60.

[7] محمد سعيد نمور، أصول الإجراءات الجزائية، شرح لقانون أصول المحاكمة الجزائية، الطبعة 2، دار الثقافة للنشر والتوزيع، عمان، سنة 2013. ص327.

[8] عادل يحي قريني، علي حسني، تقنية الاتصال المرئي المسموع وسيلة للتحقيق والمحاكمة الجنائية عن بعد،الفكر الشرطي، المجلد 18، العدد 71، سنة 2009.ص19.

[9] عمارة عبد الحميد، المرجع السابق، ص62.

[10] الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، الشبكة القانونية العربية . متواجدة على الموقع: www.arablegalnet.org.

بتعديل قانون الإجراءات الجزائية بموجب الأمر رقم 20-04 وذلك باستحداث " الكتاب الثاني مكرر" تحت عنوان " استعمال وسائل الاتصال المسموعة والمرئية أثناء الإجراءات" والذي تضمنت 3 أبواب، الباب 1" الأحكام العامة" ، الباب 2" استعمال المحادثة المرئية عن بعد في مرحلة التحقيق القضائي، " الباب 3 " استعمالالمحادثة المرئية عن بعد في مرحلة المحاكمة". وذلك وفق شروط محددة مع مراعاة القواعد المنصوص عليها في قانون الإجراءات الجزائية واحتراما لضمانات التي تقوم عليها المحاكمة العادلة.

وبهذا يكون المشرع قد استعمل تكنولوجيات الإعلام والاتصال الحديثة في تسيير الإجراءات القضائية وذلك بغرض تطوير مرفق العدالة.

ثانيا: شروط استعمال تقنية المحادثة المرئية عن بعد

يتبين من خلال استقراءناللمادة 441 مكرر من الأمر رقم 20-04 المعدل والمتمم لقانون الإجراءات الجزائية أن المشرع قام بتحديد شروط للجوء إلى استعمال هذه الوسيلة، والتي يمكن تقسيمها إلى شروط موضوعية وأخرى تقنية.

1- الشروط الموضوعية لاستعمال تقنية المحادثة المرئية عن بعد

أ- **لمقتضيات حسن سير العدالة:** فمن أهم مبررات اللجوء لاستعمال تقنية المحادثة المرئية عن بعد هو حسن سير العدالة وهذا يعد ضمانا لعدم عرقلة انعقاد جلسات المحاكمة الحضورية وهذا ما حصل فعلا بعد تفشي جائحة كورونا.

ب- **الحفاظ على الأمن والصحة العمومية:** سبق القول أنه بعد تفشي جائحة كورونا توقف العمل القضائي وذلك ما أدى إلى إصدار العديد من التدابير للتصدي لها والحد من انتشارها، إذ أصدروزير العدل قرارا يتضمن تمديد سريان مفعول المذكرة الوزارية الصادرة بتاريخ 16 مارس 2020 والمذكرة الإضافية الصادرة بتاريخ 21 مارس وذلك إلى غاية 15 أبريل 2020، والمذكرتين تشملان الجهات القضائية والمؤسسات العقابية إذ تضمنتا مجموعة من الإجراءات منها أساسا توقيف بعض أنواع الجلسات، تعليق زيارة المحبوسين....[11]. ونظرا لاستمرار فيروس كورونا في الانتشار أمر وزير العدل بإمكانية اللجوء إلى تقنية المحادثة المرئية عن بعد في إجراءات استجواب وسماع الأطراف من طرف قاضي التحقيق وفقا لأحكام القانون رقم 15-03 على أن يقتصر هذا الإجراء على القضايا البسيطة[12]. وذلك حفاظا على الامن والصحة العمومية ومن ثم أصبح اللجوء لهذه التقنية الحل الأمثل لمواكبة هذه الحالات[13].

ج- **أثناء الكوارث الطبيعية :** قد تطرأ بعض الكوارث الطبيعية والتي يكون من شأنها تعطيل الفصل في الدعاوى ومن ثم على سرعة المحاكمة مما يؤثر سلبا على مصلحة المتهم ولتفادي هذه الأوضاع أجازت المادة 441 مكرر السالفة الذكر اللجوء إلى تقنية المحادثة المرئية عن بعد.

د- **احترام مبدأ الآجال المعقولة:** من أسمى أهداف القضاء العادل أن يتم النظر في الدعاوى والبث فيها على وجه السرعة والتي تضمن مصلحة المجتمع من خلال ضمان فعالية العقوبة الجزائية في تحقيق أغراضها والمتمثلة أساسا في الردع[14]. ولتفادي تعطيل هذا الهدف اجازت المادة المذكورة أعلاه اللجوء لتقنية المحادثة المرئية عن بعد

---

[11] الجريدة الرسمية، وزارة العدل، بيانات – بيان 31 مارس 2020.

[12] مذكرة بخصوص تدعيم الوقاية من انتشار فيروس كورونا، الجريدة الرسمية، وزارة العدل، 16 ماي 2020.

[13] تومي يحي، المثول عن بعد امام المحاكم الجزائية عبر وسائل الاتصال المسموعة والمرئية في القانون الجزائري، مجلة الدراسات القانونية، المجلد 7، العدد2، السنة 2011، ص257.

[14] اكرم طرد الفايز، السرعة في المحاكمة الجزائية بين النظرية والتطبيق، دراسة في القانون الجزائي الأردني، مجلة العلوم القانونية، مجلد 33، العدد 1، سنة 2018، ص25.

لدواعي احترام مبدأ الآجال المعقولة. وتعد هذه الأخيرة كقاعدة عامة من النظام العام تهدف لحسن سير الإجراءات وتوفير الأمن القضائي[15].

هـ- **احترام الحقوق والقواعد المنصوص عليها في قانون الإجراءات الجزائية:** وهذا الشرط يعد حفاظا على ضمانات المحاكمة العادلة ومن أهمها " الحق في الدفاع" إذ يخول هذا الأخير للخصم إثبات ادعاءاته القانونية أمام القضاء والرد على كل دفاع مضاد.

2- **الشروط التقنية لاستعمال تقنية المحادثة المرئية عن بعد**

أ- **سرية الاتصال وأمانته:** وذلك لتأكد من سلامة الوسائل والأجهزة المستعملة في عملية الإرسال من الناحية التقنية.

ب- **التقاط وعرض كامل وواضح لمجريات الإجراء المتخذ:** فلا بد وأن تتم كافة أطوار المحاكمة وفقا لهذه التقنية بوضوح وسلامة تضمن وصول الصورة والصوت إلى كافة أطراف المحاكمة الجزائية.

ج- **تسجيل التصريحات على دعامة إلكترونية تضمن سلامتها وترفق بملف الإجراءات:** يجب أن يتم تسجيل التصريحات وكافة أطوار المحاكمة التي تتم وفق تقنية المحادثة المرئية عن بعد على دعامة إلكترونية[16]. إذ تتم عبر شبكة اتصال خاصة والتي استحدثت في قطاع العدالة تحت تسمية " الشبكة القطاعية لوزارة العدل "[17] والتي تضمن الاتصال الإلكتروني والتبادل الفوري والمؤمن للمعلومات بين مختلف مصالح القطاع وفق نظام الإنترنت.

المحور الثاني: نطاق استعمال تقنية المحادثة المرئية عن بعد

يتبين لنا من خلال المادة 441مكرر2 أن المشرع الجزائري قد اعتبر اللجوء لاستعمال تقنية المحادثة المرئية عن بعد أثناء الإجراءات القضائية أمرا جوازيا وذلك من خلال عبارة " يمكن جهات التحقيق[18]أن تستعمل المحادثة المرئية عن بعد..." وأيضا المادة 441مكرر7 والتي تنص: " يمكن جهات الحكم أن تلجأ لاستعمال المحادثة المرئية عن بعد...".

وبناء على ذلك سنتطرق في هذا المحور إلى مرحلتي التحقيق والمحاكمة والتي أجاز المشرع فيها استعمال تقنية المحادثة المرئية.

أولا- في مرحلة التحقيق القضائي:

بالرجوع للمادة 441مكرر2 نلاحظ أن المشرع حدد الإجراءات القضائية التي بموجبها يتم اللجوء لهذه التقنية والمتمثلة في:

- استجواب المتهم،
- سماع شخص أو اجراء مواجهة بين أشخاص،
- في التبليغات التي يستوجب قانون الإجراءات الجزائية تحرير محضر بشأنها.

---

[15] تومي يحي، المرجع نفسه، ص257.

[16] ويقصد بها : كل وسيلة مادية تستخدم لتخزين وتداول المعلومات والبيانات الالكترونية www.almaany.com .

[17] تتشكل الشبكة القطاعية لوزارة العدل التي تمت برمجتها في شهر سبتمبر 2004 وشرع العمل في إنجازها في نوفمبر 2005 كقاعدة تحتية قابلة للتوسع في التطبيقات المعلوماتية الى جانب الضمانات الضرورية للأمن المعلوماتي، راجح مزيتي فاتح، مظاهر رقمنة مرفق العدالة وأثارها على تحسين الخدمات العمومية للمتقاضين، مجلة ببليوفيليا لدراسة المكتبات والمعلومات، المجلد الأول، العدد 04، سنة 2019، ص21.

[18] يقصد بجهات التحقيق في مفهوم هذا الباب " الباب. الثاني المعنون بـ" استعمال المحادثة المرئية عن بعد في مرحلة التحقيق القضائي" قاضي التحقيق وغرفة الاتهام وجهة الحكم في حالة تطبيق احكام المادة 356 من هذا القانون" طبقا للمادة 441مكرر2 \ 3.

غير أنه باستقراء مختلف النصوص القانونية المنصوص عليها في هذا الباب[19]نلاحظ أن المشرع قد فرق بين حالة الشخص فيما إذا كان ذلك الشخص غير موقوف أو كان محبوسا.

1- **<u>الشخص غير الموقوف</u>**:

أ- **في حالة إقامته بالقرب من مقر المحكمة:** إذ يتم استجوابه أو سماعه أو إجراء مواجهة بينه وبين غيره باستعمال تقنية المحادثة المرئية عن بعد بشروط والمتمثلة في:

- أن يتحقق وكيل الجمهورية المختص إقليميا من هويته،
- أن يتم تلقي تصريحاته بحضور أمين الضبط،
- يتعين على المحامي الحضور وذلك ضمانا لحقه في الدفاع،
- يتم تحرير محضر من طرف أمين الضبط عن سير عملية استعمال المحادثة المرئية عن بعد ويوقعه ثم يرسله بمعرفة وكيل الجمهورية إلى الجهات القضائية المختصة لإلحاقه بملف الإجراءات.

كما يجب على الشخص الذي تم سماعه عن بعد أن يوقع على نسخة المحضر المرسل إليه وذلك بأية وسيلة من وسائل الاتصالبعد توقيعه مباشرة من القاضي وأمين الضبط لدى الجهة القضائية المختصة، وإن امتنع عن التوقيع أو تعذر عليه، نوه عن ذلك في المحضر. وتعاد النسخة المذكورة بنفس وسيلة الإرسال إلى جهة القضائية المختصة لإلحاقها بملف الإجراءات.

وتجدر الإشارة إلى أن مع مراعاة أحكام المادة 108 من قانون الإجراءات الجزائيةتحرر محاضر الاستجواب والمواجهة وفق الأوضاع المنصوص عليها في المادتين 94 و95 كما تطبق أحكام المادتين 91 و92 في حالة استدعاء المترجم.[20]

ب- **في حالة إقامته بدائرة اختصاص محكمة أخرى:** إذ توجه جهة التحقيق المختصة طلبا لوكيل الجمهورية للمحكمة الأقرب لمحل إقامته قصد استدعائه للتاريخ المحدد للقيام بالإجراء. ومن ثم لابد على جهة التحقيق تطبيق الأحكام المقررة في المادة 105 من قانون الإجراءات الجزائية وهذا طبقا للمادة 441 مكرر3.

ج- **في حالة ما إذا صدر أمر بوضع المتهم المسموع عن طريق نفس التقنية رهن الحبس المؤقت من طرف جهة التحقيق المختصة:** فهنا لابد من تبليغه شفاهةً وبحيطه علما بحقوقه المنصوص عليها في المادة 123مكرر من هذا القانون، وينوه عن ذلك في محضر السماع. كما ترسل نسخة من الأمر بالإيداع للتنفيذ عن طريق إحدى وسائل الاتصال حسب الحالة، إلى وكيل الجمهورية أو مدير المؤسسة العقابية[21].

2- **<u>الشخص المحبوس:</u>**

إذا تعذر استخراج أو تحويل المتهم أو الشخص الموقوف لأحد الأسباب المنصوص عليها في المادة 441مكرر السالفة الذكر، يمثل أمام جهة التحقيق عن طريق تقنية المحادثة المرئية عن بعد وذلك بعد إخطار مدير المؤسسة العقابية، وبحضور أمين ضبط المؤسسة العقابية طبقا للمادة 441مكرر1/4 .

واشترطت الفقرة الثانية والثالثة من المادة نفسها، أن يتم تحرير محضر عن سير هذه العملية من طرف أمين ضبط المؤسسة العقابية، ويوقعه ويرسله بمعرفة مدير المؤسسة العقابية إلى الجهة القضائية المختصة لإلحاقه بملف الإجراءات. كما يحق للدفاع الحضور رفقة موكله بمكان سماعه و/أو أمام جهة التحقيق المختصة.

---

[19] الباب الأول والثاني من الكتاب الثاني مكرر والمعنون بـ" استعمال وسائل الاتصال المسموعة والمرئية اثناء الإجراءات" من الامر رقم 20-04 السالف الذكر.

[20] وذلك طبقا للمادة 441 مكرر5 من الامر السالف الذكر.

[21] وذلك طبقا للمادة 441مكرر 6 من الامر السالف الذكر.

وتجدر الإشارة؛ أنه عندما يتعلق الأمر بباقي أطراف الدعوى والشهود والخبراء والمترجمين تطبق عليهم نفس الإجراءات المنصوص عليها أعلاه . كما قد سمح المشرع لوكيل الجمهورية أو لقاضي التحقيق استعمال تقنية المحادثة المرئية عن بعد في حالتين:

- في حالة تمديد التوقيف للنظر
- في حالة القبض على المتهم خارج دائرة اختصاص قاضي التحقيق الذي اصدر الامر بالقبض. وفي كلتا الحالتين لابد من ان يشار الى ذلك في المحاضر المحررة بشأنهما[22].

ثانيا : في مرحلة المحاكمة

إذ يمكن لجهات الحكم أن تلجأ لاستعمال المحادثة المرئية عن بعد من تلقاء نفسها أو بناء على طلب النيابة العامة أو أحد الخصوم أو دفاعهم، في استجواب أو سماع شخص أو في إجراء المواجهة بين الأشخاص طبقا للمادة 441مكرر 7 .

1- **من تلقاء نفسها:** إذا ارتأت جهة الحكم اللجوء لاستعمال هذه التقنية من تلقاء نفسها، لابد من أن تستطلع رأي النيابة العامة وتحيط باقي الخصوم علما بذلك.غير أنه إذا اعترضت النيابة العامة أو قدم أحد الخصوم أو دفاعه أو المتهم الموقوف أو دفاعه دفوعا لتبرير رفضه الامتثال لهذا الإجراء وارتأت جهة الحكم عدم جدية هذا الاعتراض أو هذه الدفوع فإنها تصدر قرارا غير قابل لأي طعن باستمرار المحاكمة وفق هذا الإجراء.

كما سمح المشرع للدفاع الحضور وفق موكله بمكان سماعه و/أو امام جهة الحكم المختصة وهذا طبقا للمادة 441مكرر8 .

2- **في حالة إذا طلبها أحد الأطراف أو دفاعه:** فإن الجهة القضائية المقدم أمامها الطلب هي التي تبت في الطلب بالقبول أو الرفض بعد استطلاع رأي باقي الأطراف أو دفاعهم والنيابة العامة، غير أنه استثناء يجوز لها مراجعة قرارها إذا ظهرت ظروف جديدة بعد تقديم الطلب[23].

وبعد الانتهاء من إجراء المحادثة المرئية عن بعد بالمؤسسة العقابية يحرر أمين ضبط المؤسسة العقابية محضرا عن سير عملية استعمال هذه التقنية، ويوقعه ثم يرسل بمعرفة رئيس المؤسسة العقابية إلى الجهة القضائية المختصة لإلحاقه بملف الإجراءات طبقا للفقرة الثانية من المادة 441مكرر8.

والملاحظ؛ أن المتهم الذي تقرر إجراء محاكمته وفق تقنية المحادثة المرئية عن بعد يعد حاضرا وذلك تطبيقا لمبدأ الحضورية التي تقوم عليه المحاكمة العادلة. ومن ثمإذا رفض المتهم الإجابة أو قرر التخلف عن الحضور تطبق عليه أحكام الفقرة الثانية من المادة 347 من قانون الإجراءات الجزائية والتي اقرتأن النطق بالحكم في هذه الحالة أي عن طريق تقنية المحادثة المرئية عن بعد يعد حكما حضوريا وهذا ما جاء في المادة 441مكرر10.

[22] طبقا للفقرة الثالثة والرابعة من المادة 441مكرر1 من الامر نفسه.

[23] وهذا ما جاء في المادة 441مكرر9.

خاتمة:

إن استعمال تقنية المحادثة المرئية عن بعد في التحقيق والمحاكمة الجزائية قد ظهر كحتمية نتيجة التطور الحاصل في مجال تكنولوجيات الإعلام والاتصال، فاستخدام وسائل الاتصال المرئية والمسموعة في الإجراءات الجزائية تعد مرحلة جديدة وقفزة نوعية في مجال عصرنة قطاع العدالة. كما زادت أهميتها عند انتشار جائحة كورونا إذ أصبحت ضرورة لا غنى عنها تقتضيها متطلبات حفظ الأمن والصحة العمومية وأيضا لمتطلبات حسن سير العدالة.

كما يمكن القول؛ أن المحادثة المرئية عن بعد وإن كانت تخرج عن الطابع التقليدي في التحقيق والمحاكمة والتي كانت ولازالت تتم في حيز جغرافي معين إلا أنها تساهم في تحقيق محاكمة علنية وعادلة لأطراف الدعوى وذلك من خلال تكريس الحق في الدفاع والحضورية والفصل في الدعاوى في آجال معقولة.

قائمة المصادر والمراجع:

1- المصادر:

- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية، الشبكة القانونية العربية . متواجدة على الموقع:www.arablegalnet.org
- القانون رقم 15-03 المؤرخ في 01 فبراير 2015 والمتعلق بعصرنة قطاع العدالة، الجريدة الرسمية، الجمهورية الجزائرية، العدد 06، الصادرة بتاريخ 10 فبراير 2015.
- أمر رقم 20-04 المؤرخ في 30 غشت 2020 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية ، العدد 51، الصادرة بتاريخ 31 غشت 2020.

2- المراجع:

- اكرم طرد الفايز، السرعة في المحاكمة الجزائية بين النظرية والتطبيق، دراسة في القانون الجزائي الأردني، مجلة العلوم القانونية،مجلد33، العدد 1، سنة 2018، الصفحة من 19 إلى 59.
- تومي يحي، المثول عن بعد أمام المحاكم الجزائية عبر وسائل الاتصال المسموعة والمرئية في القانون الجزائري، مجلة الدراسات القانونية، المجلد 7، العدد2، السنة 2011، الصفحة من 244 الى 267.
- رامي متوي القاضي، إجراءات التحقيق والمحاكمة عن بعد – دراسة تحليلية مقارنة- مجلة جامعة الشارقة للعلوم القانونية، المجلد 19، العدد 2، سنة 2022، الصفحة من 364 إلى 402.
- صفوان محمد شديفات، التحقيق والمحاكمة الجزائية عن بعد عبر تقنية vidéo conférence، دراسات " علوم الشريعة والقانون"، المجلد 42، العدد 1، سنة 2015، الصفحة من353 إلى 364.
- عادل يحي قريني، علي حسني، تقنية الاتصال المرئي المسموع وسيلة للتحقيق والمحاكمة الجنائية عن بعد،الفكر الشرطي، المجلد 18، العدد 71، سنة 2009، من الصفحة 15 إلى 70.
- عمارة عبد الحميد، استخدام تقنية المحادثة المرئية عن بعد في التحقيق والمحاكمة الجزائية، مجلة دراسات وابحاث، مجلد 10، العدد 3، سنة 2018، من الصفحة 57 الى 75.
- محمد سعيد نمور، أصول الإجراءات الجزائية، شرح لقانون أصول المحاكمة الجزائية، الطبعة 2، دار الثقافة للنشر والتوزيع، عمان، سنة 2013.
- مزيتي فاتح، مظاهر رقمنة مرفق العدالة واثارها على تحسين الخدمات العمومية للمتقاضين، مجلة ببليوفيليا لدراسة المكتبات والمعلومات، المجلد الأول، العدد 04، سنة 2019، الصفحة من 12 إلى 30.

المو اقع الالكترونية:

- https://www.mjustice.dz/
- https://www.almaany.com/

تم الاطلاع عليهما بتاريخ: 12\08\2022.

الجمهورية الجزائرية الديموقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة الجزائر 1 – بن يوسف بن خدة –

كلية الحقوق – سعيد حمدين –

مداخلة في الملتقى الدولي الافتراضي الموسوم بـ (القانون الجنائي في ظل التطور التكنولوجي إشكالات ومعالجات) يومي 28–29 سبتمبر 2022.

- رئيسة الملتقى: دكتورة خطاب كريمة
- إعداد المداخلة: الدكتورة بلعشي مريم
- محور المداخلة: التقاضي الالكتروني وضمانات المحاكمة العادلة
- العنوان الإلكتروني: belaachidroit@gmail.com
- رقم الهاتف: 06 64 18 99 27

ملخص:

مس التطور التكنولوجي مختلف مجالات الحياة فظهرت الحكومة الالكترونية، الادارة الالكترونية، التعليم الالكتروني، التوقيع والتصديق الالكترونين.

كما حرصت الجزائر على مواكبة هذا التطور بعصرنة العدالة وفقا لقانون (15–03)، وتعديل قانون القضاء العسكري بموجب قانون (18–14)، وتعديل قانون الإجراءات الجزائية بأمر (20–04) .

حيث أدرجت فيه استعمال وسائل الاتصال المسموعة والمرئية أثناء الإجراءات (التحقيق والمحاكمة)، ومراعاتها للضمانات الدستورية للمحاكمة العادلة.

إن هذه القفزة الواعية تعد البذرة الأولى لما لا لإنشاء المحكمة الالكترونية مستقبلا في الجزائر.

الكلمات المفتاحية:

التطور التكنولوجي – عصرنة العدالة – إجراءات التقاضي عن بعد – الضمانات الدستورية للمحاكمة العادلة .

مقدمة:

نجم عن التطور التكنولوجي تطور الجريمة بمختلف أنواعها، لذلك بات لزاما على المشرع الجزائري تطوير الآليات القانونية لضبطها في مختلف المجالات عن طريق مرفق العدالة الذي يعد أهم المرافق المعتمد عليها في إرساء السلم والأمان في المجتمع، لذلك بذلت الجزائر مجهودات معتبرة في عصرنته[1]، ثم شاءت الظروف أن شهد العالم انتشار وباء كورونا في 2019، رفاقه الحجر الصحي مما اضطر بالعديد من الدول لتطبيق التباعد الاجتماعي واللجوء إلى وسائل الإعلام والاتصال والشبكة العنكبوتية لتسيير شؤونهم في مختلف المجالات.

لذلك لجأت أغلب الدول بما فيها الجزائر إلى اعتماد نظام التقاضي عن بعد في الإجراءات (التحقيق – المحاكمة)، معدلة بذلك قوانينها، قانون القضاء العسكري (18–14)[2]، وقانون الإجراءات الجزائية أمر (20–04)[3]، مؤكدة على ضرورة المحافظة على احترام الضمانات الدستورية المتعلقة بالحقوق والحريات لتتجاوب مع ركائز الامن القانوني.

---

[1]قانون رقم 15-03 المؤرخ في 11 ربيع الثاني عام 1436 هـ الموافق 2015/02/01 م، المتضمن عصرنة العدالة، ج ر العدد 6، السنة 52، الموافق 2015/02/10 م.

[2]أمر رقم 71-28 مؤرخ 26 صفر عام 1391 هـ، الموافق 1971/04/22م، يتضمن قانون القضاء العسكري، ج ر العدد 38، سنة 68 المؤرخ 1971/05/11 م المعدل والمتمم ... بالقانون رقم 18-14 المؤرخ في 16 ذي القعدة عام 1439 هـ، الموافق 2018/07/29م، ج ر العدد 47، سنة 57، الموافق 2018/08/01 م.

[3]أمر 66-155 المؤرخ في 18 صفر عام 1386 هـ الموافق 1966/06/08 م المتضمن قانون الإجراءات الجزائية، ج ر العدد 48، السنة 03 الموافق 1966/06/10م، المعدل والمتمم عدة مرات، منها أمر 20-04 مؤرخ في 11 محرم عام 1442 هـ، الموافق 2020/08/30م، ج ر العدد 51، السنة 57، الموافق 2020/08/31، المعدل والمتمم بأمر 21-11 المؤرخ في 16 محرم عام 1443 هـ، الموافق 2021/08/25م، ج ر 65عدد ، السنة 58، الموافق 2021/08/26م.

تتجلى أهمية الدراسة في تبيان مدى فعالية نظام التقاضي عن بعد في شقه الجزائي سواء في مرحلة التحقيق أو المحاكمة.

تهدف هذه الدراسة إلى تسليط الضوء على مدى توافق نظام التقاضي عن بعد مع ضمانات المحاكمة العادلة وعدم المساس بالحقوق والحريات الشخصية.

بناء على ما تقدم يمكن صياغة الإشكالية التالية:

ما مدى فعالية استعمال وسائل الاتصال المسموعة والمرئية أثناء الإجراءات (تحقيق ومحاكمة) في المحافظة على الحقوق والحريات وتجاوبها مع ضمانات المحاكمة العادلة المقررة دستوريا؟

وللإجابة على هذه الإشكالية قسمنا دراستنا إلى مبحثين، تضمن الأول الإطار القانوني للتقاضي عن بعد ومبرراته، أما المبحث الثاني، خص توافق التقاضي عن بعد في مرحلة التحقيق والمحاكمة مع مبادئ المحاكمة العادلة المقررة دستوريا.

وقد اعتمدت في إعداد هذه الدراسة على المنهج الوصفي وذلك بوصف مختلف جوانب الموضوع، وعلى المنهج التحليلي بتحليل مختلف المواد القانونية ذات الصلة ومقارنتها مع ما جاء به المشرع الفرنسي.

المبحث الأول: الإطار القانوني للتقاضي عن بعد ومبرراته

إن التقاضي عن بعد وليد التطور التكنولوجي اعتمد من قبل الدول المتطورة قبل وباء كورونا في إطار عصرنة العدالة وتطويرها. لتوفير الجهد والوقت على القضاة والمتقاضين خاصة في الجرائم الخطيرة (المافيا، قضية viola–c–ITALIA) و (asciutto–c–ITALIA) لتفادي هروب المجرمين وحماية الضحايا والشهود وحذف اللجوء إلى المرافقة الأمنية الخاصة[1] غير أنه بظهور جائحة كورونا اضطر الوضع المحافظة على الصحة العامة والأمن في المجتمع، تسارع الدول الأخرى لاعتماده تشريعيا وتطبيقيا في الأنظمة القضائية المعاصرة، لتسهيل العمل القضائي والمحافظة على الصحة العامة والحقوق والحريات العامة.

وللإلمام بمحور الإطار القانوني للتقاضي عن بعد ومبرراته، لابد من التطرق إلى مفهومه في المطلب الأول، ثم تطور نشأته على المستوى الدولي والوطني في المطلب الثاني.

المطلب الأول: مفهوم التقاضي عن بعد

التقاضي عن بعد، مصطلح حديث يقابله مصطلح التقاضي التقليدي حيث يتفقان في تمكين المواطن من رفع دعواهم أمام الجهات القضائية، ويختلفان في طريقة التقاضي.

حيث يعتمد التقاضي التقليدي على طريقة التقليدية اليدوية، أما التقاضي عن بعد، فيعتمد على الوسيط الالكتروني[2].

[1] Jerome Bossan « la visioconférence dans le procès pénal ; un outil à maitriser » revue de science criminelle et de droit pénal comparé n°= 2011/4 page 804.

[2] عصماني ليلى "نظام التقاضي الالكتروني آلية لإنجاح الخطط التنموية" مجلة المفكر، العدد 13، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، ص 226.

إن التقاضي عن بعد يتعدى منشأ القعدة القانونية إلى رجال القانون والأشخاص الفاعلين في القضاء والمعنية بالجريمة، ويخص مواقع الكترونية متعددة[1].

أولا: تعريف التقاضي عن بعد

إن التقاضي عن بعد وسيلة حديثة تستدعي تأقلم التقنية والقانون، استعمل في البداية في الجرائم الخطيرة لتفادي هروب المجرمين وحماية الضحايا والشهود[2]، أما الآن فهو محصور في المخالفات والجنح فقط، يقوم على تفادي تنقل القضاة المكلف، ويحذف المسافات في المجال القضائي الدولي، فهو وسيلة اختيارية استثنائية في نفس الوقت[3].

عرف التقاضي عن بعد أنه "الانتقال من أسلوب التقاضي التقليدي إلى أسلوب الكتروني، قوامه إعادة هيكلة قطاع العدالة، بعصرنته وتحسين أدائه وتوفير الوقت والجهد على القضاة والمتقاضين، وأعوان العدالة وأكد من البيروقراطية والرفع من مستوى أداء الموارد البشرية فيه بالاستثمار في تكنولوجيا المعلومات"[4].

كذلك عرف التقاضي عن بعد أنه "نظام قضائي معلوماتي جديد يتم بموجبه تطبيق كافة إجراءات التقاضي عن طريق المحكمة الالكترونية بواسطة أجهزة الحاسوب المرتبطة بشبكة الانترنت وعبر البريد الالكتروني، لغرض سرعة الفصل في الدعاوى وتسهيل إجراءاتها على المتقاضين وتنفيذ الأحكام الكترونيا"[5].

---

[1] Laurence dumoulin et christian licoppe « justice et visioconférence : les audiences à distance genèse et institutionnalisation d'une Um ovation, télécom paris tech 13 version :20 nov 2009 page 3.

[2] Jerome bossin op-cit page 802.

[3] Ibid, page 806.

[4]بن عيرد عبد الغني، بضياف هاجر "التقاضي الالكتروني عبر ضوء أحدث التعديلات بين التطلعات والتحديات"، مجلة الدراسات والبحوث القانونية، مجلد 6، العدد 2 (2021)، ص15.

[5]يوسفي مباركة، حنان عكوش "التقاضي الالكتروني في الجزائر"، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 1، (2022)، ص 545.

إن التقاضي عن بعد وسيلة اتصال فعالة تنقل الصوت والصورة للأشخاص المعنية بالجريمة، والأشخاص الفاعلة في ضبطها ومحاكمتها والموجودون في مواقع مختلفة في وقت واحد.

يستخلص من هذه التعاريف مجموعة من الأسس والمميزات والخصائص التي يبنى عليها التقاضي عن بعد.

ثانيا: أسس التقاضي عن بعد ومميزاته

يقوم التقاضي عن بعد على مجموعة من الأسس ويتميز بمجموعة من المميزات.

أ- أسس التقاضي عن بعد:

أسس التقاضي عن بعد قانونية، بشرية، مادية:

الأسس القانونية: تمثل الإطار التشريعي والتنظيمي للتقاضي عن بعد وسنفصله في أوانه.

الأسس البشرية: تشكل الإطار البشري المتكون من المختصين في المجال الفني والتقني والقانوني ويدخل في هذا الإطار الهيئة القضائية بتنوعها وهيئة الدفاع، وكل الفنيين والتقنيين الموكل لهم تسهيل عملية التقاضي عن بعد وحل المشاكل إذا طرأت.

الأسس المادية: تشمل العتاد وما يحويه من الحواسيب وشبكة الانترنت[1] تشكل هذه الأسس ركائز يقوم عليها نظام التقاضي عن بعد وهذا يوضح جليا مميزاته التي نوجزها كالتالي.

ب- مميزات التقاضي عن بعد:

يتميز التقاضي عن بعد بـ:

- استمرارية وجود المواقع على الشبكة وتقديم الخدمات طيلة أيام الأسبوع مما يستلزم إشراف الإطارات الأكفاء على هذه المواقع، مع ضرورة توفير مصادر أخرى بديلة للطاقة في الحالات الطارئة.

[1] بن عيرد عبد الغني، بضياف هاجر، المرجع السابق ، ص 16.

- سهولة الوصول إلى المواقع الخاصة بالمحكمة باستخدام المقاييس المعمول بها عالميا كاختيار اسم النطاق ولغة عنوان الانترنت ... إلخ.
- توفير الحماية الأمنية اللازمة من الاختراق والترميز من أجل الحفاظ على السرية وخصوصية الموقع والمحافظة على الوثائق والمعلومات التي تحفظ في الموقع[1].

ثالثا: خصائص نظام التقاضي عن بعد

- التقاضي عن بعد شخصي يستدعي حضور وموافقة المشتبه فيه أو المتهم ودفاعه[2].
- عدم استخدام الوثائق الورقية في كافة الإجراءات والمراسلات بين طرفي التقاضي، لتحل الدعائم الالكترونية محل الدعائم الورقية بصفة نهائية.
- تسليم المستندات والعرائض الكترونيا عبر شبكة الاتصال، حيث يطلق عليه التسليم المعنوي أو التنزيل عن بعد والمقصود به استقبال ونقل أو تنزيل أحد البرامج أو البيانات عبر الانترنت الخاص للمستخدم، إذ يمكن نقل المستندات والملفات على الخط دون اللجوء إلى العالم الخارجي.
- سرعة تنفيذ إجراءات التقاضي، حيث تتم عملية إرسال واستلام المستندات والمذكرات دون الحاجة لانتقال أطراف الدعوى إلى مقر المحكمة وفي ذلك توفير للوقت والجهد والمال وتقليل لازدحام واكتظاظ المحاكم[3].
- من حيث سداد المصاريف القضائية، تحل وسائل الدفع الالكتروني محل الدفع النقدي العادي.

---

[1] بن قلو ليلى، "المحكمة الالكترونية بين المفهوم والتطبيق"، مجلة البحوث القانونية والاقتصادية، المجلد 64، العدد 2 (2011)، ص98.

[2] Laurence dumoulin, « la visioconférence dans le droit pénal : une solution pragmatique devenue le vecteur d'une politique managériale de la justice » entretien, LEXIS-NEXIS- sa droit pénal n°= 36 juin 2018, page 9.

[3] يوسف مباركة، حنان عكوش، المرجع السابق ص 547.

- من حيث اثبات إجراءات التقاضي عن بعد، يتم عن طريق المستند والتوقيع الالكترونيين عكس التقاضي التقليدي الذي يعتمد على الكتابة والتوقيع اليدويين.
- الاعتماد على الوسيط الالكتروني، والمتمثل في جهاز الكمبيوتر المتصل بشبكة الاتصالات الدولية (انترنت) ،أو شبكة الاتصال الخارجية الخاصة (الاكسترانيت) التي تقوم بنقل التعبير عن الإرادة الالكترونية في نفس اللحظة رغم البعد المكاني لأطراف النزاع[1].

من خلال ما ذكر سابقا نتساءل عن كيفية نشأته وتطوره دوليا ووطنيا ؟ وهذا ما يتم تفصيله في المطلب الثاني.

المطلب الثاني: نشأة وتطور التقاضي عن بعد

لتفصيل نشأة وتطور التقاضي عن بعد يستلزم الأمر البحث عن تأطيره على المستوى الدولي من خلال المعاهدات والاتفاقيات الدولية على المستوى الوطني.

أولا: التقاضي عن بعد على المستوى الدولي

إن تأطير التقاضي عن بعد على المستوى الدولي يحيلنا مباشرة للبحث على اعتماده كنظام قضائي جديد متجانس مع التطور التكنولوجي في الاتفاقيات الدولية.

حيث يعتبر النظام الأساسي للمحكمة الجنائية الدولية (نظام روما الأساسي 1998) الأساس الأول والأسبق لاستخدام تقنية المحادثات المرئية عن بعد في قطاع العدالة على المستوى الدولي، نص عليها البند الثاني من المادة 69 من هذا النظام "يدلي الشاهد في المحاكمة بشهادته شخصيات، إلا بالقدر الذي تتيحه التدابير المنصوص عليها في المادة 68 أو في القواعد الإجرائية وقواعد الإثبات، ويجوز للمحكمة أيضا أن تسمح بالإدلاء بإفادة شفوية أو مسجلة من الشاهد بواسطة تكنولوجيا العرض المرئي أو السمعي ... ويجب ألا يمس هذه التدابير حقوق المتهم أو تتعارض معها".

[1] عصماني ليلى، المرجع السابق، ص 218.

وفي سنة 2000م، تم اعتماده في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، من خلال البند 18 من المادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والمتعلق بالمساعدة القضائية المتبادلة "عندما يتعين سماع أقوال شخص موجود في إقليم دولة طرف، بصفة شاهد أو خبير، أمام السلطات القضائية لدولة طرف أخرى، يكون ذلك ممكنا ومتفقا مع المبادئ الأساسية للقانون الداخلي، يجوز للدولة الطرف الأولى أن تسمح، بناء على طلب الدولة الأخرى، بعقد جلسة استماع عن طريق الفيديو إذا لم يكن ممكنا أو مستعصيا مثول الشخص المعني بنفسه في إقليم الدولة الطرف الطالبة..."[1].

كما أشار البروتوكول الإضافي الثاني للاتفاقية الأوروبية 2001، للمساعدة القضائية في المادة الجزائية والذي دخل حيز النفاذ بتاريخ 2001/11/08، حيث يعد من أهم المواثيق التي نصت واعتنقت موضوع المحاكمة عن بعد، بموجب البند الأول من المادة 9 "إذا كان الشخص موجود في أراضي أحد الأطراف وتعين الاستماع إليه كشاهد أو خبير من قبل السلطات القضائية لطرف آخر، يجوز للطرف الآخر عندما يكون من غير الممكن سماعه شخصيا أمام الجهة القضائية، أن يطلب عقد جلسة الاستماع عبر المحادثة المرئية على النحو المنصوص عليه في الفقرات من 2 إلى 7".

كما نصت الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الوطنية (الاتفاقية العربية 2010) في البند الثاني من المادة 36 على "تنظر الدول الأطراف في أن تشمل التدابير المشار إليها في الفقرتين السابقتين ما يلي:

أ- توفير الحماية لأولئك الأشخاص من خلال تغيير أماكن اقلمتهم وعدم إفشاء أية معلومات تتعلق بهوياتهم وأماكن وجودهم.

[1]يزيد بوحليط، خليل الله خليفة "المحاكمة عن بعد: سرعة الإجراءات أم إهدار للضمانات" مجلة العلوم القانونية والسياسية، المجلد 12، العدد 01، أفريل 2021، ص 890.

ب- إتاحة الادلاء بالشهادة على نحو يكفل سلامة الشهود والخبراء والضحايا، ويجوز استخدام التقنيات الحديثة في هذا المجال".

بالرجوع إلى هذه النصوص، نلاحظ ان مضمونها يصب في مجمله على استخدام تقنية المحادثة المرئية عن بعد مع ضرورة مراعاة القواعد الإجرائية وقواعد الاثبات لحقوق وضمانات المتهم[1].

ثانيا: اعتماد نظام التقاضي عن بعد في التشريعات الوطنية

أخذ المشرع الجزائري بنظام التقاضي عن بعد في تعديل قانون الإجراءات الجزائية من خلال المادة 65 مكرر 27، وقانون عصرنة العدالة (15-03)، وتعديل قانون القضاء العسكري (18-14)، وتعديل آخر لقانون الإجراءات الجزائية أمر (20-04).

غير أننا سنفصل تعديل قانون القضاء العسكري مع تعديل قانون الإجراءات الجزائية أمر (20-04) في أوانه وسنقتصر في هذا المقام على تفصيل احكام المادة 65 مكرر 27 وقانون ع إلى التقاضي عن بعد الذي تأمر به المحكمة من تلقاء نفسها أو بطلب أحد أطراف الدعوى عندما يستدعي الأمر سماع الشاهد متخفي بصورة وصوت لتفادي تعريضه للخطر[2].عصرنة العدالة (15-03) .

إشارة المادة 65 مكرر 27 الى التقاضي بعد الذي تامر به المحكمة من تلقاء نفسها او بطلب احد اطراف الدعوى ، عندما يستدعي الامر سماع الشاهد متخفي صورة وصوت لتفادي تعريضه للخطر[3].

أما قانون عصرنة العدالة (15-03) يتكون من 19 مادة موزعة عن خمس فصول.

---

[1] يزيد بوحليط، خليل الله خليفة، المرجع السابق، ص 891.

[2] المادة 65 مكرر 27 ق ا ج "يجوز لجهة الحكم، تلقائيا أو بطلب من الأطراف سماع الشاهد مخطي الهوية عن طريق وضع وسائل تقنية تسمح بكتمان هويته بما في ذلك السماع عن طريق المحادثة المرئية عن بعد ...".

[3]

تضمن الفصل الأول، في مادته الأولى، الأحكام العامة والهدف من وضع هذا القانون "يهدف هذا القانون إلى عصرنة سير قطاع العدالة من خلال:

- وضع منظومة معلوماتية مركزية لوزارة العدل،
- إرسال الوثائق والمحررات القضائية بطريقة الكترونية،
- استخدام تقنية المحادثة المرئية عن بعد في الإجراءات القضائية".

أما الفصل الثاني، فتطرق إلى المنظومة المعلوماتية المركزية لوزارة العدل، والإشهاد على صحة الوثائق الالكترونية.

كما تولى الفصل الثالث، مسألة إرسال الوثائق والإجراءات القضائية بالطريق الالكتروني وفقا للمادة 9، ومحافظة هذه الوسائل الالكترونية على سلامة الوثائق المرسلة وأمن وسرية التراسل وفقا للمادة 10.

نظم الفصل الرابع استعمال المحادثة المرئية عن بعد أثناء الإجراءات القضائية أما الفصل الخامس تضمن تقرير الأحكام الجزائية على المخالفين لأحكام هذا القانون من أجل حماية نظام الرقمنة.

من خلال هذه المواد القانونية تتضح أهم إنجازات عصرنة العدالة في الجزائر منها:

1. المنظومة المعلوماتية:

تعد مجموعة من الأنظمة الآلية المصخرة لتسيير مرفق العدالة وتقديم الخدمات الإلكترونية للمواطن او المؤسسات، تعتمد على ربط جميع المؤسسات القطاعية بشبكة اتصال داخلية وتسييرها عن طريق المعالجة والتخزين في وحدة مركزية على مستوى العاصمة وهذا ما نصت عليه المادة الثانية من ق (15-03) "تحدث منظومة معلوماتية مركزية للمعالجة الآلية للمعطيات تتعلق بنشاط وزارة العدل والمؤسسات التابعة لها وكذا الجهات القضائية للنظام القضائي العادي والنظام القضائي الإداري ومحكمة التنازع".

كما نصت المادة الثالثة "تضمن الحماية التقنية للمعطيات المذكورة في المادة 2 أعلاه، قراءة وكتابة، بواسطة برنامج الكتروني يرخص باستعمال معطيات المنظومة".

ان هذه المنظومة المعلوماتية وفرت العديد من الخدمات الإلكترونية نذكر منها:

النظام الآلي لتسيير الملف القضائي: الغرض من استحداثه تقريب الإدارة من المواطن وتخفيف عبء التفرد ذلك من خلال التسيير الالكتروني لملف أي قضية من بدايتها إلى غاية الفصل فيها حتى يتمكن صاحبها بوجود التسجيل من الحصول على رقم سري يدخل من خلاله إلى الموقع الالكتروني الخاص ليري مآل القضية (حفظ ملف) مداولة. تأجير، وفي أي مستوى محكمة مجلس[1].

كما استحدثت أرضية النيابة الإلكترونية على الموقع الالكتروني لوزارة العدل ودخولها حيز الخدمة بتاريخ 2020/07/28، وهي أرضية مخصصة لتلقي الشكاوى والعرائض عن بعد.

وبتاريخ 2020/11/05، راسلت مديرية الشؤون القضائية والقانونية بوزارة العدل الاتحاد الوطني لمنظمات المحامين، قصد تعيين قاعدة المعطيات الخاصة بالمحامين في تطبيقه تسيير مهن الأعوان القضائيين، لأجل ربطها بالنظام الآلي للتقاضي الالكتروني[2].

2- نظام صحيفة السوابق العدلية: هو نظام يمكن متابعة السوابق العدلية للمواطنين وتحيينها والحصول على هذه الوثيقة من أي مكان عبر التراب الوطني بعدما كان محصور الحصول عليها فقط في محكمة مكان الولادة.

يتم الإشراف على هذا النظام من المركز الوطني لصحيفة السوابق العدلية المعمول به بتاريخ 2004/02/06 والموصول بجميع الهيئات القضائية.

[1]محمد العيدوني، يوسف زروق، المرجع السابق، ص 509.

[2]بن عيرد عبد الغني، بضياف هاجر، المرجع السابق ص 18.

عبر كامل التراب الوطني، كما يمكن هذا النظام مختلف الإدارات العمومية والمؤسسات داخل الوطن وخارجه من طلب صحيفة السوابق العدلية رقم (02) أو مرسوم التجنس أو شهادة الجنسية، ومن خلال البريد الالكتروني لوزارة العدل.

3-نظام تسيير الأوامر بالقبض: هو نظام آلي تجمع فيه كل أوامر القبض الصادرة عبر كامل التراب الوطني وكذا الاخطارات الخاصة بالكف عن البحث، حيث يكفي إدخال اسم أي شخص ليعرف إن كان مطلوب للعدالة أم لا، سواء في الموانئ أو المطارات أو المراكز الحدودية ... إلخ.

4- النظام الآلي لتسيير الجمهور العقابي: هو نظام يحتوي على ملف رقمي لنزلاء المؤسسات العقابية، يحمل رقم وطني موحد يتكفل بتسيير نشاط النزلاء طيلة فترة البقاء في المؤسسة العقابية، وفي حالة العود يستمر نفس الملف حتى وإن تغيرت المؤسسة العقابية، كما يساعد في الإجراءات السريعة والفعالة في حالة العفو ومعرفة كل الوضعيات في وقتها وإفراج، إطلاق سراح مشروط ... إلخ[1].

ثانيا :الشباك الالكتروني عبر الانترنت:

استحدثت وزارة العدل بوابة الكترونية لخدمة المواطنين والإجابة عن استفساراتهم وتزويدهم بالمعلومات الضرورية التي يطلبونها، وتوجيههم للجهات القضائية المناسبة، ومؤخرا تم إطلاق مواقع الكترونية خاصة بكل مجلس قضائي ومحكمة العليا ومجلس الدولة ومحكمة التنازع.

ثالثا : السوار الكتروني:

هو وسيلة الكترونية تحمل شريحة الكترونية تحدد موقع وتثقل حاملها تأتي في شكل سوار[2] موضع في الرجل، يصعب نزعه أو العبث به، اعتمدته الجزائر للتخفيف من عبء نزلاء

[1]محمد العيداني، يوسف زروق، المرجع السابق، ص 510.

[2]المادة 150 من قانون رقم 18-01 مؤرخ في 12 جمادى الأولى عام 1439 هـ الموافق 30 يناير 2018م، يتمم قانون رقم 05-04 المؤرخ في 27 ذي الحجة عام 1425 هـ الموافق 2005/02/06م المتضمن قانون تنظيم السجون والمادة

السجون خاصة في فترة التوقيف للنظر، أو حالات معينة كالحكم النهائي على المتهم بأقل من ثلاث سنوات او عندما تكون الفترة المتبقية من المدة العقابية أقل أو تساوي ثلاث سنوات وفقا للمادة 150 مكرر 1 من قانون (18-01) "يمكن للقاضي تطبيق العقوبات تلقائيا أو بناء على طلب المحكوم عليه شخصيا أو عن طريق محاميه، أن يقرر لتنفيذ العقوبة تحت نظام المراقبة الالكترونية، في حالة الإدانة بعقوبة سالبة للجريمة لا تتجاوز مدتها ثلاث سنوات أو في حالة ما إذا كانت العقوبة المتبقية لا تتجاوز هذه المدة ...".

رابعا : نظام المحاكمات عن بعد

هو نظام جديد يعتمد على تقنية الصوت والصورة داخل أروقة المحاكم، بفعل شبكة الألياف البصرية التي يتم بها ربط كل المحاكم والمجالس القضائية والمؤسسات العقابية عبر كامل التراب الوطني مما يسمح بالتحادث المرئي عن بعد في مرحلة التحقيق والمحاكمة من محاسنه تخفيف عبء التنقل الأطراف والشهود والخبراء والمحبوسين، وعدم تأجيل القضايا بسبب الغياب.

وبتاريخ 2015/10/07 تمت أول محاكمة عن بعد في الجزائر كانت في محكمة القليعة، وبتاريخ 2016/07/11 أقيمت أول محاكمة دولية، بمجلس قضاء المسيلة أين خوطب الشاهد بتقنية الصوت والصورة وهو بمجلس قضاء نانتير الفرنسية[1].

الإدماج الاجتماعي للمحبوسين، ج ر العدد 5، السنة 55، الموافق 2018/01/30 م "الوضع تحت المراقبة الالكترونية إجراء يسمح بقضاء المحكوم عليه كل العقوبة أو جزء منها خارج المؤسسة العقابية يتمثل الوضع تحت المراقبة الالكترونية في حمل الشخص المحكوم عليه، طيلة المدة المذكورة في المادة 150 مكرر 1 سوار الكتروني يسمح بمعرفة تواجده في مكان تحديد الإقامة المبين في مقرر الوضع الصادر عن قاضي تطبيق العقوبات".

- محمد العيداني، يوسف زروق، المرجع السابق، ص 511.

[1]المرجع نفسه ص 512.

خامسا : شخصنة الشريحة للإمضاء الالكتروني:

استحدث بوزارة العدل مركز وطني لشخصنة الشريحة للإمضاءات الالكترونية وقد دخل حيز الخدمة بتاريخ 2014/02/13، وتم بمقتضاه تزويد القضاة والنواب العامون وامناء الضبط عبر كامل التراب الوطني بشرائح الكترونية مخصصة لتخزين الامضاء الالكتروني الشخصي لكل واحد فيهم، والذي يسمح بتوقيع وتسليم كل الوثائق التي يمكن إرسالها عن طريق الوسائط الالكترونية، كما يسمح بتبادل الوثائق الكترونيا بين الجهات القضائية وكل الجهات الأخرى ذات العلاقة كما تم استحداث سلطة التصديق الالكتروني الخاصة بوزارة العدل والتي مهمتها إصدار شهادات التصديق لأعضاء التوقيع الالكتروني، وهذا من أجل تعزيز قوته الثبوتية وحجيته القانونية[1].

كما نص قانون الإجراءات الجزائية السويسري الصادر 2007/10/05، على التقاضي عن بعد بموجب المادة 144[2] ق إ ج س، وقانون الإجراءات الجزائية الفرنسي وفقا للمادة 706-71/2[3].

---

[1] محمد العيداني، يوسف زروق، المرجع السابق، ص 513.

[2] Article 144 c pp suisse audition par vidéoconférence « le ministère public ou le tribunal compètent une audition par visioconférence si la personne à entendre est dans l'impossibilité de comparaitre personnellement ou ne peut comparaitre qu'au prix de démarches disproportionnées.
L'audition est enregistrée sur support préservant le nom l'usage ».
https://www.fedlex.admin.ch>eli
المادة 144 ق إ ج س مأخوذ من الموقع الالكتروني بتاريخ 2022/08/18 على الساعة 10:45

[3] Article 706-71/2 c p95 version en rigueur depuis le 27/12/2020 modifié par la loi n°= 2020-1672du 24/12/2020 art 27... « ... lorsque les nécessités de l'enquête ou de l'instruction le protifient, l'audition ou l'interrogatoire d'une personne ainsi que la confrontation entre plusieurs personnes peuvent être effectués en plusieurs points du territoire de la république ou entre le territoire de la république et celui d'un état membre de l'union européenne dans le cadre de l'exécution d'une décision d'enquête européenne et se trouvant reliés par des moyens de télécommunication garantissant la confidentialité de la transmission … il est alors dressé, dans chacun des lieus un procès-verbal des opérations qui y ont été effectuées, ces

نستخلص أن التطور التكنولوجي مس شتى المجالات ومن بينها قطاع العدالة، لذلك تسارعت الدول بتعديل قوانينها وعصرنة جهاز العدالة، بإدراج التقاضي عن بعد (التحقيق/المحاكمة) توفيرا للجهد والوقت، وهذا ما تبناه المشرع الجزائري بالنص عليه في قانون عصرنة العدالة (15-03) وفي تعديل قانون القضاء العسكري (18-14) من خلال المواد 40 مكرر، و40 مكرر 1، وتعديل قانون الإجراءات الجزائية بموجب المواد 65 مكرر 27، 441 مكرر إلى 441 مكرر 11، وهذا ما يتم تفصيله في المبحث الثاني أدناه.

المبحث الثاني: توافق التقاضي عن بعد مع مبادئ المحكمة العادلة المقررة دستوريا

لإبراز مدى توافق التقاضي عن بعد مع مبادئ المحاكمة العادلة المقررة دستوريا وقانونيا لابد الفصل بين مرحلة التحقيق القضائي عن بعد ومرحلة المحاكمة عن بعد وهذا ما يتم تفصيله في مطلبين أساسيين.

المطلب الأول: التحقيق عن بعد ومبادئ المحاكمة العادلة المقررة قانونيا ودستوريا

يعتبر التحقيق القضائي، المرحلة الثانية في الدعوى العمومية بعد مرحلة الاتهام التي تتحرك بها الدعوى العمومية من النيابة العامة أو من غيرها[1] وهو عمل قضائي عبارة عن مجموعة من الإجراءات تباشرها سلطة قضائية مختصة تبحث فيه عن أدلة النفي والاتهام[2].

والتحقيق إجباري في الجنايات واختياري في الجنح، كما يجوز إجراؤه في المخالفات[3].

---

opérations peuvent faire l'objet d'un enregistrement audiovisuel ou sonore, les dispositions des troisième à huitième alinéa, de l'article 706-52 sont alors applicable …. » https://www.legifrance.gouv.fr > le 17/09/2022, à 10h 35.

[1] المادة 68، ق إ ج "يقوم قاضي التحقيق وفقا للقانون ... بتحري عن أدلة الاتهام وأدلة النفي ...".

[2] علي شملال المستحدث في ق إ ج، الكتاب الثاني، التحقيق والمحاكمة، نسخة معدلة ومتممة 2017، دار هومة للطباعة والنشر والتوزيع، الجزائر، ص14.

[3] المادة 66 ق إ ج "التحقيق الابتدائي وجوبي في موعد الجنايات أما في الجنح فيكون اختيار ... كما يجوز اجراؤه في المخالفات إلا طلبه وكيل الجمهورية".

ويكون في درجتين من قبل غرفة التحقيق وغرفة الاتهام، كما قد تباشره جهة الحكم وفقا للمادة 356 ق إ ج. وإن التحقيق القضائي قد يكون بالطريقة الكلاسيكية المعتادة أو عن بعد .

فهل تضبطه نفس الضوابط الشكلية الموضوعية والتي هي في الحقيقة ترجمة لمبادئ المحاكمة العادلة المقررة قانونيا ودستوريا؟.

قبل تفصيل ذلك لا بد من التمييز بين مرحلتين أساسيتين في التقاضي عن بعد قبل 2019 وبعددها.

<u>أولا:</u> مرحلة التقاضي عن بعد قبل 2019

عدل المشرع الجزائري في هذه الحقبة الزمنية السليمة والخالية من الأوبئة والأمراض، كل من قانون الإجراءات الجزائية (المادة 65 مكرر 27) كما استحدث قانون عصرنة العدالة ق (15-03) المشار إليها سابقا وفي 2018 عدل قانون القضاء العسكري بموجب ق (18-14) حيث نظم استعمال المحادثات المرئية عن بعد في الإجراءات القضائية (تحقيق محاكمة) بموجب أحكام المادتين 40 مكرر و40 مكرر 1.

أشارت المادة 40 مكرر إلى استعمال المحادثة المرئية عن بعد في الإجراءات القضائية العسكرية سواء في مرحلة التحقيق أو المحاكمة من خلال القيام باستجواب المتهم أو مواجهته أو سماع الأطراف الأخرى مع احترام الحقوق المقررة قانونا ودستوريا منها سرية وأمانة الإرسال وتسجيله على دعامة الكترونية وتدوينه يدويا من قبل كاتب الضبط وتوقيع القاضي المكلف بالملف.

كما تولت المادة 40 مكرر 1 تحديد الاختصاص المحلي للتقاضي العسكري عن بعد في كل الإجراءات القضائية، يكون أمام الجهة القضائية العسكرية الأقرب من المكان المتواجد فيه الشخص المطلوب سماعه بحضور ممثل النيابة العامة العسكرية وكاتب الضبط، مع تأكد وكيل الجمهورية العسكري من هوية الشخص محل السماع وإعداد محضر بذلك.

أما إذا كان الشخص محبوس تتم المحادثة المرئية في المؤسسة العقابية التي يكون فيه المعني بالأمر.

إن الدافع اللجوء إلى التقاضي عن بعد قبل تعديل 2019، كان بهدف تطوير جهاز العدالة ومواكبته للتطور التكنولوجي الذي سعت إليه العديد من الدول، بتعديل قوانينها، توفيرا للوقت والجهد وبسط الفعالية والنجاعة في التقاضي بما يخدم مرفق العدالة والمواطن.

ثانيا: مرحلة التقاضي عن بعد بعد 2019

ميز عام 2019 انتشار وباء كورونا والذي رافقه الحجر الصحي والتباعد الاجتماعي، حيث تميزت هذه الحقبة الزمنية بالركود في مختلف المجالات حتى قطاع العدالة لذلك ارتأى المشرع الجزائري على غرار مختلف دول العالم مباشرة الحياة الطبيعية ولو ببطئ حفاظا على حقوق وحريات الأفراد بتعديل قانون الإجراءات الجزائية بموجب أمر 20-04 المتضمن استعمال وسائل الاتصال المسموعة والمرئية أثناء الإجراءات (تحقيق-محاكمة) بموجب المواد 441 مكرر إلى 441 مكرر 11.

إن هدف هذا التعديل المحافظة على الأمن والصحة العمومية واحترام الآجال القانونية لصيانة الحقوق والحريات العامة لتجسيد الأمن القانوني من خلال تفعيل مبدأ الشرعية الشكلية والموضوعية، وفي هذا الإطار أشارت محكمة النقض الفرنسية أن السبب الوحيد الذي يستدعي اللجوء إلى التقاضي عن بعد هو وجود الاخطار والمساس بالأمن العام، أو هروب المتهمين[1].

[1] Jerome Bossin op-cit page 810 « la cour de cassation affirme que cette occasion que le seul motif de refus et bien conformément au texte de l'article 706-71, l'existence de risques prouves de troubler à l'ordre public ou d'évasion, crim, 11 oct, 2011, à publier Dalloz actualité 14 nov 2011, obs- Lena.

لم يعرف المشرع الجزائري التقاضي عن بعد باستعمال وسائل الاتصال المسموعة والمرئية أثناء الإجراءات فقط أشار إلى ظروف استحداث هذه الوسائل وضرورة مراعاة مبادئ المحاكمة العادلة والمشار إليها قانونيا ودستوريا[1]، وأنها تستعمل في مرحلة التحقيق والمحاكمة.

بالنسبة لاستعمال المحادثة المرئية عن بعد في مرحلة التحقيق القضائي سواء أكانت درجة أولى أو ثانية أو أمام جهة الحكم، تكون عبارة عن استجواب أو سماع أو إجراء مواجهة بين الأشخاص أو في التبليغات التي يستجوب قانون الإجراءات الجزائية تحرير محاضر بشأنها. في كل الأحوال يجب التقيد بالضوابط المشار إليها في احكام المادة 11 ق إ ج وهي السرية واحترام حقوق الدفاع، وقرينة البراءة وحرمة الحياة الخاصة.

1. بالنسبة لخاصية السرية في التقاضي عن بعد، تشمل :

التحقيق والمحاكمة ويقصد بها عدم العلانية[2]، يستثنى منها المتهم، بقية أطراف الدعوى، القضاة (تحقيق الحكم، النيابة العامة)، الدفاع[3] نص عليها الدستور الجزائري في مادته 47 "لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت ...".

وقانون عصرنة العدالة (15-03) في مادته 2/14 "... يجب أن تضمن الوسيلة المستعملة سرية الارسال وأمانته ..." أيضا المادة 11 ق إ ج "تكون إجراءات التحري والتحقيق سرية، ما لم ينص القانون على خلاف ذلك، ودون إضرار بحقوق الدفاع كل شخص يساهم في هذه

[1]المادة 14 من ق (15-03) "... يمكن استجواب وسماع الأطراف عن طريق المحادثة المرئية عن بعد مع مراعاة احترام الحقوق والقواعد المنصوص عليها في ق إ ج ....".
- المادة 441 مكرر أمر (20-11) "يمكن الجهات القضائية ... استعمال المحادثة المرئية عن بعد في الإجراءات القضائية، مع احترام الحقوق والقواعد المنصوص عليها في هذا القانون"
- المادة 40 مكرر (18-14) "يمكن جهات التحقيق أو الحكم أن تقوم باستجواب المتهم ... عبر المحادثة المرئية باحترام الحقوق والقواعد المنصوص عليها في ق إ ج ...".

[2]عبد الله أوهايبية "شرح قانون الإجراءات الجزائية الجزائري الجزء الأول، الطبعة الثانية (2018) طبعة مزيدة منقحة بأحدث التعديلات، دار هومة للطباعة والنشر والتوزيع، الجزائر، ص 525.

[3]حسن بوسقيعة "التحقيق القضائي"، الطبعة الثانية عشرة منقحة ومتممة في ضوء الجديد في القانون والاجتهاد القضائي 2018، دار هومة للطباعة والنشر والتوزيع، الجزائر، ص 16.

الإجراءات ملزم بكتمان السر المهني بالشروط المبنية في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه ..."

كذلك نصت عليها المادة 441 مكرر (أمر 20-04) "... يجب أن تضمن الوسائل المستعملة سرية الإرسال وأمانته كذا التقاط وعرض كامل وواضح لمجريات الإجراء المتخذ وفق هذه التقنية ...".

كما أشار المشرع الفرنسي إلى السرية في كل الإجراءات القضائية، بما فيها إجراءات استعمال لوسائل الاتصال المسموعة والمرئية وفقا لأحكام المادة 706-1/71 ق إ ج ف[1].

ولتكريس هذه السرية حرص المشرع الجزائري على ضرورة تسجيل التصريحات على دعامة تضمن سلامتها وترفق بملف الإجراءات، بالإضافة إلى تدوين كاتب الضبط التصريحات كاملة حرفيا على محضر يوقع من طرف قاضي التحقيق المكلف بالملف وفقا للمادة 3/14 و4 من ق (15-03) "يتم تسجيل التصريحات على دعامة تضمن سلامتها وترفق بملف الإجراءات تدون التصريحات كاملة وحرفيا على محضر يوقع من طرف القاضي المكلف بالملف وأمين الضبط".

[1] Act 706-71/1 c pp F « mod, LN 2011-267, 14 mars 2011, LN°= 2011-392, 14 avril, 2011 en vigueur le 1/06/2011, lorsque les nécessités de l'enquête ou de l'instruction le justifient, l'audition ou l'interrogatoire d'une personne ainsi que la confrontation entre plusieurs personnes peuvent être effectué en plusieurs points de territoire de la république se trouvant reliés par moyens de télécommunications garantissant la confidentialité de la transmission … »

Gilbert Azibekt c pp F 2014, Lexis-Nexis,

- Jerome Bossin op-cit page 811.

وأن ما يبرر وجوب الحفاظ على سرية مجريات التحقيق والمحافظة على أصل البراءة وعدم المساس بسمعة المتهم وكرامته ومنع التشهير به لأن قرينة البراءة قاعدة ملزمة[1] كرستها المواثيق الدولية[2] والتشريع الجزائري[3].

إن التحقيق عن بعد قد ينصب على متهم محبوس وغير محبوس، مهم تراعي فيه ضمانات المحاكمة العادلة كالسرية، حقوق الدفاع، قرينة البراءة وقد ينجر على إجراء التحقيق عن بعد إصدار قاضي التحقيق للأوامر القضائية كتمديد التوقيف للنظر، إصدار أمر القبض وفقا للمادة 441 مكرر 1 "... كما يمكن لوكيل الجمهورية أو قاضي التحقيق اللجوء إلى المحادثة المرئية عن بعد في حالة تمديد التوقيف للنظر وكذا في حالة القبض على المتهم خارج إدارة اختصاص قاضي التحقيق الذي أصدر الأمر بالقبض ...".

---

[1]كريمة خطاب، قرينة البراءة، أطروحة الدكتوراه ، جامعة الجزائر 01 كلية الحقوق ،السنة الجامعية 2014-2015 ص 24.

[2]المادة 14 من العهد الدولي للحقوق المدنية والسياسية الصادر عن الأمم المتحدة في 1966/12/16، المصادق عليه بالمرسوم الرئاسي رقم 84-67 المؤرخ في 11 شوال عام 1409 هـ الموافق 1985/05/16 يتضمن الانضمام إلى العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية والعهد الدولي الخاص بالحقوق المدنية والسياسية والبروتوكول الاختياري المتعلق بالعهد الدولي الخاص بالحقوق المدنية السياسية الموافق عليه من طرف الجمعية العامة للأمم المتحدة يوم 1966/12/16م ج ر العدد 20 سنة 26 الموافق 1989/05/17م "من حق كل متهم بارتكاب الجريمة أن يعتبر بريئا إلى أن يثبت عليه الجرم قانونا".

[3]المادة 41 من دستور الجمهورية الجزائرية الديموقراطية الشعبية الصادر في 1996/11/28م والساري المفعول بموجب المرسوم الرئاسي رقم 96-438 المؤرخ في 26 رجب عام 1417هـ الموافق 1996/12/07م، المتعلق بإصدار نص تعديل الدستور المصادق عليه في استفتاء 1996/11/28م، ج ر العدد 76، السنة 33، الموافق 1996/12/08م المعدل بموجب:

- قانون رقم 02-03 المؤرخ في 27 محرم عام 1423 هـ الموافق 2002/04/20م، المتضمن التعديل الدستوري، ج ر العدد 25، السنة 39، الموافق 2002/04/14م
- قانون 08-19 المؤرخ في 17 ذي القعدة عام 1429 هـ الموافق 2008/11/15م يتضمن التعديل الدستوري، ج ر العدد 63، السنة 45، الموافق 2008/11/16م
- قانون 16-01 المؤرخ في 26 جمادى الأولى عام 1437هـ الموافق 2016/03/06م المتضمن التعديل الدستوري، ج ر العدد 14 السنة 53، الموافق 2016/03/07م
- المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 هـ الموافق 2020/12/30 المتضمن التعديل الدستوري المصادق عليه في استفتاء 2020/11/01 ج ر 82 الموافق 2020/12/30م "كل شخص يعتبر بريء حتى تثبت جهة قضائية إدانته في إطار محاكمة عادلة".
- المادة 1 ق إ ج "إن كل شخص يعتبر بريئا ما لم تثبت إدانته بحكم قضائي حائز لقوة الشيء المقضي فيه ...".

المادة 11 ق إ ج ".... تراعي في كل الأحوال قرينة البراءة وحرمة الحياة الخاصة".

كذلك اصادر قاضي التحقيق لأمر الوضع في الحبس المؤقت وفقا لنص المادة 441 مكرر 6 "إذا أمر قاضي التحقيق وضع المتهم المسموع عن طريق تقنية المحادثة المرئية عن بعد رهن الحبس المؤقت، يقوم عن طريق نفس التقنية، بتبليغه هذا الامر شفاهة ويحيطه علما بحقوقه المنصوص عليها في المادة 123 مكرر من هذا القانون وينوه عن ذلك في محضر السماع ...".

2. حق الدفاع والتقاضي عن بعد:

يعد حق الدفاع وسيلة لحماية قرينة البراءة، وبالتالي ضمان هذا الحق هو ضمان أصل البراءة[1] لذلك أقرت المواثيق الدولية[2] والقانون الجزائري[3] من مواقع مختلفة أهمها قانون عصرنة العدالة في المادة (15-03) في المادة 1/14 "... يمكن استجواب وسماع الأطراف عن طريق المحادثة المرئية عن بعد مع مراعاة احترام الحقوق والقواعد المنصوص عليها في قانون الإجراءات الجزائية".

والمادة 1/144 مكرر ق إ ج "... استعمال تقنية المحادثة المرئية عن بعد في الإجراءات القضائية مع احترام الحقوق والقواعد المنصوص عليها في هذا القانون ...".

والمادة 441 مكرر 4 ق إ ج "يحق للدفاع الحضور رفقة موكله بمكان سماعه و/أو أمام جهة التحقيق المختصة".

---

[1] كريمة خطاب، المرجع السابق، ص 139.

[2] المادة 3/14 من العهد الدولي للحقوق المدنية والسياسية "لكل شخص الحق في طلب المساعدة من محام يختاره بنفسه، لحماية حقوقه اثباتها وللدفاع عنه في جميع مراحل الإجراءات الجنائية".

[3] المادة 175 من التعديل الدستوري 2020 "الحق في الدفاع معترف به . الحق في الدفاع مضمون في القضايا الجزائية"
المادة 177 من التعديل الدستوري 2020 "يحق للمتقاضي المطالبة بحقوقه أمام الجهات القضائية، ويمكنه أن يستعين بمحام خلال كل الإجراءات القضائية".
المادة 100 ق إ ج "... ينبغي للقاضي أن يوجه للمتهم بأن له الحق في اختيار محام عنه..".
المادة 102 ق إ ج "يجوز للمتهم المحبوس بمجرد حبسه أن يتصل بمحاميه ..."
المادة 105 "لا يجوز سماع المتهم أو المدعي المدني أو إجراء مواجهة بينهما إلا بحضور لمحاميه ... يوضع ملف الإجراءات تحت طلب محامي المتهم قبل كل استجواب بأربع وعشرين ساعة على الأقل ...".

والمادة 40 مكرر من قانون القضاء العسكري (18-14) "يمكن جهات التحقيق أو الحكم أن تقوم باستجواب المتهم ومواجهته أو سماع الأطراف عبر المحادثة المرئية باحترام الحقوق والقواعد المنصوص عليها في قانون الإجراءات الجزائية وطبقا لأحكام هذا القانون ..."، والقانون الفرنسي[1].

إن عدم مراعاة قاضي التحقيق لهذا الحق يترتب عليه بطلان الإجراءات[2] ورغم هذه الضمانة المقررة للمشتبه فيه أو للمتهم، فإن دور المحامي ليس إيجابي عند الاستجواب عدا توفير الراحة النفسية للمتهم أو المشتبه فيه، ذلك أنه حتى طرح الأسئلة يكون بموافقة قاضي التحقيق عليها[3]، وليس له الحق بالمرافعة أمامه عكس النيابة العامة التي تطرح الأسئلة مباشرة عند الاستجواب.

وعليه إن الدور الإيجابي للدفاع يكون في مرحلة المحاكمة من خلال المرافعة وإن هذا التمييز بين هيئتين (الدفاع والنيابة العامة) والتي يعد كل منهما خصم في القضية، يشكل تعدي على مبدأ مساواة الخصوم أمام القانون.

فهل روعيت مبادئ المحاكمة العادلة في المحاكمة عن بعد؟ وهذا ما نتطرق له في المطلب الثاني.

---

[1] Aet 114 CPP F « les parties ne peuvent être entendues, interrogées ou confrontées, à moins qu'elles n'y renoncent expressément, qu'en présence de leurs avocats de ces derniers dument appelés … ».

[2] المادة 157 ق إ ج "تراعي الاحكام المقررة في المادة 100 المتعلقة باستجواب المتهمين والمادة 105 المتعلقة بسماع المدعي المدني واولا ترتب على مخالفتها بطلان الإجراء نفسه وما يتلوه من إجراءات ...".

[3] المادة 107 ق إ ج "لا يجوز لمحامي المتهم ولا لمحامي المدعي المدني أن يتناولا الكلام فيما عدا توجيه الأسئلة بعد أن يصرح قاضي التحقيق لهما بذلك ...".

المطلب الثاني: المحاكمة عن بعد وضمانات المحاكمة العادلة

من ضمانات المحاكمة العادلة، الحق في قطاع مختص[1]، مستقل[2]، ومحايد[3]، وحق المتهم في محاكمة وجاهية وشفوية وعلانية والحق في إنهاء إجراءات المحاكمة خلال فترة معقولة والحق في الطعن في الأحكام بالإضافة إلى تكريس حق الدفاع.

تعد مرحلة المحاكمة من أهم المراحل التي تقرر فيها إدانة او براءة المتهم، وقد نظم المشرع الجزائري استعمال المحادثة المرئية عن بعد في مرحلة المحاكمة بموجب المواد 441 مكرر 7 إلى 441 مكرر 1 ق إ ج.

فهل المحاكمة عن بعد تمتثل لمبادئ المحاكمة العادة المنصوص عليها قانونيا ودستوريا؟ وهذا ما سنفصله كالتالي:

أولا: التقاضي عن بعد أو مبدأ العلنية

يعد مبدأ العلنية من مبادئ المحاكمة العادلة نص عليه الدستور بالمادة 169 "... ينطق بالأحكام القضائية في جلسات علنية" كما نص عليه قانون الإجراءات الجزائية في العديد من المواد منها: 184، 212 المقابلة لنص المادة 427[4] ق إ ج ف، 285، 342، 355، 398، والمادة 135 قانون القضاء العسكري والمادة 89 قانون حماية الطفل.

---

[1]"الاختصاص القضائي هو أهلية جهة قضائية معينة للنظر أو الفصل في الدعوى الجزائية معينة" مأخوذ من كتاب الدكتور أحمد الشافعي "البطلان في ق إ ج دراسة مقارنة" الطبعة الخامسة 2010 دار هومة للطباعة والنشر والتوزيع، الجزائر، ص 67.

[2]المادة 163 من التعديل الدستوري 2020 "القضاء سلطة مستقلة، القاضي مستقل، لا يخضع إلا للقانون".

المادة 165 من التعديل الدستوري2020 "يقوم القضاء على أساس مبادئ الشرعية والمساواة القضاء متاح للجميع يضمن القانون التقاضي عن درجتين ويحدد شروط وإجراءات تطبيقه".

[3]المادة 10 من الإعلان العالمي لحقوق الانسان المعتمد والمنشور بموجب قرار الجمعية العامة للأمم المتحدة رقم 217 الف (د-3) المؤرخ في 10 كانون الأول/ ديسمبر 1948م "لكل انسان على عدم المساواة التامة مع الآخرين، الحق في أن تنظر قضيته محكمة مستقلة محايدة، نظرا منصفا وعلنيا، للفصل في حقوقه والتزاماته وفي أية تهمة جزائية توجه إليه".

[4] Art 427 cpp F « … hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction.

يقصد بالعلانية فتح باب الجلسة لحضور الجمهور غير أنه يستثنى أن تكون الجلسات سرية إذا كان في علنيتها مخالفة للنظام العام والآداب العامة.

إن فتح باب الجلسات القضائية امام عامة الناس، تمكن من ممارسة هؤلاء الرقابة الشعبية على القاضي للتطبيق السليم للقانون فيما يخص حقوق الخصوم والمساواة بينهم.

تشمل علانية المحاكمة كل إجراءات المحاكمة، من مناداة الخصوم والشهود وسؤال المتهم عن التهمة، أو اتلائها عليه، وطلبات الادعاء العام، ودفاع الخصوم وسماع كافة الإجراءات.

إن المحاكمة عن بعد مضبوطة بأحكام المواد من 441 مكرر 7 إلى 441 مكرر 11، تلجأ إليها المحكمة من تلقاء نفسها، أو بناء على طلب النيابة العامة أو أحد الخصوم، أو دفاعهم، كما تقوم المحكمة باستطلاع رأي النيابة العامة وتحيط باقي الخصوم علما بذلك. وفي حالة اعتراض النيابة العامة وتحيط باقي الخصوم علما بذلك. وفي حالة اعتراض النيابة العامة او أحد الخصوم أو دفاعه تفصل المحكمة فيه بإصدار قرار غير قابل لأي طعن باستمرار المحاكمة وفقا لهذا الإجراء ان هذا القرار يشكل إخلال بمبدأ التقاضي على درجتين المكرس دستوريا وقانونا باعتباره دعامة من دعائم المحاكم العادلة.

تبقى المحاكمة عن بعد استحدثت في فترة عصيبة هددت صحة العالم كلها، وحفاظا على المصلحة العامة التي هي أولى بالحماية من المصلحة الخاصة من خلال المحافظة على الآجال القانونية وحقوق وحريات الأفراد إذ كان لزاما اعتمادها والنص عليها.

ثانيا: التقاضي عن بعد ومبدأ الوجاهية والشفوية

إن مبدأ الوجاهية دعامة أساسية في مرحلة المحاكمة ومخالفتها ترتب البطلان للإجراءات والحكم الصادر بالنتيجة في القضية[1] وفقا للمادة 157 ق إ ج يعني مبدأ الوجاهية ضرورة

Le juge ne peut prendre sa décision que sur les preuves qui lui sont apportées au cours des débats en contradictoirement disputées devant lui … ».

[1]أحمد الشافعي، المرجع السابق، ص 198.

حضور أطراف الدعوى أو الخصوم أمام القاضي خلال المناقشة والمرافعة وأن يحضروا خلال جميع مراحل التحقيق النهائي وأن يردوا على الأدلة المقدمة بالحجج والبراهين المتبادلة وأن يوضحوها وأن يتمكنوا من الدفاع عن أنفسهم شخصيا أو بواسطة المحامين يعينونهم بأنفسهم أو تعينهم لهم المحكمة تلقائيا[1].

إن مبدأ الوجاهية يقوم على تحقيق القاضي التوازن الدقيق بين المراكز المتساوية وتقدير الأدلة تقديرا موضوعيا ولا يتأتى هذا إلا بتمكين كل الخصوم من حضور جميع إجراءات المحاكمة وتقديم ما لديهم من أدلة وإحاطة القاضي علما بكل طلب أو دفاع يتقدم به الخصم كما يتاح له حق مناقشة الخصم الآخر ودحض أدلته[2] وفقا لأحكام المادة 212 ق إ ج كما نصت المادة 441 مكرر 7 على مبدأ الوجاهية "يمكن جهات الحكم ... أو في إجراء المواجهة بين الأشخاص" والمادة 441 مكرر 10 "يمكن استعمال المحادثة المرئية عن بعد عند النطق بالحكم ويكون الحكم في هذه الحالة حضوريا".

يرتبط مبدّأ الوجاهية بمبدأ الشفوية هو الآخر نص المشرع الجزائري عليه في المادة 1/233 "يؤدي الشهود بشهادتهم شفويا ..." وهي نفس المادة المقابلة للمادة 452 ق إ ج ف.

« Les témoins déposent oralement ... »

إلا أن مبدأ الشفوية يتضح أكثر في محكمة الجنايات وفقا للمادة 285 ق إ ج "جلسات المحكمة علنية ..." كما نصت تشريعات مختلف الدول على وجوب تلاوة التقرير الشفوي من طرف المستشارين وهذا ما نصت عليه المادة 431 ق إ ج "يفصل في الاستئناف في الجلسة بناء على تقرير شفوي من أحد المستشارين ويستجوب المتهم ..." وهي المادة المقابلة للمادة 513 ق إ ج ف .

[1] عبد الله أوهايبية "شرح قانون الإجراءات الجزائية الجزائري" الجزء الثاني، التحقيق النهائي والمحاكمة طبعة 2017-2018 مزيدة ومنقحة بالتعديلات، دار هومة للطباعة والنشر والتوزيع، الجزائر، ص 31.

[2] فاضل زيدان حمد "سلطة القاضي الجنائي في تقدير الأدلة دراسة مقارنة" دار الثقافة للنشر والتوزيع طبعة 2006، ص 269.

« L’appel est juge à l’audience sur le rapport oral d’un consuller, le prévenu est interrogé »

أيضا بعد ضابط الشفوية ضمانة أساسية للتقدير السليم للأدلة، وله صلة قوية بمبدأ القناعة القضائية للقاضي من حصيلة المنافسات التي تجري في جلسة المحاكمة كما أنه يحقق رقابة فعالة على جدية الأدلة التي حصلت في مرحلة التحقيق ومن خلالها يتم مخاطبة وجدان القاضي وضميره[1] طبقا للمادة 307 ق إ ج "يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسات. ...".

نصت المادة 441 مكرر 6 على مبدأ الشفوية "إذا أمر قاضي التحقيق وضع المتهم المسموع عن طريق تقنية المحادثة المرئية عن بعد رهن الحبس المؤقت، يقوم عن طريق نفس التقنية، بتبليغه هذا الأمر شفاهة ...".

[1]فاضل زيدان محمد، المرجع السابق، ص 354-355.

خاتمة:

يعتبر التقاضي عن بعد سلاح ذو حدين من جهة يساهم في تسهيل العمل القضائي على القضاة والمحامين ومن جهة أخرى هناك بعض الخروقات مبادئ المحاكمة العادلة.

يعد مرفق العدالة من أصعب المرافق التي تطبق فيها الرقمنة رغم أنها أثبتت نجاعتها في المجال الإداري في استخراج الأحكام والوثائق الإدارية ... إلخ.

وما التقاضي عن بعد سواء التحقيق أو المحاكمة إلا استفادة من مزايا التقنية والرقمية التي أفرزتها الشبكة العنكبوتية.

ابتدأت الجزائر باعتماده تدريجيا من خلال تقدير قانون الإجراءات الجزائية ثم استحدث قانون عصرنة العدالة ثم تعديل قانون القضاء العسكري ثم إصدار أمر 20-04 المنظم للتقاضي الالكتروني سواء في مرحلة التحقيق أو المحاكمة، حيث دعت إليه ضرورة حماية المصلحة العامة والصحة العامة وألأمن من جراء انتشار جائحة كورونا وقد حاول المشرع الجزائري قدر الإمكان صياغة هذه النصوص القانونية لتوافق المبادئ الدستورية والقانونية المتماشية مع ضمانات المحاكمة عن بعد.

ومن خلال هذه الدراسة **خلصنا** إلى جملة من النتائج والتوصيات:

أ- النتائج:

1- يعد التقاضي الالكتروني أسلوب جديد وأحد آليات رقمنة قطاع العدالة .

2-المسار البطيئ لاستعمال المحادثة المرئية والمسموعة في الإجراءات القضائية على المستوى الوطني والدولي.

3-اعتمدته الاتفاقيات الدولية ثم التشريعات الوضعية الوطنية والأجنبية.

4-حرص الدول قد الإمكان على استدراك النقائص التشريعية، فيما يخص مبادئ المحاكمة العادلة وحقوق الانسان.

5-استفادة المؤسسات العقابية من عصرنة العدالة بتنظيم ملفات النزلاء عن طريق رقمنة ملفاتهم.

ب- التوصيات:

1-توسع تطبيق الحكومة الالكترونية في مختلف المجالات بما فيها رقمنة قطاع العدالة.

2-مراجعة فعلية ودقيقة لمختلف المواد الإجرائية والعقابية لتسهيل تطبيق التقاضي عن بعد وسد الثغرات القانونية.

3-الامتناع عن تطبيق التقاضي عن بعد في المواد الجنائية إلا إذا استدعت الضرورة ذلك لسبب خطير بليغ، واستحالة نقل المتهم أو تحويله لأسباب صحية نظرا لخصوصية هذا النوع من المحاكم التي تتطلب الحضور المادي للمتهم لحقيق مبدأ الاقناع الشخصي للقضاة والمحلفين زد على ذلك الأمية الرقمية للقضاة، والمحامين، والمحلفين، والإداريين التابعين لقطاع العدالة.

4-ضرورة الإسراع في تكوين كل من له صلة بجهاز العدالة رقميا للنهوض بالقطاع.

5-محاربة الأمية الرقمية بكل أفراد المجتمع لتسهيل حياتهم في مختلف المجالات.

قائمة المصادر والمراجع

أولا : المصادر التشريعية :

1. العهد الدولي للحقوق المدنية والسياسية الصادر عن الأمم المتحدة في 1966/12/16، المصادق عليه بالمرسوم الرئاسي رقم 84-67 المؤرخ في 11 شوال عام 1409 هـ الموافق 1985/05/16 يتضمن الانضمام إلى العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية والعهد الدولي الخاص بالحقوق المدنية والسياسية والبروتوكول الاختياري المتعلق بالعهد الدولي الخاص بالحقوق المدنية السياسية الموافق عليه من طرف الجمعية العامة للأمم المتحدة يوم 1966/12/16م ج ر العدد 20 سنة 26 الموافق 1989/05/17م
2. الإعلان العالمي لحقوق الانسان المعتمد والمنشور بموجب قرار الجمعية العامة للأمم المتحدة رقم 217 الف (د-3) المؤرخ في 10 كانون الأول/ ديسمبر 1948م
3. دستور الجمهورية الجزائرية الديموقراطية الشعبية الصادر في 1996/11/28م والساري المفعول بموجب المرسوم الرئاسي رقم 96-438 المؤرخ في 26 رجب عام 1417هـ الموافق 1996/12/07م، المتعلق بإصدار نص تعديل الدستور المصادق عليه في استفتاء 1996/11/28م، ج ر العدد 76، السنة 33، الموافق 1996/12/08م المعدل بموجب:

- قانون رقم 02-03 المؤرخ في 27 محرم عام 1423 هـ الموافق 2002/04/20م، المتضمن التعديل الدستوري، ج ر العدد 25، السنة 39، الموافق 2002/04/14م
- قانون 08-19 المؤرخ في 17 ذي القعدة عام 1429 هـ الموافق 2008/11/15م يتضمن التعديل الدستوري، ج ر العدد 63، السنة 45، الموافق 2008/11/16م
- قانون 16-01 المؤرخ في 26 جمادى الأولى عام 1437هـ الموافق 2016/03/06م المتضمن التعديل الدستوري، ج ر العدد 14 السنة 53، الموافق 2016/03/07م

– المرسوم الرئاسي رقم 20–442 المؤرخ في 15 جمادى الأولى عام 1442 هـ الموافق 2020/12/30 المتضمن التعديل الدستوري المصادق عليه في استفتاء 2020/11/01 ج ر 82 الموافق 2020/12/30م

القوانين :

1. قانون رقم 15–03 المؤرخ في 11 ربيع الثاني عام 1436 هـ الموافق 2015/02/01 م، المتضمن عصرنة العدالة، ج ر العدد 6، السنة 52، الموافق 2015/02/10 م.
2. قانون رقم 18–01 مؤرخ في 12 جمادى الأولى عام 1439 هـ الموافق 30 يناير 2018م، يتمم قانون رقم 05–04 المؤرخ في 27 ذي الحجة عام 1425 هـ الموافق 2005/02/06م المتضمن قانون تنظيم السجون والمادة الإدماج الاجتماعي للمحبوسين، ج ر العدد 5، السنة 55، الموافق 2018/01/30 م

الأوامر :

1. أمر 66–155 المؤرخ في 18 صفر عام 1386 هـ الموافق 1966/06/08 م المتضمن قانون الإجراءات الجزائية، ج ر العدد 48، السنة 03 الموافق 1966/06/10م، المعدل والمتمم عدة مرات، منها أمر 20–04 مؤرخ في 11 محرم عام 1442 هـ، الموافق 2020/08/30م، ج ر العدد 51، السنة 57، الموافق 2020/08/31، المعدل والمتمم بأمر 21–11 المؤرخ في 16 محرم عام 1443 هـ، الموافق 2021/08/25م، ج ر 65عدد ، السنة 58، الموافق 2021/08/26م.
2. أمر رقم 71–28 مؤرخ 26 صفر عام 1391 هـ، الموافق 1971/04/22م، يتضمن قانون القضاء العسكري، ج ر العدد 38، سنة 68 المؤرخ 1971/05/11 م المعدل والمتمم ... بالقانون رقم 18–14 المؤرخ في 16 ذي القعدة عام 1439 هـ، الموافق 2018/07/29م، ج ر العدد 47، سنة 57، الموافق 2018/08/01 م.

ثانيا – الكتب :

1. أحمد الشافعي "البطلان في ق إ ج دراسة مقارنة" الطبعة الخامسة 2010 دار هومة للطباعة والنشر والتوزيع، الجزائر،
2. حسن بوسقيعة "التحقيق القضائي"، الطبعة الثانية عشرة منقحة ومتممة في ضوء الجديد في القانون والاجتهاد القضائي 2018، دار هومة للطباعة والنشر والتوزيع، الجزائر.
3. عبد الله أوهايبية "شرح قانون الإجراءات الجزائية الجزائري الجزء الأول، الطبعة الثانية (2018) طبعة مزيدة منقحة بأحدث التعديلات، دار هومة للطباعة والنشر والتوزيع، الجزائر،
4. عبد الله أوهايبية "شرح قانون الإجراءات الجزائية الجزائري" الجزء الثاني، التحقيق النهائي والمحاكمة طبعة 2017-2018 مزيدة ومنقحة بالتعديلات، دار هومة للطباعة والنشر والتوزيع، الجزائر،
5. علي شملال المستحدث في ق إ ج، الكتاب الثاني، التحقيق والمحاكمة، نسخة معدلة ومتممة 2017، دار هومة للطباعة والنشر والتوزيع، الجزائر.
6. فاضل زيدان حمد "سلطة القاضي الجنائي في تقدير الأدلة دراسة مقارنة" دار الثقافة للنشر والتوزيع طبعة 2006.

ثالث – أطروحة الدكتوراه:

1. كريمة خطاب، قرينة البراءة، أطروحة الدكتوراه ، جامعة الجزائر 01 كلية الحقوق ،السنة الجامعية 2014-2015 .

رابعا – المقالات :

2. بن عيرد عبد الغني، بضياف هاجر "التقاضي الالكتروني عبر ضوء أحدث التعديلات بين التطلعات والتحديات"، مجلة الدراسات والبحوث القانونية، مجلد 6، العدد 2 (2021).
3. بن قلو ليلى، "المحكمة الالكترونية بينن المفهوم والتطبيق"، مجلة البحوث القانونية والاقتصادية، المجلد 04، العدد 2 (2011).
4. عصماني ليلى "نظام التقاضي الالكتروني آلية لإنجاح الخطط التنموية" مجلة المفكر، العدد 13، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة.
5. يزيد بوحليط، خليل الله خليفة "المحاكمة عن بعد: سرعة الإجراءات أم إهدار للضمانات" مجلة العلوم القانونية والسياسية، المجلد 12، العدد 01، أفريل 2021، ص 890.
6. يوسفي مباركة، حنان عكوش "التقاضي الالكتروني في الجزائر"، مجلة الحقوق والعلوم الإنسانية، المجلد 15، العدد 1، (2022).

المراجع باللغة الفرنسية

1. Code de procédure pénale français gilbert azibert 2014 lexis-nexis .
2. Jerome Bossan « la visioconférence dans le procès pénal ; un outil à maitriser » revue de science criminelle et de droit pénal comparé n°= 2011/4 .
3. Laurence dumoulin et christian licoppe « justice et visioconférence : les audiences à distance genèse et institutionnalisation d'une Um ovation, télécom paris tech 13 version :20 nov 2009 .
4. Laurence dumoulin, « la visioconférence dans le droit pénal : une solution pragmatique devenue le vecteur d'une politique managériale de la justice » entretien, LEXIS-NEXIS-sa droit pénal n°= 36 juin 2018.

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة الجزائر 1

الملتقى الدولي الافتراضي الموسوم بالقانون الجنائي في ظل التطور التكنولوجي اشكالات و معالجات

المحور الخامس بعنوان تأثير الوسائل العلمية الحديثة على الإثبات الجنائي

عنوان المداخلة :

الطب الشرعي الرقمي كآلية مستحدثة في الإثبات الجنائي

Digital forensics as an emergingmechanism in criminal proof

ط.د جديدي ضياء الدين رمضان

معهد الحقوق و العلوم الاقتصادية ، المركز الجامعي احمد بن عبد الرزاق حمودة – سي الحواس – بريكة

مخبر افاق الحوكمة للتنمية المحلية المستدامة

dhiaeddine.djedidi@cu-barika.dz

ط.د دراجي شهرزاد

معهد الحقوق و العلوم الاقتصادية ، المركز الجامعي احمد بن عبد الرزاق حمودة – سي الحواس – بريكة

مخبر افاق الحوكمة للتنمية المحلية المستدامة

Chahrazed.deradji@cu-barika.dz

الملخص:

على مدار السنوات القليلةالماضية برز دور الطب الشرعي الرقمي الى الواجهة كطريقة مهمة لتحديد ومحاسبة مجرمي الأنترنت ؛ فعرف هذا النوع منالطب الشرعي على انه تطبيق المعلومات التقنية لضمان العرض الصحيح لبيانات اثبات الجرائم الإلكترونية في المحاكم ،مع ضمان الحفاظ على سلامة هذه الأدلة الرقمية بشكل أساسي خلال جميع مراحل التحقيق، وذلك في سبيل تعزيز الثقة في وسائل الإثبات الرقمية و إعطاءها درجة من اليقينية تجعلها حجة ومرجعا للإثبات امام القضاء الجزائي.

فالهدف النهائي من عملية الطب الشرعي الرقمي هو الحصول على الأدلة من اجل الإجابة على جملة من الأسئلة الرئيسية تتمثل في : ماذا حدث ؟ واين حدث ؟ ولماذا حدث ؟ وكيف حدث؟. تؤدي الإجابة على هذه الأسئلةالى تأكيد او نفي مزاعم القضية ، و اثباتوقوع الجرائم الإلكترونية ونسبها لمرتكبها ، تحقيقا لضمانات المحاكمة العادلة.

الكلمات المفتاحية : الطب الشرعي الرقمي ؛ الجرائم الإلكترونية ؛ البيانات الإلكترونية ؛ حجية الأدلة الرقمية ؛ الاثبات الجنائي ؛ الشرعية الجزائية .

Abstract:
Over the past few years, the role of digital forensics has come to the fore as an important method for identifying and holding cybercriminals accountable; This type of forensic medicine is defined as the application of technical information to ensure the correct presentation of evidence of electronic crimes in the courts, while ensuring that the integrity of this digital evidence is fundamentally preserved during all stages of the investigation, in order to enhance confidence in digital means of proof and give it a degree of Certainty makes it an argument and a reference for proof before the criminal judiciary.The ultimate goal of the digital forensics process is to obtain evidence in order to answer a number of key questions: What happened? And where did it happen? And why did it happen? How did it happen? . Answering these questions will lead to confirming or denying the allegations of the case, and proving the occurrence of cyber crimes and attributing them to the perpetrator, in order to achieve the guarantees of a fair trial.

Keywords: digital forensics; cybercrimes; electronic data; Authentic digital evidence; criminal proof; Criminal legitimacy.

مقدمة:

اصبح التفكير الرقمي في الواقع الحديث امرا شائعا و جزء لا يتجزأ من الحياة اليومية للفرد و المجتمع ، فالعديد من الأشياء التي كنا نعتبرها في الماضي خيالا علميا اضحت امرا واقعا لا مفر منه في العصر الحالي ؛ بداية من أنترنت الاشياء بناء على نظم التعاون المركزي التي تعد اساس نظام البلوكشين المستخدم في العملات الرقمية ، مرورا بنظام اقتصادي جديد يعتمد في اساسه على البيانات ، انتهاءا بنظام التقارب المادي الرقمي الذي دمج بين العالمين المادي و الرقمي كخطوة حيوية لرقمنة المجتمع.

ادى هذا التطور و بالرغم مما جلبه من مزايا ساهمة بشكل ايجابي في تسهيل اسلوب حياتنا الى ارتفاع معدل الإجرام عبر الانترنت بشكل متزامن جنب الى جنب مع نمو النشاط الاجتماعي الرقمي للمجتمع ، هذا التزامن مع التطور التكنولوجي جعل في المقابل مجرمي الانترنت اكثر ابداعا و ابتكارا ، مما خلق تحديا جديدا في مجال الإثبات الجنائي ، فقبول الادلة العلمية في محكمة قانونية يستلزم تطبيق تقنيات تحقيق معينة لتأكيد حادث امني وقع فعلا او محتمل الوقوع ، غير ان هذه التقنيات ركزت في الاساس على استخلاص الادلة الرقمية التقليدية استنادا على اجهزة الكمبيوتر المكتبية و الخوادم التي تكون غالبا خاضعة لسيادة الدولة علي فضائها الرقمي مما يبرر الاعتماد الكلي علي الهيئات العامة في التحقيق ، لكن في المقابل فإن تطور التكنولوجيا الحديثة في الوسائط و المنصات الرقمية و أثرها على نشاط المجتمع استلزم ايجاد الية فعالة لتحقيق في المجالات الفرعية الأخرى بما في ذلك الاجهزة المتنقلة و قواعد البيانات و الشبكات و المنصات القائمة علي السحابة و أنترنت الاشياء ؛ و ذلك في سبيل إيجاد منظومة تقنية حديثة تختص بشكل اساسي في التحقيق الرقمي يشتى انواعه مما سوف يساهم بشكل فعال في الوصول الى الادلة الرقمية وتسهيل مهمة الإثبات الجنائي امام القضاء.

تتجلى اهمية هذه الدراسة في بيان فرع جديد من فروع الطب الشرعي الذي تزامن ظهوره مع تطور البيئة الرقمية الا وهو الطب الشرعي الرقمي الذي يعد امتدادا لطب الشرعي الحاسوبي ومدى فاعليته في الاثبات الجنائي ، لذلك سوف تتمحور هذه الدراسة للإجابة علي الاشكال التالي :

فما مدى فاعلية الطب الشرعي الرقمي كألية مستحدثة في الإثبات الجنائي ؟

نهدف من خلال هذه الورقة البحثية الي بيان ماهية منظومة الطب الشرعي الرقمي كآلية ناتجة عن تقاطع التكنولوجيا الرقمية و انتهاكات القانون ، خاصة في ظل ما تواجهه وحدات الشرطة المتخصصة من تحديات ناتجة عن تسارع حجم عبء العمل حيث اصبح الجريمة الإلكترونية مشكلة اجتماعية أكبر مما كانت عليه ، ولم يقابلها تطور في موارد الوحدات و تحسين في مستوى المهارات والتدريب داخل الوحدات بالشكل

الكافي لمعالجة الطبيعة الفريدة للإثبات الجنائي في البيئة الرقمية و التعقيدات المتزايدة في ضبط الجريمة الإلكترونية.

اعتمدنا من خلال هذه الدراسة علي المنهجين الوصفي و التحليلي و ذلك في سبيل بيان ماهية منظومة الطب الشرعي الرقمي وكذا اظهار موقف المشرع الجزائري من حجية الادلة الرقمية .

و للإجابة علي الإشكالية سابقة الذكر ارتئينا تقسيم خطة البحث الى محورين نتناول في المحور الأول ماهية الطب الشرعي الرقمي اما المحور الثاني فنخصصه لدراسة حجية دليل الطب الشرعي الرقمي وفقا لتشريع الجزائري

المحور الأول: ماهية الطب الشرعي الرقمي

لقد اعادت تقنيات الانترنت واجهزةالكمبيوتر والهواتف الذكيةالمحمولة تشكيل المجتمع الحديث بشكل كبير ، فظهور شبكة الويب العالمية والهواتف الذكية والاتصالات التي تتم بواسطة الكمبيوتر قد اثر بشكل كبير على طريقة التي يتفاعل بها الاشخاص عبر الانترنت او خارجها ، ولذلك قد تزايد عدد الأفراد الذين ينخرطون في اعمال غير مقبولة اجتماعيا عبر الفضاء الرقمي لما يوفره من سريه في التواصل و فرص لا تحصى لارتكاب الاخطاء وسوء استعمال التكنولوجيا ، وبالتالي ازدادت الحاجة الى سبل لإثبات هذه الجرائم الإلكترونية؛ ومن هنا تبرز اهمية الطب الشرعي الرقمي كعلم في الاثبات الجنائي و هو الذي سوف نتناول ماهيته على النحو التالي:

أولا :مفهوم الطب الشرعي الرقمي

تتكون الأدلة في مجال الجنائي الرقمي من مستندات ، يتكون كل منها من سلسلة من البيانات يتم تقديمها في مسألة قانونية ما لمساعدة القضاء في اثبات وقائع القضية[1] ، هذه الأدلة لا تقدم عادة من طرف أطراف القضية كما هو الحال في الجرائم التقليدية بل يلزم لتقديمها أشخاص مؤهلون باستخدام منهجية معينة بشكل صحيح وهذه المهمة تسند في الأساس الى ما يسمى بالطب الشرعي الرقمي.

1. تعريف الطب الشرعي الرقمي

لقد اصبح الطب الشرعي الرقمي في الواقع الحديث أحد اكثر مجالات البحث شهرة في علوم الكمبيوتر نظرا لطبيعته المتأصلة في توفير وسائل للحصول على الأدلة وفحصها وتحليلها والابلاغ عنها لاستخدامها في المسائل القانونية[2]، فمع تزايد عدد الأجهزةالرقمية في مجتمعاتنا زادت الحاجة في المقابل لنظام لتتبع الأدلةالرقمية في التحقيقات والمحاكمات الجنائية؛ التي يجب ان تعتمد في الاساس على أدلة جيدة لضمان

الإدانات، والطب الشرعي الرقمي كعلم جنائي هو المسؤول عن هذا الضمان لتأكيد ثقه المحكمة بالأدلة الجنائية[3].

وكاستجابة لهذه الحاجة وفي سبيل مكافحة الجرائم الإلكترونية كان على الحكومات والمنظمات تطوير وسائل لإجراء التحقيقات في مثل هذا النوع من الجرائم ذات الصلةبالبيئةالرقمية ، وعلى الرغم من ان هذا التحقيق مشابه للتحقيق التقليدي لما في ذلك من جمع للبيانات واعادة بناء مسرح الجريمة في محاوله لمعرفه المسؤول عن الحادث او ربما اتخاذ اجراءات قانونية معينة ، الى ان استخدام مصطلح الطب الشرعي الرقمي يقصد به الدلالة على الاستحواذ والحفظ والتحليل وعرض الأدلةالرقميةالمنتجة في جرائم الكمبيوتر والجرائم الرقمية بصفة عامة، فالطب الشرعي الرقمي يعرف عادة على انه العلم الذي يهتم بالعلاقة بين البيئةالرقمية والقضايا القانونية في سبيل تحديد الدليل الرقمي في إجراءات التحقيق ، ويجمع هذا النوع من الطب الشرعي بين الكمبيوتر ومفاهيم العلوم بما في ذلك هندسة الكمبيوتر وانظمة تشغيل والملفات والبرمجيات وكذلك الاجراءات القانونية ذات الطابع الجنائي والتقاضي المدني والقانون السيبراني وقواعد الاثبات[4].

و تشمل عملية الطب الشرعي الرقمي ؛ تحديد النشاط الذي يتطلبه التحقيق بما في ذلك تحديد المصادر الرقمية ذات الصلة وجمع المعلومات والحفاظ عليها من المتغيرات المقصودة والغير مقصودة، وتحليل المعلومات والابلاغ عن نتائج الفحص[5].

فالطب الشرعي الرقمي او السيبراني كما يشار إليه احيانا يتضمن تطبيق العلم لجعل الأدلة في المحاكمة اكثر وضوحا .

2. **نطاق الطب الشرعي الرقمي**

بداية وكما سبق الذكر فان الطب الشرعي الرقمي هو فرع من فروع علم الطب الشرعي ، يهتم باستخدام المعلومات الرقمية التي يتم انتاجها وتخزينها ونقلها بواسطة اجهزة الكمبيوتر في التحقيقات والاجراءات القانونية؛ فلا طالما كان الطب الشرعي الرقمي موجودا منذ ان خزنت اجهزة الكمبيوتر البيانات التي يمكن استخدامها كدليل في الإثبات[6].

ومع تطور الأجهزةالإلكترونية وبقاء الهدف من عمليه الطب الشرعي الرقمي هو الدليل الرقمي ؛ شملت هذه العمليةبالإضافة الى اجهزة الكمبيوتر ؛ الكاميرات الرقميةوالأجهزةاللوحية واجهزة الالعاب والهواتف المحمولة ، وشبكات الانترنت المتصلة في ذات الأجهزةبيما في ذلك رسائل البريد الالكتروني والتواصل الاجتماعي الرقمي ،بالإضافة الى الوسائط الرقمية التي تدعم ذات الأجهزةالسابق ذكرها، مثل الاقراص المضغوطة والاقراص المرنة والاقراص الرقميةمتعددة الاستخدامات[7].

وما تطور البيئةالرقميةايضا أدى التصغير المستمر للأجهزة وزيادهالكفاءة الى امكانيه دمج الذكاء في الأجهزةالعادية ، فازدادت الأجهزةاليومية غير الذكية ذات القدرات الحسابية او ما يعرف بأنترنت الاشياء مع مجموعة متنوعة من التطبيقات ؛ مثل تشغيل الالي للمنزل والشبكات والمدن الذكية وادارة البنيه التحتيةالحيوية مما جعلها هدفا لمختلف الهجمات الكترونية[8] .

وفي النهاية ومع تطور المستمر للبيئةالرقمية فان نطاق الطب الشرعي الرقمي يشمل جميع مجالات الفضاء الرقمي والأجهزةالتابعة له .

3. **ضوابط الطب الشرعي الرقمي :**

يشمل الطب الشرعي الرقمي العديد من العوامل التي يجب استفاؤها قبل امكانية الحصول على الأدلة ،فيتضمن كل من المجالات الاستقصائيةوالتقنية والعلاقات الإنسانيةوالقانونية ، فيجب على محقق الطب الشرعي الرقمي التأكد من أن عمليةالتحقيق تستوفي هذه العوامل في جميع الاوقات؛ من خلال التقييد الصارم بجوانب وظيفته ، لان هذا يمكن ان يؤثر بشكل كبير هذا نتائج التحقيق، وهذا يرجع في الاساس الي ان حقيقة الهدف العام من التحقيق هو جمع وتحديد وحفظ الأدلةالرقمية التي يمكن استخدامها في نهاية المطاف في المحاكم[9].

وتتغير هذه العوامل بسبب التغيرات السريعة في التكنولوجيا التي يستخدمها الافراد ، مما يستوجب على منهجيات وادوات الطب الشرعي الرقمي ايضا ان تواكب هذه التغيرات فهي جزء مهم في التحقيقات الجنائيه للجرائم الإلكترونية وجمع الأدلةالرقمية في القضايا المعروضة امام المحاكم[10].

كما يجب ايضا ان يكون الافراد الذين يتعاملون مع هذه الأدلة مدربين وعلى دراية كامله بالمجال حتى ، تكون قراراتهم سليمه وصحيحة؛ مما يساهم في قبوليه الأدلة امام المحكمة، مما يستلزم تدريبات رسمية للعمل مع الأدلةالرقمية او اجراءات التحقيق في الطب الشرعي الرقمي[11] ، مع ضرورة توحيد كيفيه الحصول على الأدلة والحفاظ عليها، فيجب ان تدرك المنظمات البحثية؛ ان الطب الشرعي الرقمي يتطلب اكثر بكثير من مجرد شخص يميل تقنيا للتحقيقات الرقمية فالكميات الهائلة من البيانات اليوم وتقنيات المعلومات والاتصالات الغير متجانسة والبنيه التحتيةالسبيرانية ، تشكل تحديا كبيرا لخبراء الامن ووكالات تطبيق القانون التي تحقق في الجرائم الإلكترونية[12] .

ومع اعتماد الطب الشرعي الرقمي على الاشكال المختلفةللأدلة في التحقيقات الجنائيه المعقدة ، فإن التدابير المتخذة لضمان جودتها تواجه تدقيقا متزايدا لضمان التطبيق السليم للمبادئ العلمية والتفسير الدقيق للنتائج والابلاغ عنها ، في سبيل إبراز ادلة علم الطب الشرعي الرقمي ، وذلكلتوفير ضمانات لجميع المشاركين

في نظام العدالة الجنائيه ،خاصة لما يواجهه هذا المجال من الطب الشرعي من نقص مقارنة بالعلوم الشرعية الاخرى بصفته احد احدث الفروع في الطب الشرعي[13].

ثانيا : أساسيات عملية الطب الشرعي الرقمي

عاده ما تكون ادلة الطب الشرعي كامنة حيث لا يمكن الوصول اليها الا من خلال محاولة اكتشاف الحقيقة على المستوى المطلوب من التفاصيل ، وذلك من خلال استخدام جملة من الأدوات والتقنيات .

غير ان استخدام هذه الادوات والتقنيات لا يكفي وحده لضمان جودة الادلةالرقمية في الاثبات ، بل يجب ان يتم استخدامها بشكل صحيح وفقا لمعايير قانونية ، بيد اشخاص مؤهلين؛ فالعامل البشري ايضا يلعب دورا هاما في هذه العملية ولذلك سوف نتناول اسس عملية الطب الشرعي الرقمي وفقا لما يلي:

1. **الاتساق القانوني لعملية الطب الشرعي الرقمي**

يعد الطب الشرعي الرقمي جزء حيويا في كل تحقيق جنائي ، نظرا لكمية المعلومات المتاحة والفرص التي تتيحها البيانات الإلكترونية للتحقيق في الجريمة واثباتها ، ومع ذلك فإجراءاتالعدالة الجنائية غالبا ما تنظر نظرة شك وعدم يقين في الدليل الجنائي الرقمي ، ففي الوقت الحاضر وعلى المستوى الدوليتعرض إستخدام تقنيات الطب الشرعي الغير المثبتة علميالانتقادات شديدة في الاجراءات القانونية[14]؛ لذلك كان واجبا النظر الى الأدلةالرقمية في ضوء السياق القانوني للمسألة قيد النظر ويتضمن هذا السياق على سبيل المثال للحصر ما يلي :

تحديد القوانين والعمليات القانونية المعمول بها والنظريات القانونية والمنهجيات ، وتطبيق تلك المنهجيات ومتطلبات قبول الأدلة وقبول الشهود الخبراء، والعديد من المعايير الاخرى المماثلة التي تؤثر على الأدلة الجنائيةالرقمية واستخدامها.

طبيعةالقضية سواء كانت مدنيه او جنائية ؛ بحيث تؤثر هذه الفروق الفرعية على معايير الاثبات و المقبولية وقواعد المحاكمة ، والعديد من الجوانب الاخرى التي يمكن استخدامها في المسالةالقانونيةالتي يتم دعمها من خلال الأدلة الجنائية[15].

القيود المفروضة على عناصر القضية مثل عمليات البحث والمصادرة والتي قد تكون فورية او بعد الواقعة، او الزامية او تصريحية ، و مضبوطةبطرق محددةلضمان عدم التعسف بها ، وتشكل هذه الطرق السياق التي يجب ان يعمل فيه فاحص الطب الشرعي الرقمي[16].

الآجالالقانونية؛ ففي كثير من الحالات يكون هناك القليل من الوقت للقيام بالإجراءات التي تتعلق بأدلة الطب الشرعي الرقمي ، كما قد تؤثر هذه الآجال على التسلسل الذي بتم به التعامل مع الأدلةالرقمية[17].

التكلفة كذلك عامل مهم لان الموارد الماليةالمتاحةمحدودة في حين انه قد يكون هناك نطاق هائل من التحليل الذي يمكن اجراءه ، وبالتالي قد لا يتم اجراء الكثير من التحليلات بسبب قيود التكلفة.

وفي النهاية فان الاتساق مصطلح يجب استخدامه بحذر في سياق الطب الشرعي الرقمي ، يشير معناها الي طريقة اداء منتظمة وقابلة للتكرار في ما يتعلق بإجراءات التحليل الجنائي ، يكون هذا السلوك مرادفا لسمات الموثوقيةوالجدارة ، التي توفر بدورها اساسالاستخلاص نتائج يمكن الاعتماد عليها في سياق عملية التحقيق فيعتبر الاتساق بشكل عام علامة على الجودة ومعيار اساسي يجب تحقيقه في جميع جوانب عملية الطب الشرعي الرقمي[18].

2. العامل المعرفي و البشري في عملية الطب الشرعي الرقمي

تعتبر قراراتالأطباء الشرعيين حاسمة في تحقيقات الشرطة واجراءات المحاكمة ،لأنها تساهم بشكل كبير في الفصل في القضية المعروضة امام المحكمة[19]،ولكن ورغم اعتماد فاحصي الطب الشرعي الرقمي على ادوات الذكاء الاصطناعي الى ان عملية الطب الشرعي الرقمي تفرض ازدواجية الادراك وذلك بتفاعلفاحصي الطب الشرعي الرقمي بشكل تحليلي مع كل توصية وشرح فردي لذكاء الاصطناعي[20] ، لذلك غالبا ما تكون أحكام الطب الشرعي الرقمي نتيجة للتقييم البشري وبالتالي فهي ذاتية وعرضة للتحيز[21] ؛ ومن هنا تبرز اهمية العامل المعرفي والبشري في عملية الطب الشرعي الرقمي ،ولكن وقبل التطرق لهذه العوامل فتجدر بنا الإشارة الى ان التحيزاتالمعرفية؛ يقصد بها تلك التحيزات التي قد تنشأ من كيفية معالجة العقل للمعلومات ، وليست قضايا اخلاقية التي قد تنشأ عن نقص في التدريب او دوافع ذاتية او نقص في الكفاءة، فالمقصود هنا تلك التحيزات التي تكون نتيجةلمفاضلات العقل الحسابية التي تحدث في الدماغ[22] ، وبالتالي فهي ليست افعال مقصودة ، ومن بين اهم العوامل التي قد تؤثر على قرار عمليه الطب الشرعي الرقمي مايلي :

1.2العوامل التنظيمية و الثقافية :

تتضمن هذه العوامل التفاعلات الاجتماعية والتعرف على الايديولوجيات والمنظمات والتواصل مع الاخرين ، حيث يمكن ان تتسبب الكلمات المستخدمة والمصطلحات والمفردات في حدوث اخطاء في كيفية تفسير المعلومات وفهمها ، وقد يؤثر تدفق المعلومات بين الأنظمة والمنظمات والكيانات المختلفة في الهيكل التنظيمي ايضا على الفاحص البشري وتحيز عمله ، والامر الاكثر اثارة للقلق هو كيف يمكن ان يتعاقب التحيز

ويتراكم بين العناصر المختلفة يفترض انها مستقله تشارك في التحقيقات الجنائية ، فإن كان خبراء الطب شرعي الرقمي يعتقدون انهم يعملون من أجل الادعاء او الدفاع ؛ فقد يؤثر هذا بشكل كبير على استنتاجاتهم[23].

فعلا الرغم من ان جهات التحقيق الرقمي ملزمة بالحياد والموضوعية اثناء التحقيق او المحاكمة، فإن تبعيتها لصالح الادعاء او الدفاع قد يؤثر بشكل كبير على كيفية ملاحظاتهم وما يخلصون إليه بشأن الأدلةالرقمية وكيفية تقديم هذه الأدلةللمحكمة.

2.2 المواد المرجعية :

تشكل المادةالمرجعية عاملا اساسيا في التحيز، فهي تقوم احيانا بدلا من الدليل الفعلي بتوجيه العمليةالمعرفية ، وفي الطب الشرعي الرقمي يمكن استخدام هذه المواد المرجعية ؛ فعلى سبيل المثال عندما يتم تكليف الفاحص بتحديد ما اذ كان ملف معين مثل صورة او مستند او مقطع فيديو موجود فعلا على جهاز الكمبيوتر ، فسوف يتم تنفيذ المهمة عن طريق البحث عن التطابق، وفي مثل هذه الحالة سوف يكون هناك حاجه قليلة لتفسير ، وبالتالي هناك خطر منخفض لقرار متحيز[24].

ومع ذلك فهناك مهام يمكن ان تؤدي فيها المواد المرجعية الى التحيز في تفسير الأدلةالفعلية ، فغالبا ما يستخدم الدليل الرقمي بالتحقيق مع المعلومات التي يتم الحصول عليها من خلال التحقيقات الاولية ، لذلك فغالبا ما يتعرض الفحص الرقمي للكثير من المعلومات المتحيزة اكثر مما هو ضروري لأجراء مهمة التحقيق[25] ، و لتفادى هذا التحيز فان الفاحص الرقمي لا يحتاج الى البيان الكامل ولا لكل التفاصيل ، ولكن بعض المعلومات الأساسية من البيان يمكن ان تشكل له مرجعا كافيا للتحقيق.

3.2 دليل المسألة الخاضعة للتحقيق (دليل الحالة) :

يشكل دليل الحالة نفسها اكثر العوامل المسؤولة عن التحيز المعرفي ، وتشمل هذه الفئه انواعا مختلفة من الأدلة التي يتم الحصول عليها من خلال التحقيق ، فيمكن ان يكون الدليل مصدرا للتحيز اذ كان يتضمن بطبيعته معلومات متحيزة ؛ ضمن الدليل نفسه او قد يكون الجهاز الرقمي المضبوط متحيزا في حد ذاته نظرا لأنه قد يحتوي على بعض المعلومات ؛ مثل العلامات والاسماء او الملصقات او بعض الخصائص الاخرى التي يمكن ان تؤثر على الملاحظات والقرارات ،و علاوة على ذلك فقد يكون الدليل في حد ذاته متحيزا[26]، ومن امثله ذلك : صور الاعتداء الجنسي او سجلات الدردشة حول التخطيط لهجوم الارهابي او سجل البحث على الانترنت ينقل عبارات للبحث حول كيفيه الافلات..... الخ .

3.مراحل عملية الطب الشرعي الرقمي

التحليل الجنائي الرقمي ضرورةحيوية في سبيل تحقيق محاكمة ناجحة لمجرمي الانترنت[27] ، و لإجراء تحقيق جنائي ناجح هناك عدد من الخطوات المهمة التي يجب مراعاتها واتخاذها خطوة بخطوة لجمع الأدلةالمناسبة وعرضها في محكمة قانونية ، وتتمثل الخطوات الأساسية في عمليه الطب الشرعي الرقمي في ما يلي:

1.3 تحديد الأدلة وجمعها :

نظرا لخصوصيةالجريمةالإلكترونيةفمن الشائع ان يكون هناك قدر هائل من الأدلةالمختلفةوالمتاحة لمسأله قانونية واحدة ، فمن المنطق ان لا يتم تحديد الغالبية القصوى من الأدلةالمحتملة ؛ و كمثال لذلك ضعفي الاعتبار ان كل سلسلةللأحداث داخل جهاز كمبيوتر واحد قد تتسبب في تفاعلات مع الملفات وانظمة الملفات التي توجد بداخلها ، والعمليات الاخرى والبرامج التي ينفذها ، والملفات التي ينتجها ويديرها و نظرا لطبيعة البيئةالشبكية يمتد هذا ليشمل جميع الأجهزةالمتصلةبالشبكة[28]

ولذلك فان التحديد الدقيق للأدلة ذات الصلة له دور مهم في انجاح عمليه التحقيق الجنائي الرقمي ومن اجل استخدام هذه الأدلة في المحكمة وجب جمعها بطريقه تحافظ على سلامتها طول عملية التحقيق الجنائي الرقمي من قبل فاحصي الطب الشرعي الرقمي .

2.3 حفظ البيانات :

يعد حفظ البيانات الخطوة الاولى في الكشف عن الأدلةالرقمية ويحدث هذا الحفظ اثناء مرحلة الجمع والاستحواذ في تحقيقات الطب الشرعي الرقمي ، ويشير الهدف من الحفاظ على الأدلة في الطب الشرعي الرقمي إلى عمل نسخ من الملفات الأصلية لفحصها بطريقه تقلل من إمكانيه اجراء اي تغيير على ملفات البيانات الأصلية ، تماما كما هو الحال في اي علم جنائي فمن المهم حمايه مسرح الجريمة من اجل الحفاظ على سلامةالأدلة[29] .

ولذلك وجب الحفاظ على الأدلةالرقمية تماما مثل الحفاظ على الاشكال التقليديةالمادية الاخرى ، وما يجعل الطب الشرعي الرقمي اكثر خصوصية هو حقيقة ان الحفظ المقصود يشير بشكل خاص الى القدرة على عمل نسخ مكررة من الأدلةالرقميةالأصلية.

3.3 تحليل البيانات :

تشير مرحلة التحليل الى تفسير واعادة بناء مسرح الجريمة ، ومع ذلك فإن هذه المهمة ليست مهمة سهله ؛ بسبب الكميات الكبيرة من الأدلة التي يتم الكشف عنها اثناء التحقيق الرقمي ، لذلك فان احد اهم

الخطوات في مرحلة التحليل للتحقيق الجنائي الرقمي هي تصفيةالأدلة وتقليلها ، فيفسر فحص الطب الشرعي الرقمي فقط تلك الملفات ذات الصلة بالتحقيق .

لذلك فقد تتضمن هذه العملية ازاله الملفات المكررة او البحث عن الكلمات الرئيسية او تجميع البيانات بناء على انواع الملفات فالهدف النهائي من تقليل البيانات وترشيحها هو انشاء اصغر مجموعة بيانات مع أعلى إمكانية لإحتواء الأدلةالرقمية ذات الصلة[30].

4.3 عرض الأدلة الرقمية

يجب تقديم الأدلة والتحليل والتفسير والاسناد في نهاية المطاف في شكل تقارير وشهادات ، يواجه هذا العرض العديد من التحديات ولم يتم تناوله الا في نطاق محدود من الدراسات لكون هذا العرض التقديمي يعتبر فنا أكثر من كونه علما[31]، لكن هناك بعض الضوابط في تقديم هذه الأدلة نذكر منها:[32]

- ان يكون الدليل الوارد في التقرير ذوصلة بالتحقيق
- ان يكون الدليل الرقمي الوارد في التقرير يتعلق مباشرة بوقائع القضية
- ان يتناول التقرير بالتفصيل كيفية تحديد الأدلة ذات الصلة بالتحقيق
- الشفافيةالكاملة ؛ بمعنى ذكر جميع الخطوات بالتفصيل حتى لا يترك اي غموض في عملية الطب الشرعي الرقمي
- ان يكون فنيو الطب الشرعي الرقمي على استعداد للإدلاء بشهاداتهم امام المحكمة ن
- ان يضل فاحص الطب الشرعي الرقمي موضوعيا عند استخلاص النتائج من الأدلةالرقمية

المحور الثاني : حجية دليل الطب الشرعي الرقمي وفقا لتشريع الجزائري

لقد زامن التطور التكنولوجي لوسائل المعلوماتية ظهور أنماط جديدة و خطيرة من الجرائم استغلت هذا التطور لتجديد نشاطها الإجرامي والتوسع في نطاقها الشخصي والمكاني، فقد أصبحت الجريمة في وقتنا الحالي ترتكب بوسائل تقنية و فنية جد متطور جعلت وسائل الإثبات الكلاسيكية و التقليدية تقف عاجزة أمامها، وهو ما استلزم على المشرع الجزائري البحث عن آليات و ميكانيزمات تواكب هذا التطور فكان الطب الشرعي؛ الذي يستخدم وسائل تقنية معينة في استنباط الأدلة الرقمية للكشف عن وقوع الجريمة ونسبها الى مرتكبيها ثم نقلها الى الواقع، أحدث ما توصلت اليه السياسة الجنائية المعاصرة ولكن بمقابل ذلك أصبحت مسألة الاثبات

الجنائي[33]عن طريق نظم الحاسوب و الفضاء الرقمي تثير إشكالات عديدة في مدى مشروعية و حجية هذه الأدلة الرقمية[34] بالإضافة إلى تقدير سلطة القاضي الجزائي في الأخذ بها على اطلاقه، وهو ما سنتطرق إليه بالدراسة وفقا لما يلي:

أولا: ضوابط قبول دليل طب الشرعيالرقمي في الاثبات الجنائي

ترتكز القيمة القانونية للدليل الرقمي المستمد من الحاسب الآلي؛ في مدى توفره على الشروط اللازمة التي تثبت صحته و يقينيته في دلالته على الوقائع المراد إثباتها، فبالنظر الى الطبيعة الخاصة التي تنفرد بها هذه الأدلة وذلك لارتباطها بالعالم الافتراضي وجب خضوعها الى القواعد المقررة قانونا لنظام الاثبات حتى تكتسب مشروعيتها أمام القضاء الجزائي، ومن بين الشروط التي يجب أن تحوزها الأدلة الرقمية نذكر:

1. **مشروعية دليل طب الشرعيالرقمي في الاثبات الجنائي**

تقوم قاعدة الإثبات في النظام الإجرائي على مبدأ الشرعية و الذي يقضي «أن تخضع جل إجراءات المتابعة الجزائية – بمختلف أطوارها و مراحلها– لقانون الإجراءات الجزائية"[35]

وبالتالي فالدليل الرقمي لا يكون مشروعا أو مقبولا في عملية إثبات واقعة قانونية إلا إذا كانت الاجراءات التي تم البحث و الحصول فيها على الدليل الرقمي ثم تقديمه أمام القضاء، قد تمت وفقا للقواعد المقررة قانونا ضمن أحكام قانون الإجراءات الجزائية و الذي يكفل تحقيق التوازن بين حق الدولة في العقاب و بين ضمان حق المتهم في محاكمة عادلة[36].

1.1 **مشروعية وجود دليل طب الشرعيالرقمي**

يحكم قواعد الإثبات الجنائي نظامين أساسيين يتمثلان في نظام الإثبات المقيد و الذي يتم فيه تقييد السلطة التقديرية للقاضي الجزائي في مسألة تقدير مشروعية الدليل الجنائي، فدور القاضي حسب هذا النظام يقتصر على فحص الدليل و التأكد من توفر الشروط التي حددها القانون؛ الذي يتم من خلاله حصر مجمل الأدلة الجنائية التي يجوز للقاضي الأخذ بها وقوتها لإقناعيه ، و بالتالي فإن لم ينص القانون صراحة على مشروعية الدليل الرقمي لا يمكن للقاضي الجزائي الأخذ به، بخلاف نظام الإثبات الحر الذي يمنح للقاضي الحرية المطلقة في تقدير الأدلة الجنائية لإثبات الوقائع المعروضة عليه، و بالتالي لا تثور هنا أي إشكالية بخصوص مسألة مشروعية الدليل الرقمي في إطار هذا النظام وهو ما أخذت به السياسة الجنائية الجزائرية[37]طبقا لنص المادة 212 من قانون الاجراءات الجزائية[38].

2.1 **مشروعية الحصول على دليل طب الشرعيالرقمي**

نظرا للطبيعة الخاصة للدليل الرقمي وذلك باعتبار أن جميع إجراءات الحصول عليه تمس بحقوق الأفراد و حرياتهم، ومنه فإن شرعية الإثبات الجنائي يستوجب عدم قبول أي دليل رقمي تأتى بطريقة غير مشروعة، فعملية الحصول على هذه الأدلة التي تتم عن طريق تشريح للبيانات والبرمجيات الرقمية أن تتقيد باحترام جميع ضمانات المتهم المكرسة دستوريا و التي لا يمكن تجسيدها إلا بتطبيق قواعد الشرعية الإجرائية، ومن بين شروط صحة الحصول على الدليل الرقمي نذكر:

- يجب الحصول على الدليل بصورة مشروعة تراعى فيها جميع ضمانات المتهم المكرسة دستوريا و الشرعية الإجرائية.
- العمل على تأمينالبيانات والمعلومات المتحصل عليها بما يحافظ على سريتها، وعدم إختراقها أو تلفها أو الإفصاح عنها.
- يجب أن يتم الحصول على هذه الأدلة بناءا على أمر مسبب من الجهات القضائية المختصة من أجل إثبات واقعة قانونية[39].

2. يقينية دليل طب الشرعيالرقمي في الاثبات الجنائي

تدخل الأدلة الجنائية الرقمية في تكوين قناعة القاضي الجزائي في حل القضايا المعروضة عليه وبالتالي فإن اصدار الأحكام القضائية يتم بناءا على ما تم عرضه عليه من الأدلة المستخلصة من جهاز الحاسب الآلي، و من هنا تكمن أهمية الأدلة لما لها من علاقة مباشرة لما سيؤول اليه مضمون الأحكام القضائية.

1.2 مفهوم مبدأ يقينية دليل طب الشرعيالرقمي

يقصد بمبدأ يقينية الدليل الرقمي "حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التأكيد."[40]

2.2 الشروط التي تحكم صحة يقينية دليل طب الشرعيالرقمي

يشترط لقبول صحة الدليل الرقمي أمام القضاء الجزائي اشتماله على معايير معينة تضمن سلامته من العيوب و التلاعب بمضمونه[41] عند الحصول عليه نوجزها فيما يلي :

- يجب أن تتم عملية الحصول على الأدلة الرقمية بطريقة مشروعة طبقا لمبدأ الشرعية الموضوعية و الإجرائية تحت طائلة البطلان.
- يجب أن تتأكد القوة الثبوتية للأدلة الرقمية من خلال خلوها من الشكوك، وأن تبتعد عن الظنون و التخمينات حتى يمكن للقاضي الاستناد عليها في حكمه نظرا لخصوصية مصدرها .

- أن تكون هذه الأدلة محلا للمناقشة في جلسة المحاكمة طبقا لشفوية المرافعة وذلك حتى يمكن للقاضي تكوين اقتناعه الشخصي بناءا على صحة الأدلة المعروضة عليه[42].

ثانيا : قبول دليل طب الشرعيالرقمي أمام القضاء الجنائي

تقتضي ضمانات المحاكمة العادلة أمام القضاء الجزائي إلزام القاضي بالتيقن من مشروعية الدليل الرقمي و مصدره، إذ أن المشرع الجزائري كما أشرنا إليه سابقا قد منح للقاضي الجزائي السلطة المطلقة في تقدير القيمة القانونية للدليل الرقمي و مدى مطابقته للشروط المنصوص عليها قانونا، و من ثم تكوين قناعته على أساس ما تحمله الوقائع من دلالات و إثباتات يقينية تم التطرق إليها و مناقشتها في جلسة المحاكمة.

1. مظاهر ممارسة القاضي لسلطتهفي تقدير دليل الطب الشرعي الرقمي

زامن ظهور الجرائم المعلوماتية ظهور الدليل الرقمي، ،فكانت الوسائل التي يستعملها الطب الشرعي في استخلاص الأدلة الرقمية التي تتلاءم و الطبيعة الخاصة لهذه الجرائم الآلية المستحدثة التي تساهم في مساعدة المنظومة القضائية في الحد من خطورة هذا النوع من الإجرام إلا ان التساؤل يثار حول ما هو دور القاضي الجزائي في تقدير القيمة الاثباتية لهذه الأدلة؟

1.1 الاقتناع الشخصي للقاضي الجزائي في تقدير طب الشرعيالرقمي

يقوم مبدأ الاقتناع الشخصي للقاضي الجزائي على مدى تقديره لقيمة كل دليل طبقا لقناعته الشخصية التي يبني عليها حكمه بناءا على ما توصل إليه من ادلة يقينية ترتبط بالوقائع المطروحة أمامه، و بالتالي فإن الأدلة الرقمية تخضع كذلك إلى السلطة التقديرية للقاضي الجزائي حيث أنه إذا رأى أن هذه الأدلة كافية للاستناد عليها في حكمه فإن له كل السلطة في الاعتماد عليها، استنادا على مبدا حرية القاضي في الاقتناع الشخصي[43] و الذي يقصد به «الحالة الذهنية أو النفسية أو ذلك المظهر الذي يوضح وصول القاضي بإقناعه لدرجة اليقين بحقيقة واقعة لم تحدث أمام بصره بصورة عامة."[44]

2.1 سلطة القاضي الجزائي في تقدير دليل الطب الشرعي الرقمي

تتجلى مظاهر ممارسة القاضي الجزائي لسلطته التقديرية في تحديد القوة الإثباتية للدليل الرقمي في مظهرين أساسيين تتمثلان في :

1.2.1 التيقن من مشروعية دليل الطب الشرعي الرقمي

أثارت الأدلة الرقمية التي خلفها تطور الجريمة وأساليب ارتكابها والتي استلزمت استحداث منظومة الطب الشرعي الرقميلمعالجة الطبيعة الخاصة لتلك الجرائم؛ عن طريق توفير وسائل تقنية للحصول على الأدلة وتمحيصها لاستخدامها من أجل إثبات واقعة جرمية، جدلا واسعة في مدى مشروعية هذه الأدلة الرقمية ويقينيتها، و بالتالي وجب عل القاضي الجزائي وهو في إطار حل القضايا المعروضة امامه أن يقوم بفحص هذه الأدلة و تحليلها و التأكد من صحتها قبل الاستناد عليا في إصدار أحكامه القضائية.

2.2.1 الموازنة بين أدلة الطب الشرعي الرقمي

تتسم الأدلة الرقمية بنوع من الخصوصية نظرا لطبيعتها التقنية المستخلصة من أجهزة الحاسب الآلي و ملحقاته، محكمة بقواعد علمية و حسابية قاطعة وهو ما كان السبب في منح القاضي الجزائي سلطة واسعة في الموازنة بين مختلف هذه الأدلة ثم العمل على استبعاد الأدلة التي تثير الشك و الغموض حتى إلى حد الجزم و اليقين في قناعته بكل نوع من الأدلة الرقمية سواء كانت مصغرات فيلميه أو بيانات رقمية من خلال ما يتطلع في ذهنه من تصورات و احتمالات تحدد القوة الاستدلالية لكل دليل على صدق نسبة الجريمة المعلوماتية لفاعليها[45].

2. القيود الواردة على حرية القاضي في قبول دليل الطب الشرعي الرقمي

لضمان تحقيق محاكمة عادلة للمتهم قيد المشرع الجزائري سلطة القاضي الجزائي في مجال قبوله للدليل الرقمي بنوعين من القيود يتمثل الأول في تحديد مجمل الأدلة الجنائية التي يمكن للقاضي الإسناد عليها، أما الثاني فيتمثل في مجموعة من الشروط التي يجب أن يتسم بها الدليل الرقمي ليكتسب صفة الشرعية أمام القضاء.

1.2 أنواع الأدلة الرقمية الجنائية التي يمكن الاستناد عليها في الاثبات الجنائي

يعتمد الطب الشرعي على أشكال متنوعة و مختلفة من الأدلة الرقمية في إطار ممارسة إجراءات التحقيق القضائي، ولكن هذه المسألة تثير لنا التساؤل حول ما إذا كانت كل الأدلة الرقمية المستمدة من نظام الحاسب الآلي يمكن الاعتماد عليها كوسيلة إثبات أمام القضاء الجزائي؟

1.1.2 الأدلة الرقمية التي تعد للإثبات

يتميز هذا النوع من الأدلة الرقمية بسهولة الحصول عليه دون اللجوء الى إجراءات معقدة و هذا نتيجة لكون أن هذه الادلة تكون معدة مسبقا كوسيلة إثبات للاحتجاج بها لاحقا، و تتمثل في السجلات التي تم إنشائها على مستوى برامج الحاسب الآلي كسجلات الهاتف و الحاسب الآلي.[46]

2.1.2 الأدلة الرقمية التي لم تعد للأثبات

يعرف كذلك هذا النوع من الأدلة بأدلة البصمة الرقمية"؛ و هذا النوع من الأدلة الرقمية يتم اكتشافه عن طريق القيام بمجموعة من التحقيقات القضائية عند وقوع جريمة، يتم استخلاصه من البيئة الرقمية يُعتمد عليه كوسيلة اثبات لواقعة قانونية ثم اسنادها لمرتكبيها، تتمثل هذه الادلة في كافة العمليات الإلكترونية التي تتم من خلال شبكة الانترنت[47].

2.2 الشروط التي تحكم صحة دليل طب الشرعي الرقمي

لا يكفي معرفة نوع الادلة الرقمية التي يمكن للقاضي الجزائي ان يستند إليها في حل الوقائع المعروضة أمامه، إذ يستوجب الأمر أن تشتمل هذه الأدلة على مجموعة من الشروط و الضوابط تكسبها مشروعيتها و يقينيتها أمام القضاء الجزائي ومن بين أهم هذه الشروط نذكر:

1.2.2 أن يكون الدليل الرقمي يقينيا : إذ لا يمكن للقاضي أن يعتمد في بناء حكمه على أدلة رقمية تثار الشكوك حول صحتها وحول مشروعية المصدر الذي استمدت منه، فاليقين في الأدلة الرقمية شرط لقبولها مهما كان نوعها، ويقصد به هنا اليقين في صحته و اليقين في خدمته للنزاع المعروض وصلاحية استعماله فيه، لإن تخلف احدهما لا يمكن الأخذ به[48].

2.2.2 ان يكون الدليل الرقمي مشروعا : و يقصد به أن يتم الحصول الدليل الرقمي وفقا للضوابط الموضوعيةو الشكلية المنصوص عليها قانونا، بما يضمن صحة و دقة هذا الدليل في خدمة النزاع المعروض لا تقبل التأويل، وذلك أن قواعد الإثبات و أدلته باختلاف أنواعها تخضع لمبدأ الشرعية و هذا لارتباطها بحقوق و حريات الأفراد[49].

3.2.2 ان تتم مناقشة الدليل الرقمي في جلسة الحكم: نصت المادة 212 من قانون الاجراءات الجزائية في فقرتها الثانية[50] على "لا يسوغ للقاضي أن يبني قراره إلا على الادلة المقدمة له في معرض المرافعات و التي حصلت المناقشة فيها حضوريا أمامه"

ومنه فبناءا على نص الماد أعلاه فإنه يشترط لقبول الدليل الرقمي حضوره في ملف المناقشة و أن يتاح للخصوم فرصة فحصه و تحليله ثم مناقشته في جلسة المحاكمة.

الخاتمة

مع الانتشار الواسع للتكنولوجيا الرقميةالمتطورة باستمرار في حياتنا اليومية ، والاعتماد عليها في جميع تفاعلاتنا الاجتماعية كان لابد من ان تشق نتائج هذه التكنلوجيا طريقها نحو المحكمة ، فانعكست اثارها على المنظومة القضائية ، ومن هنا برزت الحاجة لعلم الطب الشرعي الرقمي كعلم جنائي يختص في اثبات ما قد

ينجر عن تلك التكنولوجيات الرقمية من جرائم ، فحاولنا من خلال هذه الورقة البحثية معالجة هذا النوع من العلوم الشرعية من خلال التعرف على مفاهيمه وكذا مدى حجه الأدلة التي ينتجها وفقا للتسريع الجزائري.

ولذلك في من بين اهم النتائج نذكر :

- تعني رقمنة المجتمع اننا متصلون ليس فقط ببعضنا البعض ولكن ايضا بثروة من الخدمات عبر الانترنت التي تشمل جميع قطاعات العالم المعاص؛ بما في ذلك الحكومات والتعليم والصحة والاعمال والنقل وبسبب هذا القبول الواسعللأجهزةالرقمية ، والخدمات الإلكترونية فقد تفاعل معها الجميع بشكل او بأخر .
- قد تصبح هذه الأجهزةالإلكترونية والخدمات ونشاط الاشخاص عبر الانترنت في بعض الاحيان أدلة رقمية عندما تحمل بعض القيم الثبوتية ويمكن ان تساعد في اتخاذ القرار في شتى القضايا المطروحة امام المحاكم ولهذه الغاية ظهر الطب الشراعي الرقمي.
- الطب الشرعي الرقمي هو فرع من فروع الطب الشرعي يقصد به جمع وتحليل الأدلة الرقمية من واقع الكترونيه ما مرتبطة بشكل مباشر بالتحقيق ، وذلك من خلال تطبيق مبادئ العلوم التقنية في البحث عن الحقيقة في المجالات المدنيةوالجنائية.
- كما هو الحال مع الطب الشرعي التقليدي فان الهدف الاساسي للطب الشرعي الرقمي هو التحقيق واعادة بناء مسرح الجريمة للعثور على مرتكبيها وتحديد المسؤوليات التي تقع على عاتقهم.
- سلامةالأدلة امر ضروري لقبولها ويتم الحفاظ عليها من خلال استخدام اساليب تحقيق لا تؤدي الى تعديل نسختهاالأصلية ، فالحفاظ على سلامةالأدلةالرقمية شرط اساسي في مصداقيتها .
- الاتساق القانوني شرط اساسي لمصداقية للأدلة و يعتبر علامة على الجودة و معيار اساسي يجب تحقيقه في جميع جوانب عملية الطب الشرعي الرقمي.
- أخذ المشرع الجزائري بنظام تشريعي جديد فيما يخص قواعد إثبات الجريمة الإلكترونية و رصد لها مجموعة من الضوابط و الشروط تتلاءم و طبيعتها الافتراضية.
- إن الطبيعة الخاصة للأدلة الرقمية و الطبيعة غير المادية للوسائل المستمدة منها، جعلها تثير إشكالات عديدة حول مشروعية هذه الأدلة و يقينها في إثبات الجرائم الالكترونية.
- يستمد القاضي الجزائي قناعته الشخصية في بناء أحكامه القضائية على ما يتم مناقشته من أدلة في جلسة المحاكمة، إذ تخضع القيمة القانونية للأدلة الرقمية كذلك إلى السلطة التقديرية للقاضي الجزائي.

وعلى ضوء ذلك **نقترح** :

- زيادة عدد الدراسات و الاهتمام بواقع التحقيق الجنائي الرقمي كعلم يمارسهفنيو الطب الشرعي الرقمي ، وذلكلحداثة هذا الفرع من فروع العلوم الشرعية و كثرة التحديات التي تواجهه نتيجة لتطور التكنولوجي الدائم في العالم الرقمي .
- عدم حصر عملية الطبالشرعي الرقمي على الجهات الحكومية و دوائر الشرطة بل يجب ان يفتح المجال للقطاع الخاص من شركات و خبراء تقنين للاشتراك في هذه العملية كما هو الحال في باقي فروع الطب الشرعي الأخرى.
- إثراء قانون الإجراءات الجزائية بما يسمح بتحديد الطبيعة القانونية للأدلة الرقمية و حجيتها أمام القضاء الجزائي، بالإضافة إلى التحديد الدقيق للإجراءات المتبعة لاستخلاص هذه الأدلة.
- تستلزم عملية استخلاص الدليل الرقمي كفاءات فنية و تقنية في الشخص المسؤول عنها، و هو مايفرض إنشاء مراكز متخصصة لتأهيل خبراء و كفاءات في المجال المعلوماتي و التكنولوجي، لمواكبة التحديات الجديدة التي جاءت بها الجرائم الالكترونية.
- تفعيل التعاون الدولي في مجال التحقيقات المشتركة خاصة في مجال المعلوماتي و التنسيق بين الإجراءات المتخذة على المستوى الداخلي والمستوى الدولي، والاستفادة من خبرتها في هذا المجال.
- مع الاخذ بكل ما سبق في الاعتبار لا يزال الجناة دائما ما يتقدمون بخطوة على فاحصي الطب الشرعي الرقمي بغض النظر عن التكنولوجيا المستخدمة اثناء التحقيق ، وقد يكون هذا صحيحا اذا اختار جميع فاحصيالأدلة الجنائيةالرقمية الاستمرار في استخدام نفس العمليات التي تفتقر الى تقديم الدعم الكافيلتحقيق، وعلى هذا النحو لا شك انه هناك حاجة متزايدة الى نهج جديد في المراجعة والتحقيق بشأن الهجمات الإلكترونية ، وذلك من خلال تزويد فاحصي الأدلة الرقمية بالدعم الكافي خلال جميع مراحل تحقيق.

الهوامش:

[1]Cohen, Frederick B. "**Fundamentals of digital forensic evidence.**" Handbook of Information and Communication Security. Springer, Berlin, Heidelberg, 2010, p 789.

[2]OliveiraJr, E., et al. "**Digital forensics experimentation: Analysis and recommendations.**" Forensic science review 34.1 (2022) , p 21 .

[3]Jordaan, Jason. "A **sample of digital forensic quality assurance in the South African criminal justice system.**" 2012 Information Security for South Africa. IEEE, 2012 , p 1 .

[4]Hewling, Moniphia Orlease.**Digital forensics: anintegrated approach for the investigation of cyber/computer related crimes**. Diss. University of Bedfordshire, 2013,p7.

[5]Ibid , p 9 .

[6] KAUR, Ravneet; KAUR, Amandeep. **Digital forensics**. International Journal of Computer Applications, 2012, p 5 .

[7] Hewling, Moniphia Orlease, **op. cit, p** 13 .

[8]KORONIOTIS, Nickolaos; MOUSTAFA, Nour; SITNIKOVA, Elena. **Forensics and deep learning mechanisms for botnets in internet of things**: A survey of challenges and solutions. *IEEE Access*, 7 , 2019 , p 61764 .

[9] Hewling, Moniphia Orlease , **op. cit , p** 9.

[10]Gül, Murat, and Emin Kugu. "**A survey on anti-forensics techniques.**" 2017 International Artificial Intelligence and Data Processing Symposium (IDAP). IEEE, 2017 , p 2.

[11] Hewling, Moniphia Orlease , **op. cit , p** 9.

[12]Caviglione, Luca, Steffen Wendzel, and Wojciech Mazurczyk. "**The future of digital forensics: Challenges and the road ahead.**" IEEE Security & Privacy 15.6 , 2017 , p 12.
[13]Page, Helen, et al. **"A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn?."** Science & justice 59.1, 2019 , p 83.
[14]Cohen, Frederick B. "**Fundamentals of digital forensic evidence.**" *Handbook of Information and Communication Security*. Springer, Berlin, Heidelberg, 2010. P 789.
[15] ARSHAD, Humaira; JANTAN, Aman Bin; ABIODUN, Oludare Isaac. **Digital forensics:** review of issues in scientific validation of digital evidence. Journal of Information Processing Systems, 2018, 14.2 , p 346.
[16]**Ibid** , p 346 .
[17]**Ibid** , p 347 .
[18]Horsman, Graeme. "**Opinion: Does the field of digital forensics have a consistency problem?.**" *Forensic Science International: Digital Investigation* , 33 , 2020 , p 1 .
[19] Dror, Itiel, et al**. "Cognitive bias in forensic pathology decisions.**" Journal of Forensic Sciences 66.5 , 2021 , p 1751 .
[20]Buçinca, Zana, Maja Barbara Malaya, and Krzysztof Z. Gajos. "**To trust or to think: cognitive forcing functions can reduce overreliance on AI in AI-assisted decision-making.**" *Proceedings of the ACM on Human-Computer Interaction* 5.CSCW1 , 2020 , p 1.
[21] Mattijssen, Erwin JAT, et al. "**Cognitive biases in the peer review of bullet and cartridge case comparison casework: a field study.**" Science & Justice 60.4 , 2021 , p 337 .
[22]Sunde, Nina, and Itiel E. Dror. **"Cognitive and human factors in digital forensics: Problems, challenges, and the way forward.**" *Digital investigation* 29 , 2019 , p 101-102.
[23]**Ibid** , p 104 .
[24]**Ibid** , p 106 .
[25]**Ibid** , p 106.
[26]**Ibid** , p 107.
[27]Köhn, Michael, Martin S. Olivier, and Jan HP Eloff. **"Framework for a Digital Forensic Investigation."** *ISSA*. 2006 , p 1 .
[28]KORONIOTIS,Nickolaos MOUSTAFA, Nour SITNIKOVA, Elena.**OP . cit , p 4 .**
[29]Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. **Cybercrime and digital forensics:** An introduction. Routledge, 2017 , p 350 .
[30]**Ibid** , p 376 .
[31]KORONIOTIS,Nickolaos MOUSTAFA, Nour SITNIKOVA, Elena.**OP . cit , p 8.**
[32]Holt, Thomas J., Adam M. Bossler, and Kathryn C. Seigfried-Spellar. **Op . Cit , p** 379 .
[33]يقصد بالإثبات الجنائي: "هو الحجية و البينة و إقامة الدليل من طرف السلطة القضائية المختصة بالإجراءات الجنائية في البحث عن قيام الجريمة بطرق مشروعة أثناء مراحل الدعوى العمومية، فهي إثبات الوقائع المنسوبة الى المشتبه فيه و تطبيق قانون العقوبات على تلك الوقائع". انظر أسامة حسين محي الدين عبد العال، حجية الدليل الرقي في الإثبات الجنائي للجرائم المعلوماتية" دراسة تحليلية مقارنة"، مجلة البحوث القانونية و الاقتصادية ، العدد76، يونيو2021، ص613-614.
[34]الدليل الرقمي هو " الدليل الذي وجد له أساسا في العالم الافتراضي، ويقود الجريمة وهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات، والذي يؤدي الى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة الإنترنت «أنظر خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر العربي، الإسكندرية، 2019، ص 177.
[35]كريمة علا، **الشرعية الجنائية الإجرائية : نجاعة الصياغة و فعالية التطبيق**، مجلة الأستاذ الباحث للدراسات القانونية و السياسة، المجلد05، العدد02، 2020، ص1242.
[36]أسامة حسين محي الدين عبد العال، **مرجع سابق**، ص672.
[37]خالد عياد الحلبي، **إجراءات التحري و التحقيق في جرائم الحاسب و الأنترنت**، الطبعة01، دار الثقافة للنشر و التوزيع، الأردن، 2011، ص 235-237.

[38]المادة 212 من الأمر 66-155، المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 48، الصادرة بتاريخ 11 جوان 1966، معدل ومتمم، نصت على " يجوز اثبات الجرائم بأي طريقة من طرق الاثبات ماعدا الأحوال التي نص فيها القانون على غير ذلك، و للقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي."

[39]أسامة حسين محي الدين عبد العال، **مرجع سابق**، ص 685-686.

[40]نصر الدين مروك، **محاضرات في الاثبات الجنائي النظرية العامة لإثبات الجنائي**، الجزء الأول، دار هومة، الجزائر،2003،ص 491.

[41]بن مالك أحمد، الخال إبراهيم، **دور الأدلة الرقمية في الاثبات الجنائي**، مجلة العلوم الانسانية – المركز الجامعي علي كافي تندوف – الجزائر، المجلد 05، العدد01، 2021، ص 117.

[42]اسامة حسين محي الدين عبد العال، **مرجع سابق**، ص692

[43]خالد ضو، **حجية الدليل الإلكتروني و شروط قبوله في الاثبات الجنائي**، مجلة الباحث الأكاديمي في العلوم القانونية و السياسية ، المركز الجامعي أفلو/ الأغواط، العدد 08، مارس 2022، ص210.

[44]إيهاب فؤاد الحجاوي، **حجية الدليل الرقمي في الاثبات الجنائي**، مجلة العلوم القانونية و الاقتصادية، العدد 01، يوليو 2014، ص99.

[45]بن مالك أحمد، الخال إبراهيم، **دور الأدلة الرقمية في الإثبات الجنائي**، مجلة العلوم الإنسانية، المركز الجامعي علي كافي تندوف، الجزائر، المجلد05 ، العدد 01، نيسان2021، ص 118.

[46]منصور عبد السلام عبد الحميد حسان العجيل ، **الضوابط القانونية للإثبات الجنائي بالأدلة الرقمي دراسة مقارنة**، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية)، مصر،ص 3370.

[47]**المرجع نفسه**، ص 3370.

[48]خالد ضو، **مرجع سابق**، ص 208.

[49]منصور عبد السلام عبد الحميد حسان العجيل، **مرجع سابق**، ص3403.

[50]المادة 2/212 من قانون الاجراءات الجزائية.

وزارة التعليم العالي والبحث العلمي

جامعة الجزائر 1 بن يوسف بن خدة

كلية الحقوق

الملتقى الدولي الافتراضي الموسوم ب: القانون الجنائي في ظل التطور التكنولوجي

-إشكالات ومعالجات-

الاسم الكامل 01: وداد بن سالم

الرتبة العلمية: طالبة دكتوراه سنة أولى

الاسم الكامل 02: عبد الله شيباني

الرتبة العلمية: دكتوراه علوم في الحقوق

التخصص: حقوق

الجامعة: محمد لمين دباغين سطيف 02-الهضاب

رقم الهاتف: 0795120100

البريد الالكتروني: bensalemwidad12@gmail.com

محور المداخلة: المحور الخامس" تأثير الوسائل العلمية الحديثة على الاثبات الجنائي"

عنوان المداخلة باللغة العربية: مشروعية الوسائل التقنية الحديثة في الاثبات الجنائي

عنوان المداخلة باللغة الإنجليزية:Legality of Modern TechnicalMeans in CriminalEvidence

ملخص

في ظل التطور التقني والعلمي توجهت الأفكار الحديثة إلى استخدام الوسائل التقنية الحديثة في مجال الإثبات الجنائي، نظرا لفعاليتها في الكشف عن الجرائم وملاحقة مرتكبيها.

بيد أن الاستعانة بمختلف هذه التقنيات أثار إشكالية حول مدى مشروعيتها، ذلك أنه في إطار العمل بها قد يشكل انتهاكا لحق الأفراد في الخصوصية ومساسا بكرامتهم، إلا إذا كانت تمارس في الحدود التي رسمها القانون وألا تتضمن اعتداءات على حرمة الحياة الخاصة للأفراد إلا بالقدر الضروري الذي يخدم مصلحة سير العدالة.

كلمات مفتاحية: الوسائل التقنية، أجهزة التصنت والمراقبة، جهاز كشف الكذب، التنويم المغناطيسي

Abstract:

In the light of technical and scientificdevelopment, modern ideas have been directedtowards the use of modern technicalmeans in the field of criminalevidence, giventheireffectiveness in detecting and prosecuting crimes.

However, the use of different techniques has raised issues as to theirlegitimacy, as theymayconstitute a violation of individuals' right to privacy and theirdignity, unlessthey are exercisedwithin the limitsestablished by law and involveattacks on the privacy of individualsonly to the extentnecessary in the interests of the administration of justice.

Keyworlds:Technicalmeans,Listening and Monitoring Devices, Polygraph, Hypnosis

مقدمة

من المسلم به أن العالم في العصر الحديث يشهد تطورا تقنيا هائلا في مجال التكنولوجيا الحديثة والتي شملت جميع مناحي الحياة.

وكان من انعكاسات هذا التطور ظهور نوع جديد من الإجرام يختلف عن الإجرام التقليدي لا سيما من حيث أساليب ارتكاب الجريمة التي أصبحت تعتمد على وسائل وأدوات تقنية متطورة تساعد على تنفيذ مخططاتهم الإجرامية ولا تترك آثارا تدل عليه، الأمر الذي أدى إلى قصور أساليب البحث والتحري التقليدية في الكشف عن الجرائم وملاحقة مرتكبيها.

وهو ما استتبع بالضرورة الاستعانة بالوسائل التقنية الحديثة التي أفرزها التقدم العلمي في مجال التحقيق والإثبات الجنائي، منها ما يتم استخدامها بشكل خفي كأجهزة التصنت والمراقبة، ومنها ما يستخدم بشكل علني كجهاز كشف الكذب والتنويم المغناطيسي.

بيد أن أمر اللجوء إلى هذه التقنيات تعتريه صعوبات ومشكلات من حيث مدى مشروعية هذه الوسائل، خاصة وأن مباشرتها يشكل تعدياعلى حرمة الحياة الخاصة للأفراد.

إشكالية البحث

بات استخدام الوسائل التقنية الحديثة أكثر شويعا في مجال الإثبات الجنائي لما لها من فعالية في الكشف عن الجرائم وملاحقة مرتكبيها، إلا أنها أثارت جدلا فقهيا وقانونيا واسعا حول قبول الاستعانة بها من عدمه، مما يطرح مشكلة الموازنة بين حق الأفراد في الخصوصية وعدم انتهاكها وبين حق المجتمع في مكافحة الجريمة وتحقيق العدالة، على ضوء هذا تطرح الإشكالية التالية:

ما مدى صحة الاستعانة بالوسائل التقنية الحديثة في الإثبات الجنائي؟

يتفرع على هذه الإشكالية بعض التساؤلات هي كالتالي:

ماهو المقصود بالوسائل التقنية؟ وما هو موقف الفقه والتشريع حول مدى مشروعيتها؟

سنحاول الإحاطة بمفهوم مختلف الوسائل التقنية ونتطرق إلى موقف الفقه والتشريع منها في الخطة التالية:

المبحث الأول: الوسائل التقنية التي تباشر بشكل خفي ومدى مشروعيتها

المطلب الأول:أجهزة التصنت والمراقبة

المطلب الثاني: مدى مشروعية استخدام أجهزة التصنت والمراقبة

المبحث الثاني: الوسائل التقنية التي تباشر بشكل علني ومدى مشروعيتها

المطلب الأول: استخدام تقنية جهاز كشف الكذب

المطلب الثاني:استخدام تقنية التنويم المغناطيس

خاتمة

المبحث الأول: الوسائل التقنية التي تمارس في الخفاء ومدى مشروعيتها

مع التطور التقني لأساليب ارتكاب الجرائم وخصوصا تلك التي المتعلقة بالمجال الرقمي، أضحت الأساليب التقليدية في البحث والتحري غير فعالة لمجابهة هذه الجرائم، الأمر الذي أدى بمختلف التشريعات لاستحداث أساليب استثنائية للبحث والتحري تتوافق وطبيعة الجرائم المستحدثة، وذلك باستغلال تقنية التكنولوجيا الحديثة التي نتج عنها وسائل تقنية متنوعة كأجهزة التصنت والمراقبةتستخدم في مجال الاثبات الجنائي.

غير أن استعمال هذه الوسائل قد يشكل انتهاكا لحرمة الحياة الخاصة بالأفراد باعتبار أنها تقوم على التجسس والتصنت والتسجيل والمراقبة السرية للمعنى دون رضا منه، مما يشكك في مدى مشروعية اللجوء الى هذه الوسائل كوسيلة من وسائل الاثبات الجنائي.

المطلب الأول: أجهزة التصنت والمراقبة

نتيجة التطور التكنولوجي ظهرت أجهزة مراقبة ذات تقنية عالية تستخدم من طرف السلطات المختصة بغية الكشف عن الجرائم والبحث عن مرتكبيها، ولعل ومن أهم هذه الأساليب هي اعتراض المرسلات، تسجيل الأصوات والتقاط الصور بالإضافة الى المراقبة الالكترونية.

الفرع الأول: اعتراض المرسلات والتسجيل الصوتي والتقاط الصور

المقصود من هذه العمليات هو وضع الشخص تحت الملاحظة للتصنت وتسجيل كل وما يحدث خلسة دون موافقة المعني، بغرض الحصول على بيانات ومعلومات من شأنها أن تفيد في الكشف عن الجرائم وملاحقة مرتكبيها.

أولا: اعتراض المراسلات

الاعتراض يعني الاستيلاء بغتة[1]، ويقصد بالمراسلات التخابر والاتصال بين الأفراد فيما بينهم سواء بالكتابة أو غيرها.

واعتراض المراسلات يعني التتبع السري والدائم أو الدوري للمشتبه به قبل وبعد ارتكاهم الجريمة، ويعرف بأنه إجراء يباشر خلسة دون رضا المعني، وانتهاك لسرية الأحاديث الخاصة، تأمر به السلطة القضائية بهدف الحصول على دليل غير مادي للجريمة[2].

وكما هو معلوم أن سرية المراسلات من الحقوق اللصيقة بالشخص، والاعتداء عليها يمثل انتهاكا لخصوصية الأفراد لأنها تعبر عن أفكار الشخص المعني وتكشف جزءا من أسرار حياته الخاصة فلا يجوز الاعتداء عليها والا شكل ذلك مساسا بحرمة الحياة الخاصة، واستخدام هذه التقنية يعتبر انتهاكا صارخا لحق المتهم في الخصوصية، مما يشكك في مشروعية الاستعانة بها في البحث والتحري.

ثانيا: تسجيل الأصوات

يقصد به تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرية وخاصة، سواء في مكان عام أو خاص، ويشمل الحديث كل مايتفوه به الانسان حتى وغن كان شخصيا أو تضمن أدق أسرار حياته[3]، ويحفظ هذا التسجيل في جهاز معد لذلك للاستماع اليه مرة أخرى، كما قد يكون الكلام موجها للكافة أو لعدة أشخاص أو لشخص محدد بالذات، قد يكون الحديث في صورة حوار مفهوم أو عبارة عن كلمات مشفرة[4].

كما يعرف تسجيل الأصوات بأنه عبارة عن عميلة للتغييرات المؤقتة لموجات الصوت الخاصة بالكلام أورنينةبواسطة آلة تنقل موجات الصوت إلى اهتزازات خاصة والتي تتفق مع الأصوات التي تحدثها

---

[1]فوزي عمارة، "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كإجراءات تحقيق قضائي في المواد الجزائية"، مجلة العلوم الإنسانية، عدد 33 جوان 2010، ص 237.

[2]أنيس حسيب السيد المحلاوي، "مدى مشروعية الوسائل التي تستخدم بشكل خفي كدليل للإثبات الجنائي"، 2018، ص 2763.

[3]جميلة محلق، "اعتراض المرسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية"، التواصل في الاقتصاد والإدارة والقانون، عدد 42 جوان 2015، عنابة، الجزائر، ص 178.

[4]أنيس حسيب السيد المحلاوي، المرجع السابق، ص 2777.

بالضبط[1].

إذا يتضح من هذا أن تسجيل الأصوات هو عبارة عن حفظ لعبارات ذات معنى واضح أو غامض بواسطة أجهزة مخصصة لإعادة الاستماع إليه، ولتقديمة كدليل للكشف عن وقائع الجريمة.

ثالثا: التقاط الصور

إضافة الى ماسبق مكنت السلطات القضائية من إمكانية التقاط الصور، باعتبارها من الوسائل المهمة في الاثبات الجنائي فهي تحمل تسجيلا حقيقيا لما تراه العين، وما يعجز الفكر الإنساني عن التعبير عنه[2].

إن التقاط الصور يقوم أساسا على استخدام الكاميرات أو أي أجهزة أخرى خاصة تلتقط الصور لوضعية شخص مشتبه في أمره على الحالة التي كان عليها لغرض استخدام محتوى الفيلم كمادة اثبات[3].

والتصوير لم يعد مقتصرا على الأجهزة التقليدية كالكاميرات فقط بل تجاوز ذلك الى ظهور أجهزة تصوير فائقة الدقة تساعد على التقاط الصور بجودة عالية تمكن من معرفة أدق التفاصيل، كالتصوير بواسطة الأقمار الصناعية، التصوير باستخدام أشعة غير مرئية وغيرها من الأجهزة المستحدثة[4].

الفرع الثاني: المراقبة الإلكترونية

لعل من أبرز الوسائل العلمية المستحدثة المراقبة الإلكترونية التي تساهم بشكل معتبر في الكشف عن الجرائم والبحث عن مرتكبيها، ويقصد بها العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع بيانات ومعلومات عن المشتبه فيه سواء كان شخصا أم شيئا حسب طبيعته، مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر[5].

---

[1]رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)، المكتب الجامعي الحديث، الإسكندرية، 2013.

[2]زاهر خالد عبد الله صباح، دور الوسائل العلمية الحديثة في الاثبات الجنائي في فلسطين، رسالة ماجستير، جامعة القدس، فلسطين، 2017، ص 59.

[3]أنيس حسيب السيد المحلاوي، "مدى مشروعية الوسائل التي تستخدم بشكل خفية كدليل في الاثبات الجنائي"، المرجع السابق، ص 2801.

[4]زاهر خالد عبد الله صباح، المرجع السابق، ص 59.

[5]رشاد خالد عمر، المشاكل القانونية والفنية لتحقيق في الجرائم المعلوماتية، المرجع السابق، ص 74.

وتنصب المراقبة الإلكترونية في الغالب على المراسلات الإلكترونية مهما كان نوعها أو البرنامج الذي تمت بواسطته، حيث تخضع كل المراسلات الإلكترونية لعميلة المراقبة والتصنت ومن بين أهم تلك المراسلات التي تتم مراقبتها في الوقت الحالي هي تلك التي تتم عبر البريد الإلكتروني وعبر برامج التواصل الإلكتروني كالفيس بوك والوا تساب وغيرها من برامج التواصل الإلكتروني الحديثة[1].

كما تتم المراقبة من خلال برنامج الفيديو وفتح كاميرا الجهاز المراقب كالحاسب الآلي أو الهاتف النقال دون علم صاحبه، وهذا ما يعد انتهاكا صارخا لخصوصية الأفراد[2]، فليس من حق أي جهة كانت الاطلاع على الحياة الخاصة بالأفراد وأسرارها، حتى وإن كانت بهدف الحصول على معلومات مهمة للكشف عن الجرائم، فمثلا يمكن للمراقب القيام بالتجول داخل جهاز الشخص المشتبه به ومعرف أسرار حياته قد تخصه هو أو أحد أفراد عائلته لا يريد من أحد الاطلاع عليها، ففي هذه الحالة تعد المراقبة الإلكترونية مساسا بخصوصيته.

المطلب الثاني: مدى مشروعية أجهزة التصنت والمراقبة

كرست مختلف الإعلانات العالمية والاتفاقيات والمؤتمرات الدولية حماية الحياة الخاصة للأفراد وعدم انتهاكها، حيث حرص الإعلان العالمي لحقوق الانسان لسنة 1948[3] على تأكيد هذا الحق بموجب المادة 12 منه والتي تنص على أنه:" لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة، أو في شؤون أسرته أو مسكنه أو مراسلاته ولا لحملات تمس شرفه وسمعته، ولكل شخص حق في أن يحميه القانون من ذلك التدخل، أو تلك الحملات"، كما أكدت الاتفاقية الأوروبية لحقوق الانسان 1950[4] على احترام حقوق الإنسان التي تضمنها الإعلان العالمي فنصت المادة الثانية منه على أنه:" لكل شخص الحق في احترام حياته الخاصة والعائلية ومسكنه ومراسلاه ولا يجوز للسلطة العالمة الاعتداء عليها إلا بموجب نص خاص وللضرورة المحتمة".

---

[1]بن بادة عبد الحليم، "المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني" بين الحق في الخصوصية ومشروعية الدليل الإلكتروني، ص 392.

[2]باخويا دريس /رواق العمرية، "أثر الإثبات الجنائي بوسائل التقنية الحديثة على حقوق الانسان" مجلة الدراسات القانونية والسياسية، العدد 05–المجلد 01 جانفي 2017، ص 81.

[3]الإعلان العالمي لحقوق الإنسان المنعقد بموجب قرار الجمعية العامة 217 ألف، باريس، المؤرخ في 10 ديسمبر 1948.

[4]الاتفاقية الأوروبية لحقوق الإنسان في نطاق مجلس أوروبا، روما في 4 نوفمبر 1950.

يستشف مما سبق أن أي انتهاك لحرمة الحياة الخاصة للأفراد يعد اعتداء عليها ويشكل جريمة يعاقب عليها القانون، واستعمال الوسائل السابق ذكرها يعد مساسا بخصوصية الأفراد، لذا أثارت مشكلة مدى مشروعية استخدام أجهزة التصنت والمراقبة في مجال الإثبات الجنائي.

فيما يلي نعرض موقف الفقه والتشريع، مع بيان موقف المشرع الجزائري من إمكانية اللجوء إليها والتعويل عليها في مجال الإثبات.

الفرع الثاني: موقف الفقه من استخدام أجهزة التصنت والمراقبة

تباينت الآراء بخصوص مدى جواز استخدام أجهزة التصنت والمراقبة في مجال الإثبات الجنائي، إذ ذهب جانب من الفقه الى القول بأن الاستعانة بهذه الأجهزة يعد باطلا باعتباره يخالف المبادئ العامة للقانون والدستور، فضلا عن مخالفته لنصوص الإعلان العالمي لحقوق الإنسان والاتفاقيات الدولية نظرا لما في ذلك من انتهاك لخصوصية الفرد ومساسا بحرمة حياته الخاصة[1].

من جانب آخر يرى أنصار هذا الاتجاه أن استخدام مثل هذه الوسائل من شأنه أن يؤدي إلى فتح باب التعسف وإمكانية تزوير الأدلة المستمدة منها[2]، لذلك يرون في أن افلات المجرم من العقاب أفضل بكثير من استخدامها، وإن كان اعتمادها في الاثبات الجنائي يندرج ضمن مبدأ الحرية في الإثبات فإنه لا يخلو من مخاطر إهدار حقوق الأفراد والاعتداء على حرمة الحياة الخاصة وكشف أسرارها[3].

فيما ذهب رأي آخر يؤيد استخدام أجهزة التصنت والمراقبة، على اعتبار أنه من الوسائل الفعالة التي تساهم في الكشف عن الجرائم، خاصة حينما تكون أساليب البحث والتحري التقليدية عاجزة عن كشف الجرائم وملاحقة مرتكبيها، وهذا يرجع لتنوع وطور أساليب ارتكاب الجريمة حيث أصبحت أكثر تعقيدا، الأمر الذي يستدعي استخدام وسائل أكثر تطورامع الأخذ بعين الاعتبار أن اللجوء إليها يكون وفق ضوابط وضمانات قانونية، وهو ما أكدته الاتفاقية الأوروبية لحقوق الانسان لعام 1950[4].

---

[1] زاهر خالد عبد الله صباح، دور الوسائل العلمية الحديثة في الإثبات الجنائي، المرجع السابق، ص 60.

[2] باخويا دريس/ رواق عمرية، "أثر الإثبات الجنائي بوسائل التقنية الحديثة على حقوق الإنسان"، المرجع السابق، ص 81.

[3] زاهر خالد عبد الله صباح، المرجع السابق، ص 60.

[4] أنيس حسيب السيد المحلاوي، "مدى مشروعية الوسائل التي تستخدم بشكل خفي كدليل في الإثبات الجنائي"، ص 2767.

اذن ليس هناك ما يمنع من استخدام هذه الوسائل مادام أن الاستعانة بها تكون بغرض إحقاق التوازن بين خصوصية الأفراد وحق المجتمع في الكشف عن الجرائم، على اعتبار أن المصلحة العامة أولى بالحماية من المصلحة الخاصة.

الفرع الثاني: موقف التشريع من استخدام أجهزة التصنت والمراقبة

من المسلم به جميع تشريعات أقرت حماية قانونية للحياة الخاصة للأفراد، نظرا للأهمية التي يكتسيها هذا الحق، إلا أنها أوردت استثناءات على هذه الحماية تحقيقا للمصلحة العامة.

وفي هذا الصدد ترى التشريعات الأمريكية أنه لا يوجد ما يمنع استخدام أجهزة التصنت والمراقبة، إذ ما تمت في الحدود التي رسمها القانون، وبهذا الخصوص صدر قانون أمريكي يتضمن نصوصا تتعلق باستخدام وسئل إلكترونية جديدة تتناسب وطبيعة النشاطات التي برزت مع استخدام الانترنت وكذلك فتح قنوات تعاون بين سلطات التحقيق الفيديرالية والمحلية في مجال تبادل المعلومات عن المشتبه بهم في نشاطات إجرامية[1].

وأقرت فرنسا مشروعية اللجوء إلى أجهزة التصنت والمراقبة بناءعلى اذن من قاضي التحقيق، حيث أجاز اعتراض المراسلات وتسجيل الأصوات في الجنيات والجنح المعاقب عليها بعقوبة تساوي أوتزيد على الحبس لمدة سنتين[2].

وسارت التشريعات العربية على نفس النهج، فنجد أن الدستور المصري أقرحماية حرمة الحياة الخاصة للأفراد وعدم المساس بها بأي شكل من الأشكال، إلا في الحالات التي ينص عليها القانون وهو مانصت عليه المادة 57 من الدستور المصري[3].

---

[1] نايف شافي المظافري الهاجري، "مدى حجية الوسائل العلمية الحديثة في الإثبات الجنائي في التشريع الأمريكي"، المجلة القانونية مختصة في الدراسات والبحوث القانونية، أكاديمية سعد العبد الله للعلوم الأمنية، الكويت، (ISSN:(2537-058، ص ص 149-150.

[2] جميلة محلق، "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية"، المرجع السابق، ص 179.

[3] تنص المادة 57 من دستور جمهورية مصر العربية وفقا للتعديلات الدستورية 23 أبريل 2019 على ما يلي:(للحياة الخاصة حرمة، وهي مصونة لا تمس وللمراسلات البريدية، والبرقية، والالكترونية والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة وسريتها مكفولة، ولا يجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون...)

بدوره المشرع الجزائري كرس حماية حرمة الحياة الخاصة للأفراد، وجرم الاعتداء عليها، غير أن هذا لا يمنع من تجاوز الأمر إذا كان لمقتضيات تحقيق العدالة وبغرض الكشف عن الجرائم وهو ما تم تكريسه في المادة 47 من الدستور الجزائري لسنة 2020والتي تنص على أنه: " لكل شخص الحق في حماية حياته الخاصة وشرفه، لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل

كانت، لا مساس بالحقوق المذكورة في الفقريتين الأولى والثانية إلا بأمر معلل من السلطة القضائية..."[1]

ولقد نظم المشرع الجزائري الأحكام القانونية الخاصة بأجهزة التصنت والمراقبة بموجب القانون 06-22 المعدل والمتمم للأمر 66-155 المتضمن قانون الإجراءات الجزائية، حيث أجاز اللجوء إلى اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، مع إحاطتها بمجموعة من الضوابط والضمانات القانونية هي كالتالي[2]:

- حصر اللجوء الى استخدام هذه الإجراءات في جرائم محددة سبيل الحصر هي: جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد،
- ربط المشرع الاستعانة باعتراض المراسلات وتسجيل الأصوات والتقاط الصور بضرورة التحري في الجرائم الملبس بها أو التحقيق الابتدائي، أي حين يثبت أن وسائل البحث العادية قد فشلت في إظهار الحقيقة،
- تتم هذه العمليات بإذن من وكيل الجمهورية أو قاضي التحقيق بحسب الحالة.

هذا وفي إطار مكافحة الجرائم المعلوماتية سمح المشرع الجزائري في ظل القانون 09-04[3]بوضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية، إذا ما دعت حماية النظام العام أو لمستلزمات التحقيقات والتحريات

---

[1]المرسوم الرئاسي رقم 20-442 يتضمن التعديل الدستوري، الجريدة الرسمية العدد 82. المؤرخ في 30 ديسمبر 2020.

[2]انظر المواد من 65 مكرر05 إلى غاية 65 مكرر 18 من القانون 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 66-155 المؤرخ في 8 يونيو 1966.

[3]القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، المؤرخ في 5 أوت سنة 2009.

القضائية عندما يكون من الصعب الوصول إلى نتيجة بأساليب التحري التقليدية، وهذه الإجازة تكون حصرا للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة[1].

يظهر مما سبق أنه ومع ضمان المشرع الجزائري لحرمة الحياة الخاصة وسرية المراسلات والاتصالات السلكية واللاسلكية، إلا أنه بالنظر لخطورة بعض الجرائم خول استثناء للسلطة القضائية الاستعانة بأجهزة التصنت والمراقبة مع احاطتها بضوابط وضمانات قانونية لمحاولة الموازنة بين الحق في الخصوصية وبين حق المجتمع في الكشف عن الجرائم وملاحقة مرتكبيها.

المبحث الثاني: الوسائل التقنية التي تباشر بشكل علني ومدى مشروعيتها

إن الهدف الأساسي للتحقيق مع المتهم واستجوابه هو معرفة الحقيقة للكشف عن الجريمة وضبط مرتكبيها.

حيث تتعدد الأساليب والطرق في الإثبات والتحقيق الجنائي، فضلا عن التطور العلمي والتقني الذي أسفر عنه ظهور تقنيات حديثة تستخدم في مجال الإثبات الجنائي ولعل من أبرزها جهاز كشف الكذب والتنويم المغناطيسي، غير أن الأخذ بها به قد يشكل مساسا بالسلامة النفسية والجسدية للأفراد وهو ما يعد تهديدا للحقوق والحريات الفردية.

المطلب الأول: استخدام تقنية جهاز كشف الكذب

يعتبر جهاز كشف الكذب من أبرز التقنيات التي أسفر عنها التطور العلمي في مجال التحقيق الجنائي، وقد أثار استخدامه العديد التساؤلات تدور حول مدى مشروعية اللجوء إليه كوسيلة من وسائل الإثبات الجنائي.

الفرع الأول: مفهوم جهاز كشف الكذب

يستخدم جهاز كشف الكذب لمعرفة مدى صدق أقوال الشخص محل الاستجواب والتحقق من صحتها أو كذبها، ويلجأ إليه في المسائل التي تفتقر إلى أدلة مادية[2].

يعرف جهاز كشف الكذب بـpolygrapheوهذه الكلمة تتألف من شقين الشق الأول: poly ومعناه الخطأ والشق الثاني: graphe معناه الرسم أو الصورة أو التسجيل.

---

[1]انظر المادتين 03، 04 من نفس القانون.

[2]باخويا دريس/ رواق عمرية، "أثر الإثبات الجنائي بوسائل التقنية الحديثة على حقوق الانسان"، المرجع السابق، ص 78.

يقوم جهاز كشف الكذب برصد التغييرات الفيسيولوجية للشخص محل التحقيق إثر توجيه بعض الأسئلة إليه بغية الوقوف على صحة أقواله من عدمها، كقياس تنفسه ونبضه وضغط دمه في وقت واحد[1]، حيث يقوم الجهاز بترجمتها في شكل رسوم ومخططات بيانية تمكن القائم على العملية بتحليل نتائجها وتسمح له بتقدير المعلومات المحصل عليها منه[2].

وقد يؤدي استخدام جهاز كشف الكذب إلى اعتراف المتهم قبل البدء بالتجربة أو أثناء خضوعه للاختبار أو بعد ذلك حين يواجه المتهم بما يسفر عنه الجهاز من نتائج، وقد لا يعترف بالجرم المنسوب إليه ولكنه يحصل أن تقع شكوك حول كلامه نظرا لما يسجله الجهاز من انفعالات، وينبغي الإشارة إلى أن الاعتراف لا يتمتع بالقوة الثبوتية كدليل إلا إذا كان بملء إرادة الشخص محل الاختبار دون إكراه[3].

وتقوم فكرة الجهاز على أساس أن الشخص موضع الاختبار تعتريه بعض الانفعالات النفسية التي يصاب بها أثناء خضوعه للاختبار من جهة أنه يخشى كشف أمره وإظهار الحقيقة التي يخفيها، ومن جهة أخرى هناك من تحت تأثير الخوف والتوتر وهو ما ينعكس على الجهاز العصبي للشخص فيبدي انفعالات وبعض التغييرات من شأنها اثارة الشك حول المتهم[4].

الفرع الثاني: مدى مشروعية استخدام جهاز كشف الكذب

تباينت مواقف الفقهاء والتشريعات حول مدى مشروعية استخدام هذا الجهاز في الإثبات الجنائي.

أولا: موقف الفقه

ذهب فريق من الفقه إلى تأييد استخدام جهاز كشف الكذب، فيما ذهب جانب آخر إلى رفضه

1- الاتجاه المؤيد: يذهب أنصار هذا الاتجاه إلى جواز الاعتداد بنتائج جهاز كشف الكذب، فهو يعد وسيلة علمية فعالة تمكن من معرف الحقائق والكشف عن الجريمة ومرتكبيها.

---

[1]راضية خليفة /نصيرة مهيرة "جهاز كشف الكذب ومدى مشروعيته في الإثبات الجنائي"، مجلة الاجتهاد القضائي، المجلد 13-العدد 02 (العدد التسلسلي 27)، أكتوبر 2021، ص 11.

[2]باخويا دريس /رواق العمرية، المرجع السابق، ص79.

[3]نايف شافي المظافره الهاجري، "مدى حجية الوسائل العلمية الحديثة في الإثبات الجنائي في التشريع الأمريكي"، المرجع السابق، ص141.

[4]نور الهدى محمودي، مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي-دراسة تحليلية-أطروحة دكتوراه، كلية الحقوق، تخصص علم الإجرام والعقاب، جامعة باتنة 1 -الحاج لخضر-الجزائر، 2017-2018، ص 210.

كما أنه لا يشكل أي تهديد أو مساس بخصوصية الأفراد لأنه لا يقوم سوى بقياس بعض التغييرات التي تطرأ على الشخص موضع الاختبار[1]، إضافة إلى أنه لا يؤثر على إرادة الشخص، فهو لا يلغي الإدراك عند الشخص، فله كامل الحرية في ممارسة حقوقه أثناء الاستجواب منها حقه في الصمت وعدم الإجابة على الأسئلة المطروحة عليه، ثم إن النتائج المتحصل عليها تخضع للسلطة التقديرية للقاضي، وأن الاعترافات المتحصل عليها نتيجة استخدام جهاز كشف الكذب تعد وليدة إرادة حرة لا يشوبها عيب بشرط أن يكون الخضوع للاختبار بناء على رضا المتهم[2].

2- الاتجاه المعارض: على الرغم من محاولة أنصار الاتجاه المؤيد إبراز أهمية استخدام جهاز كشف الكذب في المجال الجنائي، إلا أنه لاقى استنكارا كبيرا وسط غالبية الفقهاء، حيث يرفض أغلب الفقه استخدام جهاز كشف الكذب وعدم اللجوء إليه سواء كان برضا المتهم أو بدونه لأن ذلك يعد من قبيل الإكراه المادي، فلا قيمة للاعترافات والمعلومات المتحصل عليها عن طريقه، فضلا على ذلك النتائج التي تم الحصل عليها غير دقيقة نظرا للانفعالات والاضطرابات المسجلة التي تنتاب الشخص قد نتيجة للتوتر أو الخوف لا نتيجة للكذب، الأمر الذي يدفع الشخص لدائرة الاتهام والإدانة[3].

ثانيا: موقف التشريع

لم يختلف موقف التشريعات كثيرا عن رأي الفقه إزاء استخدام جهاز كشف الكذب من حيث قبوله أو عدم الأخذ بهذا لأنه لم تحظ نتائجه بالاعتراف أو التأييد العلمي[4].

ففي الولايات المتحدة الأمريكية تستخدم هذا الأجهزة في التحقيقات على اعتبار أن الشخص البريء ليس له ما يخفيه ويستغل الاختبار لإثبات براءته[5].

---

[1] باخويا دريس /رواق العمرية،" أثر الإثبات الجنائي بوسائل التقنية الحديثة على حقوق الانسان"، المرجع السابق، ص 79.

[2] راضية خليفة /نصيرة مهيرة، "جهاز كشف الكذب ومدى مشروعيته في الإثبات الجنائي"، المرجع السابق، ص 18.

[3] ياسين عزاوي، الوسائل العلمية للإثبات الجنائي ومشروعيتها، ص 14 موجود على الموقع التالي:
http://9anonak.blogspot.com

[4] زهار خالد عبد الله صباح، دور الوسائل العلمية الحديثة في الاثبات الجنائي، المرجع السابق، ص 83.

[5] نور الهدى محمودي، مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي، المرجع السابق، ص 221.

إلا أن المحاكم الأمريكية ترفض الإثبات الذي يتم الحصول عليه عن طريق استعمال هذا الجهاز، واعتبرت النتائج المتحصل عليها مترتبة عن إكراه معنوي، إلى أن استقر الوضع عل أن خضوع الشخص للاختيار برضاه يزيل كل عيب يؤثر على إرادته[1].

كما رفض المشرع الإيطالي الأخذ بنتائج هذا الجهاز واعتبر استخدامه يدخل ضمن طرق التعذيب الماسة بسلامة الأفراد[2].

أما بالنسبة للمشرع الفرنسي نجده ينص في المادة 01/114 من قانون الإجراءات الجزائية الفرنسي على أنه بإمكان قاضي التحقيق أن يبنه المتهم عند حضوره أمامه لأول مرة إلى أنه حر في عدم الإدلاء بأي إقرار وأن يثبت ذلك التنبيهبمحضر التحقيق، وهو ما يفسره البعض بجواز استخدام الجهاز بناء على موافقة صريحة من المتهم[3].

وإذ ما رجعنا للتشريعات العربية نجد أنها لم تتخذ موقف صريح يفيد بجواز أو حظر استخدام جهاز كشف الكذب، بيد أنه بالرجوع إلى دساتيرها نجدها تؤكد الضمانات والحقوق الأساسية للاستجواب[4]، فبالنسبة للمشرع المصري ينص في الدستور على عدم جوزا إجراء أي تجربة طبية أو عليمة على جسد الإنسان، وفي نفس السياق نصت المادة 220 من تعليمات النيابة العامة المصرية على أنه:" لا يجوز استخدام جهاز كشف الكذب للحصول على اعتراف المتهم لأن هذه الوسيلة يحوط نتائجها بعض الشك ولذلك لن يصبح لها قيمة علمية توحي بقدر كاف من الثقة في دقة ما تسفر عن نتائج هذا الجهاز من دلالات"، أي أنه تم استبعاد استخدامه صراحة[5].

أما المشرع الجزائري فلم يتطرق لمسألة استخدام الجهاز من عدمه، لكن بالرجوع إلى الضمانات القانونية التي تكفل الحقوق والحريات الفردية نستخلص أنه لا يجوز استخدام هذا الجهاز لأنه يعتبر انتهاكا لحرمة الانسان ومساسا بكرامته[6].

---

[1]نايف شافي المظافره الهاجري، "مدى حجية الوسائل العلمية الحديثة في الإثبات الجنائي في التشريع الأمريكي"، المرجع السابق، ص1432.

[2]باخويا دريس /رواق العمرية، "أثر الإثبات الجنائي بوسائل التقنية الحديثة على حقوق الانسان"، المرجع السابق، ص 79.

[3]راضية خليفة /نصيرة مهيرة، "جهاز كشف الكذب ومدى مشروعيته في الإثبات الجنائي"، المرجع السابق، ص 15.

[4]انظر المادة 60 من دستور جمهورية مصر العربية.

[5]نور الهدى محمودي، مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي، المرجع السابق، ص223.

[6]انظر المادة 39 من التعديل الدستوري الجزائري لسنة 2020.

المطلب الثاني: استخدام تقنية التنويم المغناطيسي

يعتبر التنويم المغناطيسي من المؤثرات التي يمكن لها التحكم في العقل البشري ومعرفته ما يحتويه من أسرار، وهو ما جعل مسألة الاستعانة به أمر مختلف فيه.

الفرع الأول: مفهوم تقنية التنويم المغناطيسي

إن التنويم المغناطيسي نوع من أنواع النوم لبعض ملكات العقل الظاهر، وهو يتم بجبر الخاضع للاختبار على النوم تحت تأثير الإيحاء، يصاحبه تغيير في حالة النائم نفسيا وجسمانيا على النحو الذي تتغير معه إرادة الفعل الطبيعي للشخص الخاضع للتنويم [1]بحيث ينعدم الاتصال الخارجي للنائم، فتختفي ذاته الشعورية وتبقى خاضعة لسيطرة المنوم فيتمكن من أن يحصل على كل المعلومات المتعلقة بالجريمة في هذه الحالة[2].

وقد اتجهت الأفكار الحديثة إلى إمكانية استخدامه لمواجهة التطور الإجرامي نظرا إلى ماله من أثر على شخصية المتهم فيمكن عن طريق استخدامه استقصاء الحقائق وكل ما يحتفظ به المتهم من معلومات في سره ولا يمكن الوصول إليها عن طريق الأساليب العادية[3].

على الرغم من أهمية التنويم المغناطيسي في استخراج ما يحتفظ به الشخص الخاضع له من أسرار إلا أن له تأثيرا سلبيا عل جسد الشخص ونفسيته، حيث أثبتت بعض الحالات أن هناك آثارا استمرت معه حتى بعد انتهاء عملية التنويم، ومثال ذلك طلب فعل شيء ما فيقوم بتنفيذه، أو إجباره على اعترافات مزورة بخصوص الجريمة، كما يحدث أن هذه العملية تترك آثارا نفسية لدى الشخص منها فقدان الذاكرة ونسيان بعض الأحداث[4].

الفرع الثاني: مدى مشروعية استخدام التنويم المغناطيسي

على الرغم من أن التنويم المغناطيسي له لأثر فعال في استقصاء المعلومات والأفكار في المجال الجنائي غير أنه أثار جدلا فقهيا وتشريعيا حول قبول الاستعانة به في مجال الإثبات الجنائي من عدمه.

---

[1]زاهر خالد عبدالله صباح، دور الوسائل العلمية الحديثة في الإثبات الجنائي، المرجع السابق، ص 77.

[2]ياسين عزاوي، "الوسائل العلمية للإثبات الجنائي ومدى مشروعتيها"، المرجع السابق، ص 05.

[3]المحامية مروة أبو العلا: التنويم المغناطيسي في مجال التحقيقات الجنائية، مقال قانوني، 21 سبتمبر 2018، يوم الزيارة 2022/08/10 على الساعة 15:40، موجود على الرابط التالي:

https://www.mohamah.net/law/التنويم-المغناطيسي-في-مجال-التحقيقات/

[4]ياسين عزاوي، المرجع نفسه، ص 06.

أولا: موقف الفقه

تباينت آراء الفقهاء حول مدى مشروعية هذا الأسلوب، فذهب رأي فقهي إلى القول بجواز استخدام تقنية التنويم المغناطيسي شرط أن يتم من قبل مختص لتجنب الآثار غير المرغوب فيها والتمكن من التحكم الجيد في الخاضع للاختبار مع الموافقة الصريحة للخاضع له، بالإضافة إلى عدم الاستعانة به إلا عند الضرورة وفي الجرائم الخطيرة[1].

إذن من وجهة نظر أنصار هذا الاتجاه استخدام تقنية التنويم المغناطيسي يقف على حسن استعماله بالقدر الذي لا يؤدي لانتهاك حق الخصوصية.

فيما ذهب اتجاه آخر من الفقه للقول بعدم مشروعية التنويم المغناطيسي ولا يجيزون استخدامه حتى ولو كان محاطا بضمانات قانونية على اعتبار أن المعلومات والاعترافات المتحصل عليها عن طريقه تقع باطلة، لأن الشخص يكون خاضع لإرادة المنوم وبالتالي فإرادته منعدمة، وأن من شروط صحة الاعتراف هو التمتع بإرادة حرة دون إكراه أو تأثير من أحد[2].

ثانيا: موقف التشريعات

على صعيد التشريع يتبين أن أغلبها لم يكن لها موقف صريح بشأن هذه المسألة، إلا أن بعض التشريعات حظرت اللجوء إليه بنصوص صريحة، إذ ينص قانون العقوبات الإيطالي على معاقبة كل من تسبب في سلب حرية الإرادة والتفكير لدى شخص ما بالتنويم المغناطيسي أو استخدام المواد الكحولية أو المخدرة سواء كان بموافقته أو بدونها[3].

كما أخذ المشرع الألماني بنفس التوجه إذ منع استخدام التنويم المغناطيسي في المجال الجنائي وحرص على حماية المتهم أثناء الاستجواب من جميع المسائل التي يمكن أن تؤثر على إرادته أو حريته

---

[1] باخويا دريس /رواق العمرية، "أثر الوسائل العلمية الحديثة في الإثبات الجنائي على حقوق الانسان"، المرجع السابق، ص 80.

[2] آية لوصيف، مشروعية استخدام التنويم المغناطيسي في التحقيق–مقال قانوني، 20 يناير 2018، يوم الزيارة 2022/08/12 موجود على الرابط التالي:

https://www.mohmah.net/law/

[3] خالد زاهر عبد الله صباح، دور الوسائل العلمية الحديثة في الإثبات الجنائي، المرجع السابق، ص 79.

كالتنويم المغناطيسي أو التحليل النفسي في التحقيق وهو ما نصت عليه المادة 132 من قانون الإجراءات الألماني[1].

وقد استقر القضاء الفرنسي على أن التنويم المغناطيسي يعد أحد الوسائل التي تنطوي على اعتداء على حقوق الانسان، وهو نفس الأمر الذي أقره القضاء الأنجلوأمريكي[2].

أما بالنسبة للمشرع الجزائري فليس هناك نص صريح يفيد بجواز استخدام هذه التقنية أو منعها، غير أن بالرجوع إلى الأحكام القانونية في قانون الإجراءات الجزائية يفهم منها عدم مشروعية الاستعانة بتقنية التنويم المغناطيسي[3].

يستشف مما سبق أن استخدام التنويم المغناطيسي يعد تعديا على حرية الفرد محل الاختبار، لأنه يعدم إرادته الحرة فيما يريد الإفصاح به أو عدم الإدلاء بأي شيء وبالتالي فإن الاعترافات المتحصل عليها تقع باطلة، وإذا كانت الوسيلة في الإثبات غير مشروعة فإن الدليل المتحصل عليه عن طريقها غير مشروع.

---

[1] ياسين عزاوي، الوسائل العلمية في الإثبات الجنائي ومدى مشروعيتها، المرجع السابق، ص 10.

[2] خالد زاهر عبد الله صباح، المرجع نفسه، ص 79.

[3] انظر المادة 100 من الأمر 66-155 المتضمن قانون الإجراءات الجزائية.

خاتمة:

نظرا لقصور الأساليب التقليدية في الكشف عن الجريمة، بات الاعتماد على التقنيات الحديثة في مجال الإثبات الجنائي أمرا حتميا، إلا أنه على الرغم من ثبوت فعاليتها في الكشف عن الجرائم واستقصاء الحقائق الخفية فإن الاستعانة بها تشكل انتهاكا لخصوصية الأفراد وتعديا على حرمة حياتهم الخاصة، وهو ما خلق جدلا فقهيا وتشريعيا حول مدى مشروعيتها حيث تباينت آراء الفقهاء بين مؤيد ومعارض لاستخدامها، فذهب غالبية الفقه إلى لعدم قبولها كوسيلة من وسائل الإثبات الجنائي فالدليل المستمد منها يعد باطلا نظرا لعدم مشروعية الوسيلة المستعملة، ولم يختلف التشريع عن غالبية الفقه في عدة جواز الاستعانة بوسائل التقنية الحديثة، إلا أجهزة التصنت والمراقبة حيث تنص أغلب التشريعات على جواز اللجوء إليها متى دعت الحاجة الملحة لذلك مع إحاطتها بجملة من الضمانات القانونية لضمان عدم انتهاك حقوق حريات الأفراد حتى ولو ثبت في حقه الاتهام.

ومن خلال هذه الدراسة تم التوصل إلى النتائج التالية:

- على الرغم من الدور المهم الذي تلعبه وسائل التقنية الحديثة في الإثبات الجنائي هذا لأنها لم تحظ الاعتراف أو التأييد العلمي.
- إن النتائج المتحصل عليها من جهاز كشف الكذب وتقنية التنويم المغناطيسي قد يشوبها بعض العيوب والأخطاء، الأمر الذي يؤدي بالتشكيك حول مصداقية الدليل المستمد.
- تعد أجهزة التصنت والمراقبة من أخطر التقنيات التي يتم الاستعانة لأنها تشكل تهديدا صريحا لحرمة الحياة الخاصة بالأفراد.
- الاستعانة بالوسائل التقنية يؤثر على حقوق الانسان ويمس بكرامته.

بناء على ما سبق نقترح التالي:

- إن عجز الأساليب التقليدية يستدعي بالضرورة اللجوء لوسائل تقنية أكثر حداثة تواكب وتتوافق مع التطورات الحاصلة في عالم الجريمة، فبدون الاستعانة بها لا يمكن مكافحة الجريمة لا سيما وأن

الإجرام يتزايد ويتطور بتطور التكنولوجيا، لكن لا بد من إحاطتها بضمانات وضوابط قانونية مع إقرار جزاء صارم في حال الإخلال بها.

- صحيح أنالنتائج المتحصل عليها عن طريق استخدام التقنيات الحديثة تخضع للسلطة التقديرية للقاضي فله الأخذ بها وله عدم قبولها، إلا إمكانية التلاعب بها وتزويرها أمر وارد، لذا وجب أخذ الحيطة اللازمة في حال استخدامها.
- إذ ما تم الاستعانة بجهاز كشف الكذب أو التنويم المغناطيسي لا بد من أخذ موافقة صريحة من المعني حتى لا تكون الاعترافات المتحصل عليها نتيجة الإكراه، كما أنه يستحب عدم اللجوء لتقنية التنويم المغناطيسي لأنه يعدم الإرادة الحرة للفرد.

قائمة المصادر والمراجع:

المصادر:

الإعلانات والاتفاقيات الدولية:

- الإعلان العالمي لحقوق الإنسان المنعقد بموجب قرار الجمعية العامة 217 ألف، باريس، المؤرخ في 10 ديسمبر 1948.
- الاتفاقية الأوروبية لحقوق الإنسان في نطاق مجلس أوروبا، روما في 4 نوفمبر 1950.

الدساتير والقوانين:

- المرسوم الرئاسي رقم 20–442 يتضمن التعديل الدستوري، الجريدة الرسمية العدد 82. المؤرخ في 30 ديسمبر 2020.
- القانون 06–22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 66–155 المؤرخ في 8 يونيو 1966.
- القانون 09–04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47، المؤرخ في 5 أوت سنة 2009.
- دستور جمهورية مصر العربية وفقا للتعديلات الدستورية 23 أبريل 2019.

المراجع:

الكتب:

- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)، المكتب الجامعي الحديث، الإسكندرية، 2013.

الأطروحات:

- نور الهدى محمودي، **مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي**–دراسة تحليلية– أطروحة دكتوراه، كلية الحقوق، تخصص علم الإجرام والعقاب، جامعة باتنة 1 –الحاج لخضر– الجزائر، 2017–2018.

رسائل الماجستير:

- زاهر خالد عبد الله صباح، **دور الوسائل العلمية الحديثة في الاثبات الجنائي في فلسطين**، رسالة ماجستير، جامعة القدس، فلسطين، 2017.

المقالات:

- أنيس حسيب السيد المحلاوي، "مدى مشروعية الوسائل التي تستخدم بشكل خفي كدليل للإثبات الجنائي"، 2018.
- باخويا دريس /رواق العمرية، "أثر الإثبات الجنائي بوسائل التقنية الحديثة على حقوق الانسان" مجلة الدراسات القانونية والسياسية، العدد 05–المجلد 01 جانفي 2017.
- جميلة محلق، "اعتراض المرسلات وتسجيل الأصوات والتقاط الصور في قانون الإجراءات الجزائية"، التواصل في الاقتصاد والإدارة والقانون، عدد 42 جوان 2015، عنابة، الجزائر.
- راضية خليفة /نصيرة مهيرة "جهاز كشف الكذب ومدى مشروعيته في الإثبات الجنائي"، مجلة الاجتهاد القضائي، المجلد 13–العدد 02 (العدد التسلسلي 27)، أكتوبر 2021.
- عبد الحليم بن بادة، "المراقبة الإلكترونية كإجراء لاستخلاص الدليل الإلكتروني" بين الحق في الخصوصية ومشروعية الدليل الإلكتروني.
- فوزي عمارة، "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كإجراءات تحقيق قضائي في المواد الجزائية"، مجلة العلوم الإنسانية، عدد 33 جوان 2010.
- نايف شافي المظافري الهاجري، "مدى حجية الوسائل العلمية الحديثة في الإثبات الجنائي في التشريع الأمريكي"، المجلة القانونية مختصة في الدراسات والبحوث القانونية، أكاديمية سعد العبد الله للعلوم الأمنية، الكويت، ISSN:(2537–058).

المواقع:

- ياسين عزاوي، الوسائل العلمية للإثبات الجنائي ومشروعيتها، موجود على الموقع التالي: http://9anonak.blogspot.com

- المحامية مروة أبو العلا: التنويم المغناطيسي في مجال التحقيقات الجنائية، مقال قانوني، 21 سبتمبر 2018، يوم الزيارة 2022/08/10 على الساعة 15:40، موجود على الرابط التالي: https://www.mohamah.net/law/التنويم–المغناطيسي–في–مجال–التحقيقات/

- آية لوصيف، مشروعية استخدام التنويم المغناطيسي في التحقيق–مقال قانوني، 20 يناير 2018، يوم الزيارة 2022/08/12 موجود على الرابط التالي:

https://www.mohamah.net/law/ما–مدى–مشروعية–التنويم–المغناطيسي–في–الفقه–و–التشريع/

الملتقى الدولي: " القانون الجنائي في ظل التطور التكنولوجي إشكالات ة معالجات "

استمارة المشاركة

المحور الخامس: أثر الوسائل العملية الحديثة على الإثبات الجنائي

بن بوعبدالله نورة/ أستاذة محاضرة قسم أ

الجزائر .جامعة الحاج لخضر باتنة 1
مخبر الحوكمة والقانون الاقتصادي

norabenbouabdallah@gmail.com

ديب أكرم/ طالب دكتوراه

الجزائر .جامعة الحاج لخضر باتنة 1
مخبر الحوكمة والقانون الاقتصادي

akram.dib@univ-batna.dz

عنوان المداخلة: تداعيات الإثبات الجنائي بوسائل التقنية العلمية الحديثة على حقوق الإنسان

The repercussions of criminal proof using modern scientifictechnology on humanrights

رقم الهاتف : 07.77.80.69.09

ملخص:

من منطلق مبدأ قرينة البراءة المفترضة في جميع الأفراد بنص الدستور و نصوص قانون الإجراءات الجزائية ، يثار الجدل بخصوص القيمة القانونية للأدلة العلمية الحديثة التي كانت نتاج ما أفرزته التطورات التكنولوجية و العلمية و البيولوجية و بروز معالم النظام العالمي الجديد و صاحب ذلك ظهور أنماط جديدة من الإجرام المستحدث، حيث يكتنف استخدام الوسائل العلمية الحديثة و مباشرتها عدة إشكالات تصب في تيار التعدي و انتهاك الحريات و المبادئ الأساسية لحقوق المتهم المحمية في المواثيق الدولية و الدساتير و القوانين الداخلية للدول، و هو ما يترتب عنه ضرورة إحلال السلطات القضائية المختصة و التي يناط بها مهمة استخدام الوسائل العلمية الحديثة موازنة بين مصلحتها في

البحث عن الحقيقة و العقاب من جهة و بين مصلحة الأفراد في أن تصان حقوقهم و حرياتهم من جهة أخرى.

وتهدف هذه الدراسة بالأساس للتعرض إلى تطور أدلة الإثبات الجنائي الذي اقترن بالثورة التكنولوجية التي شهدها العالم في شتى الميادين، وإبراز المكانة التي تحتلها الأدلة العلمية الحديثة في الإثبات الجنائي من حيث قوتها التدليلية ومدى احترامها للضمانات القانونية التي تمنع المساس بالحقوق والحريات الفردية.

الكلمات المفتاحية: الأدلة العملية الحديثة _ الإثبات الجنائي _ قرينة البراءة _ الضمانات القانونية_ الحريات الفردية.

Abstract :

In terms of the presumption of innocence,Assumed in all individuals by the text of the constitution and othertextsThe Code of CriminalProcedure, controversy arises regarding the legal value of modern scientific evidence, whichwas the product of technological, scientific and biologicaldevelopments, and the emergence of the features of the new world order, accompanied by the emergence of new patterns of newlycreated crime, where the use of modern scientificmeans and its initiation are surrounded by severalproblemsthat lead to In the current of infringement and violation of freedoms and basic principles of the rights of the accusedprotected in international covenants and constitutions And the internallaws of countries, whichresults in the need to replace the competentjudicialauthoritiesthat are entrustedwith the task of using modern scientificmeans, balancingtheirinterest in the search for truth and punishment on the one hand, and the interest of individuals in protectingtheirrights and freedoms on the other hand.

These are aimedatThestudyismainly to expose the development of criminal proof evidence thatwasassociatedwith the technologicalrevolutionthat the world witnessed in variousfields.andhighlighting the positionthatOccupied by evidenceModernscientific evidence in criminal proof in terms of itsdemonstrativepowerand how muchrespectLegalguaranteesthatpreventinfringement of rightsandindividualliberties.

key words: Modern practical evidence - criminal proof - presumption of innocence - legalguarantees - individualfreedoms.

بوقادوم ـ يحياوي صليحة ـ أستاذة محاضرة أ
كلية الحقوق – جامعة الجزائر1 يوسف بن خدة
التخصص: القانون الجنائي والعلوم الجنائية
البريد الإلكتروني: sbougadoum.fdroit@gmail.com
عنوان المداخلة: تكنولوجيات الاعلام والاتصال كمحرك لعصرنة العدالة الجنائية

ملخص المداخلة

أحدث تطور تكنولوجيات الاعلام والاتصال ثورة في كل مجالات الحياة، سواء تعلق الأمر بالحياة الشخصية للفرد أو بالمجال العام الذي يتقاسمه الجميع. وانعكست آثار هذا التطور على قطاع العدالة من خلال تحويل الإدارة التقليدية إلى إدارة رقمية حديثة، بإصدار نصوص تشريعية تضمن تحسين الخدمات وترشيدها من جهة، وإدخال تعديلات على الجانب القضائي حيث كان من الضروري مواكبة هذا التطور بإدخال التكنولوجيا الحديثة في العمل القضائي للكشف عن الجرائم والمجرمين باستعمال الوسائل الحديثة للإسراع في إجراءات التحري والتحقيق وتقليص آجال المحاكمة الجنائية، من جهة أخرى.

للبحث في هذا الموضوع والمتعلق باستعمال القضاء لوسائل التكنولوجيا الحديثة نطرح الإشكالية الموالية:

هل حقق قطاع العدالة خلال التعديلات التي أدخلها المشرع لعصرنة قطاع العدالة وتطوير إجراءات التحقيق والمحاكمة بما يسمى بالتقاضي الالكتروني، مواكبة التطور التكنولوجي من الجانب الإداري ومن الجانب القضائي؟

للإجابة عن الإشكالية المطروحة، نبحث في مفهوم العصرنة وأهدافها (المبحث الأول)، وفي الوسائل التكنولوجية المستعملة في إجراءات التقاضي (المبحث الثاني).

الكلمات المفتاحية: عصرنة قطاع العدالة، التكنولوجيا الحديثة، التقاضي الالكتروني، المحاكمة العادلة.

Abstract

The development of information and communication technologies has brought about a revolution in all areas of life. Weather it is related to the personal life or the public sphere. The effects of this development have been reflected on the justice sector by transforming the traditional administration into a modern digital administration by issuing legislative texts that guarantee the improvement and rationalization of services, and amendments were made to the judicial side, where it was necessary to keep pace with this development by introducing modern technology into the judicial work to detect crimes and criminals using modern means to speed up investigation procedures and reduce the deadlines for criminal trial. To discuss this subject, we raise the following problem: Has the justice sector achieved through the amendments introduced by the legislator to modernize the justice domain and develop investigation and trial procedures to keep pace with development from the administrative side and from the judicial side? To answer the problem posed, we discuss the concept of modernity and its objectives (first), and the technological means used in litigation procedures (secondly).

Keywords: modernization of the justice sector, modern technology, electronic litigation, fair trial.

مقدمة

تظهر آثار التطور العلمي والتكنولوجي بوضوح في كافة مجالات الحياة والمرافق التي يلجأ لها المواطن في حياته العادية. إن هذه التكنولوجيات الحديثة التي لم تساهم فقط في التقدم والرقي، ولم تستعمل في الجوانب الإيجابية فحسب، بل تم استغلالها كذلك من طرف الجماعات الاجرامية التي استفادت من هذا التقدم التكنولوجي الحديث لارتكاب الجرائم وللتستر عليها. وعليه ولمواجهة الاجرام كان من الضروري التفات المشرع لتعديل القوانين بما يساير التقدم العلمي والتكنولوجي من جهة ولمواجهة المجرمين من جهة أخرى.

إذا اعتبرنا أن لوسائل تكنولوجيات الاعلام والاتصال دور مهم في تسيير قطاع العدالة من الجانب الإداري، فإن استعمالها ضروري كذلك للبحث في الجريمة والمجرمين أثناء التحقيق فيها وكذلك أثناء المحاكمة دون حضور المتهم أو الشهود عن طريق ما يسمى vidéoconférence.

للإجابة على الإشكالية المطروحة: هل تم تحقيق نتائج إيجابية من خلال التعديلات الخاصة بعصرنة قطاع العدالة وبتطوير إجراءات التحقيق والمحاكمة بما يسمى بالتقاضي الالكتروني لمواكبة التطور التكنولوجي من الجانب الإداري ومن الجانب القضائي؟ نتطرق لمفهوم عصرنة العدالة وأهدافه (المبحث الأول) وللوسائل التكنولوجيا الحديثة المستعملة للتقاضي (المبحث الثاني)

المبحث الأول

عصرنة العدالة والأهداف المنتظرة

إنّ عصرنة العدالة من الخطوات الهامة التي أدخلت تكنولوجيا الإعلام والاتصال في قطاع العدالة، للاستفادة من مزايا هذه الوسائل الحديثة لترقية الجانب الإداري للقطاع من إدارة ورقية تقليدية إلى إدارة عصرية رقمية.

من بين أهم المبررات التي تدفع بالتوجه نحو ادخال الوسائل التكنولوجية الحديثة في قطاع العدالة (الإدارة الإلكترونية)، ملاحظة النتائج الإيجابية المحققة في الدول السبّاقة في استعمالها، كما تعتبر من المبررات كذلك ملاحظة السلبيات الكثيرة للإدارة التقليدية، لاسيما الإجراءات الإدارية المعقدة والبطيئة المتسمة بالبيروقراطية السلبية والتي ترهق كاهل المواطن.

إن اعتماد نظام إدخال الوسائل التكنولوجيا الحديثة في التسيير المنطقي لشؤون الإدارة[1] يساهم بشكل واضح في ربح الوقت من خلال عدة جوانب منها الاعتماد على مفهوم العمل عن بعد، حيث يمكن للمواطن القيام ببعض الإجراءات وهو في منزله كسحب العديد من الوثائق أو تقديم شكاوى والطلبات عن بعد. وسيتّضح من خلال ما يلي مجالات عصرنة العدالة (في المطلب الأول) كما يمكن للقضاء الاستعانة بالعديد من الوسائل التكنولوجية الحديثة للوقاية من الجريمة ولتدعيم ادلة الاثبات في بعض الجرائم، ونتطرق في هذا الإطار لكاميرات المراقبة (المطلب الثاني).

[1] - Renaud Colson, Stewart Field, La fabrique des procédures pénales Comparaison franco-anglaise des réformes de la justice répressive, Dalloz « Revue de science criminelle et de droit pénal comparé » 2010/2 N° 2 | pages 365 à 393 ISSN 0035-1733 DOI 10.3917/rsc.1002.0365, p 386.

المطلب الأول

مجالات عصرنة العدالة

تتمثل عملية عصرنة العدالة في السعي أساسا لتطبيق نظام الإدارة الالكترونية، وذلك باستخدام الوسائط الالكترونية كآلية لتجسيد إجراءات التقاضي عن بعد باستعمال أجهزة الحاسوب المتصلة بشبكة الانترنت[2].

يعتبر قطاع العدالة من بين المرافق التي تم عصرنتها، وذلك بإدخال التطبيقات المعلوماتية في تسيير الإدارة (الفرع الأول) والاهداف المنتظرة من العصرنة (الفرع الثاني).

الفرع الأول: إدخال التطبيقات المعلوماتية في قطاع العدالة

لتطوير وعصرنة قطاع العدالة ولملاءمته مع معطيات العولمة، تبنت الجزائر ما يسمى برقمنة قطاع العدالة بموجب القانون 15-03، كما تم تعديل قانون الإجراءات الجزائية 20-04 لرقمنه مرفق القضاء.

لنجاح استعمال الوسائل التكنولوجيا في مرفق القضاء ونجاح عملية التقاضي الالكتروني، يستوجب العديد من الشروط منها المرتبطة بالجانب الإداري ومنها المرتبطة بالجانب القضائي.

بالنسبة للجانب الإداري فإن العصرنة مست العديد من الإنجازات يمكن تلخيصها فما يلي:

- إنشاء شبكة اتصال داخلية بين المجالس القضائية والمحكمة العليا ومجلس الدولة،
- تدعيم المؤسسات العقابية بشبكات معلوماتية تمكنها من تبادل المعلومات بصفة فورية وآمنة،
- انشاء الشباك الالكتروني الذي يعتبر بوابة الكترونية تجيب عن انشغالات المواطن،
- نظام تسيير ومتابعة الملفات القضائية (كتسجيل الطعون في مقر المجلس القضائي أمام مصلحة الطعون على مستوى الشبكة وذلك دون الانتقال إلى مقر المحكمة العليا)،
- انشاء صفحة لسحب صحيفة السوابق العدلية من موقع وزارة العدل،
- إدماج تقنية التوقيع والتصديق الالكتروني في المجال القضائي،
- استحداث صفحة خاصة بالنيابة الالكترونية[3] على الموقع الالكتروني لوزارة العدل لتلقى الشكاوى،
- ادخال نظام تسيير الأوامر بالقبض ونظام لمتابعة ملفات المحبوسين...

الفرع الثاني: الأهداف المنتظرة

لنجاح العصرنة يفترض توفر إطار قانوني واضح، ووسائل بشرية تكمن في المختصين في المجالات التقنية والفنية كما يفترض من قضاة ومساعدي القضاء من كتاب وأمناء ضبط ومحامين، الدراية الكافية بالوسائل

- [2]- بلباقي بومدين، قانون عصرنة العدالة وأثره على تحقيق المبادئ الأساسية للتقاضي، مجلة القانون والعلوم الاجتماعية، المجلد 6، العدد 4، 2021، ص 1263.

[3] - https://e-nyaba.mjustice.dz

التكنولوجية لإمكانية التعامل بها، وتعتبر هذه الوسائل من الركائز الأساسية لنجاح عملية عصرنة العدالة من جهة والتقاضي الالكتروني من جهة أخرى.

إن الأهداف المنتظرة من عمليات عصرنة العدالة ومن استعمال وسائل تكنولوجيا الإعلام والاتصال، التكّمن في الاستغلال الأمثل لهذه الوسائل لتحسين الأداء، وتسهيل عمل مستخدمي وأعوان قطاع العدالة وكذلك تقريب العدالة من المواطن. كما يساهم في تقليل النفقات بشكل ملحوظ، وخفض نسب معدلات التغيب عن العمل[4]، لتحقيق ذلك وإلى جانب ما تم تفعيله فإنه من الضروري دعم هذا المسعى وتفعيل جوانب أخرى منها:

- دعم الوسائل التكنولوجية الحديثة التي تمكن من الولوج إلى قطاع العدالة،
- تحسين وترقية الخدمات التي تقدمها المحاكم والمجالس القضائية،
- إنشاء منصة رقمية تمكن المحامين من القيام بجميع الإجراءات المتعلقة بتبادل الوثائق القضائية،
- تمكين المحامين من تسجيل القضايا عن بعد دون التنقل إلى المحاكم.
- تمكين المتقاضين والمحامين من الاطلاع على ملفاتهم ومتابعتها عن بعد مما يوفر الوقت ويقلل الكلفة.

المطلب الثاني

استعمال كاميرات المراقبة

يلاحظ في عصرنا هذا انتشار استعمال كاميرات المراقبة في الأماكن العمومية التي يقصدها عامة الناس لقضاء حوائجهم في حياتهم اليومية بصفة عادية. يتم وضع الكاميرات في المباني الحكومية والمنشآت الحيوية داخل المدن وفي المراكز الأمنية وفي المطارات والمنافذ الحدودية وفي الطرق السيارة لمراقبة سير المركبات. والهدف الأساسي من ذلك هو حماية المواطن وكذلك حفظ الأمن ومكافحة الجريمة وحماية مستعملي هذه الأماكن.

ظهرت الكاميرات الخفية وتم استخدامها لمراقبة الأشخاص المشتبه فيهم في جرائم معينة منذ وقت طويل وذلك بغرض استخدام محتوياتها للإثبات في المحاكم كما تستخدم كذلك لاتخاذ اجراءات وقائية لضبط المجرمين، او للوقاية من الاجرام.

أصبح استخدام هذه الكاميرات بصفة خفية أو علنية أمرا عاديا في المؤسسات الحساسة والمؤسسات التجارية وذلك نظرا لتزايد جرائم السرقة.

ويسمى هذا النوع من المراقبة الالكترونية بالمراقبة البصرية. ويتم من خلال كاميرات او أجهزة خاصة تلتقط الصورة والصوت دون علم الجهة المراد مراقبتها لأغراض البحث الاولى في القضايا الجنائية.

---

[4] حمدي أحمد سعد، العمل عن بعد (ذاتيته–تنفيذه): دراسة تأصيلية تحليلية مقارنة في ضوء القواعد العامة لقانون العمل، دار الشتات للنشر والبرمجيات، مصر، 2010، ص.25.

بالنسبة للمشرع الجزائري، فإنه نظم موضوع كاميرات المراقبة على مرحلتين وذلك بإصدار المرسوم الرئاسي رقم 09-337 الذي نظم إحداث مؤسسة انجاز أنظمة المراقبة بواسطة الفيديو[5]، والذي حدد فيه إنشاء مؤسسة عمومية ذات طابع صناعي وتجاري تحت تسمية «مؤسسة انجاز أنظمة المراقبة بواسطة الفيديو" وتتمتع هذه الأخيرة بالشخصية المعنوية وبالاستقلال المالي، وهي مؤسسة تابعة للقطاع الاقتصادي للجيش الوطني الشعبي. ويعتبر هذا المرسوم الخطوة الأولى لتنظيم المراقبة بواسطة الفيديو.

أما المرحلة الثانية، فتتمثل في إصدار المرسوم الرئاسي رقم 15-228[6] الذي نظم موضوع كاميرات المراقبة وحدد أحكام النظام الوطني للمراقبة بواسطة الفيديو. فيما يلي مجالات استعمال كاميرات المراقبة "المراقبة بواسطة الفيديو" والهدف من المراقبة بواسطة الفيديو (الفرع الأول)، وأماكن وشروط تنصيب هذه الكاميرات (الفرع الثاني).

الفرع الأول: مجالات وهدف استعمال كاميرات المراقبة

فيما يلي مجالات المراقبة بواسطة الفيديو (أولا)، والهداف من المراقبة بواسطة الفيديو(ثانيا).

أولا: مجالات المراقبة بواسطة الفيديو

تعتبر المراقبة بواسطة الفيديو أداة تقنية للاطلاع والاستباق ويتم استعمالها أساسا لـ:

- مكافحة الإرهاب،
- الوقاية من الأعمال الاجرامية،
- حماية الأشخاص والممتلكات،
- الحفاظ على النظام العام،
- ضبط حركة السير عبر الطرق ومعاينة المخالفات لقواعد حركة المرور عبر الطرق،
- تامين البنايات والمواقع الحساسة،
- تسيير وضعيات الازمة/ أو الكوارث الطبيعية أو غيرها.

ثانيا: الهدف من المراقبة بواسطة الفيديو

إن النظام الوطني للمراقبة بواسطة الفيديو موجه اساسا لمساعدة ودعم الترتيبات البشرية للأمن أو الإنقاذ التي تنشط في الميدان من جهة وتحسين مستوى عمل هذه الجهات بتزويدها بالمعلومات الضرورية وذلك لتحقيق عدة اهداف منها:

---

[5]- المرسوم الرئاسي رقم 09-337 المؤرخ في 2009/10/21 المتضمن إحداث مؤسسة انجاز أنظمة المراقبة بواسطة الفيديو الصادر في الجريدة الرسمية العدد 61 بتاريخ 2009/10/25.

[6]- المرسوم الرئاسي رقم 15-228 المؤرخ في 7 ذي القعدة عام 1436 الموافق 08/22/ 2015 المتضمن القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره، الصادر في الجريدة الرسمية عدد 45 بتاريخ 2015/08/23.

- منع ارتكاب الجرائم ومكافحة الجريمة بفعالية وتسهيل عملية التعرف على المجرمين والقاء القبض عليهم، حيث يمكن الاعتماد على التسجيلات في الإثبات الجنائي[7]،
- تسهيل عملية حفظ الأمن العام،
- الفعالية في العمل المباشر في الميدان بالتنسيق والانسجام اثناء التدخلات،
- رفع عمليات الإنقاذ والتقليل من الأضرار والخسائر.

الفرع الثاني: أماكن وشروط تنصيب كاميرات المراقبة بواسطة الفيديو

نص المرسوم السابق ذكره على الأماكن التي يمكن ان تكون محل مراقبة بواسطة الفيديو(أولا)، كما حدد شروط تنصيب هذه الكاميرات(ثانيا).

أولا: الأماكن التي يمكن ان تكون محلا للمراقبة بواسطة الفيديو

حددت المادة الرابعة من المرسوم المذكور الأماكن التي تكون محلا للمراقبة بواسطة الفيديو وهي:

- التجمعات الحضرية الكبرى ومناطق ضواحي المدن،
- محاور الطرق الكبرى، لاسيما منها مقاطع الطرق ذات الحركة الكثيفة،
- الأماكن المفتوحة للجمهور، كالموانئ والمطارات والمنشآت الرياضية الكبرى،
- المؤسسات الاقتصادية الكبرى.

ثانيا: شروط تنصيب كاميرات المراقبة بواسطة الفيديو

لا يخضع تنصيب كاميرات المراقبة في الأماكن العامة أو المفتوحة للجمهور إلى رخصة إدارية مسبقة، بينما يخضع تنصيب كاميرات المراقبة الموجهة لتصوير الطريق العام من أجل حماية ضواحي موقع مؤسسة اقتصادية إلى رخصة إدارية يسلّمها الوالي.

يتم تنصيب الكاميرات طبقا لمخطط رئيسي للمراقبة بواسطة الفيديو يوافق عليه الوالي مع المصادقة عليه من قِبل لجنة الأمن الولائية. ويمكن ان تستعين هذه اللجنة، لإعداد المخطط الرئيسي للمراقبة بواسطة الفيديو، بمجموعة تقنية تتكون من ممثلين مؤهلين عن مصالح الأمن وعن كل مؤسسة أو هيئة أخرى ترى ضرورة في مساهمتها.

لا يخفى على أحد الدور الإيجابي الذي ينجم عن المراقبة بواسطة الفيديو، حيث تلعب هذه الأخيرة دورا هامّا لضبط العديد من المجرمين ومعاينة الكثير من مخالفات الطرق متى توفرت الشروط الضرورية لذلك[8].

---

[7]- فرحة عبد الرؤوف – القنيعي بن يوسف، كاميرات المراقبة بين اعتبارات اثبات الجريمة وانتهاك الحق في الخصوصية، مجلة الدراسات القانونية، المجلد 08، العدد 1، 2022، ص 756، 757.

[8] -Alain Bauer, François Freynet, vidéosurveillance et videoprotection, série « que sais-je » 2eme éd., 2012, presse universitaire de France, pages 81 -92.

المبحث الثاني

الوسائل التكنولوجيا الحديثة المستعملة للتقاضي

يتطور الاجرام مع تطور العلم وتقدمه، والملاحظ ان المجرم المعاصر قد واكب هذا التطور وأصبح في بعض الحالات يتجاوز قدرات أجهزة الشرطة لمكافحة الجريمة، بإيجاد حلول لتجنبها.

لمواجهة ظاهرة الاجرام لاسيما الاجرام المنظم[9]، ولتتبع خطى المجرمين يتم استعمال العديد من الوسائل التكنولوجيا، منها وسائل نص عليها المشرع للتحقيق في الجرائم المرتكبة كالمراقبة الالكترونية واستعمال المحادثة المرئية عن بعد في الاستجواب أو سماع شخص وفي اجراء المواجهات بين عدة اشخاص اثناء التحقيق (المطلب الأول)، وأثناء المحاكمة (المطلب الثاني).

المطلب الأول

المراقبة الالكترونية واستعمال المحادثة المرئية عن بعد

يعتبر الحق في الخصوصية من حقوق الانسان ويحظى هذا الحق بحماية قانونية واسعة، حيث يوجد على مستوى الشرعية الدولية لحقوق الإنسان نصوص عديدة تضمن حماية هذا الحق في مواجهة أي تدخل من السلطات العامة في الحياة الخاصة بصورة تعسفية أو غير قانونية[10].

يعني الحق في حرمة الحياة الخاصة العيش حرا بعيد عن التلصص والتجسس. وتحظى الحياة الخاصة بأهمية كبيرة في مواجهة وسائل التحقيق الحديثة التي تملكها السلطات العامة والتي قد يعتدى بها على الحياة الخاصة للشخص.

بالرغم من ضرورة احترام الحق في الحياة الخاصة، كالحق في المحافظة على سرية المحادثات الخاصة، سواء في مواجهة التنصت على المكالمات الهاتفية أو أي تنصت آخر تقوم به السلطة العامة، وكذا الحق في سرية المراسلات. إلا أنه في بعض الحالات وعند ارتكاب الجرائم، فإن القانون سمح للسلطات القضائية

---

[9]- بسبب الخطر العالمي الذي تمثله الجريمة والجريمة المنظمة، اولت الأمم المتحدة اهتماما لمكافحتها، ويظهر ذلك في العديد من المؤتمرات الدولية بداية من 1975 إلى صدور اتفاقية **باليرمو** في عام 2000 وهي اتفاقية خاصة بمكافحة بالجريمة المنظمة عبر الوطنية، وكذلك اتفاقية بودابيست 2001 لمكافحة الجرائم المعلوماتية، والاتفاقية العربية لمكافحة الفساد المحررة بالقاهرة بتاريخ 21 ديسمبر سنة 2010 مما يظهر ضرورة استعمال التكنولوجية الحديثة لمحاربة الجريمة. كما ظهر بعد احداث 11سبتمبر 2001 نظام عالمي جديد غير الاوضاع واصبحت دول العالم ولاسيما الغربية منها تطالب بالمزيد من المراقبة الاستباقية للتحقيقات اللاحقة.

[10]– المادة 17 من الاتفاقية الدولية لحماية الحقوق المدنية والسياسية؛ المادة 11 من الاتفاقية الأمريكية لحقوق الإنسان؛ المادة 8 من الاتفاقية الأوربية لحقوق الإنسان؛ المادة 12 من الإعلان العالمي لحقوق الإنسان، المادة 21 من الميثاق العربي.

اتخاذ إجراءات تمكنها من استعمال وسائل تكنولوجية حديثة للتحقيق ولجمع الأدلة، كما سمح لها استعمال هذه الوسائل للمحادثة المرئية عن بعد لاستكمال إجراءات التحقيق.

تعتبر المراقبة الالكترونية من أهم الوسائل والتقنيات التي أتى بها التطور التكنولوجي السمعي البصري الذي يشهده العالم المعاصر، وتعتبر من أهم الوسائل للكشف عن هذه الجرائم. كما يتم استعمال المحادثة المرئية عن بعد اثناء في التحقيق، وتعتبر هذه الآلية من الآليات القانونية للتقاضي الالكتروني.
نتطرق إلى اعتراض المراسلات والتنصت (الفرع الأول) واستعمال المحادثات المرئية عن بعد (الفرع الثاني).

الفرع الأول: اعتراض المراسلات والتنصت

لم يعرف المشرع الجزائري المراقبة الإلكترونية واكتفى بالإشارة إلى شروطها وآلياتها، وذلك ما نص عليه في المادة 65 مكرر 5 من قانون الإجراءات الجزائية.
يمكن تعريف المراقبة الالكترونية على أنّها: "عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور التي تكون بإشراف قضائي محدد لجرائم معينة وفقا لضوابط محددة في قانون الإجراءات"[11].
تختلف المصطلحات المستعملة للتعبير عن هذا الإجراء من لغة إلى أخرى، فهو يطلق على التصنت عن الاتصالات، ويستعمل كذلك في مراقبة الاتصالات السلكية واللاسلكية، وعلى التسجيل الصوتي والتصوير الخفي[12]. فيما يلي نتطرق لمفهوم وشروط اعتراض المراسلات (أولا) وللتنصت(ثانيا)

أولا: اعتراض المراسلات

القانون يحمي الحياة الخاصة للأشخاص ومن ذلك سرية المراسلات والمكالمات والمحادثات الخاصة. غير ان المشرع سمح بصفة استثنائية لجهات المتابعة الخروج عن هذه الحماية لمواجهة ومحاربة الجريمة وتطورها. فأورد في قانون الاجراءات الجزائية الاحكام المتعلقة باعتراض المراسلات وتسجيل الاصوات والتقاط الصور في الجرائم الخطيرة والمذكورة على سبيل الحصر، على ان يكون ذلك تحت المراقبة المباشرة للقضاء، مما يعني عدم جواز اللجوء الى هذه التدابير في حالة التحريات العادية[13].
لم يضع المشرع تعريفا لاعتراض المراسلات، واكتفى بوضع تنظيم لعملية اعتراض المراسلات في المواد 65 مكرر 5 إلى غاية المادة 65 مكرر 10 من قانون الإجراءات الجزائية، تاركا ذلك للفقه[14]. بينما أورد تعريفا

---

[11]– بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر 1، 2015، ص 195.

[12]–روابح فريد، الأساليب الإجرائية الخاصة للتحري والتحقيق في الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر 1، 2016، ص270.

[13]– مع العلم ان المشرع سمح بموجب القانون رقم 09–04 مالؤرّخ في 5 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وفي المادة 4 منه على أنه يمكن القيام بعمليات المراقبة في الجرائم الماسة بأمن الدولة.

[14]- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، 2009، ص 138.

للمراسلات في المادة 1/10 من القانون رقم 18-04 المؤرخ في 2018/05/10 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، فمصطلح المراسلات والمعبر عليها في هذا القانون بالاتصالات الالكترونية "هي كل إرسال أو تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو بيانات أو معلومات مهما كانت طبيعتها، عبر الأسلاك أو الألياف البصرية أو بطريقة كهرومغناطيسية."

ويقصد باعتراض المراسلات[15] إجراء تحقيق يباشر خفية ودون علم المعني بالأمر وينتهك سريّة المحادثات الخاصة، ويأمر بهذا الإجراء السلطة القضائية طبقا للشروط المحددة قانونا، وذلك بهدف الحصول على أدلة مادية للجريمة تمكن من توقيف المجرم.

ثانيا: التنصت

يعتبر إجراء مراقبة المحادثات التليفونية من أهم إجراءات اعتراض المراسلات.

ويقصد بها التنصت على المكالمات الخاصة بأشخاص مشتبه فيهم، ويتطلب أمر المراقبة التنصت على المحادثات وسماعها، لأنّ مراقبة المحادثات ومتابعتها ومعاينتها يفترض سماعها والتنصت عليها.

يشمل التنصت على المحادثات سماعها من جهة وتسجيلها بأجهزة التسجيل من جهة أخرى[16].

يتم هذا النوع من المراقبة باستقبال المراسلات التليفونية عن طريق التداخل في الخطوط التليفونية أو في مواجهة الرسائل اللاسلكية، فالمراقبة تتضمن المحادثات العادية وغير العادية حتّى يتسنّى للجهة المعنية بالتنصت الحكم بصورة صحيحة على مدى مشروعية الدليل المتحصل من مراقبة المحادثات التليفونية.

يحصل التنصت او التسجيل الهاتفي من خلال الدخول الى شبكة الهواتف الارضية او النقالة والتنصت على ما يدور بين شخصين او أكثر لمعرفة ما يدور من حديث بينهم، ويتم تسجيل هذه المحادثات بالكامل.

جدير بالذكر ان عملية التنصت يمكن ان تحصل من خلال مجمل المحادثات التي تمت بين شخصين او أكثر عبر شبكات الحاسوب او الانترنت وبالتحديد الدردشة التي تحصل باستعمال برنامج Messenger، بالإضافة الى الرسائل الصوتية التي يتم تبادلها عبر الشبكة العالمية. كما يمكن لأجهزة الرادار الحديثة التقاط

---

[15]- قد يقصد كذلك بالمراسلات جميع الخطابات المكتوبة سواء أرسلت بطريق البريد أو بواسطة وسائل خاصة، وكذلك المطبوعات والطرود والبرقيات التي توجد لدى مكاتب البريد، لكن المشرع الجزائري عندما تحدث عن اعتراض المراسلات يقصد تلك التي تتم بواسطة الاتصال السلكي واللاسلكي واستبعد الوسائل البريدية حرصا منه على ضمان حريّة وسريّة المراسلات بين الأفراد المكفولة دستوريّا من جهة ومن جهة أخرى لأن أفراد الشبكات والعصابات المنظمة يستعملون في خططهم الإجرامية أدوات وتجهيزات تكنولوجية متطورّة.

[16]- تجدر الإشارة إلى ان التنصت الهاتفي أنواع منها:

التنصت القضائي: وقد أدرجه المشرع الجزائري في القانون رقم 06-22 المؤرخ في 20-12-2006 المعدّل والمتمم لقانون الإجراءات الجزائية تحت عنوان اعتراض المراسلات السلكية واللاسلكية وأسنده لكل من قاضي التحقيق ووكيل الجمهورية.

والتنصت الإداري أو الأمني: هذا النوع مقنن في بعض التشريعات التي تسمح بممارسة اعتراض المراسلات بقرار من السلطات العليا والأمنية في الدولة وذلك وفقا لشروط معينة متعلقة بجمع المعلومات حول جرائم الإرهاب، جرائم أمن الدولة، الجرائم المنظمة العابرة للحدود.

الاصوات والمحادثات عبر الاتصالات اللاسلكية التي تستخدمها الدول المتطورة في عملية المراقبة والتحقيقات التي تجريها السلطات القضائية[17].

أحاط القانون مراقبة المكالمات الهاتفية بعدد من الضمانات للحفاظ على اسرار الافراد وخصوصيتهم ويتمثل أهم ضمان في وجوب صدور أمر من القضاء يسمح بمراقبة المحادثات. ويمكن أن يصدر هذا الامر من النيابة العامة، من قاضي التحقيق او من قاضي المحكمة المختصة، إلى جانب مجموعة من الشروط الأخرى وهي:

- تسبيب القرار الذي يسمح بالتنصت[18] او التسجيل الصوتي تسبيبا يبين ضرورة اللجوء لهذا الإجراء.
- وقوع جريمة بالفعل[19].
- أن تكون هذه الجريمة من الجرائم المنصوص عليها في القانون وهي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبيض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد.
- ان يكون الهدف الاساسي من هذا التنصت اظهار الحقيقة التي عجزت عنها الوسائل التقليدية والموضوع متروك لتقدير الجهة القضائية التي تأمر بالإجراء.
- ان تكون المراقبة محددة بفترة زمنية قابلة للتجديد عند الضرورة.

حصر المشرع الجزائري اجراء اعتراض المراسلات في جرائم محددة نصت عليها المادة 65 مكرر 5 من قانون الإجراءات الجزائية وتعدّ من الجرائم الخطرة على المستوى الوطني والدولي. أما إذا كانت عملية الاعتراض في غير هذه الجرائم فيكون الإجراء باطلا.

---

[17]- محمد علي عياد، الوسيط في الاصول الجزائية، الجزء الثاني، دار النهضة العربية، القاهرة، ص115.

[18]- يتم التنصت على الاتصالات الهاتفية التي يجريها المشتبه فيه أسلوبين هما أسلوب التنصت المباشر، ويتم عن طريق ربط سلكي مباشر بالخط الهاتفي المتجه نحو المركز الذي توجد به شبكة الاتصال إلى منزل المشتبه فيه المراقب، إذ يتم توصيل السلك بسماعة الهاتف وجهاز تسجيل يتم من خلالها التنصت والتسجيل، وتعدّ هذه الطريقة قديمة ولها عيوب حيث يمكن للشخص المراقب اكتشافها لما يطرأ على الاتصال تشويش بسبب تدخل المتنصت. والأسلوب الثاني وهو أسلوب التنصت غير المباشر ويتم دون إحداث اتصال سلكي مباشر بالأسلاك الخاصة بالتليفون المشترك، حيث يمكن التقاط المحادثة مغناطيسيا، مما يجعل عملية التنصت صعب اكتشافها من طرف الشخص المراقب.

[19]- تجدر الإشارة الى أن النظام العالمي الجديد وبعد احداث 11 سبتمبر 2001 استحدث قوانين لمكافحة الارهاب تنص على ان عمليات التسجيل او التنصت تتم مباشرتها بالنسبة لجميع الاشخاص مستعملي خدمات الاتصال الهاتفية والاليكترونية وعلى الاخص منها الحاسوبية وتحت شعار "التسجيل السابق للتحقيق واللاحق" ويعد هذا انتهاك للمادة 12 من القانون العالمي لحقوق الانسان والتي تنص على احترام خصوصية الافراد وحرمة اتصالاتهم وقد تبنت الدول الغربية هذه الاجراءات وعلى راسهم الولايات المتحدة، انجلترا، فرنسا.

تقتضي عملية تسجيل المكالمات وضع تدابير تقنية لتسجيل الاصوات في الخط الهاتفي للمعني وليس مجرد نقل ما يسمعه المحقق، كما يجب ان يحتوي الإذن على العديد من البيانات [20].

عند الانتهاء من العملية يحرر العون محضرين يتعلق المحضر الاول بالجانب التقني وبتاريخ وساعة بداية العمليات والانتهاء منها. ويتعلق المحضر الثاني بمضمون المراسلات او الصور او المحادثات المعترضة والمفيدة في اظهار الحقيقة[21].

يتم الاحتفاظ بالتسجيل في حرز مختوم لضمان سلامته.

لم ينص القانون الجزائري على مصير السند المادي للتسجيل بخلاف قانون الاجراءات الجزائية الفرنسي الذي نص على تحطيمه بعد انقضاء الدعوى العمومية نهائيا المادة 100-6 منه، بينما المحاضر تبقى مدرجة بملف الدعوى.

الفرع الثاني: استعمال المحادثة عن بعد

يشمل التحقيق مجموعة من الإجراءات منها ما يمكن اتخاذها بغياب المتهم او المشتبه به كالإجراءات السابق ذكرها، ومنها ما يشترط حضور المتهم كالاستجواب وسماع الشهود وكذلك اجراء المواجهات بين الأشخاص. يفترض ان تتخذ هذه الإجراءات بحضور المتهم لكن لاعتبارات حددها المشرع فان القانون يسمح لجهات التحقيق المتمثلة في قاضي التحقيق، غرفة الاتهام، وجهة الحكم في حالة طلب تحقيق تكميلي[22] باستعمال وسائل تقنية المحادثة المرئية عن بعد.

المحادثة المرئية عن بعد هي آلية قانونية للتقاضي الالكتروني في المواد الجزائية. وقد تم النص عليها في قانون عصرنة العدالة وذلك في المواد 14 ،15 ،16، وفي تعديلات قانون الإجراءات الجزائية بالأمر 20-04، وذلك في المواد من 441 مكرر إلى 441 مكرر 6، مبينا فيها إجراءات استعمال الوسائل المرئية[23] أثناء مرحلة التحقيق، وتتمثل هذه الإجراءات في الاستجواب وسماع الشهود واجراء المواجهة بين الأشخاص وفي التبليغات. فيما يلي المبررات القانونية لاستعمال تقنية المحادثة عن بعد(أولا) وشروط وضمانات استعمال هذه التقنية(ثانيا).

---

[20]- يجب ان يتضمن الاذن البيانات التالية: -رقم الخط الهاتفي -اسم صاحب الرقم -الجريمة موضوع المتابعة -مبررات اللجوء الى هذا الاجراء -وتحديد مدة الاجراء. ويجب أن يكون العون المستعان به "مؤهلا لدى مصلحة وحدة او هيئة عمومية او خاصة مكلفة بالمواصلات السلكية واللاسلكية " ولم ينص القانون على تحليف العون المؤهل الذي يتم تسخيره ولكنه يبقى ملزما بالسر المهني.

[21]- المادة 65 مكرر 9 والمادة 65 مكرر 10 من قانون الإجراءات الجزائية.

[22]- المادة 441 مكرر 2 الفقرة 3.

[23]- تعتبر جائحة كورونا من أهم الأسباب التي دفعت المشرع اعتماد واستعمال هذه الوسيلة

أولا: المبررات القانونية لاستعمال تقنية المحادثة عن بعد

حددت المادة 441 مكرر مبررات اللجوء لاستعمال تقنية المحادثة عن بعد وتتمثل هذه المبررات[24] في:

- مقتضيات حسن سير العدالة بصفة عامة،
- الحفاظ على الامن او الصحة العمومية وأحسن دليل على ذلك وباء كورونا،
- اثناء الكوارث الطبيعية حيث تتعطل وسائل النقل وتقطع الطرقات...
- لدواعي احترام مبدأ الآجال المعقولة حيث تساهم هذه التقنية في ربح الوقت،
- حالة تمديد التوقيف للنظر،
- حالة توقيف المتهم خارج دائرة اختصاص قاضي التحقيق.

ثانيا: شروط وضمانات استعمال هذه التقنية

متى توفر مبرر المحادثة عن بعد، يتوجب الأمر احترام العديد من الضمانات وهي:

- سرية الارسال وأمانته مع ضرورة عرض كامل وواضح لمجريات الإجراء المتخذ،
- تسجيل التصريحات بشكل يضمن سلامتها ويرفق بملف الإجراءات،
- حضور المحامي مع المتهم[26]،
- توقيع المتهم على نسخة من المحضر[27]|،
- في حالة الأمر بالحبس يجب تبليغ الأمر للمتهم بنفس التقنية،
- تأسيس الامر بالحبس طبقا للمادة 123 مكرر،
- اعلام المتهم بحقه في الاستئناف خلال 3 أيام.

المطلب الثاني

الوسائل التكنولوجيا الحديثة المستعملة في المحاكمة

من اهداف التقاضي الالكتروني الذي نص عليه القانون 15-03 المتعلق بعصرنة العدالة المرور من أسلوب التقاضي التقليدي والبيروقراطي إلى نظام الكتروني سلس يتطور به الأداء بتقليل الإجراءات، وتوفير الوقت والجهد على كل المتعاملين مع الجهاز سواء تعلق الأمر بالقضاة والمحامين والمتقاضين وأعوان العدالة بصفة عامة، كما يضمن التقاضي الالكتروني السرعة والشفافية في العمل القضائي الإداري بصفة عامة.

---

[24]– ما يمكن ملاحظته بالنسبة لهذه المبررات فإنها متروكة لتقدير القاضي ووكيل الجمهورية.

[26]– طبقا لمقتضيات المادة 105 من قانون الإجراءات الجزائية

[27]– المادة 441 مكرر 5 من نفس القانون

إن المحاكمة الجنائية هي المرحلة الأخيرة للدعوى العمومية، حيث تنتهي بصدور الحكم الواجب تطبيقه على المتهم سواء كان بتبرئته أو بإدانته. تقتضي هذه المحاكمة ضرورة احترام حقوق الانسان[28] والمبادئ الأساسية التي ترتكز عليه المحاكمة العادلة[29].

نصت المادة 2/14 من القانون 15-03 [30]على أنّه يمكن لجهة الحكم أيضا أن تستعمل المحادثة المرئية عن بعد لسماع الشهود والأطراف المدنية والخبراء ويمكن لجهة الحكم التي تنظر في قضايا الجنح أن تلجأ إلى نفس الآلية لتلقي تصريحات متهم محبوس إذا وافق المعني والنيابة العامة على ذلك[31].

حددت المادة 14 من القانون 15-03 والمادة 441 مكرر 08 من قانون الإجراءات الجزائية شروط وإجراءات المحاكمة عن بعد وتتمثل في:

- وجود سبب جدي لتطبيق المحاكمة عن بعد، كبعد المسافة أو حسن سير العدالة،
- وجوب مراعاة احترام إجراءات التقاضي المنصوص عليها في قانون الإجراءات الجزائية،
- وجوب تسجيل التصريحات على دعامة تضمن سلامة التصريحات والإجراءات وإرفاقها بملف الإجراءات،
- أن تضمن الوسيلة المستعملة في المحاكمة المرئية سرية الإرسال،
- وجوب تدوين التصريحات على دعامة تضمن سلامتها كضمان لحماية المتهم،
- وجوب تحرير أمين ضبط المؤسسة العقابية محضرا عن سير عملية استعمال تقنية المحاكمة المرئية، ويوقعه، ثم يرسله إلى رئيس الجهة القضائية المختصة لإلحاقه بملف الإجراءات، وهذا بمعرفة رئيس المؤسسة العقابية المتواجد فيها المتهم المحبوس.

إن إجراءات التقاضي الالكتروني في الدعوى الجزائية وفقا لما هو معمول به في الهيئات القضائية حاليا، تتمثل في مثول المتهم من خلال شاشة معروضة في قاعة الجلسات، تقابلها شاشة أخرى في المؤسسة العقابية، ويقوم القاضي بالمناداة على المتهم ، ثم يتم استجوابه صوتا وصورة بنفس إجراءات الاستجواب العادية، تليها طلبات النيابة العامة، ومرافعات الدفاع، ويقوم أمين ضبط الجلسة بتدوين التصريحات التي تدور في الجلسة، ثم يداول القاضي في القضية وينطق بالحكم على مرأى المتهم الماثل مرئيا، ويتم الاحتفاظ بالتصريحات التي دارت في الجلسة في دعامة الكترونية ترفق بالملف الورقي .

---

[28]- مجاهدي إبراهيم، المحاكمة الجنائية العادلة في ضوء المواثيق الدولية، مجلة الدراسات القانونية المجلد 3، رقم 2، 2017، ص 2.

[29]- نجاة شائر، ضمانات الحق في المحاكمة العادلة اثناء مرحلة المحاكمة في المواد الجزائية، مجلة القانون، المجلد 4 رقم 1، 2015، الصفحات من 71-78.

[30] -القانون 15-03 المؤرخ في 2015/02/01 والمتعلق بعصرنة العدالة، الصادر في الجريدة الرسمية بتاريخ 2015/02/10، العدد 06.

[31] - تجدر الإشارة إلى أن المادة 14 من القانون 15-03 كانت تشترط الموافقة الصريحة للمتهم لأجراء المحاكمة المرئية عن بعد، لكن تراجع المشرع عن ذلك بموجب الأمر 20-04 حيث ترك الأمر للسلطة التقديرية لقاضي الحكم.

لنظام المحاكمة المرئية العديد من الإيجابيات، حيث يمكن سماع الأطراف والمتهمين المحبوسين في المؤسسات العقابية دون تحمل عبئ نقلهم وتحويلهم للهيئات القضائية، كما يعمل على عدم تاجيل المحاكمات بسبب غياب المتهم أو الشهود، وتجدر الإشارة إلى أن أول محاكمة عن بعد عرفها النظام القضائي الجزائري تمت بتاريخ 07 أكتوبر 2015 بمحكمة القليعة، وأول محاكمة دولية بتقنية الصوت والصورة كانت بتاريخ 11 جويلية 2016 بمجلس قضاء المسيلة أين تم فيها سماع شاهد متواجد بمجلس قضاء "نانتير" الفرنسي[32].

الخاتمة

إن الاعتماد على نظام عصرنة الإدارة بصفة عامة مشروع إيجابي، فهو يمكّن من تفادي مساوئ الإدارة التقليدية لاسيما الأسلوب البيروقراطي المرتبط بها. فالإدارة الإلكترونية تستلزم توفر العديد من العوامل السياسية والاقتصادية والقانونية، فتجسيدها فعليا يقتضي تظافر العديد من الجهود.

إن تجسيد عصرنة العدالة وإدخال نظام الإدارة الإلكترونية ونظام التقاضي الالكتروني يستوجب توفر أرضية مناسبة، ومستوى تأهيل مناسب لموظفي العدالة وأعوانهم.

إن التعامل الإلكتروني في قطاع العدالة يتعلق أساسا بمعطيات ذات طابع شخصي يفترض أنها محمية قانونا. وعليه يجب على الدولة أن تسعى في ترقية البرامج والأرضيات الرقمية وأن تعمل على حمايتها.

كما يجب العمل على توفير التجهيزات والمعدات الضرورية لإنجاح عملية العصرنة.

نأمل أن تسعى الجزائر إلى جانب ما تم إدخاله من تكنولوجيات إدخال الذكاء الاصطناعي في النظام القضائي مما يعتبر إضافة لتوفير الوقت وتسهيل العمل القضائي بصفة عامة.

إن عصرنة العدالة واعتماد الإدارة إلكترونية تخلق الثقة بين المواطن والعدالة لأنها تعزز مبدأ الشفافية والنزاهة، ويساهم استخدام التقنيات الحديثة في مجال التقاضي في ربح الوقت، مما يؤدي إلى احترام الآجال للفصل في الملفات المطروحة أمام القضاء، وتجنب مشكل تأجيل القضايا والنظر فيها، ويرفع الضغط عن القضاة لتمكينهم من أخذ الوقت الكافي لدراسة ملفاتهم والحكم فيها.

إلى جانب كل ما أتى به المشرع في القانون المتعلق بعصرنة العدالة وفي التعديلات التي ادخلت في قانون الإجراءات الجزائية، والقوانين الحديثة منها: المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والقانون المتعلق بالوقاية من التمييز العنصري وخطاب الكراهية ومكافحتهما... نلاحظ رغبة المشرع في مواكبة تطور الجريمة في عصر التكنولوجيا وهو أمر واضح، لكن سرعة تطور التكنولوجيا وسرعة ظهور الجرائم المرتبطة بهذا التطور يتطلب من المشرع الإسراع في إدخال التعديلات وذلك بإصدار قوانين جديدة، ومواصلة العصرنة لمواكبة التطور لتفادي النقائص الملاحظة في الميدان.

---

[32]-محمد العيداني، يوسف زروق، رقمنة مرفق العدالة في الجزائر على ضوء القانون 15-03 المتعلق بعصرنة العدالة، مجلة الباحث للدراسات الاكاديمية، المجلد 07، العدد 01، 2020، ص 512.

قائمة المراجع

النصوص التشريعية

- الامر رقم 66-155 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية المعدل والمتمم.
- القانون 15-03 المؤرخ في 2015/02/01 والمتعلق بعصرنة العدالة، الصادر في الجريدة الرسمية بتاريخ 2015/02/10، العدد 06.
- القانون رقم 18-04 المؤرخ في 2018/05/10 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية عدد 27.
- القانون رقم 09-04 مالؤرّخ في 5 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- المرسوم الرئاسي رقم 09-337 المؤرخ في 2009/10/21 المتضمن إحداث مؤسسة انجاز أنظمة المراقبة بواسطة الفيديو الصادر في الجريدة الرسمية العدد 61 بتاريخ 2009/10/25.
- المرسوم الرئاسي رقم 15-228 المؤرخ في 7 ذي القعدة عام 1436 الموافق 08/22/ 2015 المتضمن القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره، الصادر في الجريدة الرسمية عدد 45 بتاريخ 2015/08/23.

المؤلفات

- سمير الامين، مراقبة التليفون والتسجيلات الصوتية والمرئية – الطبعة الثانية – دار الكتاب الذهبي – مطابع المجموعة المتحدة 2000.
- حمدي أحمد سعد، العمل عن بعد (ذاتيته-تنفيذه): دراسة تأصيلية تحليلية مقارنة في ضوء القواعد العامة لقانون العمل، دار الشتات للنشر والبرمجيات، مصر، 2010.
- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، 2009.

رسائل الدكتوراه

- بن فردية محمد، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر 1، 2015.
- روابح فريد، الأساليب الإجرائية الخاصة للتحري والتحقيق في الجريمة المنظمة، أطروحة لنيل شهادة الدكتوراه، جامعة الجزائر 1، 2016.

المجلات

- يحيى تومي، دور نظام المراقبة بواسطة الفيديو في الاثبات الجنائي، مجلة الدراسات القانونية المجلد 3، العدد 2، الصفحات من 346 على 364.
- نجاة شائر، ضمانات الحق في المحاكمة العادلة اثناء مرحلة المحاكمة في المواد الجزائية، مجلة القانون، المجلد 4 رقم 1، 2015، الصفحات من 69-94.
- مجاهدي إبراهيم، المحاكمة الجنائية العادلة في ضوء المواثيق الدولية، مجلة الدراسات القانونية المجلد 3، رقم 2، 2017، الصفحات من 105-140.
- فرحة عبد الرؤوف – القنيعي بن يوسف، كاميرات المراقبة بين اعتبارات اثبات الجريمة وانتهاك الحق في الخصوصية، مجلة الدراسات القانونية، المجلد 08، العدد 1، 2022، الصفحات من 749-768.
- حورية بن سيدهم ورقية عواشرية، الأمن الفضائي السيبيراني: التحديات والحلول، المجلة الجزائرية للأمن الإنساني، المجلد 05، العدد 02، جامعة باتنة، 2020.
- محمد العيداني، يوسف زروق، رقمنة مرفق العدالة في الجزائر على ضوء القانون 15-03 المتعلق بعصرنة العدالة، مجلة الباحث للدراسات الاكاديمية، المجلد 07، العدد 01، 2020، الصفحات من 502-516.
- بلباقي بومدين، قانون عصرنة العدالة وأثره على تحقيق المبادئ الأساسية للتقاضي، مجلة القانون والعلوم الاجتماعية، المجلد 6، العدد 4، 2021، الصفحات 1287/1274.

Les ouvrages -

- Alain Bauer, François Freynet, vidéosurveillance et videoprotection, série « que sais-je » 2eme éd., 2012, presse universitaire de France, pages 81 -92.
- Renaud Colson, Stewart Field, La fabrique des procédures pénales Comparaison franco-anglaise des réformes de la justice répressive, Dalloz « Revue de science criminelle et de droit pénal comparé » 2010/2 N° 2 | pages 365 à 393 ISSN 0035-1733 DOI 10.3917/rsc.1002.0365
  Article disponible en ligne à l'adresse : https://www.cairn.info/revue-de-science-criminelle-et-de-droit- pénale compare-2010-2-page-365.htm

الدليل الرقمي ودوره في إثبات الجرائم الإلكترونية

د/ بطيحي نسمة

أستاذ محاضر (ب)

كلية الحقوق والعلوم السياسية (جامعة سطيف 2)

nesmabettihi@yahoo.com

الملخص:

تتميز الجريمة الإلكترونية بمميزات معينة، جعلت منها جريمة فريدة من نوعها، فهي من جهة جريمة تقنية، كون الجاني يستغل أدوات التكنولوجيا الحديثة (أنظمة الحاسب الآلي) في ارتكاب جرمه، كما أنها جريمة عابرة للحدود الوطنية، على أساس أن آثارها قد تمتد لأكثر من دولة، ما يجعل منها جريمة بالغة الخطورة.

إن هذه المميزات أدت إلى ضرورة اعتماد أساليب إثبات جديدة، لذلك ظهر ما يسمى بالدليل الرقمي، إلى جانب أدلة الإثبات الجنائي الأخرى، ويكون من المهم التعرف على هذا الدليل، وتحديد طبيعته وأهميته، كما يجب معالجة الإشكالات التي يطرحها هذا الدليل في الإثبات الجنائي، سواء كان ذلك من حيث مشروعيته ومدى قبوله كدليل في إثبات الجرائم الإلكترونية، أو من حيث سلطة القاضي الجنائي في تقديره.

الكلمات الدالة: الجريمة الإلكترونية –الإثبات الجنائي – الدليل الرقمي– الخبرة الفنية.

Abstract :

Cybercrime is characterized by certain advantages, as it is on the one hand a technical crime because the criminal exploits computer systems to commit this crime, it is also a cross-border crime on the basis that its effects may exceed one country, which makes it a very serious crime.

These characteristics led to the need to adopt new methods of proof, so the digital evidence appeared; it is important to identify this evidence and determine its nature and importance. The problems posed by this evidence in criminal evidence must also be addressed, whether in terms of it is legality and the extent of its acceptance as evidence in proving electronic crimes or in terms of the authority of the criminal judge in his assessment.

Bey Word : cybercrime – criminal proof – digital proof –technical expertise.

مقدمة:

أدى الإستخدام المتزايد لأنظمة الحاسب الآلي في مختلف المجالات إلى ظهور جرائم مرتبطة بهذه الأداة التقنية الحديثة تُعرف بالجرائم الإلكترونية، وهي تعد من أخطر الجرائم الحديثة التي باتت تهدد أمن المجتمعات والأفراد. وقد تميزت هذه الجرائم بمميزات فريدة من نوعها؛ فهي – بخلاف الأنواع التقليدية من الجرائم– تُقترف وتُنسج خيوطها في بيئة افتراضية، تختلف تمام الإختلاف عن مسرح الجريمة في حُلَتِهِ التقليدية ذات الطبيعة المادية، كما أن التعامل فيها يقع على معلومات وبيانات ذات صِبغَة إلكترونية غير ملموسة.

<u>أولا</u>: أهمية البحث

وقد فرضت الطبيعة المتميزة لهذه الجريمة اعتماد وسائل إثبات جديدة ترتكز أساسا على الدعائم الإلكترونية، تعرف بالأدلة الجنائية الإلكترونية أو الأدلة الرقمية، وهو أمر منطقي إذ لابد من أن تتماشى أدلة إثبات هذه الجريمة مع طبيعتها، خاصة مع عجز وعدم كفاية أدلة الإثبات التقليدية عن اكتشاف هذه الجرائم ونسبتها إلى مرتكبها، ومن هنا تتجلى **أهمية هذه المداخلة** من حيث كونها تسعى إلى التعرف على هذا النوع الجديد من الأدلة ومميزاته وأشكاله، والوقوف على مكانته ضمن أدلة الإثبات الجنائي المعروفة، بالإضافة إلى البحث في حجيته في مجال إثبات الجرائم الإلكترونية.

<u>ثانيا</u>: إشكالية البحث

إن وجود هذا النوع الجديد من الأدلة أثار الجدل حول مصداقيتها؛ بالنظر لقابليتها للتغيير والتحوير بكل سهولة، فمن الممكن التلاعب والعبثبشكل متعمد أو غير متعمد بمعطيات الحاسب الآلي بمجرد ضغطة زر واحدة في ثوان معدودة، بل أنه من المحتمل لمحقق جنائي قليل الخبرة أن يُتلف هذه الأدلة أو يؤثر عليها، لذلك تبحث هذه المداخلة في إشكالية بالغة الأهمية في مجال الإثبات الجنائي، تتعلق أساسا **بمدى إمكانية قبول الدليل الرقمي في مجال الكشف عن الجرائم الإلكترونية وإثباتها، وما هي قيمته القانونية في الإثبات؟**

<u>ثالثا</u>: محاور البحث

لمناقشة الإشكالية المطروحة ارتأينا تقسيم هذه المداخلة كالتالي:

المبحث الأول: مفهوم الدليل الرقمي ومكانته في الإثبات الجنائي

نتناول في هذا المبحث **تعريف الدليل الرقمي وخصائصه وأشكاله**في (المطلب الأول)، ونركز في (المطلب الثاني) على **مكانة الدليل الرقمي ضمن أدلة الإثبات الجنائية المعروفة.**

المبحث الثاني: حجية الدليل الرقمي في الإثبات

نركز في (المطلب الأول) على **فكرةقبول الدليل الرقمي في الإثبات،** وفي (المطلب الثاني) منه على**مسألة تقديره من طرف القاضي الجنائي.**

المبحث الأول: مفهوم الدليل الرقمي ومكانته في الإثبات الجنائي

إن تمكن القاضي من إصدار حكم على الوقائع المعروضة عليه ليس بالأمر السهل؛ إذ يتعين عليه أن يقيم الدليل على وقوع الجريمة وعلى نسبتها للمتهم. وهذا الأمر يوجب على القاضي أن يستعين بوسائل تُتَرجِم أمامه تفاصيل الجريمة، وهذه الوسائل تعرف بوسائل الإثبات. ويحتاج القاضي الجنائي في إثبات الجرائم الإلكترونية إلى نوع مُمَيز من أدلة الإثبات يسمى بالدليل الرقمي، هذا الأخير يعتبر أكثر انسجاما وتوافقا مع الطبيعة التقنية لهذه الجريمة.

نتعرف من خلال هذا المبحث على **تعريف الدليل الرقمي، خصائصه وأهميته** في (المطلب الأول)، ثم نبحث في **مكانته ضمن أدلة الإثبات الجنائي الأخرى** من خلال (المطلب الثاني).

المطلب الأول: تعريف الدليل الرقمي، خصائصهوأهميته

نقوم بتوضيح الدليل الرقمي، من خلال البحث في **تعريفه** في (الفرع الأول)، ثم **خصائصه** في (الفرع الثاني)، وفي (الفرع الثالث) نتناول **أهميته.**

الفرع الأول: تعريف الدليل الرقمي

لم يعرف المشرع الجزائري الدليل الرقمي،وقد يعود ذلك إلى ما تعرفه تكنولوجيا المعلومات من تطورات كثيرة قد تتجاوز أي تعريف يمكن صياغته، لذا فضل ترك الأمر للإجتهادات الفقهية[1]،وخلاف ذلك نجد بعض التشريعات تطرقت إلى هذه المسألة كالتشريع المصري مثلا، الذي عرف الدليل الرقمي على أنه: (أي معلومات إلكترونية لها قوة أو قيمة ثبوتية مخزنة أو منقولة أو مستخرجة أو مأخوذة من أجهزة الحاسب أو الشبكات المعلوماتية وما في حكمها، ويمكن تجميعها وتحليلها باستخدام أجهزة أو برامج أو تطبيقات تكنولوجية خاصة)[2].

أما عن الفقه فقد اجتهد في وضع تعريفات كثيرة للدليل الرقمي، بُغيَة الإلمام به، فمنهم من عرفه في كلمات موجزة على أنه دليل جنائي يجد أساسه في العالم الإفتراضي ويقود إلى الجريمة، ومنهم من كان أكثر تفصيلا بالقول أنه عبارة عن طريقة لِتبيَان الحقيقة، يتم فيه الإستعانة بأحد الأدوات الرقمية المتنوعة التي تدرس المحتويات داخل ذاكرة القرص الصلب والرسائل الإلكترونية المخزنة أو المنقولة رقميا[3]،أو أنه ذلك الدليل المنبثق من أو بواسطة برامج الحاسب الآلي وأجهزته ومعداته وشبكات الإتصال، من خلال إجراءات فنية وقانونية، ليتم تقديمه للقضاء بعد تحليله علميا أو تفسيره في صورة نصوص مكتوبة أو رسومات أو صور أو أشكال أو أصوات، بُغيَة إثبات وقوع الجريمة ومن ثمة تحديد البراءة أو الإدانة في شأنها[4]،أو هو الدليل المأخوذ من جهاز الحاسب الآلي، ويكون في صورة نبضات كهربائية أو مغناطيسية، يتم تجميعها أو تحليلها ببرامج وتطبيقات معينة، وهو عبارة عن مكون رقمي لتقديم المعلومات في أشكال متعددة كالنصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك لغرض الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الإعتداد به أمام الجهاز القضائي[5].

وعلى ضوء التعاريف السابقة، يمكن إبداء الملاحظات التالية:

– أن الدليل الرقمي هو عبارة عن معلومات إلكترونيةوليس بيانات، فالمعلومات هي البيانات التي تمت معالجتها وأصبح لها دلالة، فمن غير المنطقي أن تقدم البيانات في شكلها الخام كدليل جنائي لتحديد البراءة والإدانة،بل في شكل معلومات لها فائدة في إظهار الحقيقة[6].
– يظهر الدليل الرقمي في أشكال مختلفة، فقد يكون في صورة مرئية أو في شكل تسجيلات صوتية كالمحادثات الصوتية عبر الأنترنت والهاتف، أو في صورة نصوص مكتوبة كرسائل البريد الإلكتروني.
– يهدف الدليل الرقمي إلى البحث عن حقيقة الجرم المرتكب، من خلال الربط بين الجريمة ومقترفها، ولا يهم طبيعة الجريمة المرتكبة، سواء كانت جريمة إلكترونية أو عادية، وهنا لا يختلف الدليل الرقمي عن أدلة الإثبات الجنائي الأخرى.

ويرجع السبب في تسميته بالدليل الرقمي إلى أن أجهزة الحاسب الآلي تقوم باستقبال البيانات من المستخدم في شكل متقطع، ليتم تحويلها إلى أرقام وفق نظام عددي محددثم معالجة هذه البياناتحتى تقوم وحدة الذاكرة الرئيسية في جهاز الحاسوب بتخزين البرامج والبيانات الداخلة ونتائج المعالجة[7].

الفرع الثاني: خصائص الدليل الرقمي

ترتبط الخصائص التي تطبع الدليل الرقمي بالبيئة التي ترعرع فيها، التي هي البيئة الإفتراضية، فهو (أولا) **دليل علمي**، كما أنه (ثانيا) **دليل ذو صبغة تقنية**، و(ثالثا) **دليل سريع التطور**.

أولا: الدليل الرقمي دليل علمي

إن البحث عن الدليل الرقمي يكون في مجال افتراضي، لذلك فهو يتطلب في تحصيله وتحليله استعمال أساليب علمية غير تقليدية، خاضعة لقوانين الإعلام الآلي.وتستلزم هذه الطبيعة العلمية للدليل الرقمي أن يتعامل مع هذا النوع من الأدلة تقنيون في البيئة الإفتراضية[8].

ثانيا: الدليل الرقمي دليل ذو طبيعة تقنية

يعد الدليل الرقمي من طائفة الأدلة الفنية أو ما يعرف بالأدلة المستمدة من الآلة، ويتميز بالطبيعة غير المادية كونه عبارة عن نبضات مغناطيسية وكهربائية[9].

إن الطبيعة التقنية للدليل الرقمي، جعلته يتصف بمميزات فريدة من نوعها، إذا ما قورن بالدليل التقليدي المادي، تتمثل هذه المميزات في:

– بالإمكان استخراج نسخ من الدليل الجنائي، تكون متطابقة مع الأصل ولها نفس القيمة العلمية، وهو الأمر الذي قد يساعد جهات التحقيق في الحفاظ على الدليل الرقمي من التلف أو التحوير[10]. في هذا الإطار سمح المشرع الجزائري في المادة السادسة من القانون رقم 04/09 المتعلق بالوقاية من الجرائم الإلكترونية[11]بضبط الأدلة المعلوماتية من خلال نسخ البيانات المخزنة في النظام المعلوماتي، بُغية عرضها في وقت لاحق على الجهات القضائية.

– يتميز الدليل الرقمي بصعوبة إزالته ومحوه من ذاكرة التخزين وإمكانية استرجاعه من خلال برامج وتطبيقات معينة[12]، بخلاف الأدلة الجنائية التقليدية التي تتوقف قوتها في الإثبات أمام القضاء على الإسراع في جمعها وتحصيلها، فبصمات الأصابع مثلا تكون محل شك إذا ما طالت المدة الزمنية بين تاريخ ارتكاب الجريمة ووقت تحصيلها[13].

كما أن محاولة الجاني محو الدليل الرقميعتبر دليلا ضده، حيث أن قيامه بذلك يتم تسجيله في ذاكرة الآلة[14].

– إن الطبيعة الفنية للدليل الرقمي تجعل من الممكن إخضاعه لبعض البرامج والتطبيقات، بغية التعرف على ما إذا كان قد تعرض للعبث والتحوير[15].

ثالثا: الدليل الرقمي دليل قابل للتطور

إن ارتباط الدليل الرقمي بتقنية المعلومات جعل منه دليلا قابلا للتطور بسرعة كبيرة، ففي بداية عهد الأنترنت لم يكن ممكنا الحصول على صور أو فيديو من خلال الأنترنت؛ إذ اقتصرت الخدمات على الرسائل النصية، غير أن الوضع قد اختلف في الوقت الراهن، حيث بات من الممكن الإتصال بالشبكة عن طريق الهواتف اللاسلكية والأقمار الصناعية والألياف البصرية بعدما كان الإتصال لا يتجاوز خطوط الهاتف الثابت[16]. وعليه فإن مواجهة الجريمة الإلكترونية يحتاج بدوره إلى مسايرة التطور الحاصل في مجال تقنية المعلومات؛ من خلال البحث عن تقنيات فعالة للمحافظة على الأدلة[17].

الفرع الثالث: أهمية الدليل الرقمي

يكتسي الدليل الرقمي أهمية كبيرة في إثبات الجرائم الإلكترونية، حيث يساعد في معرفة كيفية وقوع هذه الجرائم ونسبتها إلى مقترفيها، ويعد الدليل الرقمي هو الوسيلة الأفضل في إثبات الجرائم الإلكترونية، كونه من ذات الطبيعة التي ارتكبت فيها. وعليه بات إنشاء المعامل الجنائية الرقمية أكثر من ضرورة لغرض فحص الدليل الرقمي وتقييم عملية الإثبات الرقمي وتحليل الجرائم في نطاق ما أصبح يعرف باسم نظم الخبرة الأمنية[18].

ودور الدليل الرقمي في الإثبات لا يقتصر على الجريمة الإلكترونية، بل يتعداه إلى الجرائم العادية، كجرائم الإتجار بالمخدرات والقتل والخطف[19]؛ إذ كثيرا ما يتم إقحام التكنولوجيا الرقمية في تسهيل ارتكاب الجرائم العادية، لذلك يكون من المفيد استخدام هذه التكنولوجيا أيضا في تحصيل الدليل الذي يثبت هذه الجرائم، كالمراسلات التي يبعث بها الجاني لشريكه عن طريق الهاتف المحمول، التي قد تتضمن معلومات عن جريمة معينة كالقتل مثلا، فمثل هذه المراسلات تصلح كدليل لإثبات هذه الجريمة، على الرغم من أن الجريمة هنا ليست إلكترونية، بل أن الأداة المعلوماتية هنا(الهاتف المحمول) هي مجرد وسيلة مسهلة في تنفيذ الجريمة[20].

وقد أدرك المشرع الجزائري أهمية تحصيل الدليل باللجوء إلى الأدوات التقنية الحديثة، لذلك رخص للجهات المختصة بموجب القانون رقم 04/09 المتعلق بالوقاية من الجرائم الإلكترونية، أن تلجأ إلى إجراء الرقابة الإلكترونية وإجراء التفتيش الإلكترونية وغيرها، وذلك بصدد جرائم المعالجة الآلية للمعطيات، المجرمة بموجب القسم السابع مكرر من قانون العقوبات، وكذا في الجرائم التي تعتبر الأنظمة المعلوماتية وسيلة في ارتكابها أو حتى مجرد وسيلة مسهلة لذلك[21].

المطلب الثاني: طبيعة الدليل الرقمي

تقسم الأدلة الجنائية وفقالمصدرها إلى أدلة مادية، قولية، قانونية وأخرى فنية[22]. ويطرح التساؤل حول مكانة الأدلة الرقمية ضمن هذا التقسيم، فهل تعتبر من قبيل الأدلة المادية، كونها تنتج من عناصر مادية ملموسة، ويستخدم العلم ونظرياته في استخلاصها، أم أنها تعد من الأدلة الفنية، لما للخبير الفني من دور فيها؟

انقسم الفقه فيما بينه في هذه المسألة إلى ثلاث اتجاهات هي:

الفرع الأول: الإتجاه الذي يرى أن الدليل الرقمي دليل مادي

يرى مؤيدوا هذا الإتجاه أن الدليل الرقمي يعد من قبيل الأدلة المادية الملموسة التي يمكن إدراكها بالحواس الطبيعية للإنسان، عن طريق الأجهزة المخبرية ووسائل التقنية العالية ومنها الحاسب الآلي، فهي إذا لا تعدو كونها مرحلة متقدمة من الأدلة المادية، وهي بذلك لا تختلف عن آثار الأسلحة وبصمات الأصابع والبصمة الوراثية[23]،فقد تتجسد الأدلة الرقمية في شكل مخرجات ورقية أو أسطوانات أو أقراص، كما قد يتم عرضها عبر شاشة الحاسب الآلي[24].

وقد انتُقِدهذا الإتجاه من حيث أن هناك من الأدلة الرقمية ما لا ينطبق عليها وصف الدليلالمادي بالمفهوم السابق، على نحو الأدلة المستمدة من الوسائل السمعية والبصرية مثل كاميرات المراقبة وأجهزة التنصت، والأكثر من ذلك أن الدليل الرقمي بحكم ارتباطه بالبيئة الإفتراضية يمكن نقله إلى أي مكان من العالم في أقل من ثانية، كما يمكن أن يتواجد هذا الدليل في أكثر من مكان في نفس الوقت من خلال نسخه، هذا الأمر لا يمكن تصوره بالنسبة للدليل المادي[25].

الفرع الثاني: الإتجاه الذي يرى أن الدليل الرقمي دليل معنوي

يرى أنصار هذا الرأيأن الأدلة الرقمية هي أدلة معنوية غير ملموسة، على أساس أنها عبارة عن مجالات مغناطيسية أو كهربائية، ويضيف أنصار هذا الرأي أن عملية إخراج الدليل الرقمي في صورة مادية ملموسة(المخرجات) لا يعن أبدا أن هذه المخرجات هي الدليل في حد ذاته، إنما هي عملية تحويل تلك المجالات من طبيعة رقمية إلى هيئة يكون من الممكن الإستدلال بها على معلومة محددة[26].

الفرع الثالث: الإتجاه الذي يرى أن الدليل الرقمي دليل من نوع خاص

يذهبأنصار هذا الإتجاه إلى أن الدليل الرقمي دليل من نوع خاص؛ إذ له من الخصائص والمواصفات ما يجعله مستقلا بذاته عن غيره من الأدلة الجنائية الأخرى، سواء كان ذلك من حيث البيئة التي نشأ فيها وهي البيئة الإفتراضية أو من ناحية الشخص الذي يقوم بجمعها، هذا الأخير الذي يشترط فيه أن يكون على دراية بتقنية المعلومات[27].

وعليه نخلص أن الدليل الرقمي هو دليل من نوع خاص؛ إذ له من المميزات والخصائص ما يجعله متفردا بذاته، ومستقلا عن أدلة الإثبات الجنائي التقليدية. وكونه كذلك فإنه يكون من الضروري البحث في مدى إمكانية قبوله كدليل في إثبات الجرائم وقوته الثبوتية.

المبحث الثاني: حجية الدليل الرقمي في الإثبات

من المتعارف عليه أن الأدلة الجنائية تخضع للمبدإ العام الذي مفاده حرية القاضي في الإقتناع، ويترتب على مبدأ الإقتناع القضائي نتيجتين هامتين (أولاهما) حرية القاضي في قبول الدليل و(ثانيهما) حريته في تقدير الدليل.

وقد أثار الدليل الرقمي إشكالات عديدة، سواء كان ذلك فيما يتعلق **بمسألة قبوله كدليل إثبات في الجرائم الإلكترونية** (المطلب الأول)، وكذا **مسألة تقديره من طرف القاضي** (المطلب الثاني).

المطلب الأول: قبول الدليل الرقمي في الإثبات الجنائي

نستعرض في (الفرع الأول) **أساس قبول الدليل الرقمي في الإثبات الجنائي**، ثم في (الفرع الثاني) **شروط قبوله.**

الفرع الأول: أساس قبول الدليل الرقمي في الإثبات

يعتبر مبدأ حرية الإثبات في المسائل الجنائية من المبادئ المستقر عليها، ويقصد بهذا المبدإ حرية جميع الأطراف في أن يقدموا ما يرونه مناسبا لإقناع القاضي بما يدعونه، كما أن هذا النظام يعطي للقاضي كامل الحرية في أن يستعين بكل طرق الإثبات للبحث عن الحقيقة. وقد أقر المشرع الجزائري هذا المبدأ بموجب المادة 212 من قانون الإجراءات الجزائية التي تنص على أنه: (يجوز إثبات الجرائم بكافة طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص).

وعليه يتضح لنا أنه يمكن للقاضي الجنائي[28] الإعتماد على الدليل الرقمي لإثبات كافة الجرائم، بما في ذلك الجرائم الإلكترونية. وعلى الرغم من أن المشرع الجزائري لم يفرد نصا مستقلا بقبول الدليل

الرقمي، إلا أنه نظم إجراءات جمعه وتحصيله، بموجب القانون رقم 04/09 المتعلق بالوقاية من الجرائمالإلكترونية، كما أنه أقدم قبل ذلك سنة 2004 بتجريم أفعال المساس بنظام المعالجة الآلية للمعطيات بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004[29]، وهو ما يؤكد اعترافه بالدليل الإلكتروني، كون هذه الطائفة من الجرائم يستحيل إثباتها بغيره[30].

وترتيبا على ما تقدم فإنه وإعمالا لحرية الإثبات الجنائي يتمتع القاضي الجنائي بدور إيجابي في البحث والتنقيب عن الدليل الجنائي– بما في ذلك الدليل الرقمي–، واتخاذ جميع الإجراءات الضرورية في سبيل الوصول للحقيقة، دون أن يكون ملزما بما يقدمه له أطراف الدعوى من أدلة، وعليه بإمكان القاضي أن يوجه أمرا إلى مزود خدمة الأنترنت بتقديم بيانات تتعلق بمستخدم معين كعناوين المواقع التي زارها ووقت الزيارة والصفحات التي اطلع عليها والملفات التي تحصل عليها والحوارات التي شارك فيها والرسائل الإلكترونية التي أرسلها أو استقبلها وغيرها من المعلومات المتعلقة بتصرفات المستخدم أثناء اتصاله بالشبكة[31].

نشير إلى أنما يجب على القاضي الجنائي أن يتأكد منه في مرحلة قبول الدليل الرقمي هو مدى مشروعيته، وذلك قبل المرور إلى مرحلة تقديره، فالقاضي لا يقدر إلا الدليل المقبول، ولا يكون كذلك إلا إذا كان مشروعا ونزيها، نوضح هذه المسألة من خلال التطرق في النقطة الموالية إلى شروط قبول الدليل الرقمي.

الفرع الثاني: شروط قبول الدليل الرقمي في الإثبات

إن حرية القاضي في الإثبات لا تَعنِأبدا أنه من المقبول البحث عن الدليل الرقمي بأية وسيلة كانت؛ إذ لابد من التقيد **بضابط المشروعية** من جهة (أولا)، و**ضابط النزاهة** من جهة أخرى(ثانيا).

<u>أولا</u>: ضابط مشروعية الحصول على الدليل الرقمي

إذا كان من المسلم به أنه للقاضي الجنائي حرية الإعتماد على كافة وسائل الإثبات في تكوين قناعته، بما في ذلك الدليل الرقمي، إلا أن هذه الحرية ليست مطلقة، بل هي مقيدة بضابط المشروعية.<u>ويقصد بمبدأ المشروعية</u>أن الدليل الجنائي لا يكون مشروعا ومن ثمة مقبولا في الإثبات إلا إذا كانت عملية البحث عنه وتحصيله وتقديمه أمام القضاء في إطار أحكام القانون،وذلك احتراما لحقوق الأفراد وعدم المساس بها إلا في الحدود المسطرة قانونا، فإن تم تجاوز هذه الحدود وتم تحصيل دليل يثبت وقوع الجريمة وجب استبعاد هذا الدليل وعدم قبوله في الإثبات[32].

وقد كرس قانون الإجراءات الجزائية مبدأ المشروعية من خلال المادة الأولى منه التي تنص على أنه: (يقوم هذا القانون على مبادئ الشرعية والمحاكمة العادلة واحترام كرامة وحقوق الإنسان)، كما وضع قانون الإجراءات الجزائية نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية، وكذلك فعل القانون رقم 04/09، المتعلق بالوقاية من الجرائم الإلكترونية، الذي حدد إجراءات تحصيل الدليل الرقمي، وأقر بمشروعية بعض الإجراءات الخطيرة كإجراء التفتيش الإلكتروني وإجراء الرقابة الإلكترونية، التي كثيرا ما أسالت الحبر حول مشروعيتها، بالنظر لمساسها بالحريات الشخصية، غير أن التشريعات المختلفة سمحت بها تغليبا للمصلحة العامة، وذلك في إطار مكافحة الإجرام الحديث، بما في ذلك الجريمة الإلكترونية، إلا أن المشرع الجزائري أكد على أن مشروعية هذه الإجراءات في تحصيل الدليل مرهون بمراعاة الضوابط القانونية، وعدم التقيد بهذه الضوابط يترتب عليه عدم صحة الدليل المستخلص منها ومن ثمة بطلانه، حيث جاء في المادة الثالثة من القانون رقم 04/09 أنه: (مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والإتصالات يمكن لمقتضيات لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الإتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية)

وعليه لا يجوز للقاضي أن يقبل في إثبات إدانة المتهم مثلا دليلا إلكترونيا تم الحصول عليه من عملية تفتيش لنظام معلوماتي لم تأذن به السلطة المختصة، أو نتيجة عملية تفتيش جرى تنفيذها بعد تمام مدة سريان الإذن[33].

ثانيا: ضابط النزاهة في الحصول على الدليل الرقمي

لاينحصر نطاق عدم مشروعية الدليل الرقمي على مخالفة النصوص القانونية المقررة لضمان الحرية الفردية، بليجب أن لا يخالف الدليل الرقمي أيضا مبدأ النزاهة، والذي يستمد وجوده من الأخلاق والآداب العامة[34]. ويقصد بمبدأ النزاهة وجوب احترام المحقق للأمانة في كل ما يقوم به من إجراءات، ويعد من تطبيقات عدم الأمانة لجوء المحقق للتحريض والتحايل للحصول على معلومات تتعلق بالجريمة، ومن ذلك مثلا ما قضت به محكمة النقض الفرنسية من أن لجوء ضابط الشرطة القضائية إلى الإتصال بشبكة الأنترنت والتنكر في شخصية طفل قاصر لم يبلغ الـ 11 سنة من عمره يبحث عن علاقات جنسية يشكل تحريضا بما يخالف مبدأ النزاهة في البحث عن الدليل[35].

المطلب الثاني: تقدير القاضي الجنائي للدليل الرقمي

يحتاج الدليل الرقمي شأنه شأن باقي أدلة الإثبات الجنائي لشروط معينة لكي يتمتع بالقوة الثبوتية، نتناول في (الفرع الأول) **شروط اكتساب الدليل الرقمي حجية في الإثبات**، وفي (الفرع الثاني)**قيمة الدليل الرقمي في الإثبات الجنائي**.

الفرع الأول: شروط تمتع الدليل الرقمي بحجية في الإثبات

إن القول بحرية القاضي الجنائي في الإقتناع بالدليل الرقمي، لا تعن أن هذه الحرية مطلقة غير مقيدة، بل أنها تخضع لشروط محددة؛ إذ لا بد من **أن يكون الدليل الرقمي يقينيا غير قابل للشك** (أولا)، وأن **يخضع لمناقشة الخصوم** (ثانيا).

أولا: يقينية الدليل الرقمي

يجب على القاضي الجنائي قبل أن يصدر حكمه أن يكون قد أدرك الحقيقة الفعلية التي لا تقبل الشك في نِسبَة الجريمة إلى المتهم، وهو لن يصل إلى هذه الحقيقة ما لم يتكون لديه يقين وجزم بحدوثها، فالمطلوب إذا أن يبني القاضي قناعته بالإدانة على الجزم واليقين لا على الشك والإفتراض والتخمين[36].

ويعتمد القاضي الجنائي عادة لبلوغ اليقين والجزم في اقتناعه بالأدلة على نوعين من المعرفة؛ الأولى هي المعرفة الحسية التي تستخلص من الحواس بعد معاينة هذه الأدلة وتفحصها، والثانية هي المعرفة العقلية التي يدركها القاضي بالتحليل والإستقراء والإستنتاج، من خلال الربط بين هذه الأدلة والملابسات التي أحاطت بها،فإن لم يصل القاضي إلى الجزم بِصِلَة المجرم بالجريمةوجب عليه الحكم ببراءته، لأن الشك يفسر لمصلحة المتهم[37].

ولكي يتحقق اليقين بالأدلة الرقمية ينبغي إخضاع هذه الأدلة للتقييم الفني بوسائل فنية من نفس طبيعة هذا الدليل، تمكن من فحصه للتأكد من سلامته من العبث،وكذا صحة الإجراءات المتبعة في الحصول عليه، فالتقنيات الحديثة تمكن بسهولة تامة من العبث بالدليل الرقمي دون أن يكون بمقدور غير المتخصصين من التقنيين إدراك هذا العبث[38]، وعليه فالخلاف حول الإعتماد على الدليل الرقمي في الإثبات لا تتعلق بمسألة مشروعيته من عدمها، بقدر ما تُثار حول مسألة موثوقيته ومصداقيته، لأن هذا الأمر هو الذي يحدد قيمته في الإثبات.

ولا يسعنا هنا إلا أن نؤكد على أهمية الخبرة الفنية في مجال البحث عن الدليل الرقمي والتحقق من مصداقيته وسلامته،لاسيما مع نقص المعرفة القضائية بالجريمة الإلكترونية، فالبحث عن معلومات داخل جهاز الحاسب الآلي مثلا يعد أمرا معقدا بالنسبة للقاضي ويتطلب وجود خبير، خاصة في حالة التشفير

وغيرها من الوسائل الفنية[39]، لذلك أبدى المشرع الجزائري اهتمامه بسلامة المعطيات التي يستخلص منها الدليل الرقمي؛ إذ جاء في المادة 5 في (فقرتها الأخيرة) من القانون رقم 04/09 أنه : (يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها ...) كما نصت المادة 6 فقرة 3 أنه: (يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجرى بها العملية).

لم يكتف المشرع الجزائري بذلك فحسب، بل أنشأ في الفصل الخامس من القانون رقم 04/09 المتعلق بالوقاية من الجرائم الإلكترونيةجهاز متخصص ومتفرغ على مَدَار الساعة لغرض مساعدة الجهاز القضائي في ملاحقة مجرمي المعلوماتية والبحث عن الأدلة التي تثبت تورطهم في الجرائم، وتتضمن مجموعة أشخاص مدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على سلامة ما يتم تحصيله من أدلة[40].

ثانيا: مناقشة الدليل الرقمي

منالمبادئ المستقر عليها في قانون الإجراءات الجزائية أنه لا يجوز للقاضي الجنائي أن يؤسس حكمه على أدلة لم يتم طرحها للمناقشة في الجلسة، حيث جاء في المادة 212 من قانون الإجراءات الجزائية أنه: (ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت فيها المناقشة حضوريا أمامه).

وتستمد هذه القاعدة أساسها من مبدإ آخر هو مبدأ شفهية المرافعة، الذي مؤداه أن لا يكتف القاضي في تقديره للأدلة على ما هو مُدوَن في محاضر التحقيق، إنما يجب عليه أن يسمع لأقوال الشهود ومزاعم المتهمين وما يدلي به الخبراء، ويطرح جميع الأدلة للمناقشة الشفوية، بحيث يواجه كل خصم الخصم الآخر بما لديه من أدلة، الأمر الذي يمكن القاضي من تكوين قناعته من حصيلة هذه المناقشات التي تُجرى أمامه في الجلسة[41].

ويطرح الدليل الرقمي إشكالات عديدة فيما يتعلق بمسألة مناقشته العلنية في الجلسة، فمن جهة تعتبر الأدلة الرقمية ذات طبيعة غير مرئية، كونها عبارة عن نبضات إلكترونية مخزنة في نظام الحاسب الآلي، لا يمكن قراءتها أو استخراجها إلا بالإستعانة بأجهزة إلكترونية خاصة، هذه الطبيعة غير المرئية تجعل من الضروري اللجوء إلى نسخ الدليل الرقمي على وسائط إلكترونية تمهيدا لعرضه أمام القضاء، والدليل المستخرج في هذه الحالة لا يرق لمرتبة الدليل الأصلي، بل هو مجرد نسخة من الدليل الأصلي

الموجود في البيئة الرقمية(النظام المعلوماتي)، وعليه هل يمكن قبول هذا الدليل المستخرج من النظام أمام القضاء؟

من جهة ثانية، إن قاعدة وجوب مناقشة الأدلة تثير التساؤل حول مدى قدرة القاضي في مناقشة الدليل الرقمي، بالنظر لطبيعته التقنية؟

1) مسألة أصالة الدليل الرقمي:

إن أصالة الدليل الرقمي لها طابع خاص، فطبيعته لا تعبر عن قيمة أصلية بمجرد رفع محتواه من البيئة الرقمية، خاصة وأنه بإمكان الجاني حذف الدليل من حاسوبه ويكون ما تبقى منه مجرد نسخة فقط، يتم استردادها من خلال إجراءات التحقيق الإلكتروني كالتفتيش الإلكتروني مثلا، فالسؤال الذي يتبادر إلى الأذهان: هل تعد النسخة (أو النسخ) من الدليل الرقمي المستخرجة من النظام المعلوماتي عقب إجراءات التحقيق التي تقوم بها الجهات المختصة دليل أصلي تُبنى على أساسه إدانة المتهم؟

لقد حسمت التشريعات أمرها في هذا الخصوص وأقرت بأن مخرجات النظام المعلوماتي تعد أدلة أصلية، أي أنها افترضت أصالة الدليل الرقمي، على الرغم من كونها نسخ من دليل أصله موجود في البيئة الرقمية، وهو ما يُفهم من المادة السادسة (6) من القانون رقم 04/09 التي تنص على أنه: (عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزينإلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الاجراءات الجزائية)، أي أن المشرع الجزائري افترض أصالة النسخة المستخرجة من النظام المعلوماتي للمتهم واعتبرها مطابقة للدليل الأصلي الموجود في هذا النظام، بشرط أن يكون الدليل المستخرج هو نفس أصل البيانات التي ضُبِطت دون أن يلحقه تغيير أثناء استخراجه أو ضبطه أو تحليله أو حفظه[42].

2) مسألة نقص المعرفة التقنية لدى القاضي:

لا يمكن للقاضي أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في الجلسة وتمت مناقشتها أمام الأطراف، وحتى يكون للقاضي السيطرة على الدعوى فلابد من أن يكون له قدر معتبر من المعرفة التقنية لكي يكون بمقدوره أن يتعامل مع الأدلة الرقمية، فالتأهيل العلمي يضمن نجاح المهمة التي يقوم بها القاضي وهو بصدد مناقشة الأدلة الرقمية[43].

لمواجهة هذه المشكلة، أنشأ المشرع الجزائري الأقطاب الجزائية المتخصصة[44]، التي ينعقد لها الإختصاص في أنواع محددة من الجرائم، التي من بينها الجريمة الإلكترونية، والعلة من وراء إنشاء هذه الأقطاب هي مواجهة الإجرام المعاصر، الذي يتميز بالطابع التقني، ما يجعل مهمة القاضي صعبة إذا لم يتلق قدرا معتبرا من التكوين حول هذه الجرائم.

الفرع الثاني: قيمة الدليل الرقمي في الإثبات الجنائي

يلعب الدليل الرقمي دورا كبيرا في إثبات الجرائم الإلكترونية وحتى الجرائم العادية، لما يتميز به من موضوعية وحياد وكفاءة، هذا الأمر دفع البعض إلى القول بأن للدليل الرقمي قوة قاطعة في الإثبات الجنائي، في الوقت الذي ينتقد فيه جانب فقهي آخر هذا الرأي، ويجزمون بوقوف الدليل الرقمي على قدم المساواة مع غيره من أدلة الإثبات الأخرى.

نناقش هذه المسألة من خلال التطرق إلى الإتجاهين معا تِبَاعا:

أولا: الرأي الذي يرى بقطعية الدليل الرقمي في الإثبات

يرى هذا الإتجاه الفقهي أن للدليل الرقمي قوة ثبوتية ملزمة للقاضي الجنائي، وحجتهم في ذلك أن الدليل العلمي – الذي يعد الدليل الرقمي أحد تطبيقاته – هو النتيجة التي تسفر عنها التجارب العلمية لإثبات أو نفي الواقعة التي يُثار الشك حولها، والتي عادة ما يتطلب فهمها معرفة ودراية خاصة، قد لا يمتلكها القاضي من منطلق تكوينه القانوني المحض، وعليه فلا يمكن للقاضي أن ينازع في قيمة ما يتمتع به الدليل الرقمي من قوة استدلالية كانت قد تأكدت له من الناحية العلمية[45].

ويضيف هذا الرأي قائلا أنه بمقدار ما يتسع فيه مجال استخدام الأدلة العلمية عموما بما في ذلك الدليل الرقمي، بمقدار ما يتقلص فيه ويتضاءل دور القاضي الجنائي في تقدير القيمة الإقناعية لهذه الأدلة، لاسيما مع نقص خبرة القضاء من الناحية التقنية، وتبعا لذلك تصبح مهمة القاضي شبه آلية؛ إذ يكون الدور البارز للخبرة التي تهيمنعلى العملية الإثباتية، ولا يبق أمام القاضي إلا الأخذ برأي الخبير دون أدنى تقدير من جانبه[46].

ثانيا: الرأي الذي يرى بعدم قطعية الدليل الرقمي في الإثبات

يربالإتجاه الغالب من الفقه أن الدليل الرقمي لا يحوز قوة حاسمة في الإثباتأمام القاضي الجنائي، إنما هو دليل كغيره من الأدلة الجنائية الأخرى لا تفوق قيمته ولا تزيد حجته عن غيره، وعليه يمكن

للقاضي أن يستند إلى الدليل الرقمي كما بإمكانه أن يستبعده، وذلك كله متوقف على قناعته واطمئنانه للأدلة المعروضة أمامه، كما لا يوجد ما يلزم القاضي بضرورة الأخذ بالدليل الرقمي حتى لو لم تكن في الدعوى أدلة غيره[47].

وردا على الإتجاه الفقهي السابق، يرى أنصار هذا الإتجاه أنه لابد من عدم الخلط بين أمرين أساسيين: (الأول) يتمثل في القيمة العلمية القاطعة للدليل الرقمي، و(الثاني) يتمثل في الظروف والملابسات التي وُجِد فيها هذا الدليل، فسلطة القاضي في التقدير لا تشمل المسألة الأولى، لأن قيمة الدليل الرقمي تقوم على أسس علمية دقيقة، ولا يمكن للقاضي أن يناقش في الحقائق العلمية الثابتة، أما المسألة الثانية فإنها تدخل في مجال سلطته التقديرية، وهي من طبيعة عمله. ومن هذا المنطلق فإنه وعلى الرغم من أنه لا يمكن للقاضي أن يجادل في قيمة ما يتمتع به الدليل الرقمي من قوة علمية، إلا أنه وعلى ضوء الظروف والملابسات التي أحاطت به، يمكنه أن يستبعد مثل هذا الدليل، في الفرض الذي يرى فيه أن وجوده لا يتوافق منطقيا مع ظروف الواقعة وملابساتها[48].

خاتمة

إنإقحام الأداة المعلوماتية في ارتكاب الجرائم، دفع إلى استخدام أدلة جديدة في إثباتها تتفق وطبيعة البيئة الرقمية التي ارتُكِبت فيها هذه الجرائم. من خلال هذه الدراسة تم الوصول إلى مجموعة من النتائج والتوصيات الهامة، نختصرها فيما يلي:

<u>أولا</u>: النتائج

- الدليل الرقمي نوع خاص من أدلة الإثبات، وهو مستقل عن أدلة الإثبات الجنائية المعروفة، بالنظر لخصائصه ومميزاته الفريدة من نوعها؛
- يحوز الدليل الرقمي أهمية كبيرة في الإثبات الجنائي، حيث أن دوره لا يقتصر على الجرائم الإلكترونية فحسب، بل يظهر أيضا بالنسبة للجرائم التقليدية، التي تستخدم فيها أنظمة الحاسب الآلي كوسيلة لارتكابها أو مجرد أداة مسهلة لذلك؛
- لا يطرح الدليل الرقمي إشكالا فيما يتعلق بمشروعيته؛ إذ يجوز للقاضي الجنائي وفقا لمبدأ حرية الإثبات الجنائي المكرس بالمادة 212 من قانون الإجراءات الجزائية أن يعتمد على كافة طرق الإثبات الجنائي في الوصول إلى الحقيقة، بما في ذلك الدليل الرقمي؛
- تلعب الخبرة الفنية دورا كبيرا في مجال البحث عن الدليل الرقمي والمحافظة عليه، لذلك أعطى المشرع الجزائري بموجب القانون رقم 04/09 المتعلق بالوقاية من الجرائم الإلكترونية للجهات

القضائية المختصة مُكنَة الإستعانة بالخبراء الفنيين للمحافظة على سلامة الأدلة الرقمية من العبث.

لم يكتف المشرع الجزائري بذلك فحسب بل أنشأ هيئة متخصصة تملك من الكوادر البشرية والإمكانيات المادية ما يمكنها من مساعدة الجهاز القضائي في مواجهة الجرائم الإلكترونية.

- يخضع الدليل الرقمي، على الرغم مما له من كفاءة وموضوعية، شأنه شأن غيره من أدلة الإثبات الجنائي الأخرى للسلطة التقديرية للقاضي الجنائي، فإن شاء أخذ به وإن شاء طرحه.

ثانيا: التوصيات

- يتميزالدليل الرقمي بالمرونة وسرعة التطور، كونه مرتبط بتقنية المعلومات،لذلك يجب دائما البحث على تقنيات فعالة في تحصيل الدليل الرقمي والمحافظة عليه لمدة طويلة؛
- كما أنه يتعين دائما إخضاع الجهات المختصة، قضاة كانوا أو ضباط شرطة قضائية، للتكوين الفني المستمر والدوري، بما يكفل تحقيق الفعالية في مواجهة الجرائم الإلكترونية؛
- تكثيف البحوث العلمية في مجال الجرائم الإلكترونية، لحل الإشكالات القانونية المتعلقة بإجراءات البحث عن الدليل الرقمي.

قائمة المراجع:

النصوص القانونية:

القانون رقم 04/09 المؤرخ في 5 سبتمبر 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، (جريدة رسمية: عدد 47، لسنة 2009).

الرسائل الجامعية:

1. براهيمي جمال الدين، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، تخصص: القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018.
2. لهوى رابح، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، دكتوراه علوم، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الموسم الجامعي: 2021/2020.
3. مولاي ملياني دلال، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، أطروحة دكتوره في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2018/2017.

4. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2009.

المقالات العلمية:

1. أسامة حسين محي الدين عبد العال، حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية، دراسة تحليلية مقارنة، مجلة البحوث القانونية والإقتصادية، العدد 76، يونيو 2021.
2. إلهام شهرزاد روابح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة البليدة 2، لونيسي علي، 2016. المجلد 5، العدد 2، 2016.
3. بن مالك أحمد، الخال ابراهيم، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، تصدر عن المركز الجامعي علي كافي، تندوف، الجزائر، المجلد5، العدد 1، 2021.
4. نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الحاج لخضر، العدد الـ 11، جوان 2017.
5. ايهاب فؤاد الحجازي، حجية الدليل الرقمي في الإثبات الجنائي، مجلة العلوم القانونية والإقتصادية، العدد الأول، السنة الـ 56، يوليو 2014

أعمال الملتقيات:

1. مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس (9- 10 ماي 2018)، ملحق خاص العدد3، الجزء الثاني، أكتوبر 2018.
2. هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، (دراسة مقارنة)، ورقة بحثية مقدمة لمؤتمر القانون والكمبيوتر، المنعقد في الفترة بين 1 و3 ماي 2000، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، الطبعة الثالثة، 2004.

[1] لهوى رابح، الشرعية الإجرائية للأدلة المعلوماتية المستمدة من التفتيش، دكتوراه علوم، تخصص: القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الموسم الجامعي: 2021/2020، ص 15.

[2] قانون رقم 175 لسنة 2018، في شأن مكافحة جرائم تقنية المعلومات. جريدة رسمية عدد 32 مكرر (ج)، بتاريخ 14 أوت 2018.

[3] أسامة حسين محي الدين عبد العال، **حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية**، دراسة تحليلية مقارنة، مجلة البحوث القانونية والإقتصادية، العدد 76، يونيو 2021. ص 641.

[4]المرجع نفسه، ص 640.

[5]إلهام شهر زاد روابح، الدليل الرقمي بين مشروعية الإثبات وانتهاك الخصوصية المعلوماتية، مجلة البحوث والدراسات القانونية والسياسية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة البليدة 2، لونيسي علي، 2016. المجلد 5، العدد 2، 2016، ص 187.

[6] لهوى رابح، المرجع السابق، ص 19.

– **فالبيانات** تعبر عن الأرقام والكلمات والرموز والحقائق أو الإحصائيات الخام، التي ليس لها علاقة مع بعضها البعض، ولم تخضع بعد للتفسير أو التجهيز للإستخدام، أي أنها تخلو من المعنى الظاهري في أغلب الحالات، أما **المعلومات** فهي المعنى الذي يستخلص من هذه البيانات.

[7]إلهام شهر زاد روابح، المرجع السابق، ص 187.

[8]بن مالك أحمد، الخال ابراهيم، دور الأدلة الرقمية في الإثبات الجنائي، مجلة العلوم الإنسانية، تصدر عن المركز الجامعي علي كافي، تندوف، الجزائر، المجلد5، العدد 1، 2021. ص 109.

[9]المرجع نفسه، 109.

[10] أسامة حسين محي الدين، المرجع السابق، ص 643، 644.

[11] القانون رقم 04/09 المؤرخ في 5 سبتمبر 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، (جريدة رسمية: عدد 47، لسنة 2009).

[12]أسامة حسين محي الدين، المرجع السابق، ص 644؛ بن مالك أحمد، الخال ابراهيم، المرجع السابق، ص 109.

[13] لهوى رابح، المرجع السابق، ص 45.

[14]أسامة حسين محي الدين، المرجع السابق، ص 644؛ بن مالك أحمد، الخال ابراهيم، المرجع السابق، ص 109.

[15]بن مالك أحمد، الخال ابراهيم، المرجع السابق، ص 109.

[16]مولاي ملياني دلال، إشكالية الإثبات في جرائم الأنترنت في التشريع الجزائري، أطروحة دكتوره في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، السنة الجامعية 2018/2017، ص 101.

[17]لهوى رابح، المرجع السابق، ص 36.

[18]نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، تصدر عن كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الحاج لخضر، العدد الـ 11، جوان 2017، ص 912.

[19]عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2009. ص 32، 33؛ إلهام روابح شهر زاد، المرجع السابق، ص 187.

[20] براهيمي جمال الدين، **التحقيق الجنائي في الجرائم الإلكترونية**، أطروحة دكتوراه، تخصص: القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018، ص 135.

[21] ويتضح ذلك من خلال المادة الثانية من القانون رقم 04/09، التي قامت بتحديد الجرائم التي يسمح فيها للجهات المختصة باتخاذ الإجراءات المرخص بها بمقتضى القانون رقم 04/09، ويتعلق الأمر بالجرائم الإلكترونية بالمفهوم الضيق (جرائم المعالجة الآلية للمعطيات المحددة في القسم السابع مكرر من قانون العقوبات)، وأي جريمة عادية يعتبر النظام المعلوماتي وسيلة في ارتكابها أو حتى مجرد أداة مسهلة لذلك.

[22] يقصد **بالأدلة المادية**، تلك الأدلة التي تنبعث منها عناصر مادية تدرك بالحواس، أما **الأدلة القولية** فهي الأدلة التي تنتج من أقوال صادرة عن الغير (الإعتراف وأقوال الشهود)، و**الأدلة القانونية** هي الأدلة التي حددها المشرع وضبط

قوة كل منها، بالشكل الذي لا يمكن معه الإثبات بدونها، **والأدلة الفنية** هي الأدلة التي تنبعث من رأي الخبير الفني وفق معايير ووسائل علمية معتمدة.

[23]روابح إلهام شهر زاد، المرجع السابق، ص 189.

[24]لهوى رابح، المرجع السابق، 65.

[25]لهوى رابح، المرجع السابق، ص 67.

[26]مسعود بن حميد المعمري، الدليل الإلكتروني لإثبات الجريمة الإلكترونية، مجلة كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس (9- 10 ماي 2018)، ملحق خاص العدد3، الجزء الثاني، أكتوبر 2018، ص 196.

[27]مسعود بن حميد المعمري، المرجع السابق، ص 197؛ عائشة بن قارة مصطفى، المرجع السابق، ص 39.

[28] يقصد بالقاضي الجنائي هنا ليس قضاء الحكم فقط، بل يشمل أيضا قضاة التحقيق، باعتبار أن مشكلة الإثبات قد تطرح في أي مرحلة من مراحل الدعوى العمومية، حتى أنه يمكن أن تُثار أثناء مرحلة جمع الإستدلالات. راجع، مولاي ملياني دلال، المرجع السابق، ص 313.

[29]القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات، جريدة رسمية عدد 71، لسنة 2004.

[30]لهوى رابح، المرجع السابق، ص 274.

[31] عائشة بن قارة مصطفى، المرجع السابق، ص 124.

[32]بن مالك أحمد، الخال ابراهيم، المرجع السابق، ص 116.

[33] لهوى رابح، المرجع السابق، ص 286.

[34] عائشة بن قارة مصطفى، المرجع السابق، ص 137.

[35] لهوى رابح، المرجع السابق، ص 291، 295.

[36]بن مالك أحمد، الخال ابراهيم، المرجع السابق، ص 117.

[37] ابراهيمي جمال، المرجع السابق، ص 153.

[38]من أجل أكثر تفصيل حول الطرق الفنية في ضمان سلامة الدليل الرقمي راجع، ايهاب فؤاد الحجازي، حجية الدليل الرقمي في الإثبات الجنائي، مجلة العلوم القانونية والإقتصادية، العدد الأول، السنة الـ 56، يوليو 2014، ص 198.

[39]عائشة بن قارة مصطفى، المرجع السابق، ص 124.

[40]من أجل أكثر تفصيل حول المسائل المتعلقة بتشكيلة هذه الهيئة وآليات عملها راجع، المرسوم الرئاسي رقم 183/20 المؤرخ في 13 يوليو 2020 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما، (جريدة رسمية عدد 40، المؤرخة في 18 يوليو 2020).

[41]إيهاب فؤاد حجازي، المرجع السابق، ص 212.

[42]من أجل أكثر تفصيل في هذه المسألة راجع، لهوى رابح، المرجع السابق، ص 338.

[43]المرجع نفسه، ص 335، 336.

[44]قام المشرع الجزائري بتكريس الأقطاب الجزائية المتخصصة فيتعديل قانون الإجراءات الجزائية سنة 2004، بموجب القانون رقم 14/04 المؤرخ في 10 نوفمبر 2004، الذي جاء ببعض القواعد الإجرائية التي تسمح بتوسيع نطاق

الإختصاص المحلي لوكلاء الجمهورية وقضاة التحقيق والحكم التابعين لتلك الهيئات إلى دائرة اختصاص محاكم أخرى، وذلك في جرائم محددة على سبيل الحصر، وهي تلك الجرائم التي على درجة كبيرة من التعقيد والتنظيم.

وفي سنة 2006 صدر المرسوم الذي يحكم وينظم عمل الأقطاب المتخصصة وهو المرسوم التنفيذي رقم 348/06، المؤرخ في 5 أكتوبر 2006 المتعلق بالإختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق (جريدة رسمية عدد: 63، بتاريخ 8 أكتوبر 2006)، وقد عدل هذا المرسوم بموجب المرسوم التنفيذي رقم 267/16 المؤرخ في 17 أكتوبر 2016 (جريدة رسمية عدد: 62، بتاريخ 23 أكتوبر 2016).

[45] ابراهيمي جمال، المرجع السابق، ص 162.

[46] لهوى رابح، المرجع السابق، ص 317.

[47] عائشة بن قارة مصطفى، المرجع السابق، ص 158.

[48] هلالي عبد الله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، (دراسة مقارنة)، ورقة بحثية مقدمة لمؤتمر القانون والكمبيوتر، المنعقد في الفترة بين 1 و3 ماي 2000، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، الطبعة الثالثة، 2004، ص 724.

استمارة المشاركة في الملتقى الدولي الافتراضي الموسوم ب: القانون الجنائي في ظل التطور التكنولوجي – إشكالات ومعالجات–

يومي28 و29 سبتمبر2022

بجامعة الجزائر1 بن يوسف بن خدة–كلية الحقوق–

الاسم:هنية

اللقب:عميروش

الرتبة العلمية:أستاذة محاضرة "أ"

الوظيفة: أستاذة جامعية

المؤسسة المستخدمة: جامعة بجاية–كلية الحقوق والعلوم السياسية–

الهاتف:05400171738

البريد الالكتروني: amiroucheasam@gmail.com

المحور المتدخل فيه: المحور الخامس: تأثير الوسائل العلمية الحديثة على الإثبات الجنائي

عنوان المداخلة:**أثر الدليل العلمي على اقتناع القاضي الجزائي**

L'impact des preuves scientifiques sur la conviction du juge pénal

The impact of the scientific evidence on the conviction of the criminal judge

الملخص:

إذا كان العلم قد استحدث الكثير من أساليب الإثبات، و أمدّ سلطات التحقيق بوسائل علمية حديثة و متطورة تستطيع أن تتغلب على كل محاولات المتهم لتضليل العدالة، و كشف ما قد يطمسه من آثار، هذا بالإضافة لما تقدمه للقاضي من مساعدة كبيرة في تكوين عقيدته في الاقتناع بصورة أشد حزما و يقينا، كما تساعد على التقليل من الأخطاء القضائية، والاقتراب من العدالة بخطوات أوسع، و التوصل إلى درجة أكبر نحو الحقيقة، غير أنّ ذلك لم يستبعد نظام الاقتناع القضائي، و ظل هذا النظام هو السائد في التشريعات الإجرائية الجنائية المعاصرة، حيث يتمتع القاضي الجنائي بسلطة واسعة في تقدير الأدلة المعروضة عليه.

Résumé :

Un grand nombre de méthodes de preuves ont étés créées et modernisées grâce à l'avancée de la science et de la technologie. Ces méthodes de preuves modernes et scientifiques permettent aux autorités chargées des enquêtes de surmonter toutes les tentatives pouvant tromper la justice. Elles représentent pour le juge une aide importante dans la formation de sa conviction ainsi qu'une aide dans la réduction des erreurs judiciaires. Cependant cela n'exclut pas le système judiciaire de conviction qui reste un système dominant dans la procédure pénale

contemporaine où le juge pénal jouit d'une large autorité pour la sélection des preuves qui lui sont présentées.

Abstract:

Science has already introduced a lot of proof methods, and granted the investigating authorities many modern scientific means, which can not only help to overcome the defendant's attempts to mislead the law and reveal the effects that he may blur, but also to help the judge in the formation of his conviction more firmly and surely, and to reduce the judicial errors in order to get closer to the justice, and to reach the truth. However, it did not rule out the judicial conviction system which has prevailed in cotemporary criminal procedural legislation.

الكلمات الدّالة:القاضي،الاقتناع،اليقين،المشروعية،الدليل العلمي،الإدانة،البراءة.

Motsclés : Juge, conviction, certitude, légitimité, preuves scientifiques, condamnation, innocence.

Key words: The judge, conviction, certainty, Legitimacy, scientific evidence,condemnation, innocence.

مقدمة:

لقد أدى تطور الجريمة وتنوع أساليبها وأنماطها إلى تطور أساليب مكافحتها بالمقابل حيث ساعدت العلوم الحديثة كالكيمياء والفيزياء والطب الشرعي وعلم النفس الجنائي وغيرها في كشف غموض العديد من الجرائم فظهر ما يعرف بالدليل العلمي، وهو دليل أفرزه تدخل العلوم الحديثة في ميدان الإثبات الجنائي.

ونظرا لما يقدّمه الدليل العلمي اليوم من فوائد في المجال الجنائي لا تقتصر فقط على إثبات وقوع الجريمة بل تتعداه إلى نسبتها إلى فاعلها بشكل قطعي قد تعجز عنه الأدلة التقليدية فهو يتميّز بموضوعية وكفاءة في إقناع القاضي نتيجة لقيامه على أسس علمية دقيقة تجعل منه يتميّز بدرجة مصداقية كبيرة، وهذا ما يدفعنا إلى طرح الإشكالية التالية: ما مدى تأثير الدليل العلمي على الاقتناع الشخصي للقاضي الجزائي؟

لأجل الإجابة على الإشكالية السابقة قمنا بتقسيم هذا البحث إلى مبحثين، تناولنا في المبحث الأول مبدأ الاقتناع الشخصي للقاضي الجزائي، تطرقنا فيه لمضمونمبدأ الاقتناع الشخصي للقاضي الجزائي في المطلب الأول، وتناولنا في المطلب الثاني مبررات مبدأ الاقتناع الشخصي للقاضي الجزائي والانتقادات الموجّهة إليه.

أمّا المبحث الثاني تناولنا فيه ضوابطالاقتناع بالدليل العلمي، تطرقنا فيه لمشروعية الدليل العلمي في المطلب الأول، ويقينية الدليل العلمي في المطلب الثاني. وختمنا هذا الموضوع بأهم النتائج والاقتراحاتالمتوصل إليها.

المبحث الأول:مبدأ الاقتناع الشخصي للقاضي الجزائي

الأصل أنّ القاضي في المواد الجزائية يبني حكمه على أساس اقتناعه الشخصي القائم على حريته في تقدير الأدلة المعروضة عليه في الدعوى، دون أن يخضع في ذلك لرقابة المحكمة العليا.

غير أنّه لا يجب أن يفهم من ذلك أنّ حرية القاضي في تكوين عقيدته هي حرية تحكمية، بحيث يمكنه أن يحلّ محل وسيلة الإثبات تخميناته وآراءه الشخصية، أو أن يقضي وفق مزاجه وأهوائه، فذلك يعني التحكّم والتعسّف، فحرية التقدير شيء والتحكّم شيء آخر.

وبناءًا على ما تقدّم، تقتضي دراسة مبدأ الاقتناع الشخصي للقاضي الجزائي، أن نعرض مضمون مبدأالاقتناع الشخصي للقاضي الجزائي في المطلب الأوّل،لنتطرقفيما بعد لمبررات مبدأ الاقتناع الشخصي والانتقادات الموجّهة إليه في المطلب الثاني.

المطلب الأوّل: مضمون مبدأالاقتناع الشخصي للقاضي الجزائي

إنّ مبدأ الاقتناع الشخصي للقاضي الجزائيمن أهم وأرقى المبادئ القانونية التّي عرفتها التشريعات الإجرائية الجنائية، ونظرًا لاختلاف الفقه في تحديد مدلول الاقتناع، كان لابدّ علينا البحث في المدلول القانوني للاقتناعثمّ العناصر التي تدخل في تكوينه، حتّى نتوصّل إلى الأساس الصحيح للاقتناع القضائي، وهو ما سوف يتم استعراضه في هذا المطلب، حيث نتطرق في الفرع الأوّل إلى تعريف الاقتناع الشخصي للقاضي الجزائي لنتولى بيان عناصرالاقتناع الشخصي للقاضي الجزائي في الفرع الثاني.

الفرع الأول: تعريف الاقتناع الشخصي للقاضي الجزائي

هناك محاولات عديدة من جانب الفقه، لتحديد مدلول الاقتناع القضائي، وسنتناول الحديث عن تعريف الاقتناع في اللّغة والاصطلاح، وذلك على النحو التالي:

أولا: تعريف الاقتناع لغة

الاقتناع مصدر اقتنع، ومعناه رضى، قبول.

اقتنع،اقتناعا ب:رضي ب... [1]، والمقنع بفتح الميم:العدل من الشهود، يقال فلان شاهد مقنع أي رضا يقنع به، والقناعة بالفتح: الرضا بالقسم، يقال: قنع فهو قانع وقنع وقنيع وقنوع أي رضي والقانع بمعنى الراضي[2].

---

[1] يوسف محمد رضا: معجم العربية الكلاسيكية والمعاصرة، الطبعة الأولى، مكتبة لبنان، بيروت،2006، ص163.

ثانيا: تعريف الاقتناعاصطلاحا

التحديد الاصطلاحيللاقتناع، تناوله كثير من فقهاء القانون الجنائي، وذلك كمحاولة منهم للوقوف على تحديد المدلول القانوني له.

فاقتناع القاضي في رأي الدكتور محمود محمود مصطفى: هو التقدير الحر المسبب لعناصر الإثبات في الدعوى[3].

وجاء في معجم روبار – Robert – أنّ الاقتناع الشخصي يعني:<< الأثر الذي يولد دليلا كافيا، ويقينا معقولا مستمدًا من أغوار النفس >>[4].

وقد عرفه الدكتور علي راشد بأنّه: تلك الحالة الذهنية والنفسية أو ذلك المظهر الذي يوضح وصول القاضي باقتناعه لدرجة اليقين بحقيقة واقعة لم تحدث تحت بصره بصورة عامة[5].

كما عرّفه الدكتور إبراهيم الغماز بأنّه عبارة عن: حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث احتمالات ذات درجة ثقة عالية من التأكيد الذي نصل إليه نتيجة استبعاد أسباب الشك بطريقة قاطعة[6].

وعرّفه أيضا الدكتور/ هلالي عبد الله أحمد بأنّه عبارة عن: حالة ذهنية وعقلانية تؤكد وجود الحقيقة، ويتم الوصول إليها عن طريق ما تستنتجه وسائل الإدراك، حيث تنشأ هذه الحالة منذ بدء الإجراءات الأولى لنظر الواقعة محل الإثبات، ونتيجة لتكامل عناصرها ومعطياتها التي تكمن في الأدلة باعتبارها السبب الأوّل والأساسي في حدوثها[7].

---

[2] أبي الفضل جمال الدين محمد بن مكرم إبن منظور: لسان العرب، المجلد الخامس، دار صادر، بيروت، 1997، ص329.

[3] محمود محمود مصطفى: الإثبات في المواد الجنائية في القانون المقارن، الجزء الأوّل، الطبعة الأولى، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، 1977، ص 03.

[4] مروك نصر الدين: محاضرات في الإثبات الجنائي، الجزء الأوّل، النظرية العامة للإثبات الجنائي، دار هومه،الجزائر،2007، ص621.

[5] عبد الله بن صالح بن رشيد الربيش: سلطة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المملكة العربية السعودية، بحث تكميلي لنيل درجة الماجستير في قسم العدالة الجنائية، أكاديمية نايف العربية للعلوم الأمنية، الرياض،2003، ص75.

[6] إبراهيم إبراهيم الغماز: الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1980، ص627.

[7] هلالي عبد الله أحمد: النظرية العامة للإثبات في المواد الجنائية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة أسيوط، 1987، ص 398.

وفي تقدير الدكتور/ فاضل زيدان محمد اقتناع القاضي هو: عملية عقلية منطقية لتحليل الدليل، والتعرف على فحواه ومضانه، وما يترتب عليه من نتائج، ومن خلال هذا التحليل المدرك والواعي والمنضبط بقواعد العقل والمنطق يمكن أن يصل القاضي إلى تقدير القيمة الفعلية للدليل المعروض عليه[8].

وفي رأي الدكتور كمال عبد الواحد الجوهري الاقتناع القضائي هو: << حالة ذهنية وجدانية، وهي محصلة عملية علمية منطقية تستثيرها وقائع (القضية الجنائية) في نفس القاضي، فتنشط ذاكرته لتستدعي القواعد القانونية ذات (الوقائع النموذجية) المرشحة للتطابق مع (وقائع القضية)، وتتوقف طبيعة هذه الحالة على نتيجة عملية المطابقة بين الواقعتين، فقد تكون ارتياح الضمير القاضي وإذعانه أو تسليمه بدون أدنى شك بثبوت الوقائع في جانب المتهم، وثبوت مسؤوليته عنها، وقد تكون الشك في ذلك، وأخيرًا قد تكون ارتياح ضميره وإذعانه أو تسليمه بعدم حدوثها أو عدم مسؤولية المتهم عنها مطلقا >>[9].

ويرى الدكتور حسين على محمد علي الناعور النقبياقتناع القاضي على أنّه: التعبير عن عملية ذهنية وجدانية بمنطق وعقل، ونتيجتها الجزم واليقين[10].

ونحن نخلص إلى أنّ المدلول القانوني للاقتناع هو: << عملية ذهنية ونفسية قائمة على أسس عقلية ومنطقية، والمرتبطة بضمير القاضي ووجدانه لإدراك الحقيقة الواقعية من خلال التقدير السليم للأدلة >>.

الفرع الثاني:عناصر الاقتناع الشخصي للقاضي الجزائي

بعد استعراضنا لتعريفات التي قيلت حول الاقتناع القضائي، يمكننا استخلاص الخصائص أو العناصر التي انطوى عليها تعريف الاقتناع، وهما عنصران: أحدهما شخصي، والآخر موضوعي، ولا يكفي توافر أحد العنصرين، بل لابدّ من توافرهما معا لقيام الاقتناعالقضائي،وسوف أقوم بعرض ذلكوفق مايلي:

أولا:العنصر الشخصي

---

[8] فاضل زيدان محمد: سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة، عمان، 2006، ص 109.

[9] كمال عبد الواحد الجوهري: تأسيس الاقتناع القضائي والمحاكمة الجنائية العادلة، دار محمود، مصر، 1999، ص 14-15.

[10] حسين علي محمد علي الناعور النقبي:سلطة القاضي الجنائي في تقدير الأدلة، دار النهضة العربية،القاهرة،2007، ص ص 270- 271.

الاقتناع في ضوء العنصر الشخصي يتألف من عنصرين هما العنصر الذهني أو العقلي المنطقي والعنصر النفسي الوجداني أو الضميري، ويمثل كل عنصر منهما مرحلة من المرحلتين التي تمر بهما حالة الاقتناع، وقطعًا فإنّ العنصر الأوّل سابق في وجوده على العنصر الثاني، وذلك لأنّ العنصر الثاني يمثل خلاصة وتقويم ما تكوّن لدى عقيدة القاضي من خلال العنصر الأوّل.

أ-العنصر الذهني أو العقلي المنطقي

وهو ثمرة التفاعل بين وقائع القضية من ناحية، وما يقدّم بشأنها من دفاع وأدلة إثبات أو أدلة نفي وعقل القاضي من ناحية أخرى[11].

فالاقتناع القضائي عملية ذهنية يجريها القاضي، وتنتهي برسم صورة واضحة العناصر والملامح لحقيقة الواقع، فيرتسم في ذهن القاضي ويستقر في عقله حقيقة ما حدث.

وإنّ هذه العملية عملية عقلية منطقية لأنّ القاضي يقوم بإجرائها وفق أصول وقواعد علمية، ويعتمد على قواعد المنطق والعدالة سواء في تفسير القواعد القانونية واجبة التطبيق أو في عملية المطابقة بين وقائع القضية وتلك الوقائع النموذجية المقرّرة بنص من النصوص التشريعية أو في اختيار الجزاء المناسب الذي يوقع على الجاني في حالة إدانته[12].

ب-العنصر النفسي الوجداني أو الضميري

ويتمثل في الحالة التي يصل القاضي إليها من حيث طبيعة الاقتناع، أي أنّها تمثل طبيعة حالة الصورة الذهنية والعقلية التي تكونت لدى القاضي في المرحلة الأولى، والتي كانت تشكل جوهر العنصر الأوّل، حيث تستقر نفسه ويرتاح ضميره لما استقر لديه في المرحلة الأولى، ولا يشعر بأي ضرورة أو حاجة لمعاودة التفكير أو التقصي إذ لا توجد في عقيدته أيّ فروض أخرى تتخالف مع الفروض الذي تكونت لديه فيما يتعلق بحدوث أو عدم حدوث الواقعة[13].

---

[11] كمال عبد الواحد الجوهري، المرجع السابق، ص 19.

[12] المرجع نفسه، ص 16.

[13] كمال عبد الواحد الجوهري، المرجع السابق، ص20.

وممّا لا شك فيه أنّ الضمير، هو تشكيل معنوي في الذات الإنسانية له دوره الذي لا يمكن إغفاله في بناء وتكوين الاقتناع، ولكنّه لا يصلح لوحده في بناء الأحكام الجزائية، وذلك لتعذر ضبطه بمعيار علمي محدد ودقيق، فالضمير وسيلة رقابة ذاتية فعالة لضمان ممارسة القاضي لسلطته على نحو عادل وسليم.

ثانيا-العنصر الموضوعي للاقتناع القضائي

يقصد بالعنصر الموضوعي للاقتناع أن يستند القاضي الجنائي في حكمه على دليل يجب أن يكون أقوى مصدر ممكن للإثبات وتقرير الإدانة، ومقتضى ذلك أن يحمل الدليل في ذاته معالم قوته في الإقناع[14].

فلا يكفي أن يقتنع المرء بأنّه صاحب حق لأنّ ذلك يبقى بينه وبين نفسه، ولكن عليه إذا أراد الدفاع عن حقه عن طريق القضاء أن يثبت ما يدّعي، بل وأن يثبت مزاعمه وفقا للسبل التّي رسمها القانون، فأمام القضاء لا حقّ بدون إثبات.

والغاية النهائية من جمع الأدلة وتقديمها ليس الوصول إلى الدليل القاطع بحدّ ذاتهوإنّما هو الوصول إلى إقناع القاضي، وبطبيعة الحال هناك مجال مشترك وحد أدنى مشترك بين الجميع فيما يتعلق بتقدير الأدلة وهو نابع من المنطق السليم الذي يتفق عليه جميع العقلاء من الناس، ولكن مع ذلك هناك جانب من الفروق بين قاض وآخر بحسب نسبة ذكاء كلّ منهم، وتنوع طرق التفكير وسرعة البديهة و الرصيد المعرفي لدى كل منهم.

المطلب الثاني: مبررات مبدأالاقتناع الشخصي للقاضي الجزائي والانتقادات الموجّهة إليه

يعتبر مبدأ الاقتناع الشخصي للقاضي الجزائي من أهم المبادئ المستقرة في نظرية الإثبات بصفة عامة، و لقد نصّ عليه المشرع الجزائري من خلال نص المادة212 و307 من قانون الإجراءات الجزائية[15].

وعلى الرغم من أنّ هناك مبررات عديدة تملي منح القاضي الجزائي الحرية في تقدير الأدلة، ودورا إيجابيا فعالا في الوصول إلى أحكام عادلة،نجد أنّ هناك انتقادات موجهة للمبدأ،وهو ما سوف نتطرق إليه في هذا المطلب على النحو التالي:

الفرع الأول: مبررات مبدأالاقتناع الشخصي للقاضي الجزائي

---

[14] رمزي رياض عوض:سلطة القاضي الجنائي في تقدير الأدلة، دار النهضة العربية، القاهرة ،2004، ص 29.

[15]راجع المادتين 212 و307 من الأمر رقم 66-155 المؤرخ في08 يونيو1966 يتضمن قانون الإجراءات الجزائية، جريدة رسمية العدد48، الصادر بتاريخ 10يونيو1966 المعدّل و المتمم.

إنّ سيادة مبدأ الاقتناع الحر في مجال الإثبات الجنائي كانت قد أملتها ضرورات معينة منها أنّ تطبيق نظام الإثبات القانوني في مجال المواد الجنائية محفوف بالمخاطر، نظرا لما يتسم به من صفة تحكيمية، فهو من جهة يشكل ضررا بالبراءة، لأنّ القاضي في ظله ملزم بإدانة كل متهم اكتملت في شأنه الأدلة التي حددها القانون، ولو كان في قرارة نفسه مقتنعا ببراءته مما نسب إليه.

ومن جهة ثانية فهو ضار بالعدالة، لأنّ القاضي يكون ملزما بتبرئة كل متهم لم تكتمل بحقه أدلة الإثبات التي نص عليها القانون، ولو أن إدانته كانت جلية واضحة بالنسبة له.

وقد كان نظام الإثبات المقيّد سائدا في معظم التشريعات تقريبا حتى منتصف القرن الثامن عشر حين بدأ الفلاسفة وفقهاء القانون أمثال بيكاريا وفولتير، يهاجمون نظام التنقيب والتحري مطالبين بإجراء بعض الإصلاحات على القانون الجنائي، والتي من ضمنها إرساء مبدأ الإثبات الحر في مجال الإثبات الجنائي. وقد وجدت هذه الصيحة صدى لدى مشرعي الثورة الفرنسية، حيث وافقت الجمعية التأسيسية الفرنسية في جلستها المنعقدة في 18/ 01 / 1791 على مشروع القانون الذي يقضي بإقرار مبدأ شفوية المرافعة و الرجوع إلى نظام المحلفين الذي كان قد هجر منذ القرن السادس عشر، واعتماد مبدأ حرية الاقتناع كبديل لمبدأ الإثبات المقيّد، أو ما يسمى بنظام الأدلة القانونية.

وفي ظل نظام الإثبات الحر لا يرسم القانون طرقا محددة للإثبات يتقيّد بها القاضي الجزائي، بل يترك حرية الإثبات لأطراف الخصومة في أن يقدّموا ما يرون أنّه مناسبا لاقتناع القاضي هذا من جهة، و من جهة أخرى يترك للقاضي الحرية المطلقة في تقدير الأدلة المعروضة عليه، ذلك أنّ الإثبات في المواد الجنائية ينصب على وقائع مادية و نفسية يكون من المتعذر إثباتها ما لم تترك لقاضي الموضوع الحرية في تقديرها، وعدم تقييده بأدلة محدّدة.[16]

---

[16] حاتم حسن بكار، أصول الإجراءات الجنائية وفق أحدث التعديلات التشريعية والاجتهادات الفقهية والقضائية منشأة المعارف، الإسكندرية،2007، ص790.

ثانيا–الانتقادات الموجهة لمبدأالاقتناع الشخصي

من أهم الانتقادات الموجهة لمبدأ الاقتناع الشخصي للقاضي نابعة من طبيعة الاقتناع نفسه بما يتضمنه من ذاتية ونسبية، وتبدو الخاصية الأولى وهي الذاتية، من خلال الأساس الذي يقوم عليه الاقتناع، وهو كونه نشاطا عقلي يهدف إلى استنباط الحقيقة من خلال استقراء الأدلة واستيحاء قوتها في الدلالة عليها.

و لأنّه نتاج الحالة العقلية، والتي عند تقديرها للأدلة قد تتأثر من غير شكّ بمدى قابلية القاضي واستجابته للدوافع الذاتية المختلفة، ممّا قد يؤدي بالقاضي إلى الخطأ في تقديره للأدلة، و من ثمّ لا يمكن الجزم بإمكانية الوصول إلى اليقين التام أو المطلق.[17]

أمّا الخاصية الثانية ألا و هي النسبية، وتعني أنّ اليقين الذي يصل إليه القاضي ليس مطلقا بل هو يقينا نسبيا، ومن ثم فإنّ النتائج التي يمكن التوصل إليها، تكون عرضة للتنوع والاختلاف في التقدير من قاضي لآخر، تبعا لما يتمتع به من تكوين شخصي وتأهيل علمي و إدراك عال وضمير عادل يحصّنه ويحميه من أن يتأثر بالدوافع و الأفكار القابعة في مكنوناته عند تكوين اقتناعه في مجال تقديره للأدلة.

ومع التطور العلمي والتكنولوجي الذي شهده عصرنا الحالي، اتجه الفقه الجنائي الحديث إلى القول بأنّ هناك مرحلة جديدة من مراحل تطور الإثبات الجنائي تتميّز في خصائصها عما سبق من المراحل، لأنّها تعتمد على الاكتشافات والبحوث العلمية وما تسفر عنه من نتائج بدءا من مرحلة وقوع الجريمة ومعاينة مسرحها وكشف غموضها، إلى مرحلة تقديم الدليل للقضاء، أطلق عليها الفقه نظام الأدلة العلمية أو الإثبات العلمي.

ولقد كان لدخول هذا النوع من الإثبات أثره الواضح في تقريب الحقيقة القضائية من الحقيقة الواقعية، ممّا دفع جانبا كبيرا من الفقه، وعلى رأسهم الفقيه الإيطالي فري" E. Ferri" يرى ويتوقع أن يحل نظام الأدلة العلمية محل نظام الاقتناع القضائي.[18]

---

[17] فاضل زيدان محمد، المرجع السابق، ص 113.

[18] geneviève giudicelli–delage: les transformations de l’administration de la preuve pénale, société de législation comparée, paris, 2006, p75.

لكن هذا الرأي في اعتقادنا قد جانب الصواب، لأنّ ذلك يعني أن يصير الخبير هو قاضي الدعوى، وهذا يؤدي إلى حرمان المتهم من ضمانات الحرية الفردية والكرامة البشرية التي لا يحسن توفيرها غير قاضبالإضافة إلى أنّ مباشرة الخبير عمله تفترض تحديد عناصر مهمته ثم تقدير قيمة تقريره، وهما وظيفتان قضائيتان، وفي النهاية فإنّ الفصل في الدعوى الجنائية يثير مسائل قانونية لا يحسن الخبير البت برأي فيها.

المبحث الثاني: ضوابط الاقتناع بالدليل العلمي

الأصل أنّ القانون خوّل للقاضي الجزائي سلطة واسعة وحرية كاملة في تقدير أدلة الإثبات بغير معقب عليه، كما وإنّ له أن يستخلص من سائر العناصر المطروحة على بساط البحث الصورة الصحيحة لواقعة الدعوى حسبما يؤدي إليه اقتناعه، وأن يطرح ما يخالف ذلك الواقع من صور أخرى، على أنّه يتعيّن على القاضي في تكوين اقتناعه أن يراعي شروطا وضمانات معيّنة. وهذا ما سنتولى دراسته في هذا المبحث حيث نتطرق في المطلب الأول إلى مشروعية الدليل العلمي وفي المطلب الثاني يقينية الدليل العلمي.

المطلب الأول: مشروعية الدليل العلمي

إنّ الدليل لا يكون مشروعا إلاّ إذا كان وليد إجراءات مشروعة، الأمر الذي يترتب عليه أنّ أيّ إجراء في مختلف مراحل الخصومة الجنائية سواء في مرحلة جمع الاستدلالات أو التحقيق أو المحاكمة يجب ضرورة مراعاة مشروعيته، وإلاّ أهدر ذلك الإجراء وكافة ما يترتب عليه من نتائج تطبيقا لقاعدة ما بني على باطل فهو باطل.

ومن ثم يتضح أنّ مشروعية الدليل العلمي تستلزم ضرورة أن يكون ذلك الإجراء المستمد منه الدليل مشروعا، وهذا ما سوف نتناوله بالدراسة في الفرع الأول تحت عنوان مشروعية إجراءات جمع الأدلة كأساس لمشروعية الدليل، لنتناول في الفرع الثاني قيمة الدليل غير المشروع في الإثبات.

الفرع الأول: المشروعية الإجرائية كأساس لمشروعية الدليل

حدّدت التشريعات المختلفة وسائل وإجراءات لتحصيل أدلة الإثبات لتجعل منها إجراءات أو وسائل خاضعة لمبدأ الشرعية، يرجع إليها القاضي أثناء تكوين اقتناعه الشخصي كمعيار لتحديد مدى مشروعية الدليل المستند عليه في ذلك، في حد ذاته.

من هذا المدخل، يمكننا أن نفسر الارتباط الوثيق بين مشروعية الدليل كمبدأ، وبين شرعية الإجراء الموصل إليه، فوجود الأول متوقف أساسا على مدى وجود الثاني، ولا غنى لأيّ منهما عن الآخر.

فهدف الإثبات أولا وأخيرا، مهما اختلفت وسائله، هو إظهار الحقيقة لا غير، ولا يمكن بأيّ حال من الأحوال أن يبرّر هذا الهدف استعمال أيّة وسيلة حتى لو خرجت عن الإطار الذي رسمته لها الشرعية التي أوجدها المشرع حماية للفرد أولا، وللمجتمع بعد ذلك كي لا يخرج هذا الأخير أثناء تأديته لوظائفه عن قواعد العدالة، وحتى لا يخرق حقوق الدفاع التي ضمنها القانون للشخص المتهم.

فالعبرة ليست بتوافر الأدلة وحشدها، لكن بنزاهة وشرعية تحصيلها، وهذا ما نصت عليه أغلب الدساتير والقوانين، وقبلهم الشريعة الإسلامية في عدّة حوادث عرفها التاريخ الإسلامي، كتلك الحادثة التي أهدر فيها أمير المؤمنين – عمر ابن الخطاب–دليلا توصل إليه عن طريق التصنّت على اعتبار هذا الأخير طريقا غير مشروع للإثبات لمخالفته لقواعد الآداب والسلوك. [19]

وإذا كان القاضي لا يجد نفسه في إشكال كبير إذا ما تعلق الأمر بتطبيق دليل تقليدي تكون التشريعات قد وضعت طرقا معيّنة، يتعيّن احترامها للحصول عليه، فإنّ الإشكالات تبدأ بالظهور، إذا كنّا بصدد دليل علمي يفرض نفسه بقوّة حجيّته وقطعيته على اقتناع القاضي الجنائي، ولم يكن المشرع قد وضع قواعد محدّدة لتنظيم أو لتقنين إجراءات الحصول عليه فيجد القاضي نفسه هنا سواء بين خيار عدم الأخذ بهذا الدليل، لعدم وجود نص قانوني يحدّد مدى شرعية إجراءات الحصول عليه من جهة، أو لمساسه بالحريات الفردية وقواعد السلوك و الآداب من جهة أخرى، أو بين خيار الأخذ به معتمدا على نص المادة 212 من قانون الإجراءات الجزائية التي تبيح له استعمال كل الطرق التي يمكنها أن توصله إلى الحقيقة وبذلك تكون قد أعطته كل الحرية في اختيار أيّ وسيلة، أو الأخذ بأيّ دليل يجده كافيا لتكوين اقتناعه الشخصي.

ونظرا لكون شرعية الحصول على دليل ما، تستلزم شرعية الإجراء الموصل إليه فوجود الأوّل متوقف أساسا على مدى وجود الثاني، ولا غنى لأيّ منهما عن الآخر، وفي حالة سكوت المشرع عن إجراءات تحصيل أدلة الإثبات يتعيّن استبعاد كل تلك الوسائل التي تشكّل انتهاك لحق الإنسان في سلامته الجسدية والذهنية وتمسّ بالحريات الفردية، مثل التنويم المغناطيسي، وجهاز كشف الكذب، والتحليل التخديري وغيرها، ويتعيّن حظر استخدامها بموجب نصوص صريحة.

الفرع الثاني: قيمة الدليل غير المشروع في الإثبات

---

[19] فوزية خربوش: الأدلة العلمية و دورها في الاثبات الجنائي، رسالة ماجستير في القانون الجنائي و العلوم الجنائية، كلية الحقوق و العلوم السياسية، جامعة الجزائر،2002، ص 208.

طبقا لمبدأ الشرعية الإجرائية والتي يتحصل من خلالها الدليل، لا يكون الدليل مشروعا ومن ثم مقبولا في عملية الإثبات، والتي يتم من خلالها إخضاعه للتقدير، إلاّ إذا جرت عملية البحث عنه أو الحصول عليه وعملية تقديمه إلى القضاء أو إقامته أمامه بالطرق التي رسمها القانون والتي تكفل تحقيق توازن عادل و دقيق بين حق الدولة في العقاب، وحق المتهم في توفير الضمانات الكافية لاحترام كرامته الإنسانية و عدم امتهان حقوقه الأساسية.

فمتى ما تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد بقيمته مهما كانت دلالته على الحقيقة الواقعية، وذلك لعدم مشروعيته، وإن كان هذا الكلام ينطبق على دليل الإدانة، فإنّ الأمر ليس كذلك بالنسبة لدليل البراءة، وهذا ما سوف نحاول تبيانه، وذلك على النحو الآتي:

أولا: بالنسبة لدليل الإدانة

يجب أن يؤسس القاضي الجنائي اقتناعه الذاتي للحكم بإدانة المتهم على أدلة مشروعة، وذلك انطلاقا من قاعدة أنّ الأصل في الإنسان البراءة، فالمتهم يجب أن يعامل على أساس أنّه بريء في مختلف مراحل الدعوى إلى أن يصدر بحقه حكم بات، وهذا يقتضي أن تكون الأدلة التي يؤسّس عليها حكم الإدانة مشروعة.

ولو أجزنا للقاضي الجنائي الحكم بإدانة المتهم ولو بأدلة أو إجراءات غير مشروعة فإنّ الضمانات التي كفلها القانون لحماية حقوق المواطن وكرامته وحرمة مسكنه لا قيمة لها، كما أنّ القواعد التي يسنها المشرع لا أهمية لها متى ما أمكن إهدارها وعدم الالتزام بها. [20]

وبالتالي فليس للقاضي أن يعطي الدليل المستمد بطريق غير مشروع أو بوسيلة مخالفة للقانون أيّ قيمة في الإثبات وإلاّ كان الحكم المبني على ذلك باطلا.

ثانيا: بالنسبة لدليل البراءة

بيّنا في الفقرة السابقة أنّ حكم الإدانة يجب أن يكون مستندا على دليل مشروع، ولا يجوز أن تبنى الإدانة على دليل باطل وفقا للرأي الراجح، فهل ينطبق هذا القول على دليل البراءة؟

في الحقيقة لقد أثار هذا التساؤل جدلا فقهيا كبيرا بين فقهاء القانون الجنائي، تمخض عنه ثلاثة اتجاهات رئيسية:

---

[20] محمد عطية راغب المحامي: النظرية العامة للإثبات في التشريع الجنائي العربي المقارن، دار المعرفة، القاهرة، 1960، ص177.

الاتجاه الأول: يرى بأنّه ليس هناك ما يمنع من تأسيس حكم البراءة على دليل غير مشروع انطلاقا من مبدأ افتراض البراءة باعتبارها هي الأصل، وبالتالي المحكمة ليست بحاجة لإثباتها، بل كل ما تحتاجه هو التشكيك في الإدانة لكي تصدر حكمها ببراءة المتهم ممّا نسب إليه. [21]

هذا بالإضافة إلى أنّ بطلان دليل الإدانة الذي تولّد عن إجراء غير مشروع إنّما شرع لضمان حرية المتهم، فلا يجوز أن ينقلب هذا الضمان وبالا عليه [22].

الاتجاه الثاني: يرى أنصار هذا الاتجاه أنّه ليس للقاضي أن يحكم ببراءة المتهم بناءا على دليل جاء من طريق غير مشروع، أي لا يفرق بين ما إذا كان الدليل سوف يؤدي للبراءة أو للإدانة فهي على حد سواء. وأضافوا أنّه ليس للقضاء أن يقرّ قاعدة أنّ الغاية تبرر الوسيلة كمبدأ قانوني صحيح، وهو إذا أقرّها في خصوص جواز إثبات البراءة بكل السبل، فقد يقال فيما بعد أنّه حتّى التزوير، و وشهادة الزور، وإرهاب الشهود حتى يعدلوا عن أقوالهم تصبح كلها أمور مشروعة لإثبات البراءة، وهذا مالا يمكن أن يقول به أحد، ولكن ينتهي إليه حتما منطق هذا القضاء الخاطئ[23].

الاتجاه الثالث: هو اتجاه توفيقي، يرى أنصاره جواز استناد المحكمة في تبرئة المتهم إلى دليل غير مشروع، ولكن في حدود معيّنة، وذلك عن طريق التفرقة في شأن دليل البراءة بين ما إذا كانت وسيلة الحصول عليه تعدّ جريمة جنائية، أم أنّها مجرد مخالفة لقواعد الإجراءات.

فإذا كان الدليل متحصلا من جريمة جنائية، فإنّه لا يمكن الاعتداد به، لأنّ القول بغير ذلك مفاده الدعوة لارتكاب بعض الجرائم، وإخراجها من دائرة العقاب، وهذا الأمر لا يقبله لا العقل ولا المنطق القانوني السليم.

أمّا إذا كان الحصول على الدليل يخالف قاعدة إجرائية فحسب، فهنا يصح الاستناد إلى هذا الدليل في تبرئة المتهم تحقيقا للغاية من تقرير البطلان، لأنّ الغرض من البطلان الذي شاب وسيلة

---

[21] أحمد فتحي سرور: الوسيط في شرح قانون الإجراءات الجنائية، دار النهضة، القاهرة، 1981، ص501.

[22] سامي حسني الحسيني: النظرية العامة للتفتيش في القانون المصري المقارن، دار النهضة العربية، القاهرة، 1972، ص470.

[23] نصر الدين ماروك: مبدأ المشروعية والدليل الجنائي، مجلة النائب، العدد10، ص10.

التوصل إلى الدليل إنّما يرجع إلى فعل من قام بالإجراء الباطل، وبالتالي لا يصح أن يضار المتهم بسبب لا دخل له فيه. [24]

ونحن نؤيد هذا الرأي الأخير لأنّه في رأينا هو الأكثر تحقيقا للعدالة، كما أنّه اتجاه متوازن لا يغلب لا كفة البراءة ولا كفة الإدانة، كما أنّه يحافظ على الأصل العام، ألا وهو البراءة، ذلك أنّه من غير المقبول القول بإهدار دليل للبراءة من شأنه أن يظهر براءة متهم لمجرد أنّه لم يستوف بعض الإجراءات الشكلية اللازمة قانونا، لأنّ هذا سيؤدي إلى نتيجة خطيرة للغاية وهي إدانة بريء، وفي هذه الحالة يتحمل المجتمع ضررين، عقاب بريء أقام دليل على براءته، وإفلات مجرم من العقاب.

المطلب الثاني: يقينية الدليل العلمي

إذا كان المبدأ العام في الدعوى الجزائية في تشريعات الدول المختلفة، بما فيها التشريع الجزائري هو أنّ القاضي الجزائي يتمتع بقدر كبير من الحرية في تكوين عقيدته، إلاّ أنّ هذه الحرية ليس معناها أنّ القاضي يملك الحكم في الدعوى على غير أساس من التثبت واليقين.

وسنتطرق في هذا المطلب إلى تحديد مفهوم اليقين في الفرع الأول، لنتناول القيمة القطعية للدليل العلمي في الفرع الثاني.

الفرع الأول: مفهوم اليقين

تتّحد كل الإجراءات أو التشريعات الجنائية المختلفة، في أن يصيب القاضي الحقيقة في إصدار الحكم الجنائي، سواء أكان بالإدانة أو بالبراءة، ولن يتمكن من ذلك إذا لم يتوفر لديه اليقين.

واليقين هو أساس العدالة الإنسانية ومصدر ثقة المواطنين، ومن الطبيعي أن نتعرف أولا على مدلول اليقين، ثم نقوم بتمييزه عما قد يختلط به من مصطلحات ثانيا.

أولا: تعريف اليقين

اليقين لغة هو قرار الشيء، يقال: يقن الماء في الحوض، أي استقر، وهو في الاصطلاح حصول الجزم بوقوع أمر أو بعد وقوعه، أمّا الشك فهو في اللّغة التردّد، والمراد به تردّد الفعل بين الوقوع وعدمه.

ومن هنا يتبيّن أنّ اليقين والشك نقيضان، فلا مجال للشك عند وجود اليقين، ولا يتصور اليقين حيث يقوم الشك، وإذا كان اجتماع النقيضين محالا، فإنّ الشك قد يطرأ بعد حصول اليقين.

وقد تعرض الفقهاء لهذا الغرض فوضعوا قاعدة أصولية مؤداها أنّ اليقين لا يزول بالشك، فاليقين أقوى من الشك، والقوي لا يزول بضعيف، فما ثبت بيقين لا يرتفع بالشك وإنّما يرتفع بيقين مثله[25].

---

[24] سامي الحسيني، المرجع السابق، ص ص471-473.

أمّا اصطلاحا فهو عبارة عن حالة ذهنية أو عقلانية تتولد لدى القاضي محدثة انطباعا مؤكدا عن كيفية حدوث الواقعة الإجرامية، ويتوقف تكامل هذا اليقين في ضمير القاضي على قدرة الأدلة المطروحة على توصيل القاضي إلى هذه المرحلة، بحيث أنّه إذا استطاع إدراكها فإنّه في هذا الفرض تتطابق حالة الذهن والعقل مع حالة الواقع والحقيقة، وعلى العكس من ذلك يتباعد مصطلح اليقين في حالة تشكك القاضي وعدم قدرة أدلة الدعوى على توصيله إلى تلك المرحلة من اليقين[26].

ويكون تطبيق القانون عادلا، إذا بيّن القاضي الواقعة بيانا صحيحا وكافيا يؤدي هذا البيان في نهاية الأمر إلى استخلاص اليقين للواقعة، ومن ثم تطبيق العقوبة التي تتفق ودرجة جسامة الجريمة فليست حرية اقتناع القاضي سببا لإدانة الأبرياء أو تبرئة المدانين، بل هي طريق يسلكه حتى يصل بحكمه من العدالة ويقترب به إلى اليقين.

ثانيا: تمييز اليقين عمّا قد يختلط به

لا يمكننا الوقوف على معنى الجزم واليقين، دون تحديد العلاقة بين كلمة اليقين والاقتناع، فهل هما كلمتان مترادفتان في المعنى أم لا، كما قد يتبادر في الذهن أنّه لا فرق بين الحقيقة التّي يسعى القاضي إلى الوصول إليها واليقين الذي يستمد منه اقتناعه، ولكن الأمر ليس كذلك، وهو ما سوف نتناوله بالتفصيل على النحو الآتي:

أ-تمييز اليقين عن الاقتناع

اختلف الفقه في تحديد وجه الخلاف بين الاقتناع واليقين، فذهب البعض إلى القول أنّ الاقتناع (la conviction)يراد به: " إذعان نفس لما يجده المرء من أدلة تسمح له بقدر من الرجحان والاحتمال كاف لتوجيه عمله "، وبمعنى آخر هو حكم ذهني جازم غير قابل للشك، وهنا يشترك الاقتناع مع مفهوم الاعتقاد(croyance) لكونه هو الآخر حكما ذهنيا جازما، إلاّ أنّه قابل للتشكيك[27]، فهو في مرتبة أدنى من الاقتناع.

---

[25] وهبة بن مصطفى الزحيلي: التفسير المنير في العقيدة والشريعة والمنهج، المجلد الثاني، الجزء الثالث، دار الفكر المعاصر، دمشق،1997، ص109.

[26] مروك نصر الدين، محاضرات في الإثبات الجنائي، المرجع السابق، ص ص491- 492.

[27] حاتم حسن بكار، المرجع السابق، ص 848.

أمّا اليقين فهو حالة ذهنية تلتصق بالحقيقة دون أن تختلط بأيّ شك، فهي من الناحية الشخصية تتعارض مع الشك، ومن الناحية الموضوعية فوق الجهل والغلط، ودرجة اليقين تختلف بحسب المكنات المعطاة[28].

ورغم أنّ اليقين والاقتناع يتّحدان في أنّ كلا منهما غير قابل للتشكيك، إلاّ أنّ اليقين أكثر دقة وتأكيدا من الاقتناع، فالاقتناع لا يخلو تماما من بعض الاحتمال ولو بنسبة ضئيلة[29].

وهناك من يرى[30] أنّ اقتناع القاضي لا يعني أكثر من تسليمه بثبوت الوقائع كما دونها في حكمه ثبوتا كافيا، فالاقتناع– في مفهومه القضائي– ليس يقينا، لأنّ القاضي لا يملك وسائل إدراك اليقين كحالة ذهنية تلتصق بالحقيقة دون أن تختلط بأيّ شك على المستوى الشخصي أو بجهل أو غلط على الصعيد الموضوعي.

وحسب هذا الرأي الاقتناع ليس اعتقادا لأنّ القاضي لا يجوز أن يحكم بناء على أسباب شخصية صلحت لحلمه هو نفسه على التسليم بثبوت الوقائع لكنّها لا تصلح إذا نظر إليها من الناحية الموضوعية أو من جانب الآخرين، وإنّما يقف الاقتناع في منطقة الوسط بين "اليقين" والاعتقاد" يفوق الاعتقاد لأنّه لا يقوم على أسباب شخصية وإنّما على أدلة وضعية تدنيه من اليقين، ويختلف عن اليقين في استقامته على التسبيب والتعليل وقبول التسبيب والتحليل أمر شخصي لا يتسم بصرامة اليقين.

ب–تمييز اليقين عن الحقيقة

اليقين بالمعنى السابق يختلف عن الحقيقة، فحقيقة الواقعة الإجرامية تمثل النموذج الواقعي لكيفية حدوثها وطريقة ارتكابها، ومن اشترك أو ساهم فيها، وغير ذلك من التفاصيل التي حدثت بالفعل على مسرح الجريمة، وتكون وظيفة الأدلة هي نقل وتصوير هذا الواقع أمام المحكمة، في حين أنّ اليقين يمثل حالة ذهنية أو عقلانية تتولد لدى القاضي، محدثة انطباعا مؤكدا عن كيفية حدوث تلك الواقعة الإجرامية ويتمكن القاضي من الوصول إلى هذه الحالة عن طريق قدرة الأدلة المطروحة على توصيل القاضي إلى ذلك الانطباع لتلتقي الحقيقة باليقين.

---

[28] فاضل زيدان محمد، المرجع السابق، ص 110.

[29] حاتم حسن بكار، المرجع السابق، ص 848.

[30] محمد زكي أبو عامر: الإجراءات الجنائية، الطبعة السابعة، دار الجامعة الجديدة، الإسكندرية، 2005، ص 729–730.

وقد يتطابق المفهومان في حالة تمكن القاضي من الوصول إلى مرحلة اليقين العقلاني الكاشف له عن تفاصيل حقيقة الواقعة المرتكبة، وفي تلك الحالة تتطابق حالة الذهن والنفس بمسبباتها مع حالة الواقع بتفاصيلها، وقد يتنافر المفهومان ويتباعدان في حالة تشكك القاضي، وعدم قدرته على الوصول إلى تلك المرحلة من اليقين، فيستحيل عليه كشف حقيقة الواقعة المرتكبة[31].

الفرع الثاني: القيمة القطعية للدليل العلمي

لقدقطعالتقدمالتقنيوالعلميخطواتهائلةفيالمجالالجنائيلذلككانمنالضروريأنيلجأالقاضيإلىالاستعانةبأهلالخبرة،لفصل النزاعات عندماتعرضعليه مسائليستعصيعليهفهمها، فمنالمنطقيأنّثقافةالقاضيمهماكانتواسعة،فلايمكنأن تستوعبجميعالمشاكلالتيتعرضعليهخاصةبعدالتطورالعلميالذيشهدتهالبشرية،وظهوروسائلفنيةحديثةممايجعلاللّجوء إلىالخبرةضروريا.

وهكذا أصبحتالخبرةتحتلمكانا هامافيالعملالقضائيباعتبارهاطريقامهم بالمسائلالفنيةالبحتةالتييلتزمالقاضيبتعيينخبيرفيها لفهممعطياتالنزاع.

وفي الحقيقة إنّ ما يصل إليه الخبير منإثباتالواقعةيمثلوجهةنظرفنيةمحضةويجبأنتقترن بوجهةنظرقانونية، لكيتكتسبوجهةنظرهقيمةفعليةفيمجالالإثبات. [32]

وإذا كان تقدير القاضي لا يتناول القيمة العلمية القاطعة للدليل العلمي، وذلك لأنّ قيمة الدليل تقوم على أسس علمية دقيقة ولا حرية للقاضي في مناقشة الحقائق العلمية الثابتة،أمّا الظروف والملابسات التي وجد فيها الدليل فإنّها تدخل في نطاق التقدير الذاتي للقاضي فهي من اختصاص عمله، حيث يمكنه أن يطرح مثل هذا الدليل رغم قطعيته من الناحية العلميةوذلك لعدم تناسقه منطقيا مع ظروف وملابسات القضية.

والواقع أنّه مهما اتسعت السلطة التقديرية للقاضي في رقابة تقرير الخبير واستمداداقتناعه منه فإنّ هذه السلطة لها حدود معيّنة لا تعدو أن تكون تحكمية، و إنّما يتحرى بها مدى جدّية تقرير الخبرة و مقدار ما يوحي به من ثقة، ويتبع القاضي في ذلك أساليب الاستدلال المنطقي التي يقرها العلم ويجري بها العمل القضائي[33]، ولذلك قيل أنّ القاضي هو الخبير الأعلى في الدعوى.

---

[31] حسين علي محمد علي الناعور النقبي، المرجع السابق، ص.ص285- 286.

[32] فاضلزيدان،المرجعالسابق،ص112.

[33] فودة عبد الحكيم، حجية الدليل الفنّي في المواد الجنائية و المدنية، دار الفكر الجامعي، الإسكندرية، 1996،ص27.

خاتمة

لقد أدّى التطور التكنولوجي و المعلوماتي إلى استفادة محترفي الإجرام من وسائل متقدّمة و أدوات تقنية متطورة في إرتكاب الجرائم و خاصة الإجرام المنظم العابر للحدود الوطنية، و ساعدتهم أيضا في إخفاء معالم الجريمة، ومن ثم كان على أجهزة العدالة الجنائية مواكبة هذا التطور الكبير وإدخال وسائل جديدة في عملية اكتشاف الجرائم حتّى يكون للسياسة الجنائية دور إيجابي و فعال في مكافحة الإجرام المستحدث، ومواكبة لهذا التطور تطورت طرق الإثبات الجنائي وظهرت طرق علمية جديدة مستحدثة سمّية بالأدلة العلمية، ولقد أشرنا إلى هذا النوع من الأدلة و إلى كيفية احتلالها الصدارة بين أدلة الإثبات الأخرى أمام القاضي الجنائي، حيث أنّها أصبحت الأكثر استعمالافي ميدان الكشف عن الجريمة و إثبات الحقيقة مما جعلها تشكل واقعا مفروضا على القاضي بسبب دقتها و يقين نتائجها العلمية.

و ما تجدر الإشارة إليه أنّ السياسة الجنائية الحديثة المستندة على ا
إلى فتح آفاق كبيرة للقضاء على الجريمة عن طريق مسايرة كل ما هو جديد في المجال الجنائي أمام الأدلة العلمية، قد اصطدمت أثناء عملية تطورها بإشكالات عديدة، إذ من أهم ما تثيره الأدلة العلمية من مشاكل من الناحية العملية، مشكلة المشروعية أو مشكلة المصلحة الأولى بالرعاية، فالكثير من هذه الأدلة يمثل في حدّ ذاته اعتداء صارخا على حرية الفرد أي الشخص المتهم أثناء البحث أو محاولة الحفاظ على مصلحة المجتمع، وهنا يثور التساؤل عن مصلحتي الفرد و المجتمع، من منهما الأولى بالرعاية.

إنّ محاولة تفادي الاصطدام الذي قد تحدثه عملية الأخذ بالأدلة الحديثة في إثبات الجريمة مع مبدأ قرينة البراءة ومحاولة تحديد المصلحة الأولى بالرعاية تدفعان بالقاضي أو المشرع إلى محاولة كفالة التوازن بين حق المجتمع في الحصول على الدليل الذي يوصله إلى الحقيقة وبين حق المتهم في إثبات براءته، وذلك عن طريق اتخاذ كافة الاحتياطات والضمانات التي تمنع المساس بحرية الفرد إلاّ بالقدر اللازم لتفيد الإجراءات التي يتخذها المجتمع أثناء بحثه عن الحقيقة.

ورغم أهمية الدليل العلمي وحجّيته في الإثبات، فهو لا يزال يقف عاجزا أمام الكثير من الجرائم التي تطوّرت في حدّ ذاتها مع تطور وسائل الكشف عنها، فالتكنولوجيا الحديثة التي ساهمت في الكشف عن الجريمة هي نفسها التي وضعت بين أيدي محترفي الإجرام الوسائل المتقدمة لاستخدامها في إرتكاب

أخطر جرائمهم وإخفائها، فلقد أصبح ذكاء المجرم في تطور طردي مع تطور الوسائل العلمية لمكافحة إجرامه.

وإذا كانت الأدلة العلمية قد تقلّص من السلطة التقديرية للقاضي الجنائي أثناء تكييفه لها بسبب طبيعتها العلمية البحتة، الأمر الذي قد يؤثر على مبدأ اقتناعه الشخصي في حد ذاته أو حتّى إلغائه في بعض الأحيان، فالقاضي الجزائي مقيّد بكل ما هو وارد في تقدير الخبرة لأنّ الدليل العلمي يقوم على أسس علمية دقيقة ولا حرية ولا سلطة للقاضي الجزائي في مناقشتها باعتبارها تشكل حقائق علمية ثابتة، إلّا أنّ الظروف والملابسات التي وجد فيها الدليل فإنّها تدخل في نطاق تقديره.

هذه كانت أهم النتائج المتوصّل إليها، أمّا عن الاقتراحات التي نرجو الأخذ بها، فتتمثل فيما يلي:
إنّ العالم اليوم في تقدم مستمر و متسارع بما يحويه من وسائل تعمل على تطوير الجريمة في حدّ ذاتها تطويرا يخرجها من سيطرة الجهاز القائم على مكافحتها، أو حتى من الحدود الجغرافية التي ارتكبت فيها، لذا فقد أصبح لزاما على الجهات الأمنية و التشريعية و القضائية أن تطوّر أساليبها و وسائلها و تخضعها لهذا التطور كي تتمكن من التعامل و التعايش مع عصر الثورة المعلوماتية، و في ظل التقدم العلمي الذي فتح آفاق جديدة و جلب معه أيضا مشكلات و مخاطر جديدة، فإن لم نستطع التعامل معها بكفاءة عالية فإنّ ذلك سيهدّد الحياة الخاصّة، و لذلك لابدّ من وضع برامج علمية و أساليب فعّالة للتّعامل مع هذا الواقع الجديد الذي فرض نفسه على الأفراد و المجتمعات على مستوى العالم.

و إلى جانب الاهتمام بتقنين هذه الوسائل الحديثة في جمع الأدلة يجدر بنا الإشارة إلى أنّه أضحى من الصعب إسناد عملية تجميع هذه الأدلة إلى الشرطة القضائية بمعناها الضيق بما تحويه مهامها طبقا للتشريع القائم من بحث و تحري وجمع للأدلة فحسب، كون الأدلة العلمية وبحسب طبيعتها، تستلزم أن يكون الجهاز القائم بالتنقيب عليها و البحث فيها جهاز علميا جنائيا وتقنيا كما هو عليه الحال فيما يسمى بالشرطة العلمية، وهنا تجدر بنا الإشارة إلى محاولة إلقاء الضوء على وضع هذه الهيئة في القانون الجزائري الذي ومنذ الاستقلال يكتنفه الكثير من الغموض خلافا لما هو عليه الحال بالنسبة للشرطة القضائية فنحن لا نجد لها ذكرا في قانون الإجراءات الجزائية من الناحية التشريعية رغم وجودها كجهاز قائم بذاته مستقل نسبيا عن الشرطة القضائية من الناحية العملية.

قائمة المراجع:

I-المراجع باللّغة العربية :

أولا-الكتب

01-أبي الفضل جمال الدين محمد بن مكرم إبن منظور: لسان العرب، المجلد الخامس، دار صادر، بيروت، 1997.

02-أحمد فتحي سرور: الوسيط في شرح قانون الإجراءات الجنائية، دار النهضة، القاهرة، 1981.

03-حاتم حسن بكار، أصول الإجراءات الجنائية وفق أحدث التعديلات التشريعية والاجتهادات الفقهية والقضائية منشأة المعارف، الإسكندرية،2007.

04-حسين علي محمد علي الناعور النقبي: سلطة القاضي الجنائي في تقدير الأدلة، دار النهضة العربية، القاهرة،2007.

05-رمزي رياض عوض: سلطة القاضي الجنائي في تقدير الأدلة، دار النهضة العربية، القاهرة ،2004.

06-سامي حسني الحسيني: النظرية العامة للتفتيش في القانون المصري المقارن، دار النهضة العربية، القاهرة، 1972.

07-فاضل زيدان محمد: سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة، عمان، 2006.

08-فودة عبد الحكيم، حجية الدليل الفنّي في المواد الجنائية والمدنية، دار الفكر الجامعي، الإسكندرية، 1996.

09-كمال عبد الواحد الجوهري: تأسيس الاقتناع القضائي والمحاكمة الجنائية العادلة، دار محمود، مصر ،1999.

10-محمد عطية راغب المحامي: النظرية العامة للإثبات في التشريع الجنائي العربي المقارن، دار المعرفة، القاهرة، 1960.

11 -محمد زكي أبو عامر: الإجراءات الجنائية، الطبعة السابعة، دار الجامعة الجديدة، الإسكندرية، 2005.

12-محمود محمود مصطفى: الإثبات في المواد الجنائية في القانون المقارن، الجزء الأوّل، الطبعة الأولى، مطبعة جامعة القاهرة والكتاب الجامعي، القاهرة، 1977.

13-مروك نصر الدين: محاضرات في الإثبات الجنائي، الجزء الأوّل، النظرية العامة للإثبات الجنائي، دار هومه،الجزائر،2007.

14-وهبة بن مصطفى الزحيلي: التفسير المنير في العقيدة والشريعة والمنهج، المجلد الثاني، الجزء الثالث، دار الفكر المعاصر، دمشق،1997.

15-يوسف محمد رضا: معجم العربية الكلاسيكية والمعاصرة، الطبعة الأولى، مكتبة لبنان، بيروت،2006.

ثانيا: الرسائل والأطروحات الجامعية

01-إبراهيم إبراهيم الغماز: الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1980.

02-عبد الله بن صالح بن رشيد الربيش: سلطة القاضي الجنائي في تقدير أدلة الإثبات بين الشريعة والقانون وتطبيقاتها في المملكة العربية السعودية، بحث تكميلي لنيل درجة الماجستير في قسم العدالة الجنائية، أكاديمية نايف العربية للعلوم الأمنية، الرياض،2003.

03-فوزية خربوش: الأدلة العلمية ودورها في الاثبات الجنائي، رسالة ماجستير في القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الجزائر،2002.

04-هلالي عبد الله أحمد: النظرية العامة للإثبات في المواد الجنائية، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة أسيوط، 1987.

ثالثا: المقالات

-نصر الدين ماروك: مبدأ المشروعية والدليل الجنائي، مجلة النائب، العدد10، سنة 2010.

رابعا: النصوص القانونية

- الأمر رقم 66-155 المؤرخ في08 يونيو1966 يتضمن قانون الإجراءات الجزائية، جريدة رسمية، العدد48، الصادر بتاريخ 10يونيو1966 المعدّل و المتمم.

II-المراجع بالّغة الفرنسية

-Geneviève giudicelli-delage: les transformations de l’administration de la preuve pénale‹ société de législation comparée‹ paris, 2006 .

الإثبات في الجرائم الالكترونية

الدكتور: بن لخضر محمد
أستاذ محاضر "أ"
معهد الحقوق والعلوم السياسية (المركز الجامعي نور البشير البيض)
البريد الالكتروني: mbenlakhdar2004@gmail.com

الملخص:

تعد الجريمة الالكترونية من الجرائم الحديثة التي فرضت نفسها على المستوى الوطني والدولي على حد سواء، لذا فإن معالجتها القانونية يجب أن تتم في إطار شمولي لا يخلو من التكاملية، حيث أن خصوصية التجريم نابعة من وقوع غالبية هذه الجرائم في العالم الافتراضي دون المادي، والتي يلزمها خصوصية في إثبات هذا النوع من الجرائم المرتكبة عبر الإنترنيت التي لا تخلو من الصعاب الجمة والتي تكتنف رصد واحتواء الدليل الرقمي المتحصل عليه من مسرح الجريمة سواء المادي أو الافتراضي، وصلاحية هذا الدليل للإثبات ومدى شرعيته وقبوله لدى القاضي الجنائي، وذلك كون الأدلة الرقمية صعبة الاحتواء وسهلة الاختفاء والمحو، بالإضافة إلا أنه يمكن التضليل بشأن كشفها أو الاطلاع على مضمونها.

الكلمات المفتاحية: الجريمة الالكترونية، دليل الإثبات، شرعية الدليل، القاضي الجنائي.

مقدمة:

إن أهم ما يلفت النظر في السنين الأخيرة، هو التوسع الكبير في استخدام الحاسوب الآلي والانترنت من قبل جميع شرائح المجتمع، بل والاعتماد عليها في كثير من مجالات الحياة سواء الاقتصادية أو الاجتماعية أو التواصل والاتصال، والتي تجعلها تكتسب أهمية كبرى بالنسبة إلى أفراد المجتمع بكل فئاته، إلا أن هذا التطور سرعان ما أفرز مجموعة من الممارسات والأفعال التي استغلت الوسائل التقنية الحديثة لتستهدف مصالح محمية جنائياً، وأحدثت اضطراباً اجتماعياً بعدما تمكنت من المس بمصالح الأفراد، بل وتهديد الاستقرار والأمن السياسي والاقتصادي لعديد الدول.

مكنت هذه الثورة التقنية عالماً جديداً لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، ونتج عنها ظهور وابتكار أشكال وأساليب إجرامية جديدة تجاوزت تهديد المصالح التقليدية التي تحميها القوانين والتشريعات الجنائية إلى المساس بمصالح ومراكز قانونية استحدثتها تقنية المعلومات، مما خلق إشكالات قانونية لا تقتصر على ضبط هذه الجرائم فحسب، وإنما أثارت أيضا تحديات أكثر تعقيداً من ناحية إثباتها، وعليه يمكن طرح مشكلة البحث في التساؤل الرئيس التالي : **هل يمكن القول بأن الإثبات بوسيلة إلكترونية يقتصر فقط على الجريمة الالكترونية بمعناها الضيق أم يمكن اللجوء إليه لو تعلق الأمر بجريمة عادية وإن لم تقترف بوسيلة الكترونية ؟**

وسنقتصر في موضوعنا هذا على فكرة شرعية الدليل الالكتروني، لذلك فإن موضوعنا سيلامس الجانب المتعلق بتقدير الدليل الالكتروني المقدم أمام القضاء الجزائي وما إذا كانت لهذا الأخير سلطة في الأخذ به أو تركه من أجل الفصل في الدعوى العمومية.

إن الإجابة على هذه الإشكالية سيتم وفق التالي:

المبحث الأول: الإثبات الجنائي في البيئة الإلكترونية بين الحرية والتقيد.

المبحث الثاني: حجية الدليل الإلكتروني الجنائي.

المبحث الأول:

الإثبات الجنائي في البيئة الالكترونية بين الحرية والتقييد.

هناك نظامين رئيسيين: **الأول** نظام الإثبات الحر فهو يسود في ظل الأنظمة اللاتينية، ووفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في إثبات الوقائع المعروضة عليه، فلا يلزمه القانون الاستناد إليها في تكوين قناعته، أي أن الأصل في هذا النظام مشروعية وجودها، فالدليل الرقمي سيكون مشروعا من حيث الوجود استصحابا للأصل **(المطلب الأول)**.

أما عن **الثاني** نظام الأدلة القانونية يسود هذا النظام في الأنظمة الانجلوسكسونية، بمعنى أن المشرع يحدد الأدلة التي يجوز للقاضي اللجوء إليها في الإثبات، كما يحدد القيمة الإقناعية لكل دليل، فلا سبيل للاستناد إلى أي دليل لم ينص القانون عليه صراحة ضمن أدلة الإثبات، كما أنه لا دور للقاضي في تقدير القيمة الإقناعية للدليل، ولذا يسمى هذا النظام بنظام الإثبات القانوني أو المقيد **(المطلب الثاني)**.

المطلب الأول

حرية إثبات الجرائم الكلاسيكية المرتكبة بوسيلة الكترونية

ونقصد هنا بالجرائم الكلاسيكية تلك الجرائم العادية أو التقليدية التي تقترف بوسائل الكترونية، وقد ازدادت هذه الجرائم تفاقماً في ظل البيئة الإفتراضية التي تمثلها شبكة المعلومات الدولية (الأنترنت) الواسعة الانتشار، ما أفرز نوعاً جديداً من الجرائم لم يكن معهوداً من قبل وعليه نتسأل حول ما إذا كانت حرية الإثبات فيها هي الأصل؟

كما هو معلوم فإن نظام الإثبات الحر هو الذي يحكم الجرائم بصفة عامة، ولذلك وجد هذا النظام صداه في معظم التشريعات الجنائية، ومنها التشريع الجزائري عندما نص عليه في 212 من قانون الإجراءات الجزائية[1]، وهي المادة التي تؤكد أن لأطراف الدعوى العمومية (سواء النيابة العامة أو المهتم) كامل الحرية في أن يقدموا ما يتوفرون عليه من أدلة إثبات أمام المحكمة، وأن هذه الأدلة يجب

---

[1]– تنص **المادة 212** من قانون الإجراءات الجزائية على أنه :" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك. وللقاضي أن يصدر حكمه تبعاً لاقتناعه الخاص. ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضورياً أمامه" تقابلها المادة 427 من قانون الإجراءات الجزائية الفرنسي.

أن تناقش حضورياً أمام القاضي الجنائي، حتى يحصل الاقتناع الشخصي للمحكمة التي تنظر في النزاع الجنائي، ذلك أنه لا يمكن إدانة شخص ما إلا إذا وجد من الأدلة ما يكفي لإثبات وجود الجريمة ذاتها واثبات نسبتها إليه دون غيره[1]، وهو ما لا يمكن أن يتم إلا بتوفر أدلة الإثبات الكفيلة بذلك، والتي تؤدي بالضرورة إلى خلق نوع من الاقتناع الشخصي للقاضي الجنائي، باعتبار ذلك جزءا لا يتجزأ من تصور ونظرة المجتمع للدور الذي يجب أن يلعبه القاضي الجنائي من أجل الوصول إلى الحقيقة.[2]

فنظام الإثبات الحر لا يلزم القاضي بقبول أو رفض أي دليل، وإنما يكون لهذا الأخير الحرية التامة في الاستعانة بأي دليل يراه كاشفاً للحقيقة[3]، لأن اعتماده قائم على فكرة أن الجريمة ما هي في آخر المطاف إلا واقعة قانونية أو مادية، لا يمكن للقانون أن يحدد طرق إثباتها بصورة حصرية، لتمكين أطراف الدعوى وبكل حرية من أن يقدموا أي دليل يرونه مناسبا[4]، وفي هذا السياق يُطرح التساؤل حول ما إذا كان تصور المشرع لفكرة الإثبات في المجال الجنائي يبقى تصوراً ثابتاً مهما كانت الطريقة التي ارتكبت بها الجريمة أم أن تنوع الوسائل التي يمكن أن ترتكب بها الجريمة " **الكلاسيكية** " يؤثر سلبا وإيجابا على قبول فكرة الحرية في الإثبات؟

إن هذا التساؤل يبقى مشروعا متى تعلق الأمر بالجرائم " **الكلاسيكية** " التي يتم ارتكابها بطرق الكترونية، ذلك أن انفصال مفهوم الجريمة كبناء قانوني عن الوسيلة التي ترتكب بها يخلق العديد من الإشكالات المرتبطة بالإثبات في المجال الجنائي، ففي الوقت الذي نسلم فيه بكون حرية الإثبات تبقى هي الأصل مادام أن الأمر يتعلق بجريمة " **كلاسيكية** "، نجد أن ارتباط هذا الإثبات بالوسيلة التي ارتكبت

---

[1]– **الحكماوي عبد الحكيم**، الإثبات في الجريمة الالكترونية، سلسلة ندوات محكمة الاستئناف بالرباط، مطبعة الأمنية الرباط، العدد السابع، 2014، ص 149.

[2]– يعتبر **الاقتناع الشخصي (الوجداني)** من أهم المبادئ التي تقوم عليها العدالة في النظم الديمقراطية، ولا يمكن اعتبار الاقتناع الشخصي مجرد انطباع يحصل في نفس المحكمة أو القاضي الذي يتولى النظر في النزاع الجنائي؛ وإنما يجب النظر إليه باعتباره خلاصة مجموعة من الانطباعات العقلية والذهنية التي تحصل في ذهن القاضي انطلاقا من عرض أدلة الإثبات أمامه ومناقشتها وبسط وجهات النظر فيها من قبل كل أطراف الخصومة الجنائية، على أن تكون تلك الانطباعات مدعومة ببناء منطقي يقود إلى استنتاج الحقيقة من أدلة الإثبات المعروضة على المحكمة علانية وحضوريا بالشكل الذي ينفي الجهالة عن الجريمة ذاتها ويبدد كل شك في كون الجريمة منسوبة للمتهم (**الحكماوي عبد الحكيم**، الإثبات في الجريمة الالكترونية، سلسلة ندوات محكمة الاستئناف بالرباط، مطبعة الأمنية الرباط، العدد السابع، 2014، ص 149.).

[3]– **بوعناد فاطمة زهرة**، مشروعية الدليل الإلكتروني في مجال الإثبات الجنائي، أطروحة دكتوراه في العلوم تخصص علوم قانونية فرع علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس– سيدي بلعباس– السنة الجامعية : 2013/2012، ص 260.

[4]– من خلال نظام الإثبات المعتمد يتم ضمان أمرين، أولهما ضبط استفاء الأمن والاستقرار للمجتمع وثانيهما التأكد من عدم مساس حريات وحقوق الفرد بأي نوع من أنواع الاعتداء باعتباره الطرف الضعيف في الدعوى العمومية بغرض عرض ما يتوفر عليه من أدلة إثبات ومن حجج يمكن أن يدافع بها عن براءته متى وجد نفسه أمام أدلة إثبات قد تجعل الحكم الجنائي لغير صالحه.

بها الجريمة يثير صعوبة بشأن الحد الفاصل، وعلى هذا الأساس تطرح فكرة إثبات ارتكاب جريمة **كلاسيكية** ما ونسبتها إلى شخص معين، مسألة جوهرية تتعلق بضرورة إثبات أن الشخص مرتكب الجريمة قد ارتكبها بوسيلة الكترونية تدخل تحت سيطرته وأنه هو من يتحمل المسؤولية عنها وعما يمكن أن تحدثه من أضرار للغير.[1]

وإذا كان المنطق القانوني السليم يلفظ هذه النتيجة، إذ لا يمكن أن تكون أداة ارتكاب الجريمة وحدها سبباً في إعادة تبويب الجرائم ومراجعة أحكام القانون الجنائي، فإن ذلك لا يمنع من رصد وجود بعض التقاطعات بين الإجرام الكلاسيكي والإجرام المعلوماتي، والتي تفرض إعادة النظر في النص الجنائي قصد ملاءمته مع خصوصيات الإجرام المعلوماتي[2]، ولعل هذا التحدي الذي تطرحه الوسائل الالكترونية في إثبات الجرائم الكلاسيكية هو ما جعل واضعي اتفاقية "**بودابست**" الموقعة في 2001/11/23 المتعلقة بالإجرام الكوني "الجرائم المعلوماتية" يؤكدون على فكرة ضرورة ملائمة التشريعات الوطنية لما تضمنته مقتضيات تلك الاتفاقية وبخاصة ما يرتبط بمجال تطبيقها.[3]

لذلك يظهر أن الإثبات في الجرائم " **الكلاسيكية** " التي يتم اقترافها بوسائل الكترونية يتجه نحو التقييد، وهو ما يتنافى مع طبيعة تلك الوسائل التي يستحيل على الأفراد العاديين وحتى الأجهزة المكلفة بإنفاذ القانون أن تتوفر عليها، اللهم إلا إذا خول لها القانون إمكانية التعاون مع الجهات المحتكرة للخدمات المعلوماتية والحصول على المعلومات والبيانات المفيدة في البحث والإثبات في الميدان الجنائي، لذلك يبقى من الأكيد القول بأنه بالقدر الذي أخذ الفكر القانوني يتراجع فيه عن فكرة الحرية في الإثبات في هذا النوع من الجرائم نتيجة الإكراهات التقنية والمادية، فقد بدأ التفكير في نقل جزء من عبء الإثبات إلى جهات الاتهام بصورة مطلقة، ويثبُت ذلك كله من خلال منع الأفراد العاديين من التعامل مع مزودي الخدمات الالكترونية مباشرة وجعل هذا التعامل حكراً على الأجهزة المكلفة بالبحث والتحري وجمع الاستدلالات عن الجرائم كالشرطة القضائية.[4]

ولعل هذا التراجع الذي بدأ يشهده مبدأ حرية الإثبات في مجال الجريمة " **الكلاسيكية** " متى ارتبطت بوسيلة الكترونية، يعد مؤشراً صريحاً حول كون التشريعات الوطنية التي تهتم بالجريمة الالكترونية تقترب أكثر فأكثر إلى تقييد فكرة الإثبات في مجال مكافحة الجريمة الالكترونية متى كانت

---

[1]– **الحكماوي عبد الحكيم**، المرجع السابق، ص 150.

[2]– **اللمتوني عبد الرحمان**، الإجرام المعلوماتي بين ثبات النص وتطور الجريمة، سلسلة ندوات محكمة الاستئناف بالرباط، مطبعة الأمنية الرباط، العدد السابع، 2014، ص 52.

[3]– وهو ما دعا المشرعين في عدد من الدول بالتدخل وإصدار قانون يتعلق بجرائم الكمبيوتر منهم المشرع الأمريكي الذي أصدر قانونه عام 1986، أما المشرع الفرنسي فقد أدمج بابا في قانون العقوبات الفرنسي يتحدث عن بعض الجرائم المعلوماتية وذلك في 1994/3/1، وفي بلجيكا صدر قانون مكافحة الإجرام المعلوماتى في 2001/2/3، أما الاتحاد الأوربي فقد حرص على التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات وذلك في اتفاقية بودابست.

[4]– **الحكماوي عبد الحكيم**، المرجع السابق، ص 151.

تلك الجريمة قد استهدفت نظاما الكترونيا كيفما كان نوع الاستهداف، وارتكبت بوسيلة الكترونية وهو ما سوف نتطرق إليه في المطلب الثاني.

المطلب الثاني

تقييد إثبات الجرائم الالكترونية البحتة

يبدأ الحديث حول مدى حرية الحصول على دليل إثبات الجرائم الالكترونية فهي الجرائم التي تستهدف النظم والبرنامج وقواعد البيانات المعلوماتية، إذ في هذا الصنف من الجرائم يمكن تصور تقييد الإثبات كقاعدة، ذلك أن صعوبة امتلاك الدليل الالكتروني من طرف الأفراد يجعل مسألة الدفاع عن حقوقهم أمراً صعباً من شأنه التأثير على عمل المحققين وجهات إنفاذ القانون كالنيابة العامة وقضاة التحقيق، ولذلك فإن المشرعين الوطنيين واستلهاما منهم للمبادئ التي جاءت بها اتفاقية **بودابست** والاتفاقية المرتبطة بها، شرعوا في وضع مجموعة من المقتضيات القانونية التي تفرض على مزودي الخدمات الالكترونية التعاون مع الأجهزة المكلفة بالبحث عن الجرائم الالكترونية، وفي هذا السياق يمكن القول بأن محاربة الجريمة الالكترونية بالقدر الذي تبدو أهميتها فهي تهدد مجموعة من الخصوصيات المرتبطة بالحياة الخاصة للأفراد.[1]

ويظهر أن انحصار الحصول على الدليل الالكتروني من طرف الجهات المكلفة بالبحث والتحري وجمع الاستدلالات في الجرائم الالكترونية وإلزام الجهات المشرفة على تقديم الخدمات الالكترونية على تزويدهم بالبيانات والمعطيات الضرورية لذلك، يدخل في نطاق مفهوم الاستثناء الوارد بقانون الإجراءات الجزائية والذي نصت عليه المادة 45 الفقرة الأخيرة[2] من قانون الإجراءات الجزائية التي لا تعفي من اتخاذ جميع التدابير اللازمة لضمان احترام السر المهني عندما يجري التفتيش في محلات يكون أصحابها ملزمون بكتمان السر المهني، كما أن جميع هذه الإجراءات الاستثنائية تستوجب الحصول على إذن مسبق من وكيل الجمهورية عندما يتعلق الأمر بحالة تلبس أو بتحقيق ابتدائي[3]، إذ أن القوانين المنظمة لوظائف الجهات المكلفة بتسيير وحفظ البيانات الشخصية ذات الطبيعة الالكترونية تفرض على هذه الجهات الحفاظ على السر المهني إلا ما استثني بمقتضى القانون، وبالتالي فإن رغبة الأفراد العاديين في الحصول على تلك المعطيات والبيانات تصطدم بهذا المقتضى القانوني وهو ما يجعل الحصول على الدليل المستعمل في إثبات الجريمة الالكترونية يخضع لشكليات وقيود قانونية.[4]

---

[1]– **Olivie leroux et yves poullet** ; « en marge de l' affaire GAIA, de la recevabilité de la preuve pénale et du respect de la vie privée ».revue générale de de droit civil belge, année 2003, p163. (نقلا عن: **الحكماوي عبد الحكيم**، المرجع السابق، ص 151.)

[2]– تنص المادة 45 من ق إ ج على " غير أنه عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر. ".

[3]– **الأخضري مختار**، الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الافتراضي، نشرة القضاة، وزارة العدل، العدد 66، ص 62.

[4]– **الحكماوي عبد الحكيم**، المرجع السابق، ص 153.

إن الحديث عن عدم قدرة الأفراد في الحصول على الدليل، واقتصار ذلك على الجهات المكلفة بإنفاذ القانون يندرج في خانة اتجاه الرأي نحو التقييد من حرية الإثبات، بل وحصرها في الشكليات التي أقرها المشرع من أجل الحصول على الأدلة المرتبطة بالجريمة الالكترونية، وبالتالي فإن فكرة حرية الإثبات كما نادت بها المدرسة اللاتينية الجرمانية لم تصبح ذات أهمية، مادام أن طبيعة الدليل الالكتروني تأبى أن يكون هذا الأخير متاحاً للأفراد نظراً لاتصاله بحياتهم الخاصة، لكن بالرغم من ذلك، فإن الجهات القضائية المكلفة بإنفاذ القانون وإن كانت تملك صلاحية الحصول على الدليل الالكتروني لإثبات الجريمة الالكترونية كيفما كان نوعها، فإن السؤال الذي يبقى مطروحا في هذا لسياق هو ما إذا كان الحصول على الدليل الالكتروني يجب أن يخضع لشكليات معينة أم أن الأمر يتجاوز ذلك كنتيجة منطقية للخصائص التي يتميز بها ذلك الدليل من جهة ولمتطلبات التعاون في مجال مكافحة الجريمة المعلوماتية من جهة أخرى؟[1] إن الجواب عن هذا التساؤل هو ما سوف نحاول الإجابة عنه في المبحث الموالي.

المبحث الثاني

حجية الدليل الالكتروني الجنائي

لم يتطرق المشرع الجزائري لمسألة حجية الدليل الالكتروني، إلا أنه مادام يعتنق نظام الإثبات الحر فيكون الدليل الالكتروني مقبولا في الإثبات، وهذا يعني أن للقاضي الجزائي مطلق الحرية في أن يصل إلى الحقيقة من أي دليل قانوني مهما كان نوعه بما في ذلك الدليل الالكتروني، فيستمد القاضي قناعته من أي دليل يطمئن إليه من الأدلة التي تقدم إليه دون التقيد بدليل معين ما لم ينص القانون على خلاف ذلك، ويمكن الأخذ بالدليل الالكتروني سواء في الإدانة أو البراءة إذا توافرت فيه الشروط المطلوبة[2]، ويرتبط الدليل عموما بفكرتي الشرعية والحقيقة، فمن جهة يجب أن يتميز هذا الدليل بكونه مشروعا أي تم الحصول عليه وفق ما يقتضيه القانون **(المطلب الأول)**.

---

[1]– **الحكماوي عبد الحكيم**، المرجع السابق، ص 153 – 154.

[2]– أ– **المشروعية:** يجب أن يتميز هذا الدليل بكونه مشروعا أي تم الحصول عليه وفق ما يقتضيه القانون.

ب– **الصحة والمطابقة:** أي أن يكون الدليل الالكتروني المقدم إلى المحكمة هو نفس الدليل الذي تم الحصول عليه، وأن لا يطرأ عليه أي تغيير خلال فترة تخزينه.

ج– **الدقة:** أي أن نظام الحاسوب الذي استخرج منه الدليل يعمل على نحو دقيق وسليم، بحيث لا يتطرق الشك في دقته (أنظر **بوعناد فاطمة زهرة**، مشروعية الدليل الإلكتروني في مجال الإثبات الجنائي، أطروحة دكتوراه في العلوم تخصص علوم قانونية فرع علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس– سيدي بلعباس– السنة الجامعية : 2013/2012، ص 258.)

ومن جهة أخرى يعتبر الدليل الوسيلة الوحيدة للوصول إلى الحقيقة المراد إثباتها أمام القضاء **(المطلب الثاني)**.

المطلب الأول

مشروعية الحصول على الدليل الإلكتروني في الإثبات الجنائي

يجب الحصول على الدليل بصورة مشروعة وغير مخالفة لأحكام القانون، وحتى يكون للدليل الإلكتروني قيمة قانونية أمام القاضي الجنائي، يجب أن تكون الطريقة التي تم التوصل بها إلى الدليل تمت بطريقة مشروعة[1] بعيدة عن أي زيف أو خداع، الأمر الذي يحتم على من أسند إليهم أمر تحصيل الدليل الإلكتروني، إتباع طرق قانونية ومشروعة تكون الغاية من ورائها إدانة المتهم من جهة، وقبول الدليل من طرف القاضي الجنائي من جهة أخرى، ويقصد بمشروعية الدليل الجنائي بما يتضمنه من أدلة إلكترونية هو: " التوافق والتقيد بالأحكام القانونية في إطارها ومضمونها العام فهي تهدف إلى تقرير ضمانة أساسية وجدية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة وبالتطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الإجتماعي وبنفس القدر لتحقيق حماية مماثلة للفرد ذاته "[2].

ويقصد بها كذلك ضرورة إتفاق الإجراء مع القواعد القانونية والأنظمة الثابتة في وجدان المجتمع المتحضر، كما أن مشروعية الدليل لا ترتبط فقط بالقواعد القانونية فقط، بل يجب كذلك مطابقتها مع إعلانات حقوق الإنسان والمواثيق والإتفاقيات الدولية وكذلك حتى مع قواعد النظام العام وحسن الآداب السائدة في المجتمع[3].

ومبدأ المشروعية يمثل أحد الدعائم الأساسية التي نصت عليها التشريعات الجنائية المعاصرة إلا أنها لا تكفي وحدها لحماية حرية الإنسان في حالة القبض عليه أو اتخاذ الإجراءات اللازمة لمحاكمته مع افتراض إدانته، فكل إجراء يتخذ ضد الإنسان دون افتراض براءته سيؤدي حتما إلى تكليفه عبئ إثبات براءته من الجريمة المنسوبة إليه، فإذا عجز عن إثبات هذه البراءة اعتبر مسؤولا عن جريمة لم تصدر عنه.[4]

ويؤدي هذا الوضع إلى قصور الحماية التي يكلفها مبدأ الشرعية طالما كان من الممكن المساس بحرية المتهم من غير طريق القانون، أو كان من الممكن إسناد الجرائم لأحد ما ولو لم يثبت ارتكابه لها عن طريق افتراض إدانته، لذلك فإن الموازنة بين حقوق المتهم باعتباره إنساناً من جهة وحقوق المجتمع من جهة أخرى، وبين هذه الحقوق وضرورة احترام القواعد الشرعية والقانونية أثناء البحث عن الدليل أي

---

[1]- **كمال محمد عواد**، الضوابط الشرعية والقانونية للأدلة الجنائية في الفقه الإسلامي والقانون الوضعي، الطبعة الأولى، دار الفكر الجامعي، مصر، 2011، ص167 .

[2]- **زروق محمد**، حجيته الدليل الالكتروني ومشروعية أمام القاضي الجنائي، مجلة منازعات الأعمال، العدد 32، مايو 2018، ص 66.

3- المرجع نفسه، ص 66.

[4]- **أحسن بوسقيعة**، الوجيز في القانون الجنائي العام، دار هومة، الطبعة السادسة، 2008، ص 50.

في البحث الجنائي عموما وفي مجال الجريمة الالكترونية على وجه الخصوص، تعتبر أساس سؤال شرعية الدليل ذاته، فهل يمكن للمحكمة التي عرض عليها دليل تم الحصول عليه بطريقة غير قانونية أن تلتفت إليه أم أن دواعي احترام القانون يجب أن تقدم على دواعي البحث عن الحقيقة؟[1]

وإذا كان الحصول على الدليل يخضع لروح القانون، فإن هناك مجموعة من الجناة قد يتلاعبون بالأدلة[2] التي قد تثبت إدانتهم فتضيع حقوق الضحايا وتندثر الأدلة ولا يحصلون جراء ذلك على حقوقهم كما لا يحصل المجتمع باعتباره المتضرر الأكبر من الجريمة على حقه في معاقبة الجاني، من هنا كان من اللازم تدعيم هذه القاعدة بقاعدة ثانية تحكم تنظيم الإجراءات تتخذ ضد المتهم، على نحو يضمن احترام الحقوق والحريات الفردية وهذه القاعدة تسمى بالشرعية الإجرائية، أو قاعدة مشروعية الدليل.[3]

وفي إطار مشروعية الأدلة الإلكترونية، نجد أن قانون الإجراءات الجنائية الفرنسي رغم أنه لم يتضمن أي نصوص تتعلق بمبدأ الأمانة أو النزاهة في البحث عن الحقيقة، إلا أن الفقه والقضاء كانا بجانب هذا المبدأ سواء في مجال التنقيب عن الجرائم التقليدية، أم في مجال التنقيب في جرائم الحاسوب والإنترنت، ففي فرنسا مثلا تم تناول حجية مخرجات الأنظمة الآلية ضمن ما يسمى بالأدلة العلمية التي يجب أن تتوفر فيها شروط معينة ومقررة لها سلفاً حتى تقبل كوسيلة من وسائل الإثبات.[4]

ويشير رأي فقهي فرنسي إلى أن القضاء قد قبل استخدام الوسائل العلمية الحديثة في البحث والتنقيب عن الجرائم تحت تحفظ أن يتم الحصول على الأدلة الجنائية، ومن بينها الأدلة المتحصل عليها

---

[1]- **الحكماوي عبد الحكيم**، المرجع السابق، ص 155.

[2]- يضع الجاني في بعض الحالات عقبات فنية لمنع كشف جريمته وضبط أدلتها باستخدام تقنيات التشفير (التشفير يعني، مناهج لخط البيانات من خلال لوغاريتمات أو خوارزميات بحيث لا يمكن لشخص ثالث قرائتها) أو كلمة السر، وذلك بقصد حجب المعلومة عن التداول العام ، ومنع الغير بما فيه أجهزة الرقابة من الوصول غير المشروع إلى البيانات والمعلومات المخزنة أو التلاعب فيها، وقد أثبتت التحقيقات في بعض الجرائم الإلكترونية بألمانيا وجود صعوبات تواجه البعض من هذه التحقيقات نتيجة استخدام مرتكبي هذه الجرائم لتقنيات خاصة كالتشفير والترميز لإعاقة الوصول إلى الأدلة التي تدينهم ، ومن الأمثلة التي لجأ فيها الجاني إلى أسلوب التشفير، كوسيلة لمنع ضبطه والإيقاع به، واقعة حدثت في الولايات المتحدة عام 1996، إذ كان المشتبه به مشغلا للوحة إعلانات bbs، وبعد الوصول إلى جهاز الحاسب الشخصي الذي يستخدمه في إدارة اللوحة الالكترونية، حاول محققو الشرطة العثور على كلمة المرور الخاصة بالمشتبه به، فقاموا بأخذ نسخة احتياطية من محتويات القرص الصلب، وقاموا بكتابة برنامج يحاول تشغيل النسخة الاحتياطية، وبعد فحص ملف المستفيدين استطاع المحققون الوصول بسهوله إلى أسماء المستفيدين وأرقامهم، ولكن لم يتمكنوا من العثور على كلمة المرور الخاصة بالمشتبه به، خاصة وأنها كانت مشفرة، ولولا تشفير كلمة المرور لأمكن إضافة مستفيد جديد بكلمة مرور جديدة، ثم تتبع هذه الكلمة داخل قاعدة بيانات المستفيدين حتى يتم معرفة مكانها، ولكن التشفير حال دون ذلك (**مفتاح بوبكر المطردي**، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلي المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 23 – 25 / 9 / 2012، ص 58 .).

[3]- **مروك نصر الدين**، محاضرات في الإثبات الجنائي، (النظرية العامة للإثبات الجنائي) الجزء الأول، دار هومة، 2003، ص 540-541.

[4]- **أحمد ضياء الدين محمد خليل**، مشروعية الدليل في المواد الجنائية، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعية في مجال الإجراءات الجنائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة عين شمس، القاهرة، 1986، ص 239.

من الحاسوب والإنترنت، بطريقة شرعية ونزيهة[1]، وهكذا فإن القضاء الفرنسي بعد أن كان متمسكا بشرعية الحصول على الدليل باعتبار ذلك تجسيد لإرادة المشرع التي ظهرت في شكل قواعد قانونية واجبة الاحترام، أصبح يتجه شيئا فشيئا إلى اعتماد الدليل المُؤدي إلى الحقيقة بغض النظر عن طريقة الحصول عليه، لأن الدليل المعتمد حسب هذا الاتجاه القضائي هو الدليل المُوصل للحقيقة ولو تم الحصول عليه بطريقة غير مشروعة ونفس الشيء نجده في سويسرا.[2]

وقد كان تحول موقف القضاء على النحو المذكور أعلاه محل نقاش بين الفقه ومن طرف الخصوم ذاتهم، لذلك فمنهم من تمسك بضرورة احترام القواعد القانونية باعتبارها ضامنة لحقوق الإنسان خلال سريان الإجراءات[3] وعرض النزاع على المحكمة، ومنهم من اعتبر أن ذلك التوجه يخالف التعهد الدولي وخاصة ما يتعلق بالالتزام بحقوق الإنسان[4]، ومن هنا فقد كان الاعتقاد في بادئ الأمر بأن ما ذهب إليه القضاء الفرنسي من ضرورة الالتزام بالكشف عن الحقيقة بدل التقيد بالشكليات القانونية من أجل استخلاص الدليل، المخالف لمقتضيات المادة السادسة من الاتفاقية الأوروبية لحقوق الإنسان، ذلك أن الحق في المحاكمة العادلة يقتضي بالضرورة التمسك والتقيد بما أقره القانون من قواعد واجبة الإتباع.

لكن هذا الرأي لم يصمد طويلا وخاصة بعد تنامي تأسيس التوجه القضائي الجديد على تبني فكرة الحقيقة كأساس لفلسفة الدليل، ومن ثم فقد ذهب أنصار هذا التوجه إلى اعتماد معيار أخلاقي ينبني على فكرة كون الدليل وسيلة للكشف عن الحقيقة، ولما كان الأمر يتعلق بنقل واقع أمام القضاء فإن القانون لن يستطيع تحديد سلوك الأفراد للوصول إلى غاياتهم ولو تم اعتماد معايير يخضع لها ذلك السلوك، وكنتيجة لهذا التوجه فقد رأى أنصار هذا التيار بأن مسألة التقيد بالشروط التي حددها القانون من أجل الحصول على الدليل أضحت مسألة مُتجَاوزة في ظل ضرورة احترام حق الخصوم في المناقشة الشفاهية والحضورية لوسائل الإثبات المثارة من قبلهم، فمادام أن الأطراف قدموا أدلتهم ووسائل إثباتهم وناقشوها حضوريا أمام

---

[1]– **عفيفي كامل عفيفي**، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، دار الفكر الجامعي، 2007، بدون دار النشر، ص20.

[2]– **الحكماوي عبد الحكيم**، المرجع السابق، ص 156.

[3]– أوصى المؤتمر الدولي لقانون العقوبات الذي عقد في ريو ديجانيرو بالبرازيل في مجال إصلاح الإجراءات الجنائية وحماية حقوق الإنسان الذي عقد في الفترة الممتدة بين 28 و 29 أكتوبر 2009 بمجموعة من التوصيات منها التوصية رقم 12 التي تنص على: " أن كل الأدلة التي يتم الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة ولا يمكن التمسك بها أو مراعاتها في أي مرحلة من مراحل الإجراءات. ".

[4]– دائما ما يقترن الحديث عن مشروعية الحصول عن الأدلة الجنائية بوجوب حماية واحترام حقوق الإنسان، على اعتبار أن جميع الإجراءات القانونية التي تستهدف الحصول على الأدلة الجنائية تمس بحقوق الأفراد وحرياتهم، ومن بين هذه الحقوق الحق في الخصوصية، لذا فإن اتخاذ إجراء المراقبة الالكترونية أو اعتراض المراسلات يمثل دون أدنى شك اعتداء على الحياة الخاصة، هذا الذي جعلها موضوع اهتمام كبير من قبل الإعلانات والمواثيق الدولية، ومثال ذلك ما نصت عليه المادة 12 من الإعلان العالمي لحقوق الإنسان، إذ" :لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات." (**معتصم خميس مشعشع**، إثبات الجريمة بالأدلة العلمية، مجلة الشريعة والقانون، العدد 56، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2013، ص 34.).

المحكمة، فإن هذه الأخيرة تملك كامل صلاحيتها في تقدير دليل كل طرف من أجل الوصول إلى الحقيقة، وبالتالي فإن تمتع المحكمة بسلطة تقديرية في هذا المجال يعتبر ضمانة مهمة من ضمانات المحاكمة العادلة متى احترم شرط العلانية والحضورية في مناقشة الدليل.[1]

كما أن أنصار هذا الاتجاه يؤكدون على أن هذا الأخير جاء من أجل مساعدة الطرف الضعيف في الخصومة، وذلك بتمكينه من إيجاد وسائل إثبات دفع الضرر عنه، سواء بإثبات براءته أو إثبات الضرر الحاصل له، حتى لا تكون لطرف الغلبة على الطرف الآخر، كما يؤكد هذا التيار أن ما ذهب إليه القضاء الفرنسي مطابق لروح مقتضيات المادة السادسة من الاتفاقية الأوروبية لحقوق الإنسان ما دام يضمن الشروط الكاملة للمحاكمة العادلة[2]، وتجدر الإشارة إلى أن شروط المحاكمة العادلة المنصوص عليها في المادة 06 من الاتفاقية التي تم تفصيل مقتضياتها في بعض البروتوكولات الإضافية قد تمت إعادة صياغتها في المواد 47 الفقرة (02) إلى 50 من ميثاق الحقوق الأساسية.[3]

كما أن الخصائص التي يتميز بها الدليل الالكتروني من كونه غير مادي بالمفهوم التقليدي، يؤكد الصعوبات التي تعترض عملية استخلاصه والحصول عليه بالطرق القانونية العادية بما يقتضيه ذلك من ضرورة سلوك إجراءات معقدة قد يؤدي احترامها إلى تفويت الفرصة على العدالة لتقول كلمتها، خاصة في الحالة التي يعمد فيها الأفراد إلى التلاعب بأدلة إثبات ما اقترفوه من جرائم والعبث بها بل وإتلافها في الغالب من الأحيان، نظرا للسهولة التي تتميز بها هذه العملية واستغراقها لوقت قصير جدا[4] فمرتكبي الجريمة المعلوماتية يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به، ولذلك فإنهم يسعون دائما لمحو وتدمير أو حتى تعديل أي دليل يؤدي إلى إدانتهم، عن طريق التلاعب غير المرئي في أنظمة الحاسب الآلي ومحتوياته.

---

[1]– يقول الفقيه **بيكاريا** في مؤلفه الجرائم والعقوبات: " إن فكرة اليقين الذاتي المطلوبة في المواد الجزائية لا يمكن أن تتقيد بقواعد إثبات محددة سلفا تسلبها حقيقة مضمونها، ولا يمكن الوصول إلى الحقيقة بجزم ويقين إذا انحصر القاضي في دائرة مغلقة من الأدلة التي يحددها القانون ".

[2]– **الحكماوي عبد الحكيم**، المرجع السابق، ص 158 – 159.

[3]– **محمد عمرتي**، حماية حقوق الإنسان في أوروبا: قراءة في مصادر ومضمون ميثاق الاتحاد الأوروبي للحقوق الأساسية، المجلة المغربية للاقتصاد والقانون، العدد السادس، 2002، ص31.

[4]– **هشام محمد فريد رستم**، أصول التحقيق الجنائي الفني، في **بحوث مؤتمر القانون والكمبيوتر والإنترنت**، المجلد الثاني، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2004 ، ص 429.

المطلب الثاني

حقيقة الدليل الرقمي

إن اقتران الحقيقة بالدليل يجعل هذا الأخير هو الأساس في التركيب المنطقي للأحداث والوقائع انطلاقا من مقدمات معلومة للوصول إلى واقع تترجمه وسائل الإثبات المعروضة في النزاع، ولذلك فإن مفهوم دليل الإثبات عند البعض هو: " وسيلة الوصول إلى معرفة حقيقة الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه "[1] غير أن الحقيقة المتحدث عنها في هذا السياق هي الحقيقة القضائية المتسمة بنوع من النسبية وليست الحقيقة الواقعية التي تجسد حقيقة الجريمة باعتبارها واقعة مادية مشهودة ومحسوسة، فالحقيقة المطلقة لا مجال للحديث عنها في ميدان الإثبات عموما والإثبات الجنائي على وجه الخصوص، نظرا لارتباط الحقيقة في الميدان الجنائي بالحكم القضائي المُعبر عنها، والذي يعتبر بدوره مجرد تعبير عما خلص إليه القاضي جراء ما وصل إليه اقتناعه الصميم، لأن أعظم ما يقع على عاتق القاضي هو تقدير أدلة الإثبات والاقتناع بها، وذلك حتى لا يدان بريء ولا يفلت مجرما، فالقاضي قبل أن يصدر حكمه يقوم بالبحث عن الحقيقة، وهو في سبيل ذلك يقوم بفحص الأدلة الجنائية ويطرحها في الجلسة ليتناولها الخصوم بالفحص سعيا للوصول إلى الحقيقة التي ترضي ضميره، وتكون اقتناعه الشخصي لتحقيق العدالة.[2]

لذلك فافتراض شرعية الدليل كأساس للوصول إلى الحقيقة قد يكون سببا معيقا لذلك الوصول، وهو الأمر الذي ذهب بالقضاء إلى البحث عن الحقيقة باعتبارها غاية المشرع من إقرار قواعد الإثبات، وأن الأدلة التي لا توصل إلى إقرار الحقيقة أدلة لا قيمة لها ولا تنسجم وإرادة المشرع، لذلك فإن تبني مبدأ علاقة الدليل بالحقيقة يعتبر مسلكا منتجا لتسيير الأدلة في الخصومة الجنائية ما دام أن الأطراف يبقى لهم الحق في مناقشة علنية وحضورية ليتم الحصول عليه من تلك الأدلة.[3]

ومما يزيد من أهمية هذا التوجه، هو أن الدليل المستخلص من الوسائل الالكترونية، قد يكون هدفا للمنازعة فلا يتم اعتماده إلا بالتأكد من صحته وفق ما يقتضيه القانون، كما أنه يجب التأكيد على أن ارتباط الدليل في الجريمة الالكترونية بوسائل تقنية يؤدي بالضرورة إلى الوقوف على حد من حدود ذلك الدليل وهو نسبة الفعل المرتكب إلى الأداة التي استعملت في ارتكابه، وليس إلى الشخص المالك لتلك الأداة، وهكذا ففي الفضاء الالكتروني يظهر أن إثبات نسبة الفعل الإجرامي إلى الشخص الطبيعي تبقى أمرا صعب المنال، وقد وقف القضاء على هذه الحقيقة من خلال مجموعة من قراراته، ومما يرتبط

---

[1] – **مأمون محمد سلامة**، الإجراءات الجنائية في التشريع الليبي، الجزء الثاني، منشورات المكتبة الوطنية، الطبعة الثانية، بنغازي، جمهورية ليبيا، 2000، ص 176.

[2] – **طاهري عبد المطلب**، الإثبات الجنائي بالأدلة الرقمية، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2015/2014، ص 58.

[3] – **الحكماوي عبد الحكيم**، المرجع السابق، ص 155– 156.

بهذا المعطى كون المنازعة في جمع وفحص عناوين البروتوكول (IP)[1] هل تعتبر مساس بالمعطيات الشخصية أم لا، لذلك فقد ذهب القضاء الفرنسي إلى القول بكون مجرد جمع تلك المعطيات لا يعتبر مساس بالخصوصية ولا بالمعطيات الشخصية، ولعل هذا التوجه الذي سار عليه القضاء الفرنسي يؤكد كون عناوين البروتوكول لا تثبت العلاقة المباشرة بين الجريمة المقترفة والشخص الطبيعي بقدر ما تثبت تلك العلاقة والآلة التي ارتكبت بها.[2]

وعلى كل ذلك يبقى أمر البحث عن دليل نسبة الجريمة إلى الشخص الطبيعي أمر خاضعا للقواعد العادية، بعد التأكد من كون الأداة التي توجد بحوزته هي الوسيلة الحقيقية التي استعملت في ارتكاب الجريمة، من أجل كل ذلك يبقى البحث والحديث عن شرعية الدليل ومدى قدرته على إثبات الحقيقة أساسا لاعتماده أو عدم اعتماده من طرف القاضي الجزائي خلال المحاكمة[3] والذي سيحتكم إلى المنطق والعقل في حكمه، لأنه ملزم بأن يتحرى المنطق الدقيق في تفكيره الذي قاده إلى اقتناعه، وبالتالي فإنه سيميل إلى اعتماد أدلة الإثبات التي يمكنه أن يقف على صحة مطابقتها مع العقل والمنطق واستنباطها استنباطا علميا بالحكمة والدقة والموضوعية[4]، لذا عندما يصل القاضي إلى اليقين[5] فإنه يصبح في هذه المرحلة مقتنعا بالحقيقة، لأن اليقين في الأصل هو وسيلة لاقتناع القاضي، أو بعبارة أخرى أن اقتناع القاضي بالحقيقة هو ثمرة اليقين وليس اليقين ذاته،لأنه مهما علت القيمة العلمية والفنية للدليل الجنائي الرقمي في الإثبات، إلا أنه يجب أن يتمتع القاضي بالسلطة التقديرية، لأن هذه الأخيرة تكون لازمة لكي تجعل من الحقيقة العلمية حقيقة قضائية.

خاتمة:

اقترنت تقنية استخدام المعلومات بظهور جرائم من نوع خاص تختلف عن الجرائم العادية أو الكلاسيكية، إذ قلبت العديد من المفاهيم القانونية السائدة سواء على مستوى القانون الموضوعي من حيث التجريم والعقاب بفعل ازدواجية طبيعتها بين جريمة معلوماتية محضة تستهدف الأنظمة والبيانات

---

[1]– يعمل عنوان**IP** بشكل متزامن مع بروتوكول أخر وهو بروتوكول التحكم بالنقل **TCP** والذي تكمن وظيفته في تقسيم المعلومات إلى حزم معلوماتية،ويقوم بروتوكول **IP** بعنونة كل حزمة مع إضافة معلومات أخرى إليها، ومنه فيتم استخدام عنوان **IP** من خلال البحث عن رقم الجهاز وتحديد موقعه الجغرافي، بالإضافة إلى إمكانية مراقبة المستخدم من طرف مزود خدمة الإنترنت وتقديم المعلومات التي تفيد في التحقيق، بناء على أن لكل جهاز حاسب آلي يتصل بالإنترنت عنوان IP خاص به (**ممدوح عبد الحميد عبد المطلب**، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006 ، ص 101.).

[2]– **الحكماوي عبد الحكيم**، المرجع السابق، ص 160–161.

[3]– المرجع نفسه، ص 161.

[4]– **قراوي كلثوم**، مشروعية الدليل الالكتروني في الإثبات الجنائي، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 05، العدد 01، 2022، ص 991.

[5]– **اليقين** بصفة عامة هو عبارة عن" حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التوكيد " (**مروك نصر الدين**، المرجع السابق، ص491).

المعلوماتية في حد ذاتها أو كجريمة عادية مرتكبة بواسطة تقنية معلوماتية كآلية من أجل التواصل والتخطيط لتنفيذ مشاريع إجرامية، أو على مستوى القانون الإجرائي بفعل تغلبها على القواعد الإجرائية المقررة كأصل عام للبحث والتحري وجمع الاستدلالات وملاحقة مرتكبي الجرائم العادية ومحاكمتهم.

لذلك حاولنا من خلال هذه المداخلة أن نبرز مدى شرعية الدليل الجنائي الالكتروني وما يكتنفه من صعوبات سواء من حيث طرق الحصول عليه أو من حيث طبيعته، فالحصول عليه قد يحتاج إلى القيام بعمليات فنية وعلمية معقدة، كما أن طبيعته غير المادية تسهل لمرتكبي الجريمة المعلوماتية بإخفائه وإتلافه أو حتى تشفيره لحيلولة دون الوصول إليه، يصب مباشرة في خانة الحديث عن الدليل الالكتروني عند البحث عن الجريمة الالكترونية، ذلك أن الإشكالات التي تعترض إيجاد هذا الدليل تجسد عمق النقاش الذي طرحناه سابقا على اعتبار أن امتلاك الأفراد للسيطرة على أدواتهم الالكترونية قد يشكل عائقا حقيقيا أمام البحث والتحري عن الجرائم، إذ أن وجود قيود متعددة ذات طبيعة أخلاقية أو قانونية قد يجعل من العسير على جهاز العدالة أن تتوصل إلى الدليل سواء في الوقت الطبيعي أو وفق ما يقتضيه أمر الكشف عن الحقيقة، وما يؤكد هذا هو وقوف فكرة الخصوصية وضرورة التقيد بالقواعد القانونية الحامية لها حجرة عثرة أمام الوصول إلى الحقيقة، ويدخل في هذا السياق ما قد تعترضه الضبطية القضائية المكلفة بالبحث والتحري وجمع الاستدلالات من عقبات قد تنتج عن معارضة الجاني المفترض لتمكين تلك الأجهزة من أجل فتح البريد الالكتروني مثلاً للحصول على الدليل أو مدى قدرة تلك الأجهزة في اعتراض تلك الرسائل من غير أذن مالكها أو حتى الاطلاع على بياناته الشخصية الممسوكة من طرف مزودي الخدمات، وما إذا كان ذلك مخالفا للقانون أم لا.

ونظرا لأن إجرام الذكاء والتقنية لا يكشفه ولا يحد منه إلا ذكاء وتقنية مماثلان له، بات من الضروري مواكبة المشرع الجزائري لهذا النوع من الجرائم، وذلك عبر وضع آليات قانونية ومؤسساتية كفيلة بمكافحتها لاسيما على مستوى القانون الإجرائي بعدما بادر إلى مراجعة أحكام:

1- قانون العقوبات بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 تم بموجب هذا القانون إحداث قسم جديد في قانون العقوبات تحت عنوان: " المساس بأنظمة المعالجة الآلية للمعطيات " احتوى أهم الجرائم التي تستهدف الأنظمة المعلوماتية.

2- قانون الإجراءات الجزائية المعدل بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 الذي تناول موضوع الجرائم الافتراضية.

3- القانون 05/03 المؤرخ في 19 يوليو 2003 المتعلق بحقوق المؤلف والحقوق المجاورة الذي نص على تجريم انتهاك حقوق المؤلف والحقوق المجاورة عن طريق التقليد بأي وسيلة كانت بما فيها منظومة معالجة معلوماتية.

4- القانون رقم 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتهما، والذي نص أيضا على إجراء المراقبة الإلكترونية وكذلك تفتيش أنظمة الحاسب الآلي وضبط الأدلة الناتجة عنها.

5- القانون 03/2000 المؤرخ في 05 أوت 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

وبناء على ما تم تفصيله نوصي ب:

1- العمل على تحيين القواعد القانونية الإجرائية لكي تتماشى مع خاصية تطور الجريمة المعلوماتية ووسائل إثباتها، والاعتماد عليها حتى في إثبات الجريمة التقليدية.

2- سرعة التحفظ على بيانات الحاسب الآلي المخزنة، واتخاذ ما يلزم من تدابير لطلب التحفظ الاستعجالي على هذه البيانات، وإلزام الشخص الموجودة بحوزته على حفظها وسلامتها والمحافظة على سريتها مع الكشف الجزئي لها.

3- وضع قواعد خاصة بتفتيش وحجز بيانات الحاسب الآلي المخزنة، من خلال تأمين عملية المعاينة أو التفتيش داخل أنظمة الحاسب الآلي أو أي جزء منه من طرف الخبراء الفنيين والمتخصصين، وتعطيل كافة الاتصالات الموصولة بجهاز الحاسب الآلي لمنع تخريب الأدلة الموجودة أو محوها.

4- منح السلطات المختصة صلاحية إصدار الأوامر إلى الأشخاص لتقديم البيانات الموجودة في الحاسب الآلي التي بحوزتهم أو تحت سيطرتهم، وكذلك لكل مقدم خدمة من أجل تقديم ما يتعلق بالخدمات الموجودة بحوزته أو تحت سيطرته التي تفيد في التحقيق.

5- الاهتمام بالخبرة العلمية لما لها من دور فعال في مجال الإثبات الجنائي، وذلك من خلال الاعتراف بقيمتها في الإثبات دون إخراجها من دائرة السلطة التقديرية للقاضي.

الاسم واللقب: ســـــمـيـــــــــرة عـــــابـــــد
أستاذة محاضرة "أ" بكلية الحقوق جامعة باجي مختار عنابة
التخصص : القانون الجنائي و العلوم الجنائية
تاريخ ومكان الميلاد: 17-10-1975 بعنابة
البريد الالكتروني: samira.abed.23000@ gmail.com
الهاتف: 38 91 58 73 7 213+
العنوان المهني : القطب الجامعي – أحمد البوني – عنابة.

المداخلة متعلقة بالمحور الخامس : تأثير الوسائل العلمية الحديثة على الإثبات الجنائي

مداخلة بعنوان :

حجية الدليل الالكتروني في الإثبات الجنائي

ملخص

إن التقدم العلمي و تطور الأنظمة المعلوماتية في مختلف مجالات الحياة أدى إلى ظهور أنواع جديدة من الجرائم تستغل هذا التطور المعلوماتي تعرف بما يسمى بالجرائم المعلوماتية، والتي تعد ذات طابع عابر للحدود يصعب تتبعها و الكشف عنها باستعمال أساليب التحري و التحقيق التقليدية، لذلك فقد بات من الضروري، تكييف المنظومة التشريعية بغرض استحداث طرق جديدة لمكافحة و إقامة الدليل الشرعي ضد مرتكبي هذا النوع من الجرائم، وهو ما عرفه المشرع الجزائري بموجب القانون رقم 06-22 الصادر في 20 ديسمبر 2006 المتضمن تعديل قانون الإجراءات الجزائية من خلال استحداث فصل خاص باعتراض المراسلات وتسجيل الأصوات، و كذا بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الصادر في 05 أوت 2009، واستحداث قطب متخصص في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال لكامل الإقليم الوطني بموجب التعديل الوارد أيضا على قانون الإجراءات الجزائية بموجب الأمر رقم 21-11المؤرخ في 25أوت2021.

و أن هذه الإجراءات المستحدثة أدت إلى ظهور أدلة علمية تعتمد على التقنيات الحديثة، ومن بين هذه الأدلة، الدليل الالكتروني، فنظرا لطبيعته الخاصة، فإن هذا الأخير يشير إشكالية مدى حجيته ومشروعيته في الإثبات الجنائي و مدى الأخذ به من قبل رجال القضاء.

للإجابة على هذه الإشكالية، ارتئينا تقسيم هذا البحث إلى مبحثين، المبحث الأول يتعلق بتعريف الدليل الالكتروني و شروطه، و المبحث الثاني حجية الدليل الالكتروني في لإثبات الجنائي.

الكلمات المفتاحية :حجّية - دليل - إثبات - الدليل الإلكتروني - الإثبات الجنائي

Summary

Scientificprogress and the development of information systems in various areas of life have led to the emergence of new types of crimes thattakeadvantage of this information developmentknown as the so-called information crimes, which are of a cross-border nature thatisdifficult to track and detectusingtraditionalmethods of investigation and investigation. It isnecessary to adapt the legislative system in order to develop new ways to combat and establishforensicevidenceagainst the perpetrators of this type of crime, whichiswhat the Algerian legislatordefinedunder Law No. The votes, as well as in accordance with Law N° 09-04 containing the specialrules for the prevention and control of crimes related to information and communication technologies issued on August 05, 2009, and the creation of a pole specialized in crimes related to information and communication technologies for the entire national territoryaccording to the amendmentalsocontained in the Code of CriminalProcedurepursuant to the Ordinance N° 11-21 of August 25, 2021.

And thatthese new proceduresled to the emergence of scientificevidencebased on modern technologies, and amongtheseevidence, the electronicevidence, givenitsspecial nature, the latter indicates the problematicextent of itsauthority and legitimacy in criminal proof and the extent of its adoption by the judiciary.

Keywords : Authority - evidence- proof - electronicevidence - criminal proof

مقدمة :

إن إثبات الجرائم المعلوماتية أو المرتكبة بالوسائل الالكترونية ستتأثر بطبيعة هذه الجرائم بالوسائل التقنية التي قد ترتكب بها، مما يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن ارتكابها أو عدم الوصول إلى مقترفي هذه الجرائم أو تعذر إقامة الدليل اللازم لإثباتها، مما يترتب عليه إلحاق الضرر بالأفراد و المجتمع، لذلك فقد بات من الضروري، تكييف المنظومة التشريعية بغرض استحداث طرق جديدة لمكافحة و إقامة الدليل الشرعي ضد مرتكبي هذا النوع من الجرائم، وهو ما عرفه المشرع الجزائري بموجب القانون رقم 06-22 الصادر في 20 ديسمبر 2006 المتضمن تعديل قانون الإجراءات الجزائية من خلال استحداث فصل خاص باعتراض المراسلات وتسجيل الأصوات، و كذا بموجب القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الصادر في 05 أوت 2009، واستحداث قطب متخصص في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال لكامل الإقليم الوطني بموجب التعديل الوارد أيضا على قانون الإجراءات الجزائية بموجب الأمر رقم 21-11المؤرخ في 25أوت2021.

و أن هذه الإجراءات المستحدثة أدت إلى ظهور أدلة علمية تعتمد على التقنيات الحديثة، ومن بين هذه الأدلة، الدليل الالكتروني، فنظرا لطبيعته الخاصة، فإن هذا الأخير يثير إشكالية مدى حجيته ومشروعيته في الإثبات الجنائي و مدى الأخذ به من قبل رجال القضاء.

للإجابة على هذه الإشكالية، ارتئينا تقسيم هذا البحث إلى مبحثين، المبحث الأول يتعلق بتعريف الدليل الالكتروني و شروطه، و المبحث الثاني حجية الدليل الالكتروني في لإثبات الجنائي.

المبحث الأول : ماهية الدليل الالكتروني و خصائصه في الإثبات الجنائي :

يعد الدليل الالكتروني من أهم تطورات العصر الحديث لأهميته في الإثبات الجنائي الالكتروني و الذي يتطلب التعامل معه فئات ذات كفاءات، و بالرغم من هذا، فيجد هؤلاء صعوبات في إثبات تلك الجرائم المعلوماتية.

و للدليل الالكتروني عدة تعريفات و خصائص، لذلك سنتناول في هذا المبحث ماهية الدليل الالكتروني كمطلب أول و خصائصه كمطلب ثان.

المطلب الأول : ماهية الدليل الالكتروني :

سنتناول في هذا المطلب تعريف الدليل الالكتروني في فرع أول، ثم طبيعة الدليل الالكتروني في مطلب ثاني

الفرع الأول : تعريف الدليل الالكتروني :

تعد أدلة الإثبات الجنائي محور الجريمة و روحها، لهذا سوف نتطرق إلى تعريف الدليل الالكتروني لغة ثم اصطلاحا لنأتي في الأخير إلى تعريف الدليل الالكتروني بصفة عامة.

أولا : الدليل لغة :

الدليل لغة مأخوذ من الدال و جمعها أدلة و دلائل، و الدليل لغة :المرشـــد و ما يتم الإرشاد به. [1]و الدليل أيضا هو : الإرشاد عن شيء ما، بمعنى دله عن الطريق : أي أرشده، و يدله بالضم، ودلالة بفتح الدال و كسرها، و دلولة بالضم و الفتح، و يقال أدل و الإسم الدال هو بتشديد اللام، فلان يدل فلانا أي يثق به، و قال أبو عبيدة الدال قريب المعنى من الهدى ومفهومها السكينة و الوقار. [2]

ثانيا: الدليل اصطلاحا :

الدليل اصطلاحا هو الذي يلزم من العلم به بشيء آخر غايته أن يتوصل العقل إلى التصديق القانوني اليقين بما كان يشك في صحته أي التوصل إلى معرفة الحقيقة، وأيضا يقصد بالدليل ما يمكن التوصل به إلى معرفه الحقيقة.

---

1)د. جميل صليبا، المعجم الفلسفي، الجزء الاول – دار الكتاب العالمي – الرياض سنة 1994 صفحة 564

2) محمد بن ابي بكر الرازي مختار الصحاح المطبعة الاميرية القاهرة طبعة 2016–صفحة 209.

أما الدليل في الاصطلاح القانوني : فيقصد به الوسيلة التي يستعين بها القاضي للوصول الى الحقيقة التي ينشدها ويقصد بالحقيقة في هذا السياق بانها كل ما يتعلق بالإجراءات والوقائع المعروضة على القاضي لإعمال حكم القانوني عليها ويقصد بالدليل ايضا الوسيلة الإثباتية المشروعة التي تساعد في تحقيق بطريقه سائغه،[3]كما يشار الى الدليل بانه كل اظهار لنشاط عام او خاص داخل الخصومة او من اجلها يؤدي مباشره الى التأثير في تطور رابطه الخصومة او بمعنى اخر هو كل عمل يجري في الخصومة او يهدف الى اعدادها او له قيمه في الخصومة أيا كانت طبيعته او معناه نظمه القانون بقصد الوصول الى تطبيق القانون الموضوع فيها.

وعليها يمكن القول من ذلك بان الدليل الجنائي بشكل عام هو الوسيلة التي تؤدي بالقاضي الى الحقيقة التي يطلبها عن طريق اجراءات قانونيه لإثبات واقعه معينه وعليها فالدليل يعد روح الجريمة وجسمها ولا يمكن للقاضي إدانة المتهم الا بالتوافر الأدلة المشروعة والمتصلة بالقناعة الوجدانية له وذات الصلة بوقائع الدعوى.

لذلك فان الدليل هو عبارة عن مجموعة من الوسائل المشروعة والمقدمة للقاضي بوقائع الدعوى المنظورة أمام المحكمة وللأخيرة السلطة التقديرية في وزن هذه الأدلة حيث تأخذ منها ما يؤثر في مسار الدعوى وتطرح منها ما ليس في تقديمه تأثير في الدعوى وغير منتج فيه.[4]

ثالثا : تعريف الدليل الالكتروني :

يرى بعض من الفقهاء أن الدليل الالكتروني هو عبارة عن مجموعة المجالات أو النبضات المغناطيسية او الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصه لتظهر في شكل صور او تسجيلات صوتية.

وهناك جانب آخر من الفقهاء يعرف الدليل الالكتروني على انه مجموعه من المعلومات تنسجم مع الفعل والمنطقة ويأخذ بها العلم ويتم الاستعانة بالدليل الالكتروني بواسطه اجراءات قانونية وعلمية من خلال ترجمه البيانات المخزنة في اجهزه الحاسوب وملحقاته وشبكات الاتصال ويمكن الاستناد اليها في اي مرحله من مراحل التحقيق او المحاكمة عند وقوع اي جريمة من الجرائم الإلكترونية.

---

3) الدكتور عبد الرزاق السنهوري، الوسيط في شرح القانون المدني – الجزء الثاني – دار النهضة العربية القاهرة– 1968 – صفحة 13

4) لورانس سعيد الحوامدة، حجية الأدلة الرقمية في الاثبات الجنائي دراسة تحليلية مقارنة – مجلة البحوث الفقهية والقانونية العدد 36 اكتوبر 2021 – صفحة 595

ويرى بعض من الفقهاء على ان الدليل الالكتروني هو عباره عن بيانات رقميه يمكن استخدامها عند وقوع الجريمة في العالم الافتراضي بحيث تربط بين الجاني والجري الإلكترونية عباره عن مجموعه من الارقام والنصوص المكتوبة او رسومات او الخرائط او الصور التي يمكن ان تكون ادله لأي جريمة افتراضيه.[5]

وهناك فريق اخر يرى بان الدليل الالكتروني هو عباره عن بيانات يمكن اعدادها وتراسلها وتخزينها رقميا بحيث تمكن الجهاز الحاسوب من تأدية مهمه ما وقد اخذ بهذا التعريف التقرير الامريكي المقدم في ندوه الانتربول العلمية حول الدليل الرقمي عام 2001.[6]

الفرع الثاني :الطبيعة القانونية للدليل الالكتروني :

لقد اختلف الفقهاء حول الطبيعة القانونية للدليل الالكتروني فجانب من الفقه اعتبره دليل ماديا واخر يرى بانه دليلا معنويا ليأتي فريقا اخر من الفقهاء يرى بان الدليل الالكتروني هو مزيج بين دليل ماديا ودليلا معنويا وعليه سوف نتطرق لهذه الآراء او الاتجاهات كالاتي :

الاتجاه الاول :يرى انصار هذا الاتجاه ان الدليل الالكتروني يعد من الأدلة المادية التي يمكن ادراك ان مخرجات الأدلة الإلكترونية هي ورقيه ماديه اما الأدلة الغير ماديه فيمكن استخراجها في شكل دعامات كالأشرطة الممغنطة او الاقراص المغناطيسية وبالتالي تصبح ادله ذات الطبيعة ماديه وليست معنويه اما اذا تم ضبط قرص ممغنط وفي داخله ارقام سريه لبطاقات ائتمان او بريد الكتروني فأما هذه الأدلة الكترونيه معنويه وليست ماديه لكون البيئة التي وجد بها الدليل الالكتروني الافتراضية

الاتجاه الثاني : يرى جانب من الفقه ان الدليل الالكتروني يعد دليلا معنويا وليس ماديا حيث ان الأدلة الإلكترونية هي عباره عن ادله كهربائية او مغناطيسيه وهي معنويه بطبيعتها حتى ولو تم استخراجها بصوره ماديه ملموسه وهذا لا يعني ان هذه المخرجات في الدليل انما تعني هي عمليه نقل لتلك الأدلة من طبيعتها التقنية والإلكترونية بصوره فنيه يمكن الاستدلال بها على معلومة ثمينة فقد نستفيد منها جهات التحقيق كما ان تحليل الدليل الالكتروني يتطلب بحكمه طبيعته اجهزه تقنيه خاصه لتحليله محتوى

---

5) لورانس سعيد الحوامدة، المرجع نفسه – الصفحة 196

6) دكتور مسعود بن حميد المعمري لإثباتالجريمةالإلكترونية، كلية القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي الخامس 2018 – صفحة 941

الدليل الالكتروني وبغير ذلك لا يعد للدليل الالكتروني اي قيمه في الاثبات الجنائي لعدم استطاعة جهات التحقيق معرفه الجاني في الجريمة الإلكترونية

الاتجاه الثالث : يرى انصار هذا الاتجاه ان الدليل الالكتروني يتميز بصفه وخصائص كوسيله من وسائل اثبات الجنائي يميزه عن بقيه الأدلة الجنائية التقليدية الاخرى وهو بمثابه اضافه نوعيه للأدلة الجنائية بصفه عامه سواء كانت ماديه او نوعيه او مادي او فنيه وبالتالي تعد هذه الأدلة من الأدلة التي تنطوي تحت طاولة طائلة الأدلة الجنائية التقليدية.

وعليه نستنتج من خلال الاتجاهات الثلاث ان الطبيعة القانونية للدليل الالكتروني ذو طبيعة خاصه كونه مستحدث وناتجا من جرائم معلوماتية افتراضيه وبالتالي فان مستخرجات هذا النوع من الأدلة تختلف حسب نوع الدليل التقني فبعض هذه المخرجات قد تكون ملموسه خاصه اذا كانت ورقيه اي طبعت على ورقه وقد تكون ادله تقنية معنوية كالأدلة الموجودة في البريد الالكتروني وعليه فالدليل الالكتروني يكون من هذا المنطلق ذو طبيعة مزدوجة نظرنا للتنوع مستخرجاته من الوسط التقني.[7]

المطلب الثاني : أنواع وخصائص الدليل الالكتروني :

باستقراء التعريفات التي تم اتطرق اليها سابقا نستنتج ان الدليل الالكتروني يمتاز بجمله من الخصائص وله عده تقسيمات فلهذا سوف نتطرق الى هذه الجزئية كالاتي خصائص الدليل الالكتروني كفرع أول وتقسيماته كفرع ثاني :

الفرع الاول : خصائص الدليل الالكتروني :

يمتاز الدليل الالكتروني عن بقيه الأدلة الاخرى بمجموعه من الخصائص التي تميزه عن غيره من الأدلة الاخرى لكون لكونه يعيش في بيئة رقميه جد متطورة فلهذا يمتاز الدليل الالكتروني بمجموعه من الخصائص والتي سوف نعرضها كالاتي :

أولا : الدليل الالكتروني دليل علمي :ان الطبيعة الخاصة للدليل الالكتروني والبيئة التي يعيش فيها بيئة افتراضيه غير ملموسه تجعل من الدليل الالكتروني دليلا غير مادي كذلك فهو دليل غير ملموسه يتكون من بيانات ومعلومات على هيئه الكترونيه حيث ان العالم الافتراضي التقني هو عالم اعده متخصصون في التقنية وبالتالي لا يمكن الحصول على البيانات والمعلومات في ذلك العالم التقني الا بأساليب علميه

---

7) د. مسعود بن حميد المعمري – مرجع سابق الصفحة 752

وتقنيه وهو ما يميز الدليل الالكتروني في هذه الخاصية بانه دليل فاستخراج دليل الالكتروني يحتاج الى بيئة متشابهة للبيئة التي نتج عنها بداية طلب الاستعانة بأجهزة وادوات التقنية ملائمه لاستخراج للاطلاع عليه للاطلاع واستخراجه في هيئة ملموسة ومادية وهي أحد أساليب علمية.[8]

ثانيا : الدليل الالكتروني دليل تقني : فهو دليل غير ملموس لأنه يتمثل في بيانات غير مرئيه وهذا ما يحدث بصفه خاصة في جرائم الانترنت مثل الجرائم التي ترتكب على البريد الالكتروني سيكون من الصعب على الجهات المختصة في التحقيق تحديد مصدر المرسل والطبيعة التقنية للدليل الالكتروني تقتضي أن يكون هناك توافق بن الدليل الذي تم ضبطه وبين البيئة المستمدة منها الدليل، سواء كانت هذه الجريمة موجهه للبنوك أو مؤسسة ماليةأو كانت قذفاأو سبا أو تشهيرا، و بناء على ذلك فلا يتصور بأنه يوجد دليل الكتروني خارج بيئته التقنية و إنما يحب أن يكون هناك دليل الكتروني مستمد من البيئة التي يعيش فيها وهي البيئة الرقمية والتي هي في الاساس ذو طابع تقني.[9]

ثالثا : الدليل الالكتروني دليل متطور: يختص الدليل الالكتروني بتنوعه فهو لا يوجد في صورة واحدة بل يوجد له العديد من الصور والأشكال بالتطور التقني فهو قد يكون على شكل بيانات أو صور أو ارقام أو أصوات لأن البيئة الرقمية بيئة تقنية متجددة باستمرار، فخاصيةأنه متطور، فهي تفيد أنها تستخدم في جرائم مستحدثه فجريمة النصب مثلا يمكن ارتكابها بالطرق التقليدية التي تتيح أدله مادية وكذلك أصبح أمام التقدم التكنولوجي من الممكن ارتكابها باستخدام التقنية سواء كانت باستخدام جهاز حاسب آلي أم أن يكون الحاسب الآلي محلا للجريمة أي جريمة النصب.[10]

وعليه فنلاحظ ان الدليل الرقمي متنوع تبعا للمصدر الذي نشا منه فهو يشمل كافة أنواع البيانات الرقمية التي يمكن استخراجها رقميا بحيث يكون بينها وبين الجريمة رابطه من نوع ما فالمصدر الرقمي يحتوي في داخله على مجموعه البيانات الرقمية المتنوعة قد تكون سمعيات او مرئيات او صورا.[11]

رابعا : الدليل الالكتروني الدليل الالكتروني قابل للنسخة : يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقه للأصل ولها نفس القيمة العلمية وهذه الخاصية لك وتتوافر في انواع الأدلة الاخرى مما

---

8) د. مسعود بن حميد المعمري – مرجع سابق الصفحة 198 و 199

9) د. زياد بن محمد عادي العتيبي، دراسة استطلاعيه حول حجيةالأدلةالرقمية في اثبات الجرائم المعلوماتية– المجلةالإلكترونيةالشاملةمتعددة التخصصات العدد 29 اكتوبر 2020 – صفحه 17

10) د. مسعود بن حميد المعمري – مرجع سابق– صفحة 199

11) د. زياد بن محمد عادي العتيبي، مرجع سابق – صفحة 19

يشكل حمايه شديده الفاعلية للحفاظ على الدليل ضد التلف والتغيير عن طريق نسخ طبق الاصل من الدليل ومثل هذا الامر لاحظه المشرع الامريكي فقام بتعديل قانون التحقيق الجنائي بمقتضى القانون المؤرخ في 28 نوفمبر حيث تم اضافه المادة 39 التي سمحت بضبط الأدلة الرقمية مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية.[12]

خامسا : الدليل الالكتروني يصعب التخلص منه : يمكن التخلص من الأدلة التقليدية بسهوله البصمات والادوات المستعملة في الجرائم كالأسلحة وغيرها لكن الدليل الالكتروني بشكل خاص وكل ما يتعلق بالتكنولوجيا المعلومات بشكل عام وانه كلما حدث ارتباط او اتصال مع شبكه الاتصال وسيله تقنيه المعلومات وبمعنى ادخال البيانات معينه فانه يصبح من الصعب يتخلص من ذلك ولو استخدمت ادوات الحذف والالغاء وكما ان التخلص من الدليل الالكتروني باستخدام الادوات المتوفرة في وسيله في وسيله تقنيه مثل خيارات الحذف او الالغاء لا تغير لا تعتبر من العوائق التي تمتنع من استرجاع الدليل فهناك برامج متخصصه من ذات طبيعة الدليل التقني يمكن لجهات القضائية المتخصصة من الحصول على الدليل المحذوف واسترجاع البيانات الملغات من الجهاز محل ارتكاب الجريمة يصعب التخلص منه مساء القانونية مهمه ومنها مساله التخلص من الدليل المحلات التي تعتبر جريمة مستقلة كذلك فاذا أراد استخدام برامج من قبل مرتكبي الجريمة الإلكترونية تكون مهمتها حذف البيانات وازالتها من الجهاز تشكل بذاتها جريمة وبالتالي فانه يمكن ازاله الجنات على ذلك حسب التجريم القوانين والجزاء لها.[13]

الفرع الثاني :تقسيمات الدليل الالكتروني

من أبرز خصائص الدليل الالكتروني أنه دليل متنوع تبعا للتطور الالكتروني لذلك لا يظهر في صورة واحدة بل له العديد من الأشكال، لهذا قسم الفقهاء الأدلة الالكتروني إلى أربعةأنواع على النحو الاتي :

أولا :الأدلة الرقمية الخاصة بأجهزة الكمبيوتر وشبكاتها :

وهذا النوع من الأدلة الإلكترونية تكون ناتجه من الجرائم التي تقع على اجهزه الكمبيوتر وشبكات المتصلة بها ويقصد بها كل سلوك انسان يشكل فعلا غير قانوني ويقع على اجهزه الحاسب الالي سواء

---

12) د. بهلدي محمد، حجية الدليل الرقمي في الاثبات الجنائي – مجلة البحوث والدراسات القانونيةوالسياسية– المجلد التاسع– العدد الاول – صفحة 20

13) د. مسعود بن حميد، مرجع سابق صفحه 200

كان هذا السلوك وقع على المكونات المادية او مكونات المعنوية او على قواعد البيانات الداخلية ومثالها تخريب مكونات الكمبيوتر المادية او وسائط التخزين المرئية والصلبة.[14]

ثانيا : الأدلة الرقمية الخاصة بالأنترنت

وهذا النوع من الأدلة يكون ناتج من جرائم الشبكة العالمية ويقصد به كل سلوك انسان يشكل فعلا غير قانوني ويقع على نص او مسند موجود بشبكه الإلكترونية كجريمه الاعتداء على بطاقات الائتمان والاعتداء على حقوق الملكية الفكرية وجرائم الاختراق الإلكترونية على مكونات الحاسب الآلي.[15]

ثالثا : الأدلة الرقمية الخاصة ببروتوكولات تبادل المعلومات بين اجهزه الشبكة العالمية للمعلومات

وهي الأدلة الناتجة من جرائم الانترنت ويقصد بها كل سلوك انسان غير مشروعه تقع على اليه نقل المعلومات الرقمية بين مستخدم الشبكة الرقمية للمعلومات كجرائم استخدام عنوان البروتوكول الانترنت غير حقيقيه والدخول غير مشروع لمواقف غير مصرح بها للدخول.[16]

رابعا : الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات

وهي التي يستخدم فيها الانسان الكمبيوتر كوسيله للفعل الغير مشروع كمساعده لارتكاب الجرائم وذلك مثل جرائم غسل الاموال وجرائم التهريب المخدرات.

كما أن هناك فريق آخر من الفقهاء يرى أن الأدلة الإلكترونية تنقسم إلى تقسيم آخر وهذا حسب إعدادها لتكون أداة للأثبات وهو التقسيم الذي نراه مناسبا لهذا البحث فتنقسم الأدلة الإلكترونية إلى قسمين رئيسيين :

1 – أدلة أعدت لتكون وسيلة إثبات : و تشمل السجلات التي يتم انشاؤها تلقائيا بواسطة الأجهزة الإلكترونية ومنها سجلات الهاتف وفواتير أجهزة الحاسب الآلي بالإضافة إلى تلك السجلات التي تحتوي على بيانات تم ادخالها إلى الجهاز وتم إجراء المعالجة عليها من خلال برنامج ما.

---

14) عائشة بن قارة مصطفى،حجية الدليل الالكتروني في مجال الاثبات الجنائي – دراسة مقارنة سنة 2009 جامعةالإسكندرية كلية الحقوق – صفحة 72

15) د. زياد بن محمد عادي العتيبي، مرجع سابق – ص 19

16) د. مسعود بن حميد، مرجع سابق صفحة 202

2 – أدلة لم تعد لتكون وسيله إثبات : وهذا النوع من الأدلة الإلكترونية ينشا دون إرادة الشخص فهو يعد أثرا تركه الشخص دون أن يكون قاصدا بوجوده ويسمى هذا النوع من الأدلة بالبصمة الإلكترونية أو الآثار المعلوماتية الإلكترونية وتتمثل هذه الآثار فيما يتركه الشخص عند استخدام الجهاز أو الشبكة المعلوماتية من سجلات او بيانات يتم تسجيلها عند إرسال او استقبال الرسائل والمكالمات سواء من خلال جهاز أو شبكة المعلومات العالمية، والأصل أن هذا النوع من الأدلة لم يعد أساسا للحفظ من قبل الشخص المستخدم للجهاز أو الشبكة إلا أن هذه الأجهزة والرسائل التقنية تقوم بحفظها حتى ولو بعد فترة زمنية من حدوثها، فكافة العمليات التي تم إجرائها من قبل مستخدم على الجهاز أو الشبكة والمراسلات والاتصالات التي تتم يمكن ضبطها كأداة من قبل المختصين أو بواسطة تقنيات أو برامج الخاصة بذلك.[17]كما يقسم الدليل الرقميعادة إلى ثلاث مجموعات على النحو التالي :

السجلات: وهذا النوع من الأدلة يمكن إجمالها في ما يلي :

1– **السجلات التي تم انشاؤها بواسطه الجهاز الالكتروني تلقائيا:** وتعتبر هذه السجلات من مخرجات الجهاز التي لم يسهم الانسان في انشائها مثل سجلات جهاز الهاتف النقال والسجدات البطاقةالبنكية حيث يحفظ الهاتف النقال سجل المكالمات دون الحاجه لتدخل الشخص لحفظها يدويا وكذلك بالنسبة لجهاز السحب الآلي للبنك.

2 – السجلات التي تم حفظ جزء منها بالإدخال وجزء تم انشائها بواسطه جهاز الكمبيوتر : مثل رسائل البريد الالكتروني حيث يقوم الشخص بكتابه الرسالة ويقوم الجهاز بإكمال بيانات مثل توقيت الارسال والاستلام وحفظها في البريد المرسل اليه.

المبحث الثاني : حجية الدليل الالكتروني

سوف نعالج في هذا المبحث شروط الدليل الالكتروني كمطلب أول و حجية الدليل الالكتروني كمطلب ثان.

المطلب الأول : شروط الدليل الالكتروني

لما كان من الثابت أن عبئ الإثبات في المادة الجزائية لا يقع على عاتق المتهم من منطلق أنه محمي بقرينة البراءة فانه كان لزاما أن يخضع المشرع الجزائري كغيره من التشريعات المقارنة موضوع إثبات الفعل المجرم إلى إجراءات و قيود تعتبر من النظام العام و منها الدليل الالكتروني الذي يعتبر من

---

17) د. مسعود بن حميد، مرجع سابق صفحة 203

الآليات المستحدثة لاقترانه بالجرائم التكنولوجي و المعلوماتية التي جاءت كنتيجة للتطور التكنولوجي الذي عرفه العالم و بذلك أخضع الدليل الالكتروني كغيره من الأدلة التي تبنى عليها قناعة و عقيدة القاضي الفاصل في الدعوى إلى مجموعة من الشروط التي يستوجب توفرها فيه لكي يكون مقبولا عنوانا للأخذ به من طرف القضاء و التي توجزها كمايلي :

الفرع الأول : مشروعية الدليل الالكتروني:

لقد استقر القضاء و الفقه و العمل القضائي على المبدأ الذي ينص على كل ما يني على باطل يعد باطلا و منها الأعمال الإجرائية التي اعتبرها المشرع من النظام العام و من هذا الأساس فان مشروعية الدليل الالكتروني يقصد بها تحصيله بطريقة مشروعة و ذلك بمراعاة الإجراءات و القواعد القانونية التي نص عنها المشرع و هذا من خلال احترام جميع الإجراءات لتحصيله و تقديمه للقضاء بطريقة صحيحة و سليمة تضمن مبدأ التوافق بين الحقوق حقوق المتهم و حق المجتمع الذي تمثله النيابة العامة و بذلك فمشروعية الدليل الالكتروني تعني بمفهوم القانون توافق الإجراءات التي تم تحصيل الدليل بموجبها مع القواعد القانونية و الإجرائية التي نصت عليه و اقرها المشرع لأنه وفقا لذلك فان القضاة لا يمكنهم إطلاقا أن يبنوا قناعتهم و قضائهم على الدليل الالكتروني الذي يخالف النظام العام و الآداب العامة و ذلك لكونه دليلا مشوب بعيب مخالفة القانون و مخالفة مبدأ المشروعية و من هذا الباب فان الدليل الالكتروني و على الرغم من كونه متشعب و متعدد و متنوع الأنماط ويتميز بخصائص عن باقي الأدلة الأخرى منها الدقة و الوضوح فانه لا يمكن اعتماده و الاستناد إليه إلا إذا كان مقبولا إجرائيا وغير مخالف للنظام العام ولمبدأ المشروعية باعتبارها شرطا أساسيا لصحته و حجيته.

الفرع الثاني : وجوب مناقشة الدليل الالكتروني:

بمعنى أن القاضي الفاصل في الملف المحال إليه للمحاكمة لا يمكنه أن يؤسس قناعته إلا على عناصر الإثبات التي طرحت في جلسة المحاكمة و تمت مناقشتها من أطراف الأطراف تأسيسا على مبدأ الوجاهية و الشفوية و العلانية و منه فان المقصود بوجوب مناقشة الدليل الالكتروني هو طرحه في جلسة المحاكمة لإخضاعه لرقابة المحكمة و مناقشته و التعقيب عليه من طرف أطراف الدعوى بما فيها الدفاع و مواجهة المتهم بالدليل الالكتروني مهما كان نوعه و طبيعته و نمطه و خصائصه و دقته لأن ذلك ينطوي تحت مبدأ المحاكمة العادلة التي تقتضي بالضرورة طرح كل دليل الكتروني للمناقشة و التعقيب عليه أثناء جلسة المحاكمة باعتباره من الحقوق التي ضمنها المشرع لتحقيق العدالة و منه يمكن للقاضي حينها أن يقرر و يحكم بما ترسخت لديه القناعة من مجمل ما دار بالجلسة و تمت مناقشته من أدلة.

الفرع الثالث : وجوب أن يكون الدليل الالكتروني غير قابل للشك أي يقيني :

يشترط في الأدلةالمستخرجة من الحاسوب والانترنت ان تكون غير قابله للشكل حتى يمكن الحكم بالإدانة ذلك انه لا مجال لدحض قرينه البراءة وافتراض عكسها الا عندما يصل اقتناع القاضي الى حد الجزم واليقين ويمكن توصل الى ذلك من خلال ما يعرض من الأدلةالإلكترونية وغيرها من الاشكال الإلكترونيةالمتوفرة وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات الكترونيه وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها ان يحدد قوتها الاستدلالية على صدق نسبه الجريمةالمعلوماتية الى شخص معين من عدمه ويتحقق اليقين الأدلةالرقمية اكثر بإخضارها للتقييم الفني بواسطه وسائل فنيه من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته وكذا صحه الاجراءات المتبعة في الحصول عليه فانه يخضع لقواعد اخرى للحكم على قيمته التدريبية من الناحيةالعلمية وذلك راجع للطبيعةالفنية لهذا الدليل ان النتيجة التي يطلبها اليقين قضائي في الإدانة هي وجوب تفسير الشكل لمصلحه المتهم حيث يستمد اصوله من قارنه البراءة وتعتبر قاعده الشك يفسر لمصلحه المتهم من اهم الضمانات الموضوعية لاقتناع القاضي فاذا لم تتوصل الجهةالقضائية من خلال ادله المجتمعة لديها الى اليقين بأسناد التهمه الى المتهم الماثل امامها فانه يتعين عليه ان تقضي بالبراءة اما بالنسبة الى موقف بعض القوانين حول ماذا يقينيه الأدلة فقد اشترت قانون البوليس والاثبات البريطاني لعام 1984 ان تكون البيانات دقيقه وصادره من الحاسوب بصوره سليمه وفي كندا ذهب الفقه الى القول ان يكون الدليل الرقم التي تتصل بالموضوع.[18]

المطلب الثاني : حجية الدليل الالكتروني :

يرتبط الدليل الالكتروني ارتباطا قانونيا بالجريمة الالكترونية و المعلوماتية المستحدثة و التي أطرها المشرع الجزائري من خلال ما تضمنه القانون 15/04 [19]في المواد من 394 مكرر إلى 394 مكرر 01 وكذا القانون 04/09 [20]في مادته الثانية،[21] و الذي يعتبر الوسيلة التي يعتمدها القاضي في مرحلة المحاكمة لتقرير قضائه و بالتالي فان حجيته تكمن في الأهمية و القيمة الدلالية التي يتضمنها

---

18) د. بالجراف سامية، سلطة القاضي الجزائي في قبول و تقدير الدليل الرقمي – مجلة الدراسات القانونيةالمقارنة المجلد 07 العدد 01 سنة 2021 – صفحة 687

19) قانون رقم 04–15 ممضي في 10 نوفمبر 2004 – يعدل ويتمم الأمر رقم 66–156 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون العقوبات– الجريدة الرسمية عدد 71 مؤرخة في 10 نوفمبر 2004، الصفحة 8

20) قانون رقم 09–04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ممضي في 05 غشت 2009 – الجريدة الرسمية عدد 47 مؤرخة في 16 غشت 2009، الصفحة 5

21) د. بن الطيبي مبارك و الدكتور رحموني محمد، شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الالكترونية – مجلة القانون و العلوم السياسة – جامعة أحمد دراية – ادرار – مجلد 05 عدد02 / 2019 – صفحة 28

الدليل الالكتروني الذي يتميز بخصائص منفردة تميزه عن باقي الأدلة التقليدية التي حددها المشرع في باب الإثبات و التي تؤهله لأن يعتمد عليه باعتباره نظام علمي و قانوني يمكن الاستعانة به لإثبات الجرائم التقليدية و كذا الجرائم المعلوماتية المستحدثة و تكمن كذلك أهميته و قيمته في مساهمته في الفهم الصحيح و إعطاء القراءة و الصورة الدقيقة لملف الدعوى المطروحة و ذلك من خلال إخضاعه لرقابة القاضي أثناء مرحلة المحاكمة و ذلك بممارسة سلطته التقديرية من حيث الآخذ به من عدمه كذليل بعد تمحيصه و التدقيق به و مراقبة مدى توفر شروط قيامه و قبوله كمعيار للحكم و بحسبه فان حجية الدليل الالكتروني يمكن أن نستشف من مدى قيمته الدلالية وأهميته و كـذا من مدى سلطة القاضـــي في تقديره.[22]

الفرع الأول : أهميه الاثبات بالدليل الالكتروني :

الاثبات بالدليل الالكتروني له أهمية كبيرة في المسائل الجزائية في الجريمة التي تمس بأمن المجتمع وحياه الافراد لذلك تتجه الدولة بسلطتها في متابعه الجاني لتوقيع الجزاء عليه و الردع لغيره والاصل هو براءة المتهم بما نسب اليه من جريمة وعلى جهات التحقيق ان يدحض هذا الاتهام اذا ادعت خلافه ويكون ذلك عن طريق ما يسمى بالدليل الرقمي الجزائي الذي هو أساس الاثبات في الجريمة الإلكترونية للوصول إلى الحقيقة وإصدار حكمه وفقا للنظام الذي يعتمده وبعد التأكد من توافر أركان الجريمة سواء كانت المادية أو المعنوية ومن ثم نسبتها إلى المتهم وللدليل الالكتروني كذلك مساهمة كبيرة أمام الجهات القضائية لمعرفة حجية المخرجات الصادرة من الاجهزة الإلكترونية في المسائل الجنائية كما تبرز كذلك أهميته من خلال النظر إلى القاعدة العامة في إثبات الدعوى الجزائية وهي جواز أن يكون الاثبات بكافة الطرق التي تساهم في إظهار الحقيقة والقيد على هذه الدعوى أن الدليل يتعين أن يكون من الأدلة التي يقبلها المشرع وبالتالي تظهر أهمية اعتراف النظم القانونية بالأدلة ذات الطبيعة الرقمية خاصة مع ظهور الأنشطة الجرمية المستحدثة، وعليه فقد اتجهت العديد من الدول إلى الاعتراف بحجية الدليل الرقمي الناتج عن استخدام الحاسب الآلي، فانه يصلح كذلك في إثبات الجرائم التقليدية.[23]

الفرع الثاني : سلطة القاضي في تقدير الدليل الالكتروني :

إن سلطة القاضي الجزائري في تقدير الأدلة يحكمها مبدا السلطة التقديرية للقاضي الا انه مع التطور العلوم والتكنولوجيا واستعمال اساليب تقنيه طرح التساؤل حول ما حول ما إذا كان نظام الاثبات العلمي سيحل محل أدلة الاقناع وهل يتمتع الدليل العلمي بقيمة في الإثبات تتجاوز الدليل الجنائي

---

22) د. زياد بن محمد عادي العتيبي، مرجع سابق – ص 24

23) د. زياد بن محمد عادي العتيبي، مرجع سابق – صفحة13 – 14

العادي. وفي الحقيقة وما أحدثه العلم التطور إلى أنه لم يؤثر على مبدأ القناعة الوجدانية للقاضي رغم أن الوسائل العلمية للإثبات قد تعطي نتائج لها قدر عال من الثقة إلا أن هذا لا يغني عن العملية الذهنية التي يقوم بها القاضي بهدف الوصول إلى الحقيقة.[24]

ففي الدول التي تبنت نظام الاثبات المقيدة لا يمكن الاعتراف للدليل الالكتروني بأي قيمة ثبوتية ما لم ينص القانون عليه صراحة ضمن أدلة الاثبات في المادة الجزائية، وعليه فاذا لم يذكر المشرع دليل إثبات فالقاضي في هذه الحالة عند إصداره للأحكام القضائية فإنه سيهدر قيمة الدليل الرقمي أو الالكتروني من ناحية ثبوتيته مهما توفرت فيه الشروط اللازمة لقبوله.

أما حجية الدليل الالكتروني في أنظمة الاثبات التي تأخذ بنظام الإثبات الحر، فان القاضي الجزائي في هذه الحالة يأخذ بمبدأ الاقتناع الشخصي و حريته في تقدير الأدلة المرفوعة او الموجودة بملف الدعوي، وبالتالي تكون سلطته واسعه ومطلقة في تحري الحقيقة حسب ما يمليه عليه ضميره ووجدانه، وله الحق في استبعاد أي دليل لا يرتاح إليه وله الحرية التامة في التنسيق بين الأدلة المعروضة أمامه وأن يستخلص ويستنتج منها نتيجة منطقيه يمكنه الاعتماد عليها في تقدير عناصر الدعوى وبالتالي القضاء ببراءة أو إدانة المتهم.

ساد هذا النظام في أغلب التشريعات منها الجزائر بحيث يسري على الإثبات الجنائي في قانون الاجراءات الجزائية مبدأ حرية القاضي في الاقتناع، ذلك أن نص المادة 212 من قانون الاجراءات الجزائية تنص على جواز إثبات الجرائم بأي طريق من طرق الاثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ولا يوجد نص خاص في القانون يقيد مبدأ الإثبات الجنائي في مواد الجريمة المعلوماتية فتخضع بذلك للقواعد العامة في الاثبات، ففي الجزائر فالأدلة المتحصلة من الوسائل الإلكترونية أدلة إثبات يسودها مبدأ حرية القاضي في تكوين عقيدته واقتناعه فهو يتناول حجية الأدلة الرقمية ضمن مسألة قبول الأدلة المتحصلة من الآلة أو ما يسمى بالأدلة العلمية والتي تقبل كطرق إثبات حسب نص المادة 212 من قانون الاجراءات الجزائية لم يضع المشرع أي نصوص قانونية صريحة بهذا الخصوص، حيث تم الاستناد في هذا الموضوع لذات النص والتي طبق من خلالها مبدأ حرية الإثبات.

---

24)د. بالجراف سامية،المرجع السابق – صفحة 38

لكن المشرع الجزائري أدرك وتراجع في موقفه في أن ذلك وحده لا يكفي ليواكب التطور التكنولوجي الحاصل فيما بعد بحيث استحدث القانون رقم 04-15 المؤرخ في 10 نوفمبر سنه 2004 المعدل و المتمم للأمر 66-156 المتضمن قانون العقوبات هو الذي أقر له القسم السابع تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات وقد جاء في عرض أسباب هذا التعديل مواكبة التطور التكنولوجي والمعلوماتية وانتشار وسائل الاتصال الحديثة التي أدت بدورها إلى ظهور أشكال جديده للإجرام إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الالية للمعطيات.

وكان هذا القانون كنتيجة حتميه لما افرزته ثورة تقنية المعلومات التي مست مصالح جديدة غير تلك التي يحميها قانون العقوبات، فقد تطرق المشرع الجزائري إلى تجريم أفعال المساس بأنظمة المعالجة الالية للمعطيات من خلال تعديل قانون العقوبات بموجب القانون المنوه عنه أعلاه والذي يتضمن 08 مواد يهدف من خلالها إلى حماية سرية وسلامة المعلومات ونظم معالجتها وذلك من المواد 394 مكرر إلى 394 مكرر 07، أين جرم الدخول والبقاء الغير مشروع في النظام المعالج الألي للمعطيات أو في جزء منها أو إفشاء المعطيات المتحصل عليها أو حتى الشروع في ارتكاب ترك الجرائم.

و أن المشرع و ضمانا لفعالية و سرعة التحقيق في القضايا المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض صور الإجرام المنظم عمد المشرع الجزائري مواكبة لذلك التطور وضع آليات جديدة تسمح بالكشف، التحري و مكافحة هذا النوع من الجرائم بموجب تعديل قانون الإجراءات الجزائية بسن القانون 06-22 المؤرخ في 2006/12/20،[25] منح بموجبها صلاحيات جديدة للضبطية القضائية متمثلة في أساليب حديثة للتحري كاعتراض المراسلات، تسجيل الأصوات ، التقاط الصور والتسرب، لاسيما في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و التي تجيز لوكيل الجمهورية المختص أنيأذن للضبطية القضائية اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، و كذا وضع الترتيبات التقنية ، دون موافقة المعنيين ، من أجل التقاط و تثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

وبعدها تدخل المشرع الجزائري لحمايه التعاملات الرقمية حين وضع القانون رقم 09-04 المؤرخ في 2009/08/05 للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ومن خلال هذا القانون أدرج المشرع طريقة ضبط الأدلة الرقمية :

---

25) قانون رقم 06-22 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ممضي في 20 ديسمبر 2006الجريدة الرسمية عدد 84 مؤرخة في 24 ديسمبر 2006، الصفحة 4.

الصورة الاولى : تكمن في نسخ المعطيات محل البحث عن تخزين المعلومات الرقمية على أن تكون هذه المعطيات مهيئة بشكل يجعلها قابله لحجزها ووضعها في أحراز على شكل دعامة إلكترونية حسب ما هو مقرر في قواعد تحريز الدليل في قانون الاجراءات الجزائية

الصورة الثانية : إذا استحال إجراء الحجز وفقا للصورة الأولى لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الاشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول إلى المعطيات التي تحتويها هذه المنظومة

وعليه باستقراء نصوص القانون السالف الذكر، يستشف أن عملية الضبط وتحريز الدليل الالكتروني تخضع إلى قواعد تحريز الأدلة الجنائية عموما لكن نظرا للطبيعة الخاصة لهذا الاخير فهو يحتاج إلى بعض الاجراءات الخاصة وذلك للمحافظة عليه وحمايته من الاتلاف و من التغيير وهذا ما أشارت إليه المادة 06 الفقرة الثانية من ذات القانون التي تلزم السلطات المعنية بعمليه ضبط الدليل الرقمي السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجرى بها العملية

غير أنه يجوز للسلطة المعنية استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق بشرط ألا يؤدي ذلك إلى المساس بمحتوى هذه المعطيات[26]

و قد تم بموجب الأمر رقم 21-11 [27]المؤرخ في 25أوت 2021 تعديل قانون الإجراءات الجزائية بالنص على إنشاء على مستوى محكمة سيدي أمحمد قطب جزائي وطني متخصص بالمتابعة و التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال والجرائم المرتبطة بها و بالحكم في الجرائم الالكترونية المنصوص عليها في المادتين 211مكرر 24و مكرر 25 إذا كانت تشكل جنحا أو ما يسمى بالقطب الجزائي السيبراني وقد تضمنت المواد 211 مكرر 22 إلى 211 مكرر29، الأحكام المنظمة لقواعد اختصاص هذه الجهة القضائية المتخصصة وطرق اتصالها بالقضايا بأن يمتد اختصاصها المحلي إلى كامل الإقليم الوطني بأن يؤول إلى وكيل الجمهورية لدى هذه الجهة القضائية المتخصصة وقاضي

---

26)نور الهدى محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية – مجلة الباحث للدراسات الأكاديمية– العدد 11 – جوان 2021 صفحة 923

27) أمر رقم 21-11 يتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية، ممضي في 25 غشت 2021 – الجريدة الرسمية عدد 65 مؤرخة في 26 غشت 2021، الصفحة 7.

التحقيق و رئيس ذات القطب الاختصاص الحصري بالمتابعة والتحقيق و الحكم بمقتضى المادة 211 مكرر 24 في أنواع معينة من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال على نحو ما حددها المشرع في هذا النص و كذا الجرائم المرتبطة بها بأنها:

-الجرائم المتصلة بتكنولوجيات الأعلام و الاتصال التي تمس بأمن الدولة أو الدفاع الوطني
-جرائم نشر و ترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع
-جرائم نشر و ترويج أنباء مغرضة تمس بالنظام و الأمن العموميين ذات الطابع المنظم أو العابر للحود الوطنية
-جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات و المؤسسات العمومية
-جرائم الاتجار بالأشخاص و الأعضاء البشرية أو تهريب المهاجرين.
-جرائم التمييز و خطاب الكراهية

كما يؤول الاختصاص الحصري إلى وكيل الجمهورية لدى هذه الجهة القضائية المتخصصة وقاضي التحقيق و رئيس ذات القطب بالمتابعة و التحقيق و الحكم بمقتضى المادة 211 مكرر 25 في الجرائم الالكترونية الأكثر تعقيدا على نحو ما عرفت الفقرة 2من نفس المادة المقصود بها بأنها هي الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة اثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام العام و الأمن العموميين تتطلب استعمال و سائل تحري خاصة أو خبرة فنية متخصصةأو تعاون قضائي دولي و كذا الجرائم المرتبطة

الخاتمة :

يعد الدليل الالكتروني من الأدلة العلمية الحديثة والناتجة عن ارتكاب الجرائم الإلكترونية بعد التحول الذي شهده العالم، لأن هذا الدليل قد فرض نفسه في مجال الاثبات الجنائي سواء في إثبات الجرائم المعلوماتية والمستحدثة أو في جرائم أخرى.

فالدليل الالكتروني أصبح يتمتع بقوة ثبوتية وحجية كافية في مجال الإثبات الجنائي وذلك بعد التأكد من توفر شروطه لقبوله كدليل أمام الجهات القضائية المختصة، وقد خلصنا في هذه الدراسة المتواضعة الى النتائج التالية :

أولا النتائج :

- أن الدليل الرقمي ينتمي إلى بيئة رقمية غير ملموسة داخل نظام تقني، الأمر الذي يجعل طمسه سهلا إذا ارتكبت الجريمة من قبل شخص جد محترف في مجال التكنولوجيا
- أنه لا يوجد تعريف جامع مانع للدليل الالكتروني كذلك الدليل الالكتروني دليل مساعد في إثبات الجرائم الإلكترونية بهدف تحقيق الأمن والعدالة
- الدليل الالكتروني له حجية مطلقة في الإثبات إذا توفرت فيه الشروط اللازمة لقبوله كدليل أمام الجهات القضائية وكان مستخلصا من قبل أشخاص ذوي كفاءة عالية في ميدان التكنولوجيا
- أن الدليل الالكتروني يمتاز بالتنوع أي أنه متنوع ومتطور ومتجدد باستمرار وبالتالي فهو يتطلب أساليب مكافحة جد متطورة

التوصيات :

- أن يكون للدليل الالكتروني تنظيم قانوني خاص يعالج كل المسائل الإجرائية المتعلقة بالجرائم الإلكترونية ابتداء من اكتشاف الجريمة من قبل الضبطية القضائية إلى غاية تقديم المشتبه فيه أمام النيابة العامة.
- التدريب القانوني والتطبيقي المستمر و المستحدث لضباط الشرطة القضائية و المستخدمين وكذا قضاة النيابة و التحقيق على كيفية التعامل مع الجرائم الإلكترونية والأدلة الإلكترونية المتخصصة منها.

- تعديل قانون الاجراءات الجزائية وتقنين مواد تنص على الدليل الالكتروني وتنص على كل دليل باسمه مثلا كالخبير الالكتروني أو الشاهد المعلومات
- تعديل القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها بحيث ينص على كل بطلان الاجراء المخالف إذا تم الحصول على الدليل الالكتروني بطريقه غير مشروعة.
- تشديد العقوبات على كل جاني في جريمة معلوماتية يقوم بحذف البيانات أو تزويرها أو نقلها أو تعديلها أو الدخول المواقع الإلكترونية الخاصة دون إذن بهدف مكافحة هذا النوع من الجرائم العابرة للحدود.
- تفعيل دور المؤسسات التعليمية والتربوية ودور الأسر لنشر ثقافة الوعي بين المواطنين وتحذيرهم من خطورة الجرائم المعلوماتية وإرشادهم في كيفيه اتخاذ الاحتياطات اللازمة لكي تضمن لهم عدم وقوعهم ضحايا لمثل هذا النوع من الجرائم خصوصا لفئة القصر
- توعية المواطنين في كيفيه الحفاظ على بياناتهم خصوصياتهم كحساباتهم البنكية وبطاقاتهم الائتمانية والبريد الالكتروني الخاص بهم خوفا من وقوعهم ضحايا الابتزاز الالكتروني
- تأهيل وإعداده إطارات ذوي كفاءات عالية في مجال الدليل الالكتروني كمحققين في الميدان مختصين في الجرائم الإلكترونية.

جامعة الجزائر 1 بن يوسف بن خدة

كلية الحقوق

الملتقى الدولي الافتراضي الموسوم بـــ: **القانون الجنائي في ظل التطور التكنولوجي –اشكالات ومعالجات**

مداخلة بعنوان: التطور التكنولوجي وأثره على الاثبات الجنائي

The Technological development and its impact on criminal evidence

من اعداد:

- الدكتور**ديدوني بلقاسم** استاذ محاضر (أ) جامعة عمار ثليجي بالأغواط.–
  - مخبر الحقوق والعلوم السياسية.

البريد الالكتروني:b.didouni@lagh-univ.dz

- الدكتور **محبوبي محمد** أستاذ محاضر (أ) جامعة عمار ثليجي بالأغواط.
  - مخبر الحقوق و العلوم السياسية.

البريد الالكتروني:Mahboubim@ymail.com

الملخص:

تعتبر الوسائل التكنولوجية في الوقت الراهن ذات أهمية بالغة في حياة الناس حيث أصبحت تستعمل في كل جوانب الحياة الاقتصادية والاجتماعية والسياسية حيث لا يمكن الاستغناء عليها باعتبارها جزء لا يتجزأ من وسائل العيش والتواصل بين الناس ولعل أبرزها تكنولوجيا الاعلام والاتصال حيث تستعمل في تخزينالمعلومات الشخصية من صور وفيديوهات ووثائق تتعلق بحركة وهوية الاشخاص والجماعات.

وأمام هذا التطور الهائل لهذه الوسائل أصبحت تشكل خطرا كبير بسبب شبكة الانترنت وربطها بالهواتف الذكية وظهور التطبيقات المتطورة ووسائل التواصل الاجتماعي الامر الذي صعب من مهمة التحكم فيها من طرف الدول وعلى اثر ذلك عملت على احاطتها بنظم قانونية خاصة تؤكد على ضرورة حماية الاشخاص من مخاطرها عن طريق التتبع لهويات مستعمليها وتحركاتهم مع حماية حقوق الاشخاص وحرياتهم وجعل هذه الوسائل **دليل اثبات**، ورغم هذه الضمانات الا أن الجرائم المرتبطة بهذا التطور لا تزال في توسع كبير يخرج عن السيطرة في الكثير من الحالات.

الكلمات المفتاحية: أدلة الاثبات ، الوسائل التكنولوجية ، الحماية الجنائية ، الجرائم الالكترونية

Abstract:
Technological means are considered at the present time of great importance in people's lives, as they are used in all aspects of economic, social and political life, as they cannot be dispensed with as an integral part of the means of living and communication between people. Videos and documents related to the movement and identity of people and groups.

In the face of this tremendous development of these means, it has become a great danger due to the Internet and its link to smart phones and the emergence of advanced applications and social media, which made it difficult for countries to control them. Tracking the identities of its users and their movements while protecting the rights and freedoms of people and making these means evidence of proof, and despite these guarantees, the crimes associated with this development are still in a large expansion that is out of control in many cases.
KeywordsEvidence of proof, technological means, criminal protection, electronic crimes.

مقدمة:

لقد ساهمت التكنولوجيا الحديثة الى جانب وسائل الاثبات التقليدية في مكافحة الجريمة بكل أنواعها من خلال تطوير الوسائل العلمية المختصة في الكشف ومتابعة المجرمين والتي يستعملها المحققون ورجال العدالة بغرض الوصول الى نتائج دقيقة وبالسرعة القصوى مع تحري الدقة والفعالية الممكنة .

وبالرغم من أن هذا التطور التكنولوجي السريع كان له الاثر السلبي على العدالة نتيجة عدم المواكبة الحاصلة في العالم ونقص المعلومات والتعاون الدولي الا ان أغلب الدول كان الزاما عليها بذل جهودا في الحصول على أجهزة الحماية التي تمنع ارتكاب الاعمال الاجرامية عن طريق الوسائل التكنولوجية أو بدونها واستعمالها في الجانب الايجابي من خلال البحث والتحري والكشف عن الجرائم.

وأمام هذا التطور السريع كان من الضروري تطوير المنظومة القانونية التي تسمح باستعمال التكنولوجيا في البحث والتحري وجعلها تساهم بشكل فعال في مكافحة الجريمة دون المساس بحقوق الاشخاص التي يضمنها الدستور ويمنع المساس بها ويعزز الثقة في اجهزة العدالة ويسمح باستعمالها بكل الضمانات التي تضر بالحياة الخاصةو بحقوق الاشخاص.

وتظهر أهمية الدراسة في أن استعمال التكنولوجيا في الاثبات الجنائي له ايجابيات كثيرة منها السرعة في معالجة القضايا الذي يحقق مبدأ المحاكمة العادلة كما أنه يقلل أو يقضي على الاخطاء المرتكبة أثناء التحقيق من خلال الادلة العلمية الناتجة عن استعمال التكنولوجيا بالإضافة الى أن مواجهة المتهم بالأدلة العلمية التكنولوجية يجعله يعترف بالجرم المنسوب اليه.

كما ان الوسائل التكنولوجية وسيلة مقنعة لان القاضي يعتمد على الادلة العلمية لإصدار الحكم من خلال الصور أو الفيديو أو التسجيل الصوتي أو معالجة البيانات المنشورة او المرسلة والتي كلها تعتبر أدلة لا يمكن الاعتراض عليها باعتبارها وسائل اثبات حقيقية.

ونهدف من خلال هذه الدراسة الى الاطلاع على كيفية استعمال التكنولوجيا في الاثبات الجنائي وجدية الاجهزة المختصة في ذلك بتوفير الامكانيات اللازمة المتعلقة بالتحقيق و تأكيد المعلومات المستمدة من هذه الاجهزة.

وقد اعتمدنا في هذه الدراسة على المنهج التحليلي الذي من خلاله يتم التطرق الى المواقف الفقهية والنصوص القانونية بتفسيرها وتحليلها وتقييمها بما يتوفق مع مدلولها وفحواها بالإضافة الى المنهج الوصفي لدراسة الاثار المترتبة عن الاستعمال غير الصحيح للوسائل التكنولوجية الحديثة ومدى القدرة على اعتمادها كدليل اثبات.

<u>اشكالية المداخلة:</u> كيف ساهم التطور التكنولوجي في الاثبات الجنائي؟

وللإجابة عن هذه الاشكالية اعتمدنا الخطة التالية:

المحور الاول: تطور وسائل الاثبات الجنائي التكنولوجي.

أولا : مدلول الاثبات الجنائي بالوسائل التكنولوجية وطبيعته.

ثانيا: أنواع وطرق الاثبات بالوسائل التكنولوجية.

المحور الثاني: المشاكل التي تعيق استعمال التكنولوجيا في الاثبات الجنائي.

أولا: العوائق القانونية وكيفية التعامل معها.

ثانيا: العوائق التقنية الواقعية و المحتملة.

الخاتمة.

المحور الاول: تطور وسائل الاثبات الجنائي بالوسائل التكنولوجية

الى جانب الوسائل التقليدية المعروفة في الاثبات الجنائي و هي الاعتراف او الاقرار من المتهم و شهادة الشهود و الخبرة هناك وسائل علمية و تقنية يتم الاستعانة بها للإثبات الجنائي، لذلك سوف نتطرق الى تحديد مفهوم الاثبات بشكل عام و بالطرق التكنولوجية بشكل خاص ثم كيفية الاثبات بالوسائل التكنولوجية.

أولا: مفهوم الاثبات الجنائي.

1/تعريف الاثبات:

يقصد بالإثبات هو الوسائل التي تؤدي الى إظهار الحقيقة و ثبوت الجريمة المرتكبة على المتهم الذي ارتكبها و تحديد الافعال المجرمة وفق القانون و تحديد العقوبات المقررة لها، و الاثبات يؤدي الى جعل القاضي يصدر حكما في القضية و اقتناعه بان الشخص هو المرتكب لهذه الجريمة او لا و لا يقتنع القاضي الا اذا كان الدليل قطعيا و لذلك فان الادلة نوعان ادلة قطعية و هي تلك التي تصدر عن خبير و ذات طبيعة علمية و تقنية و ادلة غير قطعية و هي الادلة غير الدقيقة علميا و تقنيا ولا يمكن للقاضي ان يقتنع بها، وكل هذه الادلة تكون مقنعة اذا كانت الوسيلة العلمية و التقنية دقيقة و متطورة اما اذا كانت خلاف ذلك فتكون غير مقنعة.[1]

2/تحديد مفهوم الاثبات بالوسائل العلمية:

أ-تعريف الدليل العلمي: يقصد بالإثبات بالوسائل التكنولوجية و العلمية هو استعمال الوسائل التكنولوجية الحديثة في اثبات الجريمة المرتكبة قصد إظهار الحقيقة بالأدلة العلمية و هذه الوسائل يجب ان تكون مشروعة تتمتع بالحجية في الاثبات ولقد تطرقت قوانين الاجراءات الجزائية الى الاخذ بالأدلة العلمية عن طريق **الخبرة** التي تلجا اليها المحكمة اثناء التحقيق و اثناء المحاكمة ، وقد نصت المادة(143) من قانون الاجراءات الجزائية الجزائري على ان قاضي التحقيق عندما تكون القضية ذات طابع فني يجب ان يأمر بانتداب خبير اما بناء على طلب النيابة العامة او من تلقاء نفسة او من طرف الخصوم.[2]

ب-خصائص و مميزات ادلة الاثبات التكنولوجية: تتميز الادلة ذات الصفة التكنولوجية و التقنية بالمميزات التالية:

---

[1] محمد علي سكيكر ، تحقيق الدعوى الجنائية واثباتها في ضوء التشريع والفقه والقضاء ، دار الفكر الجامعي ، مصر ، 2006.ص331.

[2] أحسن بوسقيعة، التحقيق القضائي، دار هومة، الجزائر،2009،ص 168.

-انها تؤدي الى الكشف عن الجرائم الحديثة المرتبطة بالتطور التكنولوجي، فالقضاء يجب ان يكون مسايرا للجرائم الحديثة و خاصة التي لهاعلاقة بالتطور التكنولوجي،

-انها وسائل دقيقة تؤدي الى نتائج مقبولة،

-انها تؤدي في غالب الاحيان الى اعتراف الجاني بأفعاله بسبب مواجهته بالأدلة العلمية،

-انها تؤدي الى اختصار الوقت في البحث و التحري،

-انها تؤدي الى عدم افلات الجاني من العقاب مهما كانت درجة ذكائه و قدرته على الفرار من العدالة

-انها وسائل تؤدي الى حماية حقوق الاشخاص،

-انها ذات اهمية في قضايا التزوير و جرائم الاختلاس و تبديد الاموال و الجرائم الاقتصادية و تلك المتعلقة بالضرائب،

ج/اجراءات الخبرة التقنية و العلمية: احاط المشرع الخبرة العلمية و التقنية بمجموعة من الاجراءات و هي تلك المتعلقة بكيفية تعيين الخبير و المهام الموكلة اليه و مسؤوليته عن الخبرة التي يقوم بها[1]:

- **كيفية ندب الخبير:** نصت المادة (147) من قانون الاجراءات الجزائية على انه يمكن ندب خبير واحد او اكثر من طرف قاضي التحقيق و ذلك من الجدول الذي يعد على مستوى المجالس القضائية بعد اخذ راي النيابة العامة، و يمكن لقاضي التحقيق بأمر مسبب انتداب خبير غير مقيد في الجدول حسب نص المادة (145) من قانون الاجراءات الجزائية و ذلك بسبب الكفاءة التي يتمتع بها هذا الخبير في القضية المعروضة على المحكمة(المادة 145-146) من قانون الاجراءات الجزائية.

- **اداء اليمين للخبير:** يشترط في الخبير ان يكون قد ادى اليمين القانونية اثناء تقييده في الجدول او اثناء انتدابه في القضية حيث يتعهد على اداء مهامه بكل احترافية و مهنية واخلاص و يحرص على ابداء رايه بنزاهة و حياد و اخلاص، و يؤدي نفس اليمين في حالة انتدابه من طرف قاضي التحقيق و يمكن للخبير ان يؤدي اليمين بواسطة الكتابة اذا وقع مانع لهمن اداء اليمين بشكل مباشر و يتم ارفاق ذلك بالملف الخاص بالخبير(المادة 145 من قانون الاجراءات الجزائية).[2]

---

[1] عبد الله أوهايبية، شرح قانون الاجراءات الجزائية الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012 ، ص 362.

[2] زروقي عاسيا ، الخبرة الجزائية ومدى سلطة القاضي الجزائي في تقديرها ، (مقال منشور) مجلة معالم للدراسات القانونية والسياسية،المجلد03 العدد01 ، 2019 ، ص 102.

– **الجهة المشرفة على الخبير:** حسب نص المادة (3/143) من قانون الاجراءات الجزائية ان الخبير يمارس مهامه تحت سلطة قاضي التحقيق و يشترط ان يمارس مهامه بالتنسيق مع قاضي التحقيق، و ان يقدم له كل المعلومات الجديدة المتعلقة بالقضية و الاجراءات الازمة التي يقوم بها المادة (2/148).[1]

كما يجب على قاضي التحقيق تقديم و سائل الاثبات التي تساعد الخبير في عمله و اذا تعلق الامر بالإحراز المفتوحة و جب على قاضي التحقيق عرضها على المتهم قبل ارسالها للخبير و فق محضر مخصص لإثبات تسليم الاشياء(المادة 150 من قانون الاجراءات الجزائية)و يمكن للخبير اثناء تنفيذ مهامه تلقي تصريح الاشخاص مع عدم قدرته على البحث عن الشهود و اذا استلزم الامر ذلك يطلب من قاضي لتحقيق القيام بهذا الاجراء(المادة 3/148 من قانون الاجراءات الجزائية).

و في حالة الاستجواب الذي يقوم به قاضي التحقيق يمكن للخبير الحضور اذا كان الاستجواب يتعلق بالخبرة و يجب في ذلك ان يكون الاستجواب وفق الاجراءات النصوص عليها في المواد(105و 106) من قانون الاجراءات الجزائية.

و يمكن للخبراء الاطباء استثناء حسب نص المادة (151 من قانون الاجراءات الجزائية) استجواب المتهم بدون حضور قاضي التحقيق، كما اجازت (152) في قانون اجراءات الجزائية للأطراف امكانية الطلب من قاضي التحقيق ان يكلف الخبير بإجراء ابحاث معينة او سماع شخص معين قد تكون له القدرة على تقديم معلومات ذات طابع فني.[2]

–**تقرير الخبرة:** نصت المواد(153و 154) من قانون الاجراءات الجزائية على كيفية تحرير تقرير الخبرة و ايداعه حيث انه يلتزم الخبير بتحرير تقرير نتيجة الخبرة المتحصل عليها و فق الآجال القانونية التي يحددها قاضي التحقيق و يتضمن التقرير الاعمال الذي قام و النتائج المتحصل عليها و توقيعه ويتم ايداعه لدى كاتب قاضي التحقيق مع محضر استلام (153).

و تعتبر نتائج التقرير المقدم من طرف الخبير غير ملزمة بقاضي التحقيق بحيث يتخذ الاجراءات التي يراها مناسبة كما نصت المادة (154) من قانون الاجراءات الجزائية ان قاضي التحقيق ملزم بإعلام الاطراف بنتائج الخبرة مع مراعاة المادتين (165) و(166) من قانون الاجراءات الجزائية.

ثانيا: الطرق و الوسائل التكنولوجية المستعملة في الاثبات الجنائي: تطبقا لنص المادة (212) من قانون الاجراءات الجزائية فان المشرع الجزائري اقر جميع و سائل الاثبات الممكنة التي لها امكانية

---

[1] قادري أعمر، أطر التحقيق، دار هومة للطباعة والنشر والتوزيع ، الجزائر،2013 ، ص 168

[2] أحسن بوسقيعة، مرجع سابق،ص111.

الكشف عن الجريمة ما عدا الحالات التي ينص فيها القانون على خلاف ذلك، و الى جانب وسائل الاثبات العلمية المعروفة على غرار البصمة بكل انواعها و تحليل الدم و مضاهاة الخطوط و الطب الشرعي، هناك ادلة اثبات مرتبطة بالتطور التكنولوجي من بينها ما يلي:

1/ المراقبة عن طريق الفيديو و الهاتف: و يقصد بها استعمال كاميرات المراقبة بكل انواعها في الثبات الجنائي حيث ان كاميرات المراقبة تقوم بنقل الصورة و الصوت او تسجيلها لحركة الاشخاص و تصوير الافعال التي يقوم بها ل فرد في الاماكن العامة و الخاصة و تعتبر هذه التقنية فعالة في اثبات الجرائم و مكافحتها حيث ان استعمالها اصبح واسع بتطوير تقنية التصوير عبر الكاميرات الثابتة و المتنقلة، و تعتبر الجزائر من الدول التي عملت على استعمال هذه الوسيلة ابتداء من سنة 2009.(المرسوم الرئاسي رقم 337/09 الصادر في 21 أكتوبر 2009 المتضمن إحداث مؤسسة إنجاز المراقبة بواسطة الفيديو، الجريدة الرسمية، عدد 61 الصادر في 2009/10/25 المعدل و المتم بموجب المرسوم الرئاسي 228/15 الصادر في 22 غشت 2015 والذي يحدد القواعد العامة المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو و سيره.[1]، حيث نصت المادة (02) على الحالات التي يهدف إليها هذا القانون من خلال هذه التقنية و هي كالآتي[2]:

-مكافحة الارهاب،

-الوقاية من الاعمال الاجرامية،

-حماية الاشخاص و الممتلكات،

-الحفاض على النظام العام،

-ضبط حركة السير عبر الطرق و معاينة المخالفات لقواعد حركة المرور عبر الطرق،

-تامين البنايات و المواقع الحساسة،

-تسيير وضعيات الازمة و الكوارث الطبيعية و غيرها،

و اقرت المادة 03 من نف القانون ان الجهة التي يمكن لها استعمال هذه التقنية هي اجهزة الامن و الانقاض، و التي يمكن ان توفر الحاجيات التالية: منع و مكافحة الجريمة و تسهيل القبض على المجرمين:

---

[1]-الجريدة الرسمية، العدد45، الصادر في 25 أوت 2015، ص03

[2]توميحيى ، دور نظام المراقبة بواسطة الفيديو في الاثبات الجنائي ، (مقال منشور) ، المرجع السابق، ص 04.

-تحسين تدابير الحفاض على النظام العام،

-منح الفعالية للعمل الميداني من اجل التنسيق و الانسجام في التدخلات،

- التقليل من الخسائر و الاضرار الى الحد الاجنى باستعمال هذه التنقية و بينت المادة(04) الاماكن التي تتم فيها المراقبة و هي:

-التجمعات الحضارية الكبرى و مناطق و ضواحي المدن،

-محاور الطرق الكبرى و التقاطع الذي يحتوي على حركة مكثفة،

- الاماكن المفتوحة للجمهور كالموانئ و المطارات و المنشئات الرياضية الكبرى،

- المؤسسات الاقتصادية الكبرى،

و لا تخضع المراقبة عبر تركيب كاميرات في الاماكن العامة الى رخصة ادارية و انما تكون عبر مخطط المراقبة بالفيديو الذي يصادق عليه الوالي و بالتنسيق مع اللجنة الولائية للأمن و كل هيئة لها علاقة بتركيب اجهزة الفيديو، و تقع مصاريف تركيب اجهزة المراقبة بالفيديو على الدولة المؤسسات المعنية بالتركيب.

وتخضع عملية المراقبة عبر الفيديو الى تنظيم مكون من مركز وطني للمراقبة عبر الفيديو و مراكز ولائية، و شبكات كاميرات فيديو منصبة في الاماكن العامة او المفتوحة للجمهور و تعتبر هذه التقنية الحديثة من اهم الوسائل المتعلقة بمكافحة و اثبات الجرائم و توقيف المجرمين من خلال كاميرات مركبة في الاماكن العامة او التصوير الشخصي بواسطة الهواتف النقالة في الاماكن العامة بالرغم مما تثيره هذه الوسيلة من مشاكل قانونية و تقنية.

2/الاثبات بواسطة الهواتف النقالة: يعتبر الهاتف النقال من الوسائل التكنولوجية الحديثة في الاتصالات حيث اصبح يستعمل في اغراض متعددة منها التسجيل و لتصوير و كوسيلة تواصل عبر شبكة الانترنت و وسيلة تخزين بالإضافة الى الوسيلة التقليدية و هي التواصل عبر المحادثة، و هو بذلك اصبح سلاح ذو حدين فهو يستعمل من جهة للتواصل و من جهة اخرى لارتكاب جرائم خطيرة. كما انه ارتبط بجرائم دولية كبرى مثل التجسس و الانخراط في الجماعات الاجرامية نظرا لسهولة استعماله و التطبيقات التي يحتوي عليها و من هنا كان لابد ان يكون وسيلة اثبات مهمة في الكثير من الجرائم[1]

[1] مستاريعادل ، أحمد حسين ، حجية الادلة المستمدة من الهواتف النقالة ، (مقال منشور) ، مجلة الفكر ، العدد 15 ، 2017 ، ص 53.

أ-الادلة المستمدة من الهاتف النقال:

- **الادلة الرقمية:**الذي يكون بواسطة التتبع باعتبار ان الهاتف النقال مرتبط بالأنترنت وبالتالي يمكن تتبع العمليات الاجرامية التي قام بها الشخص عبر هاتفه النقال.

-**الادلة الرقميةالخاصةبفحص نظام بروتوكول الانترنت:** و يقصد به العناوين و البيانات و المواقع في شبكة الانترنت لان كل هاتف نقال متصل بالأنترنت له عنوان خاص به يمكنه من الدخول الى الشبكة و تعتبر هذه الطريقة مهمة لفحص نظام الاتصال بالأنترنت و من خلالها يمكن اكتشاف الهاتف الذي ارتكب الجريمة[1]

-**الادلةالرقميةالخاصةبفحص اجهزة تدعيم خدمة الهاتف النقال:** فحص هذه الاجهزة يؤدي الى الكشف عن ادلة النفي او الاثبات عن طريق الاجهزة التي تزود بها الشركات الهواتف النقالة من و سائل التواصل و البريد الإلكتروني و هذه الوسائل المزودة لخدمة الهاتف مهمة في تتبع النشاطات التي قام بها الشخص

ب-الادلةالخاصةبفحص ذاكرة التخزين: و هي الذاكرة التي يزود بها لهاتف النقال و المخصصة لتخزين البيانات و كل حركة افتراضية قام بها المستعمل للهاتف النقال او ما قام بتخزينه و لا يستطيع المستعمل ازالة هذه البيانات المخزنة حتى و لو قام بحذفها.

ج- فحص محتويات الهاتف النقال المادية و المعنوية: و يكون ذلك من خلال تحليل البيانات المخزنة في الذاكرة من صور و تسجيلات و افلام[2].

المحور الثاني:المشاكل التي تعيق استعمال التكنولوجيا في الاثبات الجنائي

تعتبر الادلة التكنولوجية المستمدة من الوسائل المذكورة انفا ذات اهمية بالغة في الاثبات الجنائي و قد زادت اهميتها على المستوى الوطني و الدولي، غير ان هذه الادلة تصطدم بعوائق كثيرة تجعلها تفقد اهميتها و تجعل غير قابلة للتطبيق نتيجة عدم الاقتناع بها .

---

[1] مستاري عادل ، احمد حسين، المرجع السابق ، ص 55

[2] نوف حسين متروك ، حجية المستخرجات الصوتية والمرئية في الاثبات الجنائي ' دراسة مقارنة ' مذكرة ماجستير ،جامعة الشرق الاوسط، الاردن ، 2019 ،ص 37.

اولا العوائق القانونية: بالرغم من أن الادلة المستمدة من الاجهزة التكنولوجية قطعية الدلالة بسبب عدم قدرة المتهم على انكارها الا ان المختصين من الفقهاء و القانونيين اختلفوا في حجيتها متأثرين بقواعد الاثبات التقليدية التي تجعل القاضي يأخذ بها على سبيل الاستئناس فقط.

1/**الاتجاه المؤيد لأدلة الاثبات التكنولوجي:** يرى هذا الاتجاه ان اعتماد هذه الوسيلة يحقق حماية للمواطنين من الجرائم المرتكبة عبر هذه الوسائل او عبر استغلالها للحماية او الاثبات لان المجرمين لان المجرمين لا يمكنهم تفادي هذه الوسائل او الاحتراز منها مما يوقعهم في اخطاء تثبت جرائم سواء عن طريق الصورة او الفيديو او المكالمة او التواصل الاجتماعي او من غيرها الاستعمالات المتكررة للهاتف النقال او الكمبيوتر التي يحتوي عليها كما ان كاميرات المراقبة التي توضع في الاماكن العامة تساهم في مكافحة الجرائم الماسة بالأشخاص و الممتلكات و وسيلة التعرف على المجرمين.

كما ان هذا الاتجاه يعتبر ان استعمال هذه الاجهزة لا يلقى معارضة من الاشخاص في مجال حقوق و حريات الافراد و حركة تنقلهم فهذه الوسائل تستعمل بطرق قانونية و بكامل الضمانات

كما ان استعمالها أثبت نجاعته في كل الميادين فقد ساهمت كاميرات المراقبة في مجال حركة المرور و توقيف المخالفين لقانون المرور و حماية المواطنين من السائقين المخالفين و مواجهتهم بالأدلة التكنولوجية التي لا تقبل الشك.[1]

2/ **الاتجاه الرافض للوسائل التكنولوجية في الاثبات الجنائي:** يستند اصحاب هذا الراي الى ان هذه الوسائل هي انتهاك للحق في الخصوصية و الحقوق و الحريات الشخصية عن طريق التقاط الصور و الفيديوهات و خاصة في ظل انتشار ظاهرة التصوير العشوائي و نشر الصور و الفيديوهات في وسائل التواصل الاجتماعي و الترخيص باستعمال هذه الوسائل فتح المجال واسعا للتلاعب بالصور و الفيديو في ظل التكنولوجيا المتطورة بالإضافة الى ان وسائل النشر متاحة لكل العالم و التحكم فيها يعتبر امرا مستحيلا، بالإضافة الى انه تضييق للحريات الشخصية و اخذ صورهم بدون علمهم.[2]

3/ القيمة القانونية لأدلة الاثبات بواسطة الوسائل التكنولوجية: لا شك ان هذه الوسائل مهمة في مجال الاثبات الجنائي و استعمالها توسع بشكل كبير حيث ان اغلب القضايا التي تعرض على القضاء لابد ان يكون لهذه الوسائل دور فيها لكنها تصطدم بعوائق قانونية يجعل تطبيقها محدود وبالتالي فان المقارنة مع دورها في الواقع و حجيتها القانونية و بالتالي فهناك عدم تكافئ بين اضرارها المحتملة و ما تقدمه من ايجابيات و ذلك للأسباب التالية:

---

[1] تومي يحي، مرجع سابق ص08

[2] أحمد غاي،ضمانات المشتبه فيه أثناء التحريات الاولية،دار هومة ، الجزائر، 2005 ، ص 234.

– أن اغلب القوانين تقيد استعمالها بقوانين صارمة حيث تمنع هذه القوانين المساس بحقوق و حريات الاشخاص ومثال ذلك المادة (46) من الدستور الجزائري التي تمنع انتهاك الحقوق و الحريات الشخصية و الحياة الخاصة للإنسان و سرية الاتصالات و المراسلات و لا يجوز المساس بهذه الحقوق الا بواسطة اذن صريح من السلطة القضائية هذه النصوص بقدر ما تمثله من حماية للمواطنين من استعمال هذه الوسائل بقدر ماهي فرض لضوابط صارمة للحرية في استعمالها و خاصة في ظل فرض العقوبات على مخالفة هذه القواعد و منها ما نصت عنه المادة(29) من قانون العقوبات الجزائري حيث نصت على معاقبة الاعتداء الماس بشرف و اعتبار الاشخاص و حرمة افشاء الاسرار في المواد (301)و (302) و سرية المراسلات في المادة(303) و قررت المادة(303) مكرر من قانون العقوبات عقوبة الحبس من 06 اشهر الى 03 سنوات و بغرامة من 50,000 الى 300,000 لكل من يتعمد التقاط الصور و تسجيل المكالمات دون اذن صاحبها،

– كما أن الادلة التي توفرها هذه الوسائل لا تشكل دليل اثبات **قطعي** نظرا الى ان القاضي غير ملزم بالأخذ به و لو ان هذه الادلة مقدمة من طرف الخبير و بالتالي فإنها غير مقنعة له بشكل كامل و مثال ذلك ما نصت عليه المادة (212) من قانون الاجراءات الجزائية الجزائري التي اعتبرت ان القاضي لا يبني الحكم الا على اقتناعه و بالتالي فان هذه الادلة رغم دقتها لكن القاضي غير ملزم بها،

– كما نصت المادة(12) من الاعلان العالمي لحقوق الانسان بانه لا يجوز تعريض احد لتدخل تعسفي في حياته الخاصة او في شؤون اسرته او مسكنها و مراسلاته و لا لحملات تمس شرفه و سمعته و لكل شخص الحق في ان يحميه القانون من تلك التدخلات و الحملات،

– و نصت المادة(17) من العهد الدولي للحقوق المدنية و السياسية لعام1966 على ان الفرد يتمتع بحماية حياته الخاصة و ذلك في الخاصة وذلك في الحالات التالية:

*لا يجوز التدخل التعسفي و غير القانوني في المسائل الخاصة لأي شخص أو لعائلته او مسكنه او مراسلاته او كل ما يمس شرفه و سمعته،

* كل شخص يتمتع بحماية قانونية من هذه التدخلات،

و نفس القواعد تم التأكيد عليها في كل الاتفاقيات الدولية المتعلقة بحقوق الانسان التي اوجبت حماية قانونية للأشخاص من التدخل في حياتهم الخاصة و الاطلاع على مراسلاتهم.

ومن هنا نلاحظ ان التشريع الوطني و القوانين الدولية قيدت اللجوء الى استعمال هذه الوسائل في الاثبات و اعتبرتها انتهاك لحقوق الانسان وهذا ما جعل القانون لا يلزم القاضي بالاعتماد عليها كدليل اثبات قطعي.[1]

2/العوائق التقنية و الواقعية:

أ/ العوائق التقنية:

لا شك ان الوسائل التكنولوجية تعتمد على برامج معقدة و هي عرضة للمشاكل التقنية و القرصنة و التزوير و التزييف و الاختراق مما يشكل خطرا كبيرا على الحياة الخاصة للأشخاص من خلال اعتراض مراسلاتهم و اختراق حواسبهم و هواتفهم و الحصول على صورهم و فيديوهاتهم و حتى تسجيل مكالماتهم و نظرا لسهولة استعمال هذه الوسائل و اهميتها في حياة الناس اصبحت و سيلة رائجة في اعتمادها كوسيلة اثبات و التبليغ عن الاشخاص و تعريضهم لعقوبات ناتجة عن جرائم لا علاقة لهم بها.

و يعود السبب في ذلك الى مشاكل تقنية كثيرة من بينها عدم القدرة على التأكد من صحتها نتيجة استعمال الوسائل المتطورة في فبركة الصور و الفيديوهات و حتى المحادثات حيث تستعمل هذه التطبيقات في دمج الصور و تركيبها و تحرير الفيديوهات و القدرة على التعديل كل هذه التطبيقات الخطيرة تشكل عائق على الجهات المختصة. التأكد من صحتها و جعلها دليل للإثبات مع فقد الثقة في اهميتها.

بالإضافة الى ان الادلة الموجودة في هذه الاجهزة هي ادلة الكترونية فهي لا تعتبر حقيقة علمية ثابتة فالمحادثة المسجلة عبر الهاتف هي دليل مفترض فقط و لا وجود دليل مقنع ان الصوت يعود لهذا الشخص او لشخص اخر، و هذا الامر يتطلب برامج معقدة و غير متاحة بسهولة للعدالة في الوقت الحالي، و انما تعود للخبير فقط و الخبرة غير ملزمة للقاضي.

و بالتالي فان الدليل التكنولوجي يحتاج الى اجراءات كثيرو من بينها:

-التأكد ان التسجيلات تتعلق بالمتهم،

-التأكد من التسجيلات و الصور و الفيديوهات خالية تمام من التزوير و التحريف.

-التأكد من وضوح التسجيلات و الصور و الفيديوهات فان كان هناك تداخل في الاصوات او الصور او الفيديوهات فان هذا الدليل يعتبر غير واضح يعرضه الى عدم القبول.

---

[1] خويل بلخير ، الحماية الدولية و الاقليمية للحق في الحياة الخاصة،(مقال منشور)، مجلة العلوم القانونية و الاجتماعية، العدد7،ص112.

ب/ العوائق الواقعية:

لقد عملت الجزائر على غرار دول العالم على مواكبة التطور التكنولوجي من خلال عصرنة العدالة و ربطها بالتكنولوجيا الحديثة للمساهمة في تطوير القطاع العدالة و جعله يساير التطورات التكنولوجية من خلال برامج و قوانين تساهم في التحكم في التكنولوجيا التي اصبحت واقع لابد منه و هذه القوانين لا تزال لم تبلغ المستوى المطلوب.

و من ابرزها قانون 03/15 الصادر في 01 فيفري 2015 و المتعلق بعصرنة العدالة حيث اكد على وضع منظومة معلوماتية مركزية لوزارة العدل[1].

– ارسال الوثائق و المحررات القضائية بطريقة الكترونية،

– استخدام تقنية المحادثات المرئية عن بعد في الاجراءات القضائية،

بالإضافة الى الامر 02/15 المتعلق بقانون الاجراءات الجزائية الذي اعتبر ان استعمال الوسائل التقنية في سماع الشهود امرا جوازي.[2]

كل هذه القوانين و غيرها دلت دلالة واضحة على صعوبة استعمال الوسائل التكنولوجية كدليل قطعي للإثبات بسبب المشاكل التقنية التي تواجه قطاع العدالة و صعوبة التحكم في هذه التكنولوجيا المعقدة من خلال الصعوبات التقنية الحالية و المفترضة في ظل القرصنة الالكترونية التي تؤثر على التعامل بالأنترنت[3].

الخاتمة:

[1] بلباقيبومدين ، قانون عصرنة العدالة وأثره في تحقيق المبادئ الاساسية للتقاضي " قراءة في مشروع القانون 03/15 المتعلق بعصرنة العدالة ،(مقال منشور)، مجلة العلوم القانونية و الاجتماعية، 2021 ،المجلد 05 العدد 4،ص 1266.

[2] المادة(65) مكرر 27 من القانون 02/15 المعدل لقانون الاجراءات الجزائية.

[3] مريم بالطة ، أسيا برغيت، الامن المعلوماتي في مواجهة القرصنة الالكترونية ،(مقال منشور)، مجلة راسات في حقوق الانسان ، المجلد 06العدد 01 ، 2022،ص 14.

لقد كان للتطور التكنولوجي الاثر الايجابي على العلاقات الفردية و الجماعية بسبب تطور الاتصالات المتطورة حيث أن الاهتمام بهذه الوسائل كان نتيجة للآساب التالية:

-الاستعمال الواسع لهذه الوسائل مما أدى الى تنافس بين الشركات المصنعة لزيادة الارباح،

-تعدد الاستعمال للوسائل التكنولوجية الحديثة حيث أصبح لها دور لا يمكن الاستغناء عنه،

-التوجه نحو ضرورة العمل بهذه الوسائل بسبب استعمالها في الدراسة عن بعد والصحة والنقل وغيرها من نواحي الحياة.

ونظرا لهذه الاهمية نستنتج من خلال هذه الدراسة النتائج التالي:

-عدم القدرة على مسايرة التطور التكنولوجي نتيجة المنافسة الدولية على ذلك،

-عدم وجود منظومة قانونية كافية للحماية من استعمال هذه التكنولوجيا.

وعلى هذا الاساس نقترح التوصيات التالية:

-احاطة استعمال الوسائل التكنولوجية بالضمانات الكافية من خلال اعداد منظومة قانونية قادرة على تتبع التطور التكنولوجي،

- العمل على اعتبار الادلة المأخوذة من هذه الوسائل قابلة للتأكد والمراجعة .

- توسيع نطاق التحقيق في هذه الجرائم عن طريق التعاون الدولي،

- تحديث الخبرة من خلال الدراسات الحديثة و الندوات والملتقيات التي تهتم بالتطور التكنولوجي واثره على حياة الناس،

- تعديل القوانين وتقويتها بالوسائل المادية والمعنوية لمكافحة الجرائم الالكترونية المرتبة بتطور الوسائل التكنولوجية.

المراجع:

أ- القوانين :

1/ الامر رقم 155/66 الصادر في 08 جوان 1966 المتضمن قانون الاجراءات الجزائية المعدل والمتمم بالامر 02/15 الصادر في 23 جويلية 2015.

2/ المرسوم الرئاسي رقم 337/09 الصادر في 21 أكتوبر 2009 المتضمن إحداث مؤسسة إنجاز المراقبة بواسطة الفيديو، الجريدة الرسمية، عدد 61 الصادر في 2009/10/25 .

3/ المرسوم الرئاسي 228/15 الصادر في 22 أوت 2015 المتضمن تحديد القواعد المتعلقة بتنظيم النظام الوطني للمراقبة بواسطة الفيديو وسيره، الجريدة الرسمية العدد 45 الصادر في 12 أوت 2015.

ب- الكتب

1/ أحمد غاي، ضمانات المشتبه فيه اثناء التحريات الاولية، دار هومة للطباعة والنشر والتوزيع ، الجزائر،2005.

2/ أحسن بوسقيعة، التحقيق القضائي، دار هومة للطباعة والنشر والتوزيع ، الجزائر، 2009.

3/ عبد الله أوهايبية، شرح قانون الاجراءات الجزائية الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012.

4/ فضيل العيش، شرح قانون الاجراءات الجزائية بين النظري والعملي، منشورات أمين، الجزائر،2013.

5/ قادري أعمر، أطر التحقيق، دار هومة للطباعة والنشر والتوزيع ، الجزائر،2013.

6/ قادري أعمر، التعامل مع الافعال في القانون الجزائي العام، دار هومة للطباعة والنشر والتوزيع، الجزائر،2015.

7/ محمد علي سكيكر، تحقيق الدعوى الجنائية واثباتها في ضوء التشريع والفقه والقضاء، دار الفكر الجامعي، الاسكندرية،مصر،2008.

ج- المقالات:

1/ مستاريعادل ، أحمد حسين ، حجية الادلة المستمدة من الهواتف النقالة ، (مقال منشور) ، مجلة الفكر ، العدد 15 ، 2017 .

2/ زروقي عاسيا ، الخبرة الجزائية ومدى سلطة القاضي الجزائي في تقديرها ، (مقال منشور) مجلة معالم للدراسات القانونية والسياسية ، المجلد 03 العدد 01 ، 2019 .

3/ بلباقي بومدين ، قانون عصرنة العدالة وأثره في تحقيق المبادئ الاساسية للتقاضي " قراءة في مشروع القانون 03/15 المتعلق بعصرنة العدالة ،(مقال منشور)، مجلة العلوم القانونية و الاجتماعية، 2021 ، المجلد 05 العدد 04.
4/ مريم بالطة ، أسيا برغيت ، الامن المعلوماتي في مواجهة القرصنة الالكترونية ،(مقال منشور)، مجلة راسات في حقوق الانسان ، المجلد 06 العدد 01 ، 2022،.
5/ خويل بلخير ، الحماية الدولية و الاقليمية للحق في الحياة الخاصة،(مقال منشور)، مجلة العلوم القانونية و الاجتماعية، العدد7.

الإسم و اللقب:غزلاوي فاطمة الزهراء

الرتبة العلمية:طالبة دكتوراه

المؤسسة: جامعة الدكتور مولاي الطاهر سعيدة

رقم الهاتف:0771-76-87-86

الإسم و اللقب: بن عائشة زكرياء

الرتبة العلمية:طالب دكتوراه

المؤسسة:جامعة الدكتور مولاي الطاهر سعيدة

رقم الهاتف:85-68-49-79-07

ghezlaouifatimazahra@gmail.comzakaria11benaicha@gmail.com

zakaria.benaicha@univ-saida.dz

عنوان المداخلة: دور الأدلةالرقمية في الإثبات الجنائي كألية لمجابهة الجريمة الالكترونية.

المحور المشارك به : المحور الخامس :تاثير الوسائل العلمية الحديثة على الاثبات الجنائي

الملتقى الدولي الإفتراضي الموسوم بـ :القانون الجنائي في ظل التطور التكنولوجي –إشكالات ومعالجات–

المنظم من طرف جـــامعة الجزائر1–بن يوسف بن خدة– University of Algiersكليـــــة الحقــوق

الملخص

يبين هذا البحث الطبيعة الخاصة للدليل الرقمي وخصائصه، ومزاياه، وأنواع الأدلة الرقمية وأشكالها. كما يتناول البحث حجية الدليل الرقمي في الإثبات التي تتوقف على مشروعية الحصول عليه؛ بأن يكون وليد إجراءات صحيحة. وقد ظهر لنا وجود اتجاه تشريعي وقضائي وفقهي يجيز اللجوء إلى المراقبة الإلكترونية، كوسيلة حديثة للإثبات، وللكشف عن الجرائم الخطيرة أو بعض الجرائم التي تهدد النظام العام، وهذا الاتجاه يقضي بإعطاء الدليل الرقمي قوة وقيمة إثباتية بصرف النظر عن قيمته القانونية أو افتقاره للنزاهة. وبالنسبة لمكونات الحاسوب المعنوية ذهب رأي إلى صلاحيتها للتفتيش، تحقيقاً لغاية المشرع من التفتيش؛ وهي البحث عن الأدلة التي تساعد في كشف الحقيقة، وإن كان موضع البحث شيئاً معنوياً. إن تمتع الدليل الرقمي بحجية في الإثبات الجزائي رهن بقبوله من القاضي، وهذا يستلزم أن يكون استخلاص الدليل وحفظه تم بصورته الأصلية، من دون أن يتعرض لأي عبث أو تلف، وبعد التحقق من سلامة الحاسوب الآلي ودقته، ومن حفظ مخرجات الحاسوب وتخزينها في بيئة مناسبة. كما يستلزم أيضاً أن يكون للدليل أصل ثابت في أوراق الدعوى، وأن القاضي الجزائي أتاح الفرصة أمام الخصوم للإطلاع عليه ومناقشته تفصيلاً في الجلسة، وأخيراً أن يكون اقتناع القاضي بالدليل الرقمي مؤسساً على جزم ويقين، ومستنداً إلى حجج ثابتة وقطعية، تجعل هذا اليقين ثابتاً لا يناقضه شك أو احتمال آخر.

الكلمات المفتاحية : الدليل الرقمي ، حجية الدليل ، القطب الجزائي ، التحقيق الجنائي الالكتروني ، الجريمة الالكترونية

Abstact :

Digital evidence and its evidence in criminal evidence This research examines the special nature of the digital guide, its characteristics, its advantages, and the types and forms of digital evidence. It also shows that there is a legislative, judicial and jurisprudential trend that permits the use of electronic surveillance as a modern means of proof and to detect serious crimes or certain crimes that

threaten the system. General, which provides digital evidence and evidence of strength and value regardless of its legal value or lack of integrity. The jurisprudential opinion that goes to the validity of the computer components of the inspection is also likely to reach the legislator's goal of searching for evidence that helps in uncovering the truth, even if the subject is something of a moral nature. The authenticity of the digital manual depends on its acceptance by the judge. This requires that the evidence should be extracted and saved in its original form, that it was not subjected to tampering or damage, and that the computer's integrity and accuracy were checked. It also requires that the evidence has a fixed origin in the documents of the case, and that the criminal judge provided the opportunity for the litigants to view it and discuss it in detail at the hearing. Finally, the judge's conviction of the digital evidence must be based on certainty and certainty and based on fixed and categorical arguments. Contradicted by doubt or otherpossibility.

المقدمة

يعد التطور الهائل الذي شهده كل من مجال تقنية المعلومات ومجال الاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد المحور الأساسي الذي قامت عليه تقنية المعلومات، إذ أصبحت مختلف القطاعات . تعرف المعلومات بصفة عامة بأنها: "مجموعة الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو للتفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية، لما تتميز به من عنصري السرعة والدقة في تجميع المعلومات وتخزينا ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدة دول، حتى أصبح يطلق على هذا العصر عصر المعلومات وبالرغم من أهمية الوسائل الرقمية وإيجابياتها في استعمالها مثلما ذكرنا آنفا، إلا أن الاستخدام غير بالجرائم الالكترونية أو الجرائم المعلوماتية أو المشروع لها قد أدى إلى ظهور نوع جديد من الجرائم سميت جرائم الانترنت.

وللجريمة المعلوماتية كغيرها من الجرائم أركانها وعناصرها، وتمر الدعوى الجنائية في شأنها بذات المراحل التي تمربها الدعوى الجنائية في شأن الجرائم العادية كالسرقة والقتل إلا أن ما يميز هذه الجريمة أنها تقع في بيئة افتراضية تقنية لا تترك أية آثار محسوسة، إذ يغلب عليها أنها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق تلاعبهم بالبيانات، والتي ترتكب أحيانا – إن لم نقل في الغالب– في غفلة من المجني عليه، كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعقد أمركشف الجريمة وإثباتها[1].

وأما في مجال تعامل جهات التحقيق مع الأدلة الجنائية فإن هذه الأخيرة مقبلة على الانتقال من مرحلة التعامل مع الأدلة المادية الملموسة معروفة المصادر إلى مرحلة التعامل مع الأدلة الرقمية المنتشرة في أماكن افتراضية، وهو أمر لا محالة يثير مشكلات مهنية وأخرى قانونية ينبغي تحديدها بوضوح توطئة لوضع الحلول المناسبة لعلاجها[2]. وعليه حتى يتسنى لنا الغوص في هذه الدراسة جدير

---

[1] بوسائل وأشكال مختلفة". ولقد ذهب البعض إلى القول: إنه من الصعب أو المستحيل وصف المعلومة بدقة وما يمكن فقط هو إدراك أثرها. لذلك فقد اجتهد الباحثون من تخصصات وثقافات مختلفة في وضع تعاريف منها ما أورده الأستاذ "Catala" من تعريف حين عدها "رسالة ما معبر عنها في شكل يجعلها قابلة للنقل أو للإبلاغ للغير"، كما عرفت أيضا بأنها: "النقل المجرد لوقائع معينة تم الحصول عليها من مصادر متعددة. /أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي الاسكندرية، ط 02، 2006، ص87.

[2] محمد حماد مرهج البهيي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، 2004،

بنا أن نحدد الإشكالية والمتمثلة في محاولة التعرف على ماهية الدليل الرقمي، ومدى حجيته أمام جهات التحقيق والمحاكمة، وماهي أهم الضوابط الواجب مراعاتها عند استخدام هذا الدليل. وهو ما سيتم الإجابة عنه في هذه الدراسة وقبل هذا كله رأينا إبراز مفهوم الجريمة الالكترونية وأخيرا شفعنا هذه الورقة البحثية بخلاصة تناولنا فيها أهم الاستنتاجات والتوصيات

المبحث الأول: مفهوم الجريمة المعلوماتية

يعد تحديد مفهوم الجريمة المعلوماتية بوصفها ظاهرة إجرامية مستحدثة أول خطوة ثم التعرف عليها من جميع جوانبها القانونية، خاصة إذا علمنا أنه لا يوجد مصطلح قانوني موحد للدلالة على هذه الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر بسبب ذاتيتا وتميزها عن غيرها من الجرائم التقليدية.

وإذا كان التطور المتجدد والمستمر للمعلوماتية يمنع نصوص التجريم الحالية عن مواكبة ما يطرأ من صور إجرامية مستحدثة في مجال المعلوماتية إلا أن وضع قواعد قانونية مبنية على تعريف منطقي تنظم أوجه الحماية الجنائية أفضل بكثير من ترك ما يستجد[1]. كما تجدر الإشارة إلى أهم ما يميز هذه الجريمة عن غيرها من الجرائم التقليدية، وهو ما سيتم إبرازه من خلال المطالب الآتية.

المطلب الأول: تعريف الجريمة المعلوماتية

لقد ذهب فقهاء القانون في تعريف الجريمة المعلوماتية مذاهب شتى ووصفوا تعريفات مختلفة تتمايز وتتباين تبعا لموضوع العلم المنتمية إليه وتبعا لمعيار التعريف ذاته، فظهر في ذلك اتجاهان: أولهما يضيق من مفهومها والثاني يوسعه[2].

الفرع الأول: الاتجاه المضيق في مفهوم الجريمة المعلوماتية

يذهب أنصار هذا الاتجاه إلى حصر الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها، بما يجعلها في حاجة إلى نصوص خاصة تتلاءم مع طبيعتها التي تختلف عن غيرها من الجرائم المفتقرة إلى هذه الدرجة من المعرفة لتصبح جرائم عادية تتكفل ما النصوص العقابية العامة.

ومن التعريفات التي وضعها أنصار هذا الاتجاه أن الجريمة المعلوماتية هي كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، ولملاحقته والتحقيق فيه من ناحية أخرى، وفي هذا الاتجاه أيضا عرفها الفقيه دافيدتومسون أنها جريمة يتطلب لاقترافها توفر معرفة بتقنية الحاسب لدى فاعلها[3]، وحسب هذا التعريف فإنه يشترط أن يكون مرتكب الجريمة المعلوماتية على درجة كبيرة من العلم بتكنولوجيا الحاسبات، وهذا المفهوم قد أخذت به وزارة العدل الأمريكية في تقريرها الصادر عام 1989 بعد تبنيها لدراسة وضعها معهد ستانفورد الدولي للأبحاث حينما عرف الجرائم المعلوماتية بأنها أية جريمة لفاعلا معرفة فنية بالحاسبات تمكنه من ارتكابها.

وفي هذا الاتجاه أيضا عرفها جانب من الفقه بالنظر إلى معيار نتيجة الاعتداء، إذ يرى الأستاذماس(Mass) أن المقصود بالجريمة المعلوماتية هي تلك الاعتداءات التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح، كما عرف الأستاذ باركير (Parker) الجريمة المعلوماتية بأنها كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنها خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل[4].

وهناك جانب آخر أخذ في تعريفه للجريمة المعلوماتية بمعيار موضوع الجريمة كما ذهب إليه الفقيه روزانبلات (Rosenblatt) إذ عرفها على أنزها "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها[5].

---

[1] خالد عباد الحلي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة، الأردن، ط01، 2001، ص 30.

[2] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة 1994، 173

[3] أحمد أنور بدر، الجديد في الاتصال العلمي، دار الثقافة العلمية، مكتبة كلية الأداب، القاهرة 2001، ص17.

[4] محمد بن نصر السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والأنترنت، مذكرة ماجستير في العلوم الشركية، جامعة نايف للعلوم الأمنية، الرياض، 2004، ص 34.

[5] نهلا عبد القادر المومني، الجريمة المعلوماتية، ط 02، 2010، دار الثقافة، ص 48.

الفرع الثاني: الاتجاه الموسع لمفهوم الجريمة المعلوماتية

إزاء الانتقادات التي وجهت للاتجاه الأول حاول بعض رجال الفقه تعريف الجريمة المعلوماتية على نحو واسع لتفادي أوجه القصور التي شابت تعريفات الاتجاه الضيق في التصدي لظاهرة الإجرام المعلوماتي إذ أن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يضفي عليه وصف الجريمة المعلوماتية وقد تباينت مواقف أنصار هذا الاتجاه هو الآخر حسب نظرتهم إلى الدرجة التي يمكن أن تمتد إليها الجريمة المعلوماتية، فيذهب فريق من الفقهاء إلى تعريف الجريمة المعلوماتية إلى أنها كل سلوك إجرامي يتم بمساعدة الحاسب الآلي، ليوافق هذا ما جاء به الفقيه Merwe الذي يرى أن الجريمة المعلوماتية تتمثل في الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي، كما عرفها الفقيهين Richardtotty و HardcastelAnothony على أنا جرائم يكون فيها للحاسب دور إيجابي أكثر منه سلبي[1].

الفرع الثالث: نقد الاتجاهين

مما تقدم ذكره فيما يتعلق بالاتجاه الأول يلاحظ أن هذه التعريفات ضيقت في مفهوم الجريمة المعلوماتية إذ حصرتها في الحالات التي تتطلب أن يكون مقترف هذه الجريمة متمتعا بقدر كبير من المعرفة التقنية لارتكابها[2] .

أما فيما يتعلق بالاتجاه الثاني نجده قد وسع من مفهوم الجريمة المعلوماتية إذ يؤخذ عليه هذا التوسع الذي من شأنه أن يصبغ وصف الجريمة المعلوماتية على أفعال قد لا تكون كذلك لمجرد مشاركة الحاسب الآلي في النشاط الإجرامي، ولا يمكن القبول بهذا التوجه فقد لا يعدوا أن يكون الحاسب الآلي محلا تقليديا في بعض الجرائم كسرقة الحاسب ذاته أو الأقراص أو الأسطوانات المضغوطة مثلا، فلا يمكن إعطاء وصف الجريمة المعلوماتية على سلوك الفاعل لمجرد أن الحاسب أو إحدى مكوناته المادية كانت محلا لفعل الاختلاس أو السرقة[3].

وأمام هذا النقاش الفقهي والاختلاف الحاصل في شأن تحديد مفهوم هذه الجريمة دفع المهتمون بدراسة هذا النمط الجديد من الإجرام إلى بذل جهد كبير من أجل الوصول إلى تعريف مناسب يتلاءم مع الجريمة المعلوماتية، ذلك أن عدم الاتفاق على تعريف هذه الظاهرة الإجرامية إنما يؤدي إلى إثارة عدد من المشكلات العملية يتمثل أهمها في صعوبة تقدير حجم الظاهرة وتعذر إيجاد الحلول اللازمة لمواجهتها، وكذا صعوبة تحقيق التعاون الدولي لمكافحتها. إلا أن المتفق عليه أن فكرة المعلوماتية هي الفكرة الجوهرية والمركزية في دراسة هذه الظاهرة الإجرامية، ذلك أن المعلوماتية هي شرط مفترض لقيام هذا النوع من الجرائم[4].

وبعد استعراضنا لتعريف الجريمة المعلوماتية وفقا لهذين لاتجاهين فإننا نؤيد ما ذهبت إليه الأستاذة نائلة عادل قورة والأستاذ محمد عبد الله أبو بكر وغيرهم من الأساتذة، والذين يرون – وبحق– أن أي تعريف للجريمة المعلوماتية يجب أن تراعى فيه عدة اعتبارات مهمة وهي .

1/ يجب أن يتلاءم هذا التعريف مع فكرة عالمية المعلومات والاتصالات، بمعنى أن يكون التعريف مفهوما ومقبولا على المستوى العالمي

2/ يجب أن يراعى في هذا التعريف التطور المتلاحق لتكنولوجيا المعلومات والحاسبات الآلية بصفة خاصة، بحيث لا يقتصر أي تعريف للجرائم المعلوماتية على التكنولوجيا الراهنة بل يسمح باستيعاب ما قد يستحدث من صور للجريمة المعلوماتية نتيجة لهذا التطور.

---

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن،منشورات الحلبي الحقوقية، ط 01، 2012، ص 65.

[2] محمد أمين الشوابكة، جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، دار الثقافة، ط 01، 2009، ص08.

[3] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية، كلية القانون، جامعة الكوفة، العدد السابع، 2008، ص 12.

[4] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2002، ص 33.

ومن ثم يرى الأساتذة أن الجريمة المعلوماتية هي "كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دورا لإتمامه على أن يكون هذا الدور على قدر من الأهمية " ولا يختلف الأمر سواء كان الحاسب الآلي أداة لإتمام النشاط الإجرامي أم كان محلا له، ففي جريمة الإتلاف قد ينصب نشاط الفاعل على الحاسوب ذاته أو على أي من مكوناته المادية، وفي هذه الحالة لا يعدو الحاسوب محلا ماديا ينصب عليه سلوك الجاني الإجرامي دون أن يكون لوجوده أي دور في الجريمة المعلوماتية، أما إذا انصب فعل الاتلاف على المكونات المنطقية للحاسوب (كالمعلومات أو البرامج أو أنظمة التشغيل)، فإن للحاسب ونظامه في هذه الحالة دورا مهما لإتمام الجريمة المعلوماتية[1].

موقف المشرع الجزائري من الجريمة المعلوماتية

أمام الانتشار الواسع لظاهرة الجريمة المعلوماتية حاول المشرع الجزائري إدخال تعديلات على قانون العقوبات لسد ما كان من فراغ قانوني في هذا المجال، وكان ذلك بموجب القانون رقم 15/04 المؤرخ في 10/11/2004 المتمم والمعدل للأمر 66/156 المتضمن قانون العقوبات حيث تضمن القسم السابع مكرر منه تحت عنوان: المساس بأنظمة المعالجة الآلية للمعطيات، ونص على عدة جرائم هي:

- الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك (394 مكرر فقرة 1).
- الدخول أو البقاء المؤدي إلى تخريب نظام تشغيل المنظومة (394 مكرر 3)
- إدخال أو إزالة أو تعديل بطريق الغش معطيات في نظام المعالجة الآلية (395 مكررا).
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم (394 مكرر 2)
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المتحصل عليها في هذا القسم (394 مكرر 2).

ودائما في ذات الغرض أصدر المشرع الجزائري قانونا خاصا بالجريمة المعلوماتية بموجب القانون 09/04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2].

لينص في الفقرة أ من المادة الثانية منه على أن القصد من جريمة الكترونية هو كل جريمة تتضمن مساسا بأنظمة المعالجة الآلية للمعطيات المحددة والمذكورة سابقا في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية[3]

كما عرف المنظومة المعلوماتية في الفقرة ب من ذات المادة على أنها أي نظام معلوماتي منفصل أو مجموعة من الأنظمة أو البرامج المتصلة ببعضها بعضا، يقوم أحدها أو كلها بمعالجة الكترونية لمعطيات رقمية تنفيذا لبرنامج معين.[4]

أما فيما يتعلق بالجانب الإجرائي فقد تم إدراج بعض الإجراءات الجزائية الخاصة بجرائم نظم المعلومات من خلال تعديل قانون الاجراءات الجزائية الأول 14/04 المؤرخ في 10 نوفمبر 2004 والثاني قانون 22/06 المؤرخ في 20 ديسمبر 2006 المتعلق

---

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الاقتصادية (دراسة نظرية وتطبيقية) دار النهضة العربية، القاهرة، 2003، ص 23./محمد عبد الله أبو بكر، موسوعة جرائم المعلوماتية " جرائم الكمبيوتر والانترنت"، المكتب العربي الحديث، الاسكندرية، 2011، ص 13.

[2] الجريدة الرسمية، العدد 47 المؤرخ في 25 شعبان 16 1430 أوت 2009، ص 05 وما بعدها.

[3] انظر نص الفقرة أ من المادة الثانية من القانون 09/04 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع السابق، ص05.

[4] انظر نص الفقرة ب من المادة الثانية من القانون 09/04، المرجع السابق.

بتوسيع اختصاص بعض المحاكم المختصة واختصاص وكيل الجمهورية وقاضي التحقيق (المواد من 37— 40 و329) وكذا توسيع صلاحيات الضبطية القضائية من خلال تمديد الاختصاص المحلي إلى كامل التراب الوطني (المادة 16)

تضمّن العدد الأخير، للجريدة الرسمية، النص التشريعي، المتعلق بإنشاء القطب الجزائي المتخصص في الجرائم السيبرانية، الذي أمر رئيس الجمهورية، عبد المجيد تبون بالإسراع في تنصيبه. وسيختص بالمتابعة والتحقيق «والحكم» في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا وحتى تلك العابرة للحدود.

تباشر الهيئة القضائية الجديدة، المكلفة بالتصدي لما بات يعرف بحرب الجيل الرابع، مهامها، بموجب صدور الإطار القانوني الخاص بها في العدد 65 للجريدة الرسمية، المؤرخ في 26 أوت 2021.

ووقع رئيس الجمهورية، عبد المجيد تبون، الأمر رقم 21-11 يتم الأمر 66-155 المتعلق بقانون الإجراءات الجزائية، يتضمن إنشاء «القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1].«

ووفق المادة 211 مكرر 22، يتم تنصيب القطب على مستوى محكمة مقر مجلس قضاء الجزائر، يختص «بالمتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرابطة بها.«

ويعرف الجرائم المتصلة بهذا المجال «كل جريمة ترتكب أو يسهل ارتكابها، باستعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أية وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال.«

وستسند مسؤولية إدارة وتنفيذ المهام الموكلة للقطب الذي أمر رئيس الجمهورية، باستحداثه، على مستوى اجتماع للمجلس الأعلى الأمن مطلع شهر أوت، إلى رئيس للقطب، ووكيل الجمهورية وقاضي التحقيق، والذين يمارسون صلاحياتهم في كامل الإقليم الوطني، بحسب نص المادة 211 مكرر. 23.

ويحدد النص التشريعي الجديد، 5 جرائم رئيسية مرتبطة بتكنولوجيات الإعلام والاتصال، يختص فيها وكيل الجمهورية لدى القطب وقاضي التحقيق ورئيس ذات القطب «بالمتابعة والتحقيق والحكم»، بمعنى إصدار أحكام قضائية ضد المتورطين، بعد متابعتهم والتحقيق بشأن الأفعال المنسوبة إليهم.

وتتصدر هذه الجرائم، « كل جريمة تمسّ بأمن الدولة والدفاع الوطني»، إلى جانب جرائم نشر وترويج الأخبار الكاذبة بين الجمهور من شأنها المساس بالأمن والسكينة العامة أو استقرار المجتمع.

وسيتابع كل من ينشر ويروج أخبارا مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية، ولم يغفل النص التشريعي الهجمات السيبرانية على الأنظمة المعلوماتية للمنشآت الوطنية والتي تقدر بالآلاف يوميا، قصد القرصنة وتدمير قواعد البيانات السرية.

حيث وضع المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية، ضمن الجرائم التي يختص بها القطب، وكذا الإتجار بالأشخاص أو الأعضاء البشرية أو تهريب المهاجرين، وجرائم التمييز والكراهية.

وتنشط شبكات تهريب المهاجرين والإتجار بالبشر عبر وسائط التواصل الاجتماعي، والتي يستغلها البعض منصة، لبث سموم الفتنة والفرقة والتمييز، بغرض إثارة النعرات وضرب تجانس المجتمع.

وبعد صدور الإطار القانوني للقطب الجزائي، لم يتبق سوى ضبط الهيكل التنظيمي له، من خلال تعيين رئيسه ووكيل الجمهورية وقاضي التحقيق. في وقت سبق وأكد رئيس الجمهورية، أنه تم توفير كافة الوسائل التقنية والأكثر تطورا، من تعقب وتحديد مواقع أكثر «بروتوكلات الأنترنت (عناوين الآي بي) « تعقيدا.

---

[1] الأمر رقم 21-11 يتم الأمر 66-155 المتعلق بقانون الإجراءات الجزائية، يتضمن إنشاء «القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال«العدد 65 للجريدة الرسمية، المؤرخ في 26 أوت 2021.

ووفق للمادة 211 مكرر، 25. فإن القطب سيختص في «الجرائم المرتبطة بجرائم تكنولوجيات الإعلام والاتصال الأكثر تعقيدا»، ويقصد بها «الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة آثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العموميين وتتطلب وسائل تحري خاصة أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي.«

إنشاء القطب الجزائي المتخصص في الجريمة السيبرانية، سيضاف إلى القطب الاقتصادي والمالي، كهيئة نوعية متخصصة مسلحة بوسائل تقنية جد متطورة، لمكافحة جرائم خطيرة تهدد أركان الدولة، وسيباشر مهامه بالنظر في قضايا معروضة أمام الجهات القضائية تقع ضمن اختصاصه.

المطلب الثاني: خصائص الجريمة المعلوماتية

تتميز الجريمة المعلوماتية بخصائص وسمات تميزها عن غيرها من الجرائم الأخرى، فأهم ما يميز هذا النوع من الجرائم هو نعومتها وبعدها عن العنف إذ لا تتطلب لارتكابا الشدة ولا استعمال الأدوات الخطرة كالأسلحة الممنوعة أو التلاعب ، ولا تحتاج إلى مداهمات وكسر للأبواب أو تسلق للجدران فنقل بيانات بالأرصدة البنكية مثلا لا تحتاج إلا إلى لمسات أزرار، ثم إن الجريمة المعلوماتية تمتاز أيضا بإمكانية ارتكابها عن بعد فلا تتطلب لوجود فاعل في مكان الجريمة بل يمكنه تنفيذها عن بعد، فالفاعل القائم على الحاسوب في أحد المصارف في تونس مثلا يستطيع تحويل مبلغ من المال إلى أحد فروع المصارف في برلين في ألمانيا، وإن نسبة معتبرة من الجرائم المعلوماتية ترتكب عبر شبكات الانترنت حيث يكون الجاني في دولة والمجني عليه في دولة أخرى مما جعل التعاون الدولي أمرا حتميا لمكافحة هذه الظاهرة الإجرامية الجديدة[1].

أولا: الجريمة المعلوماتية متعدية الحدود (عابرة للوطنية):

إنه وبعد ظهور شبكات المعلوماتية (لأنترنيت) لم تعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر مختلف الدول، فالقدرة التي تتمتع با الحاسبات الآلية في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الأميال أسفر عنها تضرر أماكن متعددة في دول مختلفة بهذه الجريمة في آن واحد. فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي في بلد آخر وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث، أو القيام بإعداد أحد البرامج الخبيثة (Vérus) في بلد ما، ثم ينسخ هذا البرنامج ويرسل إلى مختلف الدول في العالم[2].

ثانيا: صعوبة اكتشاف الجريمة المعلوماتية وإثباتها:

تقع الجريمة المعلوماتية في بيئة افتراضية تقنية لا تترك أية آثار محسوسة، إذ يغلب عليها أزها تتم في الخفاء لأن الجناة يعمدون في كثير من الأحيان إلى إخفاء نشاطهم الجرمي عن طريق تلاعبهم بالبيانات، والذي يتحقق أحيانا إن لم نقل في الغالب في غفلة من المجي عليهم، كما أنه من السهل عليهم تدمير الأدلة ومحوها مما يعقد أمركشف الجريمة وإثباتها [3].

كم أن من بين الأسباب التي تقف وراء صعوبة اكتشاف الجريمة المعلوماتية وإثباتها وضعية المجني عليهم أنفسهم، ذلك أن هؤلاء قد يؤدون دورا رئيسيا في ذلك من خلال الإحجام عن الإبلاغ عنها حالة اكتشافها، حيث تحرص أكثر الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك وألحقت بها خسائر فادحة من جراء ذلك عن عدم الكشف عما لحقها من إجرام معلوماتي حتى بين موظفيها،

[1] محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان 2005، ص 353.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامي، ط 01، 2009، ص 08.

[3] محمد حماد مرهج البهيي، مرجع سابق، ص 165.

وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنبا للإضرار بسمعتها ومكانتها وهزا للثقة في كفاءتها .[1]

المطلبالثالث: ماهية الدليل الرقمي

يعد الدليل الرقمي من الأدلة الجنائية المستحدثة في نطاق الإثبات الجنائي، جاء بغرض التصدي لنوع مستحدث من الجرائم ألا وهي الجرائم الرقمية، وفي سبيل دراسة الدليل الرقمي كغيره من الأدلة الجنائية لابد من التطرق لماهية الدليل الرقمي.

الفرع الأول: تعريف الدليل الرقمي

سنتتعرف على تعريف الدليل الرقميو ما المقصود منه.و دور القضاء في تعريفه و تمييزه عن ما يشابهه.

–لغةيعرف الدليل في اللغة بأنه المرشد، والكاشف، وما يتم الإرشاد به، وما يستدل به، والدليل الدال، والجمع أدلة ودلالات.[2]

– الاصطلاح:

يقصد بالدليل قانونا: الوسيلة الي يستعين بها القاضي للوصول إلى الحقيقة المنشودة لإعمال حكم القانون عليها أو هو الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتري إليه، وذلك لأن الحكم هو المرحلة الحاسمة هي التي تقرر المصير النهائي في الدعوى الجزائية، وتقضي بالإدانة أو البراءة

كما عرفه قضاة المحكمة العليا بأنه البينة أو الحجة التي يستمد منها القاضي البرهان على اقتناعه بالحكم الذي يصدره، وقد يكون الدليل قوليا أو كتابيا أو علميا أو ماديا.

– فأما القولي فيتمثل في الإعتراف والشهادة.

– أما المادي فيتمثل في المعاينة والتفتيش

– أما الكتابي فيتمثل في المحاضر والتقارير التي يحررها ضابط الشرطة القضائية

– أما العلمي فيتمثل في الخبرة والبصمة الوراثية.[3]

الفرعالثاني: المقصود بالدليل الرقمي

يقصد بالدليل الرقمي بكونه الدليل الذي يجد له أساسا في العالم الافتراضي ويكشف عن الجريمة، فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات، والذي يؤدي إلى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما للجريمة باستعماله تكنولوجيات الإعلام والاتصال"

كما يعرف أيضا بأنه الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم، وذلك من أجل الربط بين الجريمة والمجرم [4].

وعلى ضوء ما تقدم يمكن القول إن الدليل في الجرائم الإلكترونية يشمل نوعين من الأدلة:

الأدلة المادية[5] في الجرائم التي تقع على التقنية الإلكترونية الرقمية وشبكاتها والأدلة المعنوية(الإلكترونية الرقمية)[6]

ويمتاز الدليل الرقمي عن الدليل المادي المأخوذ من مسرح الجريمة المعتاد بما يأتي:

---

[1] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، ط 01، 1994، ص 16.

[2] كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية، دار الفكر الجامعي، الإسكندرية، مصر، ط 2011,01، ص26.

[3] محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية، الجزائر 1999، ج 02، 327.

[4] ميسون خلف حمد الحمداني، مشروعية الأدلة الالكترونية في الإثبات الجنائي، كلية الحقوق/جامعة النهرين، 2016، 196.

[5] تنقسم الأدلة المادية إلى: جهاز الحاسب الآلي وملحقاته، جهاز الهاتف النقال، الطابعات، المودم، المرشد، الفلاش ميموري، الورق.

[6] مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، ط2008،1 ص212.

الصعوبة النسبية لتحطيم أو محو الدليل، حتى في حالة إصدار أمر من قبل الجاني بإزالته من أجهزة الكمبيوتر، فيمكن للدليل الرقمي أن يعاد تظهيره من خلال الكمبيوتر دسك.

نشاط الجاني لمحو الدليل، يسجل كدليل أيضا، حيث إن نسخة من هذا الفعل (فعل الجاني لمحو الدليل) يتم تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقا لاستخدامها كدليل إدانة ضده.

أما عن سبب التسمية بالرقمي فلأن الحواسيب الرقمية تقوم باستقبال البيانات من المستخدم بشكل متقطع وتحويلها إلى أرقام حسب نظام عددي معين ثم معالجة هذه البيانات، حيث تقوم وحدة الذاكرة الرئيسية في الحاسب الرقمي بتخزين البرامج والبيانات الداخلة ونتائج المعالجة، ويختلف طول الكلمة من حاسوب إلى آخر، وإذا طلبت تخرج على شاشة الحاسب أو الطابعة بالشكل المقروء حسب اللغة التي خزنت بمها وليس كما هي مسجلة في ذاكرته[1].

المبحث الثاني: استخدام الدليل الرقمي أمام الجهات القضائية

يحفظ الإثبات الحقوق ويصون الأنفس من أن تزهق ظلما، وينصف الناس بعضهم من بعض وتزداد أهمية الإثبات في المواد الجزائية ذلك لكون الجريمة تضر بأمن المجتمع ونظامه، ومن هنا تنشأ عنها سلطة للدولة في تتبع الجاني لتوقيع العقوبة عليه تحقيقا للردع العام والخاص، ولما كان من المحتمل أن يكون المتهم بريئا مما أسند إليه، فيجب أن تكفل له قواعد الإثبات الحق في الدفاع عن نفسه وإظهار براءته، ولذلك فإن القاضى لا يستطيع أن يقضي بالحق المدى به إلا إذا ثبت أمامه بالدليل الذي رتبه القانون له

ومن الملاحظ أن المشرع الجزائري يميز بين مرحلتين من مراحل التحقق في الجريمة، فالمرحلة الأولى التي يجمع رجال القانون على تسميتا بالتحقيق الابتدائي وهي الموكلة إلى ضباط الشرطة القضائية والمرحلة الثانية تسمى بالتحقيق القضائي والتي يقوم مها كل من قاضي التحقيق وغرفة الاتهام. وهو ما سيتم التطرق إليه فيما يأتي

المطلب الأول: معاينة وتفتيش مسرح الجريمة:

على الرغم من وجود تشابه كبير بين التحقيق في جرائم الانترنت وبين التحقيق في الجرائم الأخرى فري جميعا تحتاج إلى إجراءات تتشابه في عمومها، مثل المعاينة والتفتيش والمراقبة والتحريات والاستجواب بالإضافة إلى جمع الأدلة، كما أنها تشترك في كونها تسعى إلى الإجابة على الأسئلة المشهورة لدى المحقق، ماذا حدث؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟

الفرع الأول: المعاينة

المعاينة هي عمل من أعمال التحقيق تتطلب انتقال المحقق إلى مكان وقوع الجريمة لمعاينة حالة الأمكنة والأشياء والأشخاص، أي بمعى آخر معاينة ماديات الجريمة وهذا يقتضي سرعة لانتقال إلى مكان الجريمة قبل أن تزول معالمها أو تمتد إلى أدلتها يد العبث. وفي ذات الغرض تنص المادة 79 من ق اج يجوز قاضي التحقيق لانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات"

في كل الأحوال، فإنه عند تلقي بلاغ بإحدى الجرائم المعلوماتية وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال لمسرح الجريمة لمعاينته مع مراعاة الآتي:

1. وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الاجهزة المطلوب معاينتا وشبكاتها
2. وجود خريطة توضح الموقع الذي ستتم معاينته وتفاصيل المبنى أو الطابق موضوع البلاغ وعدد الاجهزة والخزائن والملفات ويحدد ذلك من خلال مصادر سرية لجهات الأمن.

[1] نبيل جمعة نجار، وفايز جمعة نجار، مهارات الحاسوب، الأردن عالم الكتب الحديث، 2004، ص 51.

3. تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة سواء من حيث الضبط أو التأمين أو حفظ الاوراق والمستندات المتداولة[1].

وبناء على ما تقدم يمكن القول إن معاينة الجرائم التقليدية والاطلاع على مسرح الجريمة له أهمية كيفية وقوع الجريمة وظروف وملابسات ارتكابها وتوفير الأدلة المادية التي يمكن تجميعها متمثلة في تصور عن طريق المعاينة، لكن هذه المعاينة قد لا تؤدي ذات الدور في كشف غموض الجريمة المعلوماتية وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتا إلى مرتكبها ويرجع السبب في ذلك أن مسرح الجريمة يعطي المجال واسعا أمام سلطة الاستدلالات والتحقيق في الكشف عن الجريمة والأدلة والتحفظ على الآثار المادية التي خلفتها وتحقيقا لهذ الغرض يجب أن يكون المحقق ملما بالإجراءات الاحتياطية التي ينبغي اتخاذها نحو مسرح الجريمة في الجريمة المعلوماتية والتدابير اللازمة لتأمين الأدلة وفي هذا الصدد نصت المادة 143 من قانون الإجراءات الجزائية على أن: «لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع في أن تأمر بندب خبير إما بناء على طلب النيابة العامة، وإما من تلقاء نفسها أو من الخصوم ويعد استخلاص الدليل العلمي في الجريمة المعلوماتية من المسائل الفنية التي يقوم مها الخبير، وهو يخضع لوزن القاضي وتقديره في ضوء الأدلة التي قدمت في الدعوى.

الفرع الثاني: التفتيش

يواجه ضابط الشرطة القضائية أو القاضي عندما تطرح عليه مسألة في هذا الباب – إذا بادر إلى جمع الأدلة بنفسه أو بمساعدة الضحية – احتمال إتلافها أو إبطالها من طرف المحكمة لخرقه حقوق الدفاع في كثير من الأحيان، ذلك أن القانون يحمي حرمة الحياة الخاصة للأشخاص كما هو منصوص عليه في المواد 303 و303 مكرر و303 مكررا من قانون العقوبات، فيجب أن يكون التفتيش مشروعا سواء لجهاز الحاسوب أو لدخول المكان الذي يوجد فيه ويتعين اتخاذ الحيطة والحذر فيما يتعلق بنوع البيانات المراد الحصول عليها والتمييز بين البيانات المتعلقة بالعمل وتلك المتعلقة بالشخص كبريده الإلكتروني، ومراعاة إن كان الشخص ملزما بالسر المهني فيجب اتخاذ التدابير المقررة قانونا كما هو مذكور في باب التفتيش وهناك مستندات تكون محمية برقم سري فيتعين استعمال البرامج المناسبة لإزالة حمايتها .[2]

ودائما في هذا المجال وردت المادة الخامسة من القانون 09/04 المندرجة تحت الفصل الثالث المعنون بالقواعد الإجرائية تفتيش المعطيات الالكترونية لتنص على جوازلجوء السلطات القضائية المختصة وكذا

ضباط الشرطة القضائية إلى الدخول إلى منظومات معلوماتية محددة بغرض التفتيش ولو عن بعد، دون خروج على الإجراءات الجزائية المذكورة سابقا وفي الحالات المنصوص عليها في المادة الرابعة من ذات القانون، وهذه المنظومات هي كالتالي:

1. منظومة معلوماتية أو جزء منها وكذا المعطيات الرقمية المخزنة فيها
2. منظومة تخزين معلوماتية.[3]

ولتأمين عملية التفتيش أجاز المشرع الجزائري في ذات المادة الاستعانة بأي شخص له دراية وخبرة بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها هذه المنظومة

الفرع الثالث: مراقبة الاتصالات الالكترونية

---

[1] عبد الفتاح بيومي حجازي، المرجع سابق، ص

[2] نجيي جمال، إثبات الجريمة على ضوء الاجتهاد القضائي، دراسة مقارنة، دار هومة، الجزائر 2012، 266.

[3]. انظر نص المادة الخامسة من القانون 09/04، المرجع السابق، ص 06.

لقد حصر المشرع الجزائري الحالات التي يجوز فيا مراقبة الاتصالات الالكترونية حفاظا منه على حرمة الحياة الخاصة للأفراد من جهة، وحفظا للنظام العام والأمن العام للدولة من جهة أخرى، وهو ما ورد في المادة الرابعة من القانون 09/04 إذ تنص على إمكانية القيام بعمليات مراقبة الكترونية في الحالات الآتية:

للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو مهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني

لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تخص الأبحاث الجارية من غير اللجوء إلى المراقبة الإلكترونية في إطارتنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1].

وجدير بالذكر أن المشرع قيد ذلك بشرط إجرائي مفاده عدم جواز اللجوء إلى إجراء المراقبة الالكترونية إلا بعد استصدار إذن كتابي من السلطات القضائية المختصة.

المطلب الثاني: الأجهزة الدولية والإقليمية الرامية إلى الكشف عن الجريمة المعلوماتية

نظرا لطبيعة جرائم الأنترنت وخصوصيتها، فقد استحدثت بعض الدول أجهزة مختصة تتولى تطبيق قوانين مكافحة الجريمة المعلوماتية وتتبع الجناة، نذكر أهمها على المستويين الدولي والوطني.

الفرع الأول: على المستوى الدولي

يكتسي الدليل الإلكتروني ومدى حجيته أهمية بالغة، وتظهر هذه الأهمية من خلال ارتباطه الوثيق والمباشر بظاهرة جديدة وهي الجرائم الالكترونية، حيث تعد من المواضيع الشائكة التي بدأت تشغل فكر فقهاء القانون الجنائي، ولعل خير دليل على ذلك كثرة المؤتمرات الدولية والاتفاقيات التي أبرمت في سبيل مكافحتها سواء على المستوى الدولي أو الإقليمي

1- مركز الشكاوى الخاصة بجرائم الانترنت:

ويعد هذا المركز من أهم المؤسسات التي ظهرت إلى الوجود في مجال مجابة جرائم الإنترنت تأسس في الولايات المتحدة الأمريكية سنة 1999. وتمت هيكلته بشكل رسمي سنة 2002 بولاية وست فرجينيا بالولايات المتحدة وهو يتلقى شكاوى من المعنيين في إطار جرائم الأنترنيت عبر العالم، وعن طريق الشبكة المعلوماتية وموقعه الرسمي (gov.http://www.ic3).[2]

وأما عن الإجراءات المتبعة أمام هذا المركز فيكون بتقديم المعلومات التالية: اسم وعنوان ورقم الهاتف والعنوان الإلكتروني للجاني- إذا كان متوفرا له- أو المنظمة المشتبه في قيامها بنشاط إجرامي: علاوة على تفاصيل تتعلق بكيفية وقوع الجريمة حسب اعتقاد مقدم الشكوى ووقت وقوعها وسبب وقوعها؛ بالإضافة إلى أي معلومات أخرى تدعم الشكوى.

وأما على المستوى الأوروبي فقد انعقدت أشغال اللجنة الأوربية في إطار مشروع:

(CyberTools On-line SearchforEvidence)(CTOSE)

إذ ضم نخبة من خبراء الدول الأوروبية سنت عام 2003 منهاجا، وحددت إجراءات موحدة بهدف التعرف على الجريمة الإلكترونية وضمان الحصول على الأدلة المثبتة لها بصفة ومن أمثلة الشركات العاملة في مجال إثبات الجريمة المعلوماتية الشركة لأمريكية (Ontrack) ذات السبق العالمي في هذا المضمار والتي امتد نشاطا إلى أوروبا، وهذه الشركات لتخصصها يمكن

[1] انظر نص المادة الرابعة من القانون 09/04، المرجع السابق، ص 06.

[2] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، ص 110

استعانة الضبطية القضائية أو النيابة العامة أو قضاة التحقيق باكجهة خبرة واستشارة فيما يتعلق بالجرائم المالية والجرائم المعلوماتية وجرائم الاستغلال الجنسي للأطفال[1].

وأما على مستوى الوطن العربي فلم تكن هناك جهود كبيرة في مجال مكافحة هذه الجرائم المستحدثة ما عدا بعض الجهود العلمية والأمنية بشكل خاص، حيث أصبحت متوالية في مجال رصد الظواهر الأمنية المصاحبة لانتشار الحسابات والأنترنت وتتبعها، ولعل اهمها المؤتمر العلمي الأول حول العالم الرقمي وجرائم الشبكات الإلكترونية المنعقد في القاهرة خلال الفترة من 5-4 مارس 2009 إذ تعرض لأول مرة بالدراسة لمسألة الإثبات الجنائي باستخدام الوسائل الإلكترونية، ومدى قبول الدليل الالكتروني في الإثبات الجنائي.[2]

الفرع الثاني: على المستوى الوطني

إلى جانب النصوص التشريعية التي سنها المشرع الجزائري لمكافحة هذه الجريمة بالكشف عنها ومعاقبها مرتكبيها تجدر الإشارة إلى الجهاز الذي استحدثه بموجب القانون 09/04 في الفصل الخامس منه والمسمى بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إذ تنص المادة الرابعة عشرة من ذات القانون على مهام هذه الهيئة نذكرها فيما يأتي:

تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجرمها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال وتحديد أماكن تواجدهم.

والمستخلص من هذه المهام أن هذه الهيئة جهاز متخصص متعاون مع غيره من الأجهزة القضائية الوطنية والدولية نذكر منها منظمة الشرطة الدولية (الأنتربول) تسعى لتوفير الأمن المعلوماتي للوطن والأفراد .

ووقع رئيس الجمهورية، عبد المجيد تبون، الأمر رقم 21-11 يتم الأمر 66-155 المتعلق بقانون الإجراءات الجزائية، يتضمن إنشاء «القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.«

ووفق المادة 211 مكرر 22، يتم تنصيب القطب على مستوى محكمة مقر مجلس قضاء الجزائر، يختص «بالمتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرابطة بها.«

ويعرف الجرائم المتصلة بهذا المجال «كل جريمة ترتكب أو يسهل ارتكابها، باستعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أية وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال.«

الفرع الثالث: الضوابط الواجب مراعاتها للحصول على الدليل الرقمي

يحتاج كشف ستر الجريمة المعلوماتية إلى طرق الكترونية تتناسب مع طبيعتها بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة، تصلح لأن تكون أدلة إثبات لمثل هذه الجرائم ذات الطبيعة الفنية والعلمية، ومن ثم نسبتا إلى فاعليا، وتدعى هذه الوسيلة بالدليل الرقمي وتجدر الإشارة إلى أن تأثير التطور التكنولوجيا لا يقف عند مضمون الدليل، وإنما يمتد هذا التأثير كذلك يجب أن تكون هذه الإجراءات المتطورة إلى الإجراءات التي يترتب عليها الحصول على هذا الدليل، ولذلك ذات طبيعة مشروعة لتحافظ على مشروعية الأدلة المتولدة منها. وهو ما سيتم التطرق إليه فيما يأتي.

---

[1] نجيمي جمال، المرجع السابق، ص 267

[2] أشرف عبد القادر قنديل، المرجع سابق، ص11.

أولا: مبدأ مشروعية الدليل

لم يورد المشرع الجزائري –كما هو معلوم – بصفة حصرية أدلة الإثبات في المادة الجزائية، غير أنه أورد أحكاما تخص صدقية الدليل ومن هذا المنطلق يفترض أن كل ما صدر من تدابير أو ما اتخذ من إجراءات أو قرارات يكون صادرا بنحو سليم ومتفق مع القانون. ولكن هذا الافتراض يمكن إثبات عكسه، فمن يدعي أن إجراء معينا اتخذ خلاف القانون فيقع عليه عبء الإثبات، فإذا كان الحق معه فيما ادعاه صار الإجراء المتخذ في حقه باطلا، أما إذا أخفق بقيت المشروعية ملازمة للإجراء فالشرعية الإجرائية إذن هي امتداد طبيعي لمبدأ شرعية الجرائم والعقوبات. وسنحاول من خلال هذا المطلب إبراز أهم الضوابط التي تجسد مبدأ مشروعية الدليل:

. الأصل في الإنسان البراءة: وفي هذا الصدد تقضي المادة 56 من الدستور الجزائري: «كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته، في إطار محاكمة عادلة تؤمن له الضمانات اللازمة للدفاع عن نفسه»، وفي ذات الغرض عمدت التشريعات الجنائية الحديثة من خلال قواعدها الإجرائية إلى تجسيد هذا المبدأ الهام على أرض الواقع، لذلك قيل إن الإجراءات هي الأخت التوأم للحرية يقينية الدليل المعتمد في الإثبات الجنائي: فلا محل لدحض مبدأ أن الأصل في الإنسان البراءةبالنسبة لهذه الأدلة فهذا مبدأ يقيي يترتب عليه أن كافة مخرجات الوسائل الإلكترونية سواء أكانت ورقية أو إلكترونية أو أقراص مغناطيسية أو مصغرات فيلمية تخضع لتقدير القاضي الجنائي، ويجب أن يستنتج منها الحقيقة بما يتفق مع اليقين ويبتعد عن الشك والاحتمال.

من خلال ما تقدم يمكن القول إن الطبيعة الخاصة بالدليل الرقمي في مجال الجريمة الإلكترونية انعكس على عمل الجهات المكلفة بالتحقيق والمحاكمة حيث يتطلب الكشف عن هذه الجرائم وإثباتا إتباع استراتيجيات خاصة من أجل تحديد نوعية الجريمة المرتكبة وشخصية مرتكبيها وكيف تمت، وهو ما يتطلب مهارة وخبرة تقنية فائقة ومتماشية مع التطور التكنولوي السريع في مجال الاعلام والاتصال.

ثانيا: الصعوبات العملية لضبط الدليل الرقمي

نظرا لطبيعة الدليل الافتراضية فمن الجدير الإشارة إلى بعض الصعوبات التي يثيرها هذا النوع من الأدلة وهي في الحقيقة تتعلق بطبيعته التكوينية من جهة (الشق الموضوعي منه)، وبإجراءات الحصول عليه من جهة أخرى (الشق الإجرائي منه) المشكلات الموضوعية للدليل الإلكتروني: وهي غالبا ما تتعلق بطبيعة الدليل ذاته، وذلك بسبب الخصائص الفيزيائية التي يتكون منها الدليل، سواء بسبب الطبيعة غير المرئية له، أو بسبب مشكلة الأصالة، أو بسبب ديناميكيته.

المشكلات الإجرائية للدليل الإلكتروني: لا تقف مشكلة الدليل الالكتروني عند طبيعته التكوينية، بل تمتد لتشمل إجراءات الحصول عليه، وتتمثل هذه الأخيرة في حالتين هما: ارتفاع تكاليف الحصول عليه، مما أدى إلى القول بأن الدولة، على الرغم من أن مسعاها الحقيقي هو تحقيق العدالة، لا تلجأ غالبا إلى أسلوب الإنفاق في هذا الإطار. أما المشكلة الثانية فتتعلق بنقص الخبرة الفنية والتقنية لدى سلطات الاستدلال والتحقيق والقضاء بمجال تقنية المعلومات[1].

خاتمة:

بناء على ما تقدم بيانه في هذه الدراسة يمكن القول انه بالرغم مما قام به شراح القانون في تحديد المقصود بالجريمة المعلوماتية إلا أن المسألة ما تزال غير مضبوطة بما يجعل هذا التعريف يلائم فكرة عالمية تكنولوجيات الإعلام والاتصال، بمعنى أن يكون التعريف

[1] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، د ط، 2015،ص228.

مفهوما ومقبولا على المستوى العالمي. كما يجب أن يراعى في هذا التعريف التطور المتلاحق لتكنولوجيا المعلومات والحاسبات الآلية بصفة خاصة، بحيث لا يقتصر أي تعريف للجرائم المعلوماتية على التكنولوجيا الراهنة بل يحتفظ بمرونته بما يسمح باستيعاب ما قد يستحدث من صور للجريمة المعلوماتية نتيجة لهذا التطور.

وأما بالنسبة لموقف المشرع الجزائري من هذه الجريمة نجد جاء بتقنيات جديدة ومعالم أخرى توضح القواعد الإجرائية في مجال تحريك الدعوى وتقفي أثار مجرمي المعلوماتية من خلال تحديد الترتيبات التقنية لمراقبة الاتصالات الإلكترونية ورصدها .

وكيفية تفتيش المنظومة المعلوماتية عن بعد ثم إجراءات حجز المعطيات المعلوماتية. والملاحظ أنه لم يغفل عن ذكر لالتزامات المنوطة بمقدمي خدمة الأنترنيت من أصحاب نوادي ومقاهي الأنترنيت، كما رسم معالم الاختصاص القضائي تحسبا للطابع الذي تكتسيه جريمة الأنترنيت وما تحمله من طابع دولي تتخطى الحدود الوطنية

وأما عن الرقمي فمن خلال هذه الدراسة تبين لنا أن هناك صعوبة تكتنف الدليل الجنائي بالنسبةللجرائم الإلكترونية سواء من حيث طبيعته. فالحصول عليه قد يحتاج إلى عمليات فنية وعلمية وحسابية معقدة كما وأن طبيعته قد تكون غير مرئية كالذبذبات والنبضات، وأنه من السهولة استخدام التقنية العلمية في إخفائه أو إتلافه، وقد يتم ذلك عن طريق التشفير وكلمات المرور السرية واستخدام الفيروسات المدمرة أو المتلفة، هذا من جهة ومن جهة أخرى نجد أن العاملين في الميدان قد لا تتوفر فيهم هذه المعرفة العلمية والفنية.

وعليه نوصي الجهات المعنية بما يأتي:

ضرورة إيجاد تنسيق وتعاون دوليين فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الكشف عن الجريمة المعلوماتية بين أفراد المجتمع الدولي، خاصة ما تعلق منا بأعمال الاستدلال أو التحقيق، سيما أن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة الواحدة عن طريق الضبط أو التفتيش في نظام معلوماتي معين هو أمر في غاية الصعوبة الاهتمام بتدريب العاملين في الساحة القضائية من خبراء ومحققين وقضاة للتعامل الأمثل مع الدليل الرقمي، بحيث يمكن الوصول إلى الحقيقة وإماطة اللثام عن هذه الجرائم تحقيقا لصالح المجتمع وأفراده.

يجب تحديث الأساليب الإجرائية المتبعة لجمع الأدلة في الجرائم المعلوماتية بما لا يعرض حقوق الأفراد وحرياتهم الخاصة للخطر عند الاثبات بدعوى مكافحة الجريمة المعلوماتية وتكريسا لهذا الغرض نقترح إصدار دليل إرشادي تقي وقانوني حول صور جرائم الحاسوب والأصول العلمية لكشفها والتحقيق فيها وأساليب التعامل مع الأدلة الإلكترونية، ومواصلة تحديث هذا الدليل بشكل دوري وكلما دعت الحاجة لذلك وتعميمه على العاملين في الميدان.

قائمة المصادر والمراجع:

الكتب

أحمد خليفة الملط ، الجرائم المعلوماتية، (ط 02)، مصر، دار الفكر الجامعي(2006)

أحمد أنور بدر، ، الاتصال العلي، (ط01)، مصر، دار الثقافة العلمية.(2001)

أشرف عبد القادر قنديل ، الإثبات الجنائي في الجريمة الإلكترونية، (د ط) الإسكندرية–مصر، دارالجامعة الجديدة(2015)

هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية، (ط 01)، مصر، مكتبة الآلات الحديثة.(1994)

كمال محمد عواد، ، الضوابط الشرعية والقانونية للأدلة الجنائية، (ط02)، الإسكندرية–مصر، دار الفكر الجامعي.(2011)

محمد حماد مرهج البهيي التكنولوجيا الحديثة والقانون الجنائي، (دط)، الأردن، دار الثقافة.(2004).

محمد عبد الله أبو بكر، ، موسوعة جرائم المعلوماتية "جرائم الكمبيوتر والأنترنت"، مصر، المكتب العربي الحد. (2011)

محمد أحمد عبابنة ، جرائم الحاسوب وأبعادها الدولية، (ط01)، الأردن، دار الثقافة.(2005)
محمد سامي الشوا، ، ثورة المعلومات وانعكاساتها على قانون العقوبات، (ط01)، القاهرة، دار النهضة العربية،(1994)
محمد أمين الشوابكة، ، جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)، (ط01)، الأردن، دار الثقافة.(2009)
محمد حماد مرهج البهيتي ، التكنولوجيا الحديثة والقانون الجنائي، (ط01)، عمان-الأردن، دار الثقافة.(2004)
محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، (ج02)، الجزائر، ديوان المطبوعات الجامعية.(1999)
مصطفى محمد موسى، ، التحقيق الجنائي في الجرائم الإلكترونية، (ط01)، القاهرة-مصر، مطابع الشرطة(2008)
نهلا عبد القادر المومني، ، الجريمة المعلوماتية، (ط02)، الأردن، دار الثقافة.(2010)
نائلة عادل محمد فريد قورة،، جرائم الحاسب الاقتصادية (دراسة نظرية وتطبيقية)، (ط 01)، مصر، دار النهضة العربية. (2003
نبيل جمعة نجار، فايز جمعة نجار ، مهارات الحاسوب، الأردن، عالم الكتب الحد. "(2004)
نجيمي جمال ، إثبات الجريمة على ضوء الاجتهاد القضائي (دراسة مقارنة)، الجزائر، دار هومة.(2012)
سامي النصراوي،، دراسة في قانون أصول المحاكمات الجزائية، (ج01)، بغداد-العراق، مطبعة دار السلام. (1976)
عادل يوسف عبد النبي الشكري، ، الجريمة المعلوماتية وأزمة الشرعية، (العدد السابع)، العراق، كلية القانون، جامعة الكوفة(2008)
عبد الفتاح بيومي حجازي، ، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، (ط01)، مصر، دار الكتب القانونية.(2002)
خالد عباد الحلبي، ، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، (ط01)، الأردن، دار الثقافة.(2001)
رشيدة بوكر، ، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، (ط 01)، لبنان، منشورات الحلبي الحقوقية(2012)
خالد ممدوح إبراهيم،، الجرائم المعلوماتية، (ط 01)، مصر، دار الفكر الجامعي. (2009)

القوانين

القانون رقم 09/04 المؤرخ في 05/08/2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 47 المؤرخ في 25 شعبان 16 1430 أوت 2009
الأمر رقم 21-11 يتم الأمر 66-155 المتعلق بقانون الإجراءات الجزائية، يتضمن إنشاء «القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال«العدد 65 للجريدة الرسمية، المؤرخ في 26 أوت 2021.

الرسائل الجامعية و المقالات

ميسون خلف حمد الحمداني، ، مشروعية الأدلة الالكترونية في الإثبات الجنائي، (مج 18). العراق، مجلة كلية الحقوق/جامعة النهرين.(2016)
محمد بن نصر السرحاني، ، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والأنترنت، مذكرة ماجستير في العلوم الشركية، السعودية، جامعة نايف للعلوم الأمنية(2004)
نادية سحتوت التنظيم القانوني للجريمة المعلوماتية أدلة إثبات الجريمة المعلوماتية، (ع 01) المركز الجامعي سوق أهراس، مجلة دراسات وأبحاث.(2009)،

الاسم و اللقب: الحاسي مريم

الرتبة العلمية: أستاذة محاضرة "ب"

المؤسسة: المركز الجامعي –مغنية– معهد الحقوق و العلوم السياسية

التخصص: قانون خاص

البريد الالكتروني: elhaci13meriem@gmail.com

رقم الهاتف: 0542683564

محور المداخلة: المحور الخامس الموسوم ب "تأثير الوسائل العلمية الحديثة على الاثبات الجنائي"

عنوان المداخلة: "**الدليل الرقمي بين ضرورة الاثبات الجنائي و حماية الحق في الخصوصية**"

ملخص:

لقد ادى التطور التكنلوجي الهائل و الثورة المعلوماتية الرهيبة التي يشهدها العالم في العصر الحديث الى احداث تغييرات كبيرة في كل المجالات القانونية بما في ذلك المجال الجنائي، نتيجة لهذه المستجدات و التطورات برزت جرائم جديدة لم تكن معروفة سابقا تسمى "بالجرائم المعلوماتية"، و لمواجهة تحديات هذه الجرائم الخطيرة ظهرت وسائل اثبات مستحدثة تسمى "بالدليل الرقمي" الذي يمتاز بالحداثة و الطابع العلمي و التقني يمكن استنباطه من جهاز الحاسوب و شبكة الأنترنيت و البرمجيات .

على الرغم من فعالية هذا الدليل الرقمي في الاثبات الجنائي نظرا لمزاياه المتمثلة في السرعة و الدقة الا أنه يبقى عرضة للتزوير و الاخفاء من جهة، كما أن عملية الحصول عليه تمس بالحق في الخصوصية المعلوماتية للفرد التي أضحت أهم مظاهر حياته الخاصة.

كلمات مفتاحية:

الدليل الرقمي – الاثبات– الحجية–الحق في الخصوصية.

Digital evidence between the necessity of criminal proof and the protection of the right to privacy

Summary:

The tremendous technological development and the terrible information revolution that the world is witnessing in the modern era have led to major changes in all legal fields, including the criminal field. There are new means of proof that are called digital evidence, which is characterized by modernity and scientific and technical nature. It can be deduced from the computer, the Internet, and software.

Despite the effectiveness of this digital evidence in criminal proof due to its advantages of speed and accuracy, it remains vulnerable to fraud and concealment on the one hand, and the process of obtaining it affects the right to informational privacy of the individual, which has become the most important aspect of his private life.

key words:

Digital evidence - proof - authentic - right to privacy.

مقدمة:

ترتب عن التطور التكنلوجي السريع الذي يشهده العالم انتشار الثورة المعلوماتية و رواج استخدام شبكة الأنترنيت و تقنية المعلومات الرقمية عبر مختلف مناطق العالم، مما أدى الى ظهور الجرائم المعلوماتية كجرائم مستحدثة تختلف وسائل ارتكابها وطرق اثباتها عن الجرائم التقليدية،بداية من صعوبة اكتشافها نظرا لطبيعته الخاصة كونها لا تنشأ في وسط ملموس بل في وسط افتراضي.

من أجل مواجهة هذه الجرائم و الحد من خطورتها التي قد تمس بكل فئات المجتمع و تخل بالنظام العام الاقتصادي و الأمني للمجتمع، كان على التشريعات الجنائية أن تواكب هذه المستجدات و ذلك من خلال ايجاد وسائل و آليات قانونية جديدة تسهل عملية اثبات تلد الجرائم تعرف بالدليل الرقمي، و يشترك هذا الاخير مع الدليل التقليدي في شروط قبوله للإثبات الجنائي لكنه يبقى خاضعا لاقتناع القاضي، و نظرا لاختلاف أساليب الاثبات تبعا لاختلاف الانظمة القانونية عبر العالم تختلف وجهات نظر القضاة و سلطاتهم التقديرية في مدى الاخذ بالدليلي و تفعيله.

وعلى الرغم من المزايا و الأهمية العملية للدليل الرقمي في الاثبات الجنائي الا انه يطرح اشكالات عملية، كونه يبقى قابلا للتغيير و التدليس و التلاعب مما قد يشكك في مصداقيته و درجة يقينه في الاثبات، ضف الى ذلك أن طريقة الحصول عليه تمس بالحق في الخصوصية المعلوماتية خاصة اذا كانت البيانات الشخصية هي مجال استخراج الدليل، على اعتبار أن تلك الخصوصية تشكل جزءا من الحياة الخاصة و التي تحظى بحماية قانونية على المستوى الدولي و الداخلي.

تتجلى أهمية هذا البحث في حداثته و تعلقه بجرائم متطورة في طريقة ارتكابها تعتمد على جهاز الحاسوب و شبكة الأنترنيت و دراسة دليل ثبات جديد يواكب هذا التطور اختلف الفقه و التشريعات المقارنة في قبوله و حجيته في الاثبات نظرا لخاصيته التقنية و أساليب الكشف عنه التي تمس بالحياة الخاصة للفرد.

تتمحور اشكالية البحث حول كيفية الموازنة بين مشروعية الاثبات الجنائي بواسطة الدليل الرقمي و بين مبدأ حماية الحق في الخصوصية المعلوماتية للفرد؟

للإجابة على هذه الاشكالية سنتبع المنهج التحليلي من خلال تحليل النصوص القانونية المرتبطة بالموضوع و كذا المنهج المقارن من خلال مقارنة ما هو وارد في التشريع الجزائري مع الأنظمة القانونية الاخرى بخصوص تبني هذا الدليل الجنائي المستحدث، كما ارتأينا تقسيم الموضوع الى قسمين حيث سنتناول في القسم الأول تحديد ماهية الدليل الرقمي و ستنطرق في القسم الثاني لدراسة العلاقة بين الاثبات بهذا الدليل و بين الحق في الخصوصية المعلوماتية للفرد.

المبحث الأول ماهية الدليل الرقمي

لتحديد ماهية الدليل الرقمي باعتباره وسيلة اثبات جنائية جديدة يعتمد عليها لإثبات الجرائم المعلوماتية تقتضي منا الدراسة التطرق لتعريفه و بيان خصائصه(المطلب الاول)ثم نتعرض لأنواعه(المطلب الثاني)و بعدها ننتقل لتحديد الشروط الواجب توافرها فيه لقبوله من طرف القاضي (المطلب الثالث).

المطلب الأول: تعريف الدليل الرقمي

يقصد بالدليل اقامة البينة و البرهان على واقعة قانونية متنازع عليها أمام القضاء، أما من الناحية القانونية فيعرف الدليل بأنه الوسيلة التي يستعين بها القاضي للوصول الى الحقيقة المنشودة المتعلقة بالوقائع المعروضة عليه ليطبق حكم القانون عليها[1].

و بخصوص تعريف الدليل الرقمي فقد اختلف الفقهاء في تعريفهم له باختلاف زاوية نظرتهم منهم من عرفه من جانب تقني بحث، و منهم من عرفه تعريف قانوني مركزا على اجراءات استخلاصه و اعتبره وسيلة اثبات، حيث عرفه البعض بأنه عبارة عن معلومات يقبلها المنطق و العقل و يعتمدها العلم يتم الحصول عليها بإجراءات قانونية و علمية، بترجمة البيانات الحسابية المخزنة في أجهزة الحاسوب الآلي و ملحقاتها و شبكات الاتصال، و يمكن استخدامها في أية مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شخص له علاقة بجريمة أو جان او مجني عليه[2].

بينما عرفه البعض الآخر بأنه الدليل المأخوذ من أجهزة الحاسوب الآلي و يكون في شكل مجالات او نبضات مغناطيسية او كهربائية، ممكن تجميعها في شكل دليل و تحليلها باستخدام برامج و تطبيقات و تكنولوجيات خاصة يتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء[3].

فالدليل الرقمي مجموعة بيانات رقمية تتكون من مجموعة أرقام او حروف أو رموز التي تمثل مختلف المعلومات و المعطيات تكون مخزنة في جهاز الحاسوب و ملحقاته، كالأقراص المرنة و غيرها من وسائل تقنية المعلومات كالطابعات و الفاكس أو متنقلة عبر شبكات الاتصال و الأنترنيت، و التي يمكن تجميعها و تحليلها باستخدام برامج و تطبيقات و تكنلوجيا خاصة بهدف اثبات وقوع الجريمة و نسبتها الى مرتكبها[4].

تبعا لما سبق يمكن اعتبار الدليل الرقمي بأنه ذلك الدليل الذي يتم الحصول عليه من أحد الأجهزة الالكترونية التي تمتاز بالتخزين و المعالجة، و يمكن أن يثبت حقا من الحقوق أو يكشف حقيقة الاعتداء

---

[1] أحمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، ط2، دار النهضة العربية، القاهرة، 1981، ص191.

[2] نور الهدى محمودي، حجية الدليل الرقمي في اثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد 11، جوان 2017، ص911.

[3] ممدوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الحاسوب الآلي و الأنترنيت، دار الكتب القانونية، القاهرة، 2005، ص88.

[4] بلهادي حميدة، حجية الدليل الرقمي في الاثبات الجنائي، مجلة البحوث و الدراسات القانونية و السياسية، المجلد 09، العدد 01، ديسمبر 2019، ص17

عليه و يصلح ان يكون مستندا للإثبات في الاحكام القضائية و نظرا لطبيعته الخاصة يمتاز هذا الدليل بالخصائص التالية:

1-الدليل الرقمي دليل علمي

نظرا لأن ما ينطبق على الدليل العلمي من حيث التقنية ينطبق على الدليل الرقمي كما يمتاز الدليل العلمي بخضوعه لقاعدة عدم تعارضه مع القاعدة العلمية السليمة و هذا ما ينطبق كذلك على الدليل الرقمي.

2-الدليل الرقمي ذو طابع تقني

فهو ليس كالدليل المادي الذي يمكن استخلاصه بمجرد الاطلاع عليه كما هو الحال بالنسبة للدليل المادي فلا وجود للدليل الرقمي الا في مصادر البيانات الرقمية[1].

3-قابلية الدليل الرقمي للنسخ

حيث تقلل او تعدم هذه الخاصية مخاطر اتلاف الدليل الأصلي حيث تنطبق طريق النسخ مع طريقة الانشاء، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل من الفقد و التلف عن طريق نسخ طبق الاصل منه، فلا يمكن التخلص من الدليل الرقمي حتى في حالة اصدار أمر من الجاني بإزالته فيمكن استرجاعه من خلال برامج الاسترجاع[2].

4-الدليل الرقمي دليل متطور

نظرا لتزايد التطور التكنلوجي من حيث التنوع و التعدد لذلك فان البرامج الالكترونية تحتاج الى حماية تقنية قبل الحماية القانونية لمنع التسلل غير المشروع اليها و تدميرها أو الاطلاع عليها أو تغييرها[3].

المطلبالثاني: أنواع الدليل الرقمي

---

[1]علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، ط1، دار النهضة العربية، القاهرة، 2000، ص32 و ما بعدها

[2] عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنيت، رسالة دكتوراه، تخصص قانون جنائي جامعة عين شمس، مصر، 2004، ص969.

[3] سي حسن محمد عثمان، الدليل الرقمي و أثره على الدعوى الجنائية، مجلة العلوم القانونية و الاجتماعية، جامعة جلفة، المجلد 05، العدد 03، سبتمبر 2020، ص320.

ينقسم الدليل الرقمي الى ثلاث انواع تعتبر في نفس الوقت تفسيرا لمصادره و كيفية استنتاجه لكنها غير واردة على سبيل الحصر نظرا لأن الجريمة الالكترونية جريمة متطورة بتطور علم التقنية و الحاسوب و هو ما يؤدي الى تطور وسائل اثباتها تماشيا مع ذلك.

1-السجلات المحفوظة التي يتم انشاؤها بواسطة الكومبيوتر مثل سجلات الهاتف و فواتير و أجهزة السحب الآلي.

2-السجلات المحفوظة في الكومبيوتر و هي الوثائق المحفوظة أو المخزنة فيه مثل البريد الالكتروني و ملفات و برامج معالجة المكالمات و غيرها.

3-السجلات التي تم حفظها عن طريق ادخالها أو جزء منها تم انشاؤها بواسطة الكومبيوتر مثل أوراق العمل المالية التي تحتوي على مدخلات، تمت معالجتها الى برامج و أوراق رسمية للتعامل باستخدام بعض برامج الحاسوب الآلي مثل excelو من ثم تمت معالجتهامن خلال البرامج بإجراء العمليات الحسابية عليها[1].

تجدر الاشارة بان الدليل الرقمي يتم الحصول عليه عن طريق التفتيش في الوسط الافتراضي و ضبط محتوياته سواء كانت مخرجات ورقية يتم انتاجها عن طريق الطابعات أو الرسم أو غير ورقية كالأشرطة و الأقراص الممغنطة و الفيديوهات، و يطرح الاشكال حول مدى صلاحية هذه الكيانات المعنوية في الوسط الافتراضي لكي تكون محلا للتفتيش، و قد اعتبر الفقه و القضاء في فرنسا هذه الكيانات المعنوية و البرامج حيزا ماديا في ذاكرة الحاسوب الآلي، و من ثم فتصلح لأن تكون محلا للتفتيش و يشترط لصحة ذلك أن يتم ذلك الاجراءات المنصوص عليها قانونا[2].

المطلب الثالث: شروط قبول الدليل الرقمي للإثبات الجنائي

يشترط لقبول الدليل الرقمي كدليل اثبات في المواد الجنائية مجموعة من الشروط تظفي عليه طابع المشروعية و اليقينية و المصداقية شأنه شأن الدليل التقليدي نوردها فيما يلي:

الفرع الاول: مشروعية الدليل الرقمي

[1] سي حسن عثمان، المرجع نفسه، ص310-311.

[2] سامي جلال حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية، القاهرة، 2011، ص127.

تطبيقا لقاعدة حماية كرامة الانسان و حقوقه و حرمة السكن قان اجراءات الحصول على الدليل الجنائي يجب أن تتم في اطار القانون، و على ذلك فالدليل المستمد بطريق مخالف للنصوص القانونية يعد باطلا بطلانا مطلقا لتعلقه بالنظام العام، و يجوز لكل ذي مصلحة التمسك به كما أن المحكمة تقضي به من تلقاء نفسها، و على ذلك فيكون من الضروري على المشرع صياغة نصوص قانونية اجرائية تتكفل بحماية الحياة الخاصة المخزونة في الحاسوب و الانترنيت، بحيث يمنع اقتحام الملفات الشخصية دون سند قانوني حماية للحقوق و الحريات الفردية التي يكفلها القانون[1].

لقد اختلفت الآراء حول مشروعية الدليل الرقمي و تطبيقا لقاعدة نزاهة القضاء فيجب أن يبني أحكامه و قراراته على ادلة مشروعة، و يتحقق ذلك لما تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون، و الحديث عن مشروعية الدليل الجنائي الرقمي يقتضي مشروعية طرق الحصول عليه مثل اللجوء الى ممارسة اجراء التفتيش في مختلف الوسائط التقنية الرقمية أو الوسط الافتراضي الذي ارتكبت فيه الجريمة المعلوماتية، كما ينبغي أن يمارس هذا الاجراء من ذي صفة و هو قاضي التحقيق أو ضابط الشرطة القضائية[2] و على ذلك سنتعرض لمواقف مختلف الأنظمة القانونيةحول مدى قبول هذا الدليل.

1-الدليل الرقمي في نظام الاثبات المقيد: (القانوني)

يسود في النظام الانجلوساكسوني حيث يحدد المشرع للقاضي الادلة التي يستند اليها للإثبات و قيمة الاقتناع بكل دليل فيقتصر دور القاضي على فحص الدليل للتاكد من توافر الشروط القانونية، لذلك فلا قيمة للدليل الرقمي وفقا لهذا النظام الا اذا نص عليه القانون صراحة ضمن قائمة الأدلة المعتمدة مهما تلعب درجة يقينه بالتالي تنتفي السلطة التقديرية للقاضي.

2-الدليل الرقمي في نظام الاثبات الحر:

يسود في النظام اللاتيني حيث يتمتع القاضي بالحرية المطلقة في الاثبات دون التقيد بأدلة معينة منصوص عليها قانونا لتكوين اقتناعه الشخصي، كما لا يتدخل المشرع وفقا لهذا النظام في تحديد القيمة

---

[1] ضريفي نادية، دراج عبد الوهاب، سلطات القاضي الجنائي في تقدير الدليل الالكتروني المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، المجلد 04، العدد 02، 2019، ص121.

[2] بلهادي حميدة، المرجع السابق، ص28-29.

الاثباتية للدليل بالتالي يكون للقاضي سلطة تقديرية و دور ايجابي في الاثبات و يبقى الدليل الرقمي متروك لسلطته التقديرية[1].

3-الدليل الرقمي في نظام الاثبات المختلط:

يجمع هذا النظام بين النظام اللاتيني و النظام الأنجلوساكسوني حيث تمنح للقاضي السلطة التقديرية لقبول بعض الادلة كالدليل الرقمي، بينما يلتزم بما نص عليه المشرع في حالات أخرى حيث يحدد هذا الأخير قيمة و حجية الدليل الرقمي[2].

4- موقف المشرع الجزائري من الدليل الرقمي:

تطبيقا لنص المادة 212 من قانون الاجراءات الجزائية[3] فان المشرع يأخذ بنظام الاثبات الحر حيث تنص هذه الأخيرة على ما يلي: "يجوز اثبات الجرائم بأي طريق الاثبات ما عدا الاحوال التي ينص فيها القانون على غير ذلك و للقاضي أن يصدر حكمه تبعا لاقتناعه الخاص...". بالتالي يجوز للقاضي قبول الدليل الرقمي بتوافر شروطه القانونية.

الفرع الثاني: مناقشة الدليل الرقمي خلال الجلسة

تطبيقا لقاعدة شفوية المرافعة اذا كانت مخرجات الوسائل الالكترونية تعد ادلة اثبات قائمة في اوراق الدعوى في الجريمة المعلوماتية فيجب مناقشتها أمام الخصوم[4]، و يبطل كل حكم يبنى على دليل لم يطرح للمناقشة أو لم تمنح للخصوم فرصة ابداء رأيهم بشأنه أو لم يعلموا به فيجب على القاضي أن يبني حكمه على دليل عرض في الجلسة و كان أصلا في أوراق الدعوى و الا كان الحكم عرضة للنقض[5].

الفرع الثالث: بلوغ اقتناع القاضي درجة اليقين

---

[1] خالد ضو، حجية الدليل الالكتروني و شروط قبوله في الاثبات الجنائي، مجلة الباحث الأكاديمي في العلوم القانونية و السياسية، المركز الجامعي بآفلو، العدد 088، مارس 2022، ص206-207.

[2] لورنس سعيدة الحوامدة، حجية الأدلة الرقمية في الاثبات الجنائي، مجلة البحوث الفقهية و القانونية، المملكة العربية السعودية، العدد 36، اكتوبر 2021، ص928

[3] الأمر رقم 66-155 المؤرخ في 08-08-1966 المتضمن قانون الاجراءات الجزائية المعدل و المتمم.

[4] نور الهدى محمودي، المرجع السابق، ص919.

[5] خالد ضو، المرجع السابق، ص208.

يعتبر شرط اليقين في أحكام الادلة شرط عام في أدلة الاثبات التقليدية و الحديثة لذلك يجب أن يكون الدليل الرقمي غير قابل للشك لأن الشك يفسر لصالح المتهم، و تبقى مسألة الجزم بوقوع الجريمة المعلوماتية تتطلب من القاضي نوعا من المعرفة العلمية بالأمور المعلوماتية حتى لا يقع الشك في قيمة الدليل الرقمي[1].

على الرغم من ان القاضي يتمتع بالحرية في تكوين اقتناعه الا انه ملزم بتسبيب حكمه و بيان الادلة التي استند اليها، و بالنظر الى الطبيعة الخاصة للأدلة المتحصلة من الوسائل الالكترونية و ما قد يصاحب الحصول عليها من خطوات معقدة، فان قبولها في الاثبات قد يثير العديد من الاشكالات فيمكن التلاعب بها و تغيير الحقيقة فإشكالية الدليل الرقمي قد لا تتعلق بمدى قبوله كدليل اثبات بقدر ما تتعلق بكيفية ضمان مصداقيته للوصول الى الحقيقة[2].

المبحث الثاني: العلاقة بين الدليل الرقمي و الخصوصية المعلوماتية

لقد أثارت مسالة انتهاك الحياة الخاصة للفرد جدلا فقهيا عند الاعتماد على الدليل الرقمي لإثبات الجريمة الالكترونية التي تنشأ في وسط افتراضي، و نظرا للطبيعة الخاصة لهذا الدليل غير المادي الذي يتم التوصل اليه باتباع اجراءات قد تخترق مجال خصوصية المعلوماتية للفرد، التي تشكل عنصرا من عناصر حياته الخاصة التي يجدر عدم المساس بها تجسيدا لفكرة حماية حقوق الانسان.

لقد كرس المشرع الجزائري الحماية القانونية للحق في خصوصية الفرد بداية من الدستور[3]حيثتنص المادة 47 منه على ما يلي: " لكل شخص الحق في حماية حياته الخاصة و شرفه.

لكل شخص الحق في سرية مراسلاته و اتصالاته الخاصة فيأي كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى و التالية الا بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق اساسي

---

[1] بن فريدة محمد، الدليل الجنائي الرقمي و حجيته أمام القضاء الجزائي، المجلة الاكاديمية للبحث القانوني، المجلد 05، العدد 01، جوان 2014، ص281.

[2] نور الهدى محمودي، المرجع السابق، ص921.

[3] المرسوم الرئاسي رقم 20-442 المؤرخ في 30-12-2020 المتضمن التعديل الدستوري، ج ر عدد 82، الصادرة في 30-12-2020.

يعاقب القانون على كل انتهاك لهذه الحقوق."

على ذلك سنتعرض من خلال هذا المبحث الى تعريف الحق في الخصوصية المعلومتية التي أضحت أخد اهم مظاهر الحياة الخاصة(المطلب الاول) ثم نبين كيفية مساس الدليل الرقمي بحق الشخص في خصوصيته المعلوماتية(المطلب الثاني).

المطلب الأول: الخصوصية المعلوماتية مظهر من مظاهر الحياة الخاصة للفرد

يعتبر الحق في الخصوصية المعلوماتية مظهر من مظاهر الحياة الخاصة الشخصية[1] و على ذلك سوف نتعرض لتعريف الحياة الخاصة و بعدها ننتقل لتحديد تعريف الحق في الخصوصية المعلوماتية.

الفرع الأول: تعريف الحق في الحياة الخاصة

يعتبر مفهوم الحياة الخاصة مفهوم غامض و نسبي و مرن و مختلف فيه فقها و قضاءا مع الاشارة أن المشرع لم يعرف الحياة الخاصة بل اكتفى بالنص على حمايتها قانونا فقط ، و قد اختلف آراء الفقه في تعريفها بين موسع و مضيق.

فبالنسبة للتعريف الواسع للحياة الخاصة فيأخذ به فقهاء القانون العام حيث ينظرون الى هذا المفهوم كعلاقة الفرد بالدولة، فيعتبر الفقه الانجلوساكسوني الحياة الخاصة هي ان يعيش الانسان كما يحلو له مستمتعا بممارسة انشطة خاصة حتى و ان كان على منآى من الناس، أما بالنسبة للفقه اللاتيني فيرى بأن الحياة الخاصة للإنسان قيادة الانسان لذاته في الكون المحيط به، و بالنسبة للتعريف الضيق للحياة الخاصة فيأخذ به فقهاء القانون الخاص و هو الاكثر دقة كونه يربط هذا الحق بعناصر محددة كالحق في السرية و السكينة و الألفة[2].

من خلال التعاريف السابقة فان الحق في الحياة الخاصة يمتاز بالخصائص التالية:

-الحق في الخصوصية هو حق من حقوق الانسان.

[1] محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، دراسة مقارنة، مركز الدراسات العربية للنشر و التوزيع، مصر، 2016، ص26.

[2] رشيد شميم، الحق في الحياة الخاصة، مجلة العلوم القانونية و الاجتماعية، جامعة جلفة، العدد 02، ديسمبر 2018، ص16.

-عدم قابلية الحق في الحياة الخاصة للتقادم.

--الحق في الخصوصية هو حق ملكية خاصة للإنسان و يحظى بحماية خاصة حيث يحرم القانون الاعتداء عليه[1].

الفرع الثاني: الحق في الخصوصية المعلوماتية

يقصد بالخصوصية لغة الانفراد و هو نقيض العموم أما اصطلاحا فتسمى كذلك بالحق في الخصوصية الرقمية و هو حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه و عملية معاملتها آليا و حفظها و توزيعها و استخدامها في صنع القرار الخاص به أو المؤثر فيه[2]، و يمكن اعتبار البيانات الشخصية تلك المعلومات المرتبطة بالأشخاص تتعلق بوصفهم و حالتهم الاجتماعية و الصحية بل حتى بسوابقهم القضائية[3].

كما عرف البعض الخصوصية المعلوماتية بانها حق الافراد في تحديد متى و كيف و الى اي مدى تعمل المعلومات عنه للآخرين، او هي قدرة الانسان على التحكم بدورة المعلومات المتعلقة بهم اي منع الآخرين او السماح لهم بالاطلاع أو التصرف في المعلومات المتعلقة بحياتهم الخاصة.، و على ذلك تعتبر البيانات الشخصية للفرد محل للحق في الخصوصية المعلوماتية و تشمل الاسم و اللقب و العنوان البريدي صورة الفرد بياناته المالية كمعرفة دخله و ديونه و نفقاته، حيث تخضع هذه المعلومات للسرية التامة من طرف البنوك الى جانب البيانات المتعلقة بجسم الانسان و التي تسمى بالبيانات البيوميترية[4].

---

[1] وهاب حمزة، الحماية الدستورية للحرية الشخصية، دار الخلدونية، الجزائر، 2011، ص39.

[2] حزام فتيحة، الحق في الحياة الخاصة بالبيئة الرقمية، مجلة الدراسات القانونية المقارنة، المجلد 08، العدد 01، 2022، ص624.

[3] خديجة جديلي، هروال هبة نبيلة، حماية الخصوصية المعلوماتية للمستهلك عبر الانترنيت، مجلة البحوث في الحقوق و العلوم السياسية، الجزائر، المجلد 04، العدد 01، 2018، ص218.

[4] بن سماعيل سلسبيل، الحماية الجنائية للخصوصية المعلوماتية في التشريعين الجزائري و الفرنسي، مجلة الاجتهاد القضائي، المجلد 12، عدد خاص، افريل 2020، ص741-742.

توجد البيانات الشخصية عبر مختلف الأنظمة المعلوماتية و على ذلك يمكن القول بان الحق في الخصوصية المعلوماتية يتعلق بالبيانات الشخصية المخزنة في قواعد البيانات، و الانظمة المعلوماتية كما يتعلق هذا الحق بالاتصالات و المراسلات التي تتم عبر شبكة الانترنيت[1].

و قد اعترف الاعلان الخاص باستخدام التقدم العلمي و التكنلوجي لمصلحة السلم و خير البشرية صراحة بان الحق في الحياة الخاصة أحد الحقوق الاساسية التي يكفل حمايتها في مواجهة التقدم العلمي و التكنلوجي[2]، و يبقى للفرد برضاه السماح للمساس بخصوصيته المعلوماتية و الاطلاع على بياناته الخاصة، الى جانب ذلك قد تستدعي المصلحة العامة المتمثلة في حماية النظام العام على سبيل الاستثناء الحد من تلك الخصوصية أو خرقها بالقدر اللازم للوصول الى الحقيقة، و الحد من الجرائم الخطيرة حيث تسمو على المصلحة العامة في هذه الحالة عن المصلحة الخاصة للفرد[3].

المطلب الثاني: مساس الدليل الرقمي بالحق في الخصوصية المعلوماتية

على الرغم من الدور الايجابي الذي يلعبه الدليل الرقمي في الاثبات الجنائي في مجال الجريمة المعلوماتية، فلا يمكن انكار تأثيرها على الخصوصية المعلوماتية و بالنظر الى الطبيعة الخاصة للدليل الرقمي باعتباره ذو طابع تقني، فان المراقبة الالكترونية هي أساس هذا الدليل و ما يترتب عن ذلك من مساس بالخصوصية المعلوماتية عند الولوج الى البريد الالكتروني للشخص المشتبه به، ثم تظهر براءته بعد الاطلاع على مضمون رسائله الالكترونية و لا يتم تبرير هذا المساس الا بدواعي المصلحة العامة للمجتمع التي تعلو على مصلحة الفرد و على ذلك سنتطرق لتعريف المراقبة الالكترونية و مراقبة الاتصالات الالكترونية.

الفرعالأول: المراقبة الالكترونية

---

[1] مفيدة مباركي، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة و الاقتصاد، المجلد 07، عدد 13، جوان، 2018، ص465.

[2] أحمد جاد منصور، ضمانات الحق في حرمة الحياة الخاصة في المواثيق الدولية لحقوق الانسان و القوانين الوطنية، المنظمة العربية للتنمية الادارية، جامعة الدول العربية، 2013، ص59.

[3] جلال سليم، الحق في الخصوصية بين الضمانات و الضوابط في التشريع الجزائري و الفقه الاسلامي، مذكرة ماجستير،تخصص حقوق الانسان، كلية العلوم الانسانية و الحضارة الاسلامية، جامعة وهران، 2012-2013، ص123.

تعرف المراقبة الالكترونية بانها تعمد الانصات و التسجيل محلها المحادثات الخاصة سواء كانت مباشرة أو غير مباشرة أي سواء ما تبادله الناس في مواجهة بعضهم البعض ،أو عن طريق وسائل الاتصال السلكية و اللاسلكية[1]، تعرف كذلك بطرق التصنت أو مراقبة المحادثات و قد ظهرت نتيجة للتطور التكنلوجي حيث أصبحت خصوصية الفرد مكشوفة بسبب القدرة على اعتراض المكالمات الهاتفية، و اختراق الصفحات الشخصية على شبكة الأنترنيت و يقصد بالمراقبة تسجيل الغير او استماعه جلسة لمحادثة هاتفية بين شخصين دون علمهما[2]، كما يعتبر التصوير من طرق المراقبة الالكترونية و نظرا لخطورته على الحياة الخاصة للفرد و حريته يجب مراعاة الاصول العلمية و الفنية في تنفيذ عملية التصوير، و قد تضاربت آراء الفقه حول مشروعية هذه الوسيلة في الاثبات الجنائي بين مؤيد و معارض.

فبينما اعتبرها البعض مخالفة للقواعد القانونية و المبادئ العامة و الاتفاقيات الدولية لما تتضمنه من اعتداء و مساس بخصوصية الفرد و سرية حياته الخاصة ذهب البعض الآخر الى ضرورة الاعتماد على هذه الوسيلة في مجال الاثبات الجنائي نظرا لتطور الجرائم و ضرورة مواكبة التطور التكنلوجي و تحقيق التوازن بين تطور الأساليب الاجرامية و آليات مكافحتها[3].

و لقد أقر المشرع الجزائري بشرعية اجراء اعتراض المراسلات و تسجيل الأصوات و التقاط الصور اذا اقتضت ضرورة التحقيق في بعض الجرائم الخطيرة شرط الحصول على اذن من وكيل الجمهورية و تحرير محضر بخصوص عملية نسخ المراسلات أو الصور أو المحادثات المسجلة[4]، لكنه أقر في نفس الوقت عقوبات قاسية على كل من يتعمد المساس بحرمة الحياة الخاصة للغير بأية وسيلة كانت تطبيقا لنص المادة 303 مكرر من قانون العقوبات[5]، بالتالي فضرورة مكافحة الجريمة تقتضي الاعتماد على

---

[1] أحمد مسعود مريم، آليات مكافحة جرائم تكنلوجيا الاعلام و الاتصال في ضوء القانون رقم 09-04، مذكرة ماجستير، كلية الحقوق جامعة ورقلة، 2012-2013، ص79.

[2] بوشو ليلى، قبول الدليل العلمي أمام القضاء، مذكرة ماجستير، كلية الحقوق و العلوم السياسية، جامعة الجزائر، 2010-2011، ص102.

[3] باخويا دريس، رواق عمرية، أثر الاثبات الجنائي بوسائل التقنية الحديثة على حقوق الانسان، مجلة الدراسات القانونية و السياسية، المجلد 01، العدد05، جانفي 2017، ص81.

[4] أنظر المواد 65 مكرر5، 65مكرر10 من قانون الاجراءات الجزائية.

[5] الامر رقم 66-156 المؤرخ في 08-08-1966 المتضمن قانون العقوبات المعدل و المتمم، تتمثل هذه العقوبة في الحبس من 6 أشهر الى 3 سنوات و الغرامة المالية من 50000الى 300000دج.

أسلوب المراقبة الالكترونية و الهاتفية لكن يتوجب تحقيق نوع من التوازن بين مقتضيات مكافحة الجريمة و المحافظة على حرمة الحياة الخصوصية.

الفرع الثاني: مراقبة الاتصالات الالكترونية

تعرف المادة 02 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها[1] الاتصالات الالكترونية بأنها:"أي تراسل او ارسال أو استقبال علامات أو اشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية" وتندرج ضمن الاتصالات الالكترونية الاتصالات التي تتم عبر شبكات التواصل الاجتماعي على الانترنيت.

نتيجة لذلك يمكننا القول بان احترام الحق في الخصوصية المعلوماتية للفرد يتطلب سرية حياته الخاصة التي لم تعد حقا مطلقا بل هي حق نسبي يمكن التضحية به تحقيقا للمصلحة العامة، اذ أن حدود الحق في الخصوصية ينتفي عند ارتكاب الجريمة و على ذلك فقد اباح المشرع الجزائري على سبيل الاستثناء المساس بحرمة الحياة الخاصة من خلال اعتراض المراسلات و تسجيل الأصوات و التقاط الصور، لكنه في نفس الوقت وضع ضوابط لضبط هذه الاجراءات و عدم التعسف في استعمالها من طرف السلطات المختصة حفاظا على خصوصية الافراد قد تكون هذه الضوابط موضوعية تتعلق بوجود الحق في اللجوء الى ذلك الاسلوب الذي يكون ضروريا لمواجهة الجريمة، كما قد تكون تلك الضوابط شكلية كضرورة صدور اذن من السلطة القضائية و تحريرها لمحاضر عن تلك الاجراءات المتخذة.

خاتمة:

تبين لنا من خلال هذا البحث بان الدليل الرقمي يعد من اهم وسائل اثبات الجرائم المعلوماتية خاصة نظرا لتلاءمه مع طبيعتها و توصلنا الى النتائج التالية:

-يمتاز الدليل الرقمي بالطابع العلمي و التقني.

-يستخلص الدليل الرقمي من جهاز الحاسوب الآلي أو أي جهاز خاص بتخزين المعلومات و نظرا لطابعه غير المرئي فانه يصعب الوصول اليه أحيانا و يبقى عرضة للتزوير و التشفير و الاتلاف من طرف الجاني.

[1] المؤرخ في 05-08-2009، ج ر عدد 47، الصادرة في 16-08-2009.

-تنطبق على الدليل الرقمي القواعد العامة للإثبات من حيث المشروعية و خضوعه للسلطة التقديرية للقاضي، من حيث مدى الاقتناع به و تفعيله بعد التأكد من مدى صحته و شرعية اجراءات استنباطه.

-ان المصلحة العامة المتمثلة في حماية المجتمع من الجرائم تعلو على المصلحة الخاصة للفرد المتمثلة في حماية خصوصيته المعلوماتية كما نوصي بالاقتراحات التالية:

-ضرورة تكوين المحققين من ضباط الشرطة القضائية و الخبراء على التحري حول الجرائم الالكترونية و حسن استعمال الدليل الرقمي لإثباتها من خلال التطوير المتواصل لأدوات التحليل.

-ضرورة احترام الاجراءات القانونية و مبادئ المشروعية في الحصول على الدليل الرقمي و حمايته بشكل يصعب معه محوه أو التخلص منه.

-ضرورة قبول القضاة للدليل الرقمي الا في حالة عدم مشروعيته او عدم مشروعية اجراءات الحصول عليه.

قائمة المصادر و المراجع:

أولا: قائمة المصادر

-المرسوم الرئاسي رقم 20-442 المؤرخ في 30-12-2020 المتضمن التعديل الدستوري، ج ر عدد 82، الصادرة في 30-12-2020.

- الامر رقم 66-156 المؤرخ في 08-08-1966 المتضمن قانون العقوبات المعدل والمتمم.

- الأمر رقم 66-155 المؤرخ في 08-08-1966 المتضمن قانون الاجراءات الجزائية المعدل و المتمم

ثانيا: قائمة المراجع

1-الكتب

- أحمد جاد منصور، ضمانات الحق في حرمة الحياة الخاصة في المواثيق الدولية لحقوق الانسان و القوانين الوطنية، المنظمة العربية للتنمية الادارية، جامعة الدول العربية، 2013

– أحمد فتحي سرور، الوسيط في قانون الاجراءات الجنائية، ط2، دار النهضة العربية، القاهرة، 1981.

– سامي جلال حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية، القاهرة، 2011

– ممدوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الحاسوب الآلي و الأنترنيت، دار الكتب القانونية، القاهرة، 2005.

– محمد نصر محمد، المسؤولية الجنائية لانتهاك الخصوصية المعلوماتية، دراسة مقارنة، مركز الدراسات العربية للنشر و التوزيع، مصر، 2016،

– علي عبد القادر القهوجي، الحماية الجنائية للبيانات المعالجة الكترونيا، ط1، دار النهضة العربية، القاهرة، 2000.

– وهاب حمزة، الحماية الدستورية للحرية الشخصية، دار الخلدونية، الجزائر، 2011.

2–المذكرات و الرسائل

– أحمد مسعود مريم، آليات مكافحة جرائم تكنلوجيا الاعلام و الاتصال في ضوء القانون رقم 09–04، مذكرة ماجستير، كلية الحقوق جامعة ورقلة، 2012–2013.

– بوشو ليلى، قبول الدليل العلمي أمام القضاء، مذكرة ماجستير، كلية الحقوق و العلوم السياسية، جامعة الجزائر، 2010–2011.

– جلال سليم، الحق في الخصوصية بين الضمانات و الضوابط في التشريع الجزائري و الفقه الاسلامي، مذكرة ماجستير، تخصص حقوق الانسان، كلية العلوم الانسانية و الحضارة الاسلامية، جامعة وهران، 2012–2013

– عمر محمد ابو بكر بن يونس، الجرائم الناشئة عن استخدام الأنترنيت، رسالة دكتوراه، تخصص قانون جنائي جامعة عين شمس، مصر، 2004.

3–المقالات

-باخويا دريس، رواق عمرية، أثر الاثبات الجنائي بوسائل التقنية الحديثة على حقوق الانسان، مجلة الدراسات القانونية و السياسية، المجلد 01، العدد05، جانفي 2017.

- بن سماعيل سلسبيل، الحماية الجنائية للخصوصية المعلوماتية في التشريعين الجزائري و الفرنسي، مجلة الاجتهاد القضائي، المجلد 12، عدد خاص، افريل 2020.

- بن فريدة محمد، الدليل الجنائي الرقمي و حجيته أمام القضاء الجزائي، المجلة الاكاديمية للبحث القانوني، المجلد 05، العدد 01، جوان 2014.

-بلهادي حميدة، حجية الدليل الرقمي في الاثبات الجنائي، مجلة البحوث و الدراسات القانونية و السياسية، المجلد 09، العدد 01، ديسمبر 2019.

-حزام فتيحة، الحق في الحياة الخاصة بالبيئة الرقمية، مجلة الدراسات القانونية المقارنة، المجلد 08، العدد 01، 2022.

-خالد ضو، حجية الدليل الالكتروني و شروط قبوله في الاثبات الجنائي، مجلة الباحث الأكاديمي في العلوم القانونية و السياسية، المركز الجامعي بآفلو، العدد 088، مارس 2022.

-خديجة جديلي، هروال هبة نبيلة، حماية الخصوصية المعلوماتية للمستهلك عبر الانترنيت، مجلة البحوث في الحقوق و العلوم السياسية، الجزائر، المجلد 04، العدد 01، 2018.

-رشيد شميم، الحق في الحياة الخاصة، مجلة العلوم القانونية و الاجتماعية، جامعة جلفة، العدد 02، ديسمبر 2018.

-سي حسن محمد عثمان، الدليل الرقمي و أثره على الدعوى الجنائية، مجلة العلوم القانونية و الاجتماعية، جامعة جلفة، المجلد 05، العدد 03، سبتمبر 2020.

-ضريفي نادية، دراج عبد الوهاب، سلطات القاضي الجنائي في تقدير الدليل الالكتروني المستمد من التفتيش الجنائي، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، المجلد 04، العدد 02، 2019.

-نور الهدى محمودي، حجية الدليل الرقمي في اثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد 11، جوان 2017،.

–مفيدة مباركي، الحماية الجنائية للحق في الخصوصية الرقمية في القانون الجزائري، مجلة الشريعة و الاقتصاد، المجلد 07، عدد 13، جوان، 2018.

–لورنس سعيدة الحوامدة، حجية الأدلة الرقمية في الاثبات الجنائي، مجلة البحوث الفقهية و القانونية، المملكة العربية السعودية، العدد 36، اكتوبر 2021.