الـجـمهـورية الـجزائـرية الـديمقـراطية الـشعبـية

وزارة الـتعلـيم الـعـالي و الـبحث الـعلمي

جـامعة الـجـزائـر 1

UNIVERSITÉ D'ALGER 1

المخبر القانوني للذكاء الاصطناعي والمجتمع

Laboratoire Juridique de L'intelligence Artificielle

et la société

كلية الحقوق

FACULTÉ DE DROIT

فرقة بحث

القانون الدولي وتحديات الذكاء الاصطناعي

برنامج الملتقى الوطني الافتراضي حول

حقوق الإنسان في العصر الرقمي

يوم: 07 جويلية 2022

الجلسة الافتتاحية: التوقيت: 8:00 – 9:00
آيات من القرآن الكريم
النشيد الوطني
كلمة الأستاذ الدكتور: بن تليس عبد الحكيم/ رئيس جامعة الجزائر 1
كلمة الأستاذ الدكتور: لعلاوي عيسى/ مدير كلية الحقوق، جامعة الجزائر 1
كلمة الأستاذ الدكتور: خوري عمر/ رئيس المجلس العلمي، جامعة الجزائر 1
كلمة الأستاذة الدكتورة: قمودي سهيلة/ رئيسة المخبر القانوني للذكاء الاصطناعي والمجتمع
كلمة الدكتورة: يبدة ليلى/ رئيسة الملتقى الوطني الافتراضي

الجلسة الأولى: مفهوم التكنولوجيا الرقمية وتطبيقاتها/ برئاسة: الدكتورة/كروش نعيمة

التوقيت: 9:00-10:00 (07 دقائق لكل متدخل)

اسم المتدخل	جامعة الانتماء	عنوان المداخلة
د/ خواص نصيرة	كلية الحقوق، جامعة الجزائر1	مفهوم التكنولوجيا الرقمية
د/ بوخملة فوزية	كلية العلوم الإنسانية والاجتماعية سوق أهراس	التكنولوجيا الرقمية:المفهوم، المزايا والعيوب، ومتطلبات التوطين
*د/ خفاش نبيلة *د/ بحباح فريال	*كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر3 *كليـــة العلـوم الاجتماعية ، جامعة الجزائر 2	التكنولوجيات الرقمية: المفهوم والتطبيقات
ط.د/ بوغولة فطيمة	كلية الحقوق، جامعة الجزائر 1	دور التكنولوجيا الرقمية في إدارة الموارد البشرية
د/ عرورة فتيحة	كلية الحقوق، جامعة الجزائر 1	أهمية التكنولوجيا الرقمية في المجال المصرفي
د/ سلاماني ليلى	كلية الحقوق، جامعة الجزائر 1	المواطن والموظف أمام المفاهيم الحديثة: الإدارة الإلكترونية و الحكومة الالكترونية

الجلسة الثانية : دور التكنولوجيا الرقمية في تعزيز حقوق الإنسان/ برئاسة الاستاذة الدكتورة/ قمودي سهيلة

التوقيت: 10:00-11:00(07 دقائق لكل متدخل)

اسم المتدخل	جامعة الانتماء	عنوان المداخلة
د/يبدة ليلى	كلية الحقوق، جامعة الجزائر 1	الحق في الولوج إلى الانترنت
*ط.د/بن عوفية قادة *د/دويني مختار	*كلية الحقوق و العلوم السياسية/سيدي بلعباس *كلية الحقوق والعلوم السياسية/جامعة سعيدة	الحق في استعمال وسائل الاتصال الحديثة في الحصول على المعلومة

د/رابطي زهية	كلية الحقوق، جامعة الجزائر1	حرية التعبير في الفضاء الرقمي بين التكريس والتقييد
د/حواس فتحية	كلية الحقوق، جامعة الجزائر1	حقوق المؤلف على شبكة الانترنت
*د/بوثلجي أمينة *د/كروش نعيمة	كلية الحقوق جامعة الجزائر1	أي مصير للحق في التعليم في ظل الرقمنة
د/شايب يمينة	كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة الجزائر3	دور التكنولوجيا الرقمية في تعزيز الحق في التنمية
د/بوغرارة مليكة	كلية الحقوق، جامعة الجزائر 1	الحق في الصحة في البيئة الرقمية: تحديات ورهانات

مناقشة عامة للجلستين

الجلسة الثالثة: الحق في الخصوصية في العصر الرقمي/ برئاسة الأستاذة الدكتورة/ عميمر نعيمة التوقيت: 11:00-12:30 (7 دقائق لكل متدخل)		
اسم المتدخل	جامعة الانتماء	عنوان المداخلة
*د/خليفي أسماء *د/بوصيدة فيصل	كلية الحقوق و العلوم السياسية، سكيكدة	الحق في الخصوصية في ظل المعلوماتية
د/بعلوج حسينة *د/حجيمي حميدة	كلية الحقوق، جامعة الجزائر1	استعمال التكنولوجيا الرقمية للتعدي على الحق في الحياة الخاصة والحق في السمعة
ط.د/براجل الصالح	كلية العلوم الإنسانية والاجتماعية، جامعة تلمسان	صور الانتهاك الرقمي للحق في الحياة الخاصة
د/بوروبة سامية	كلية الحقوق، جامعة الجزائر1	الإطار القانوني الدولي لحماية الحق في الخصوصية في العصر الرقمي
د/بوحزمة كوثر	كلية الحقوق والعلوم السياسية جامعة تيارت	الحماية القانونية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي وفقا للقانون 18-07
د/عمروش فوزية	كلية الحقوق جامعة الجزائر1	حماية الحياة الخاصة في قانون 18-07 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي
*د/شتوح عمر *ط.د/ العيداني أمال	كلية الحقوق، جامعة الجزائر 1	حماية المعطيات ذات الطابع الشخصي في القانون الجزائري
*ط.د/ رحيل سمير	كلية الحقوق، جامعة الجزائر 1	حماية البيانات الشخصية في التعاملات الالكترونية بموجب التشريعالجزائري
د/ميرة وليد	كلية الحقوق والعلوم السياسية جامعة مسيلة	حدود حماية الحق فيالخصوصية في الفضاء الرقمي في ضوء التشريع الجزائري
د/كباب مباركة	كلية الحقوق، جامعة الجزائر 1	نطاق الحماية القانونية للحق في الخصوصية الرقمية فيظل الاتفاقيات الدولية و التشريع الجزائري

الجلسة الرابعة: حقوق الإنسان في العصر الرقمي: التحديات والمواجهة/ برئاسة الدكتورة/ بوروبة سامية التوقيت: 12:30-14:30(7 دقائق لكل متدخل)		
اسم المتدخل	جامعة الانتماء	عنوان المداخلة
د/سماتي حكيمة	كلية الحقوق، جامعة الجزائر 1	خصوصية الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري (الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها نموذجا)
د/ضامن الجيلالي	جامعة التكوين المتواصل، تيارت	انتهاكات حقوق الإنسان بفعل الجرائم الإلكترونية
د/طريق مسعودة	المدرسة العليا للتسيير والاقتصاد الرقمي،قليعة	الجريمة الالكترونية وأثرها على المجتمع من منظور اقتصادي
*د/خشيبة حنان *د/ديش تورية	كلية الحقوق والعلوم السياسية جامعة تلمسان	مخاطر الجرائم الالكترونية الممارسة ضد النساء وطرق مواجهتها
ط.د/طوير إحسان	كلية الحقوق والعلوم السياسية جامعة سيدي بلعباس	الجرائم الالكترونية الماسة بأمن المعلومات
د/كركوري مباركة حنان	كلية الحقوق، جامعة الجزائر 1	جريمة التزوير في المحررات الإلكترونية كأداة لانتهاك حقوق الإنسان في البيئة الرقمية
د/حافظي سعاد	كلية الحقوق،جامعة تلمسان	مفهوم جرائم التمييز، وخطاب الكراهية في القانون الوطني والدولي
*ط.د/مشاهر زهرة *ط.د/هنـــي زينب	جامعة الجيلالي اليابس سيدي بلعباس	التنمر الإلكتروني على مواقع التواصل الاجتماعي و انعكاساته على المواطنة الرقمية
*د/بوقاسم محمد *د/ بوسنة وسيلة	جامعة الجزائر 02 جامعة البليدة 2	تداعيات الانترنت المظلم على الأمن الفردي والوطني
*د/عيساوي فاطمة *د/عبد العزيزحكيمة	كلية الحقوق، جامعة البويرة كلية الحقوق، جامعة بومرداس	الرقابة الرقمية بين الأمن والقمع
د/ فضيل نورة	كلية الحقوق، جامعة الجزائر1	حماية موزّعي بطاقات الائتمان من الإساءة في استعمالها

مناقشة عامة

قراءة التوصيات

كلمة رئيسة الملتقى: الدكتورة يبدة ليلى

اختتام الملتقى

وزارة التعليم العالي والبحث العلمي

جامعة الجزائر1 بن يوسف بن خدة

المخبر القانوني للذكاء الاصطناعي والمجتمع

كلية الحقوق

فرقة بحث

القانون الدولي وتحديات الذكاء الاصطناعي

ينظم

ملتقى وطني افتراضي موسوم بـــ :

حقوق الإنسان في العصر الرقمي

يوم: 2022/07/07

الهيئة الشرفية للملتقى:

أ.د.بن تليس عبد الحكيم، رئيس جامعة الجزائر1

د.مدافر فايزة ، نائبة رئيس الجامعة المكلفة بالدراسات العليا.

أ.د.خوري عمر، رئيس المجلس العلمي

مدير الملتقى الوطني: أ.د لعلاوي عيسى، عميد كلية الحقوق.

رئيسة الملتقى الوطني: د. بيدة ليلى

رئيسة اللجنة العلمية: د. بيدة ليلى

المشرفة العامة للملتقى: السيدة دلي مونة

إشكالية الملتقى:

أصبحت التكنولوجيات الحديثة سمة أساسية للحياة المعاصرة الأمر الذي يصبح معه النفاذ الشامل والمفتوح للأنترنت حقا من حقوق الإنسان لا يمكن بدونه إعمال حقوق الانسان الأخرى على الوجه الأكمل.

ولقد أعلنت الحكومات والشركات ومنظمات المجتمع المدني في القمة العالمية الأولى لمجتمع المعلومات عام 2003 رغبتهم والتزامهم المشتركين ببناء مجتمع معلومات مركّز وشامل وموجه نحو التنمية، حيث يمكن للجميع إنشاء المعلومات والمعرفة والوصول إليها واستخدامها وتبادلها وتمكين الأفراد والمجتمعات والشعوب من تحقيق امكاناتهم الكاملة في تعزيز تنميتهم المستدامة وتحسين نوعية حياتهم، على أساس مقاصد ومبادئ ميثاق الأمم المتحدة، والاحترام التام للإعلان العالمي لحقوق الإنسان والتمسك به، ويشكل هذا أثرا حاسما في التأكيد على أهمية الصلة بين الأنترنت وحقوق الإنسان.

لكن بقدر ما تمكن هذه التكنولوجيات من تيسير الولوج إلى مختلف حقوق الإنسان سواء كانت مدنية أو اقتصادية أو سياسية أو ثقافية أو بيئية، والمحمية بموجب الاتفاقيات الدولية، بقدر ما يمكن أن يتحول استعمالها إلى أداة لانتهاك هذه الحقوق والمساس بالنظام العام نتيجة سوء استخدام أدوات العالم الرقمي، على غرار انتشار الأخبار الزائفة والدعاية على الأنترنت اللذان يؤديان إلى التضليل وانتهاك حقوق الإنسان والحياة الخاصة.

وعليه نطرح الإشكالية التالية:

"كيف تساهم التكنولوجيات الرقمية في تعزيز حقوق الإنسان، وما هي الحماية الممنوحة لها في ظل التحديات الرقمية المعاصرة؟".

أهداف الملتقى:

-تسليط الضوء على الاستعمالات النافعة للتكنولوجيا الرقمية من أجل إعمال حقوق الإنسان.

-إبراز الانتهاكات الخطيرة لحقوق الإنسان التي يسببها الاستعمال السيء للتكنولوجيات الرقمية.

-ضرورة مراعاة حقوق الإنسان مع كل تطور تكنولوجي.

-توضيح أهمية وجود إطار قانوني يحمي حقوق الإنسان في الفضاء الافتراضي.

-توضيح مدى إمكانية تطبيق الحماية المقررة لحقوق الإنسان على الحقوق التي تطلبتها الثورة الرقمية.

محاور الملتقى:

المحور الأول: مفهوم التكنولوجيا الرقمية وتطبيقاتها.

المحور الثاني: دور التكنولوجيا الرقمية في تعزيز حقوق الإنسان.

-الحق في الولوج إلى الأنترنت، الحق في حرية التعبير، الحق في التظلم الفعال المشاركة في الشؤون العامة، الحق في التجمع وتكوين الجمعيات، الحق في التعليم، الحق في الصحة، الحق في الغذاء، الحق في المعرفة، الحق في العمل، الحق في مستوى معيشي مناسب.

المحور الثالث: الحق في الخصوصية في العصر الرقمي.

-مفهوم الحق في الخصوصية .

-انتهاك الحق في الخصوصية.

-حماية البيانات ذات الطابع الشخصي.

المحور الرابع: حقوق الإنسان في العصر الرقمي: التحديات والمواجهة.

- التحريض على الكراهية والعنف، نشر الأخبار الزائفة والدعايات، التمييز، الجرائم الإلكترونية.

أعضاء اللجنة العلمية:

رئيس اللجنة العلمية: د. يبدة ليلى

أ.د عميمر نعيمة.....جامعة الجزائر 1.

أ.د بن علي جميلة.....جامعة الجزائر1.

أ.د قمودي سهيلة.....جامعة الجزائر1.

أ.د علام عثمان.....جامعة بويرة.

د. كروش نعيمة.....جامعة الجزائر1.

د.بوروبة سامية.....جامعة الجزائر1.

د.بن صالح رشيدة.....جامعة الجزائر1.

د.بوغرارة مليكة .....جامعة الجزائر1.

د.حواس فتحية.....جامعة الجزائر1.

د.عرورة فتيحة.....جامعة الجزائر1.

د.طلبي ليلى..... جامعة الجزائر1.

د.سلاماني ليلى..... جامعة الجزائر1.

د.سايح نوال.....جامعة الجزائر1

د.سماتي حكيمة.....جامعة الجزائر1.

د.سنوساوي سمية.....جامعة الجزائر1

د.مراد مليكة.....جامعة الجزائر1

د.سديرة نجوى ..... جامعة الجزائر1

د.كباب مباركة..... جامعة الجزائر1.

د.خواص نصيرة..... جامعة الجزائر1.

د.رابطي زهية..... جامعة الجزائر1.

د.بن موسى وردة.....جامعة البليدة.

خلف الله بن يوسف.....المركز الجامعي أفلو الأغواط

زاغو محمد ..... جامعة حسيبة بن بوعلي شلف

كدودة عادل..... جامعة الشهيد حمة لخضر الوادي

د.براني فيروز.....جامعة الجزائر1.

د.مركب حفيزة.....جامعة الجزائر1.

د.دريش وردة جامعة الجزائر 1

د.خفاش نبيلة.....جامعة الجزائر3.

د.شايب يمينة..... جامعة الجزائر3.

د.طريق مسعودة.....المدرسة العليا للتسيير والاقتصاد الرقمي. تيبازة

د.ميرة وليد..... جامعة مسيلة.

د.عبد العزيز حكيمة..... جامعة بومرداس.

أعضاء اللجنة التنظيمية:

رئيس اللجنة التنظيمة: د بوثلجي أمينة

د.باحمد كنزة.....جامعة الجزائر1.

د.لعطر فتيحة.....جامعة الجزائر 1.

د.بحاح فريال.....جامعة الجزائر2.

د.باهي هشام.....جامعة بسكرة.

ط.دعويشات حياة.....جامعة الجزائر1.

ط.د بن عوفية قادة..... جامعة سيدي بلعباس

شروط المشاركة:

-أن [illegible]

-ألا يكون موضوع البحث قد سبق نشره، أو عرضه، أو المشاركة به في نشاطات علمية سابقة.

-أن يتصف موضوع المداخلة بالجدية وأن يكون متسما بالأصالة العلمية.

-تقبل المداخلات الفردية والثنائية.

-تقبل المداخلات باللغة العربية، الفرنسية، الانجليزية.

-ترسل المداخلات كاملة مع ملخص بلغة المقال ولغة ثانية.

-يجب ألا تقل عدد صفحات المداخلة عن 15وألا تزيد عن20 صفحة، ويكون التهميش آليا في آخر المداخلة.

-تحرر المداخلة باللغة العربية بصيغة word بخط simplified arabic بحجم 14 بالنسبة للمتن وحجم 12 بالنسبة للهوامش، والمداخلات باللغة الأجنبية تحرر بخطtimes new roman بحجم 12 بالنسبة للمتن وحجم 10 للهوامش.

-ترسل المداخلات على البريد الالكتروني الآتي:

yebdaleila@yahoo.fr

colloquenational@gmail.com

تواريخ مهمة:

-آخر أجل لإرسال الملخصات:**2022/05/26**.

-تاريخ الإعلان عن الملخصات المقبولة:**2022/05/31**.

-ترسل المداخلات كاملة قبل **2022/06/25**

-الرد على المداخلات المقبولة:**2022/06/30**.

-تاريخ انعقاد الملتقى:**2022/07/07**

استمارة المشاركة

الإسم واللقب: .....

الوظيفة: .....

الرتبة: .....

التخصص: .....

المؤسسة: .....

البريد الإلكتروني: .....

رقم الهاتف:.....

محور المداخلة:.....

عنوان المداخلة:.....

جامعة الجزائر1- كلية الحقوق

مداخلة في الملتقى الوطني الإفتراضي حول

حقوق الإنسان في العصر الرقمي

يوم 1جوان 2022

محور المداخلة : المحور الأول

عنوان المداخلة: مفهوم التكنولوجيا الرقمية

the concept of digital technology

إعداد الأستاذة : خواص نصيرة ، أستاذة محاضرة " ب"، كلية الحقوق، جامعة الجزائر 1.

الهاتف : 0556.80.55.49

e-mail : khonassira@gmail.com

الملخص :

يشهد العالم تطوراً و غير مسبوق في مجال التكنولوجيا الرقمية التي أصبحت ضرورة كبيرة في كل المجالات ، لا يمكن الإستغناء عنها كالتعليم ، التجارة ، الصحة...إلخ .

فقد إنتقلنا من مفهوم تكنولوجيا الإعلام و الإتصال إلى التكنولوجيا الرقمية التي تعتبر لغة تقنية ثنائية (صفر – واحد) التي تُستخدمفي تحويل أي رسالة إلكترونياً إلى الرقمين واحد- صفر التي تأخذ أشكالاً مختلفة مثل النصوص أو الأصوات أو الصور، تُخزنُ في ذاكرة الحاسوب و يتم تحويلها إلى جهة أخرى .

و تعد التكنولوجيا الرقمية إحدى أهم أشكال التطور التقني الحديث و مجالاً واسعاً للعديد من التطبيقات الحديثة .

فسنحاول من خلال هذه الورقة البحثية تسليط الضوء على مفهوم التكنولوجيا الرقمية .

الكلمات المفتاحية : التكنولوجيا ، الرقمية ، التطبيقات ، الإستخدام

Abstract:

The world is witnessing a huge and unprecedented development in technology, especially the digital technology that becomes an irreplaceable necessity in each field like education, health care and trade.We have moved on from the concept of information and communication technology to digital technology which is a binary technical language (zero -one),Used to transforming any electronic letter to the numbers one-zero, which take different shapes as:texts, sounds and pictures stored on the computer's memory.After that,it will be transferred to another side(party).

Digital technology is considered as one of the most important forms of technical development and a wide field to many modern applications.

We tried in this research paper to shed light on the concept of digital technology.

Key words: technology, digital, appreciations, usage.

مقدمـــــــــة :

تُستَخدَمُ التكنولوجيا كمصطلح علمي حديث في مجالات عديدة وبمعاني متباينة وأحيانا بمصطلحات غير محددة، إذا أصبح هذا المفهوم من المفاهيم الأكثر شيوعا وإستخداما في الوقت الحالي نظرًا لما يحمله من دلالات ما يصعب معه تحديد مضمونه بدقة لإنتشار إستخدامه وإستغلاله في جميع المجالات، إذ إرتبط بالبحث العلمي والتعليم والتجارة والصناعة والطب والتواصل بين الرئيس والمرؤوس وبين الناس.

كما تعتبر التكنولوجيا التطبيق العلمي للعلوم النظرية، جاءت كنتيجة لتفاعل الإنسان مع الطبيعة ما أدى إلى تطور معارف هذا الأخير من خلال الإكتشافات والإختراعات التي توصل إليها، لذلك معظم التعاريف التقليدية للتكنولوجيا محصورة في المعدات والآلات التي جاءت لتحقيق حاجيات الفرد.

لقد تطور هذا المفهوم إلى مفهوم آخر و هو التكنولوجية الرقمية ، إذا أن الرسالة المرسلة إلى ذاكرة الحاسوب مهما كانت طبيعتها تكون في شكل عددين صفر –واحد أو واحد – صفر و من خلال برامج الإعلام الألي تتم ترجمتها إكترونياً إلى صور ، أصوات ...إلخ .

من خلال ما تقدم نطرح **الإشكالية التالية : ما هو مفهوم التكنولوجيا الرقمية ؟**

للإجابة عن هذه الإشكالية نتبع الخطة التالية :

المبحث الأول : تعريف التكنولوجيا الرقمية ، خصائصها و وسائل تطبيقها .

المطلب الأول : تعريف التكنولوجيا الرقمية و تكنولوجيا الإعلام و الإتصال .

المطلب الثاني : خصائص التكنولوجيا الرقمية و وسائل تطبيقها .

المبحث الثاني : إيجابيات و سلبيات التكنولوجيا الرقمية .

المطلب الأول : إيجابيات التكنولوجيا الرقمية .

المطلب الثاني : سلبيات التكنولوجيا الرقمية .

سنتبع في دراسة هذا الموضوع المنهج الوصفي .

المبحث الأول : تعريف التكنولوجيا الرقمية ، خصائصها و إستعمالاتها .

سنسلط الضوء في هذا المبحث على تعريف (في مطلب أول) خصائص و إستعمالات التكنولوجيا الرقمية (في مطلب ثان) .

المطلب الأول : تعريف التكنولوجيا الرقمية و تكنولوجيا الإعلام و الإتصال .

التكنولوجيا الرقمية هي عبارة عن لغة تقنية ذات طابع مزدوج (صفر – واحد) تُستخدم في تحويل أي رسالة إلكترونيا إلى الرقمين واحد – صفر ، و قد تأخذ هذه الرسالة أشكالاً مختلفة مثل النصوص ، أو الأصوات أو الصور أو غيرها ، و تُخزن هذه الرسائل في ذاكرة الحاسب و يتم تحويلها إلى جهة أخرى لإسترجاعها عند الطلب إذ أنها مرتبطة بما يُعرف بإرسال الإشارات عن بعد .

كما يمكن تعريفها بأنها مختلف المعلومات سواء كانت معطيات أو بيانات على شكل إشارات إلكترونية بين قارات العالم ، دون أن تتأثر هذه الأخيرة بطول المسافة و مقاومتها للتشويش و التداخل بين الموجات ذات المصادر المختلفة ، كما أنها تضمن كذلك سلامة تلك المعلومات و سريتها (و تكون في شكل كتابات ، نصوص ، رسوم ، صور ، لقطات فيديو أو أصوات تتكفل بدمجها و نقلها من جهاز إلى آخر ، كما أن الإشارات الإكترونية الرقمية يمكن تحويلها أيضاً إلى إشارات تماثلية أو إشارات رقمية و العكس [1].

أما **تكنولوجيا الاعلام و الإتصال**فهي نتيجة التطور التكنولوجي للإتصالات والمعلوماتية إلى ظهور وسائل وتطبيقات إتصالية جديدة يطلق عليها إسم "**التكنولوجيا الجديدة للإعلام والإتصال**" **NTIC** وهي تعني أساسا تلك الموصولة بالكومبيوتر.

وتظهر التكنولوجيا الحديثة للإعلام والإتصال من خلال الجمع بين الكلمة مكتوبة ومنطوقة، والصورة ساكنة ومتحركة، وبين الإتصالات السلكية واللاسلكية أرضية أو فضائية ثم تخزين المعطيات وتحليل مضامنيها وإتاحتها بالشكل المرغوب وفي الوقت المناسب وبالسرعة اللازمة.[2]

أولا: المعني اللغوي لتكنولوجيا الإعلام والإتصال

مفهوم تكنولوجيا الإعلام والإتصالTIC/ICTS ليس مفهوما وحيد المعنى " إذ يجمع عدّة تخصصات الرياضيات، الإلكترونيك، الإعلام الآلي، الإتصال، الآداب .....إلخ).

ظهر مفهومها في ثمانينات القرن الماضي في الولايات المتحدة الأمريكية بإسم "**مصطلح تكنولوجيا الإعلام**"ثم في اليابان باسم الكمبيوتر والإتصالIT) Information technology

، و لاحقا في أوروبا و عرفت بمصطلح Communication and computerبإسم

الإتصالات عن بعد والإعلام الآلي

télécommunication et informatique و Télématique

وأخيرا وبعد إنتشار الإعلام والإتصال شاع في أوروبا المصطلح المتداول TIC/CIT.[2].

ثانيا: المعنى الإصطلاحي لتكنولوجيا للإعلام والاتصال

هي عبارة عن وسائل إلكترونية تنقل وتخزّن وتعالج وتنشر المعلومات.[3] (ويرى الكاتب " معالي فهمي حيدر" بأن التكنولوجيات الجديدة للإعلام والإتصال تشير إلى جميع أنواع التكنولوجيا المستخدمة في تشغيل ونقل وتخزين المعلومات في شكل إلكتروني، وتشمل تكنولوجيا الحاسبات الآلية و وسائل الإتصال وشبكات الربط وأجهزة الفاكس وغيرها من المعدات التي تستخدم بشدّة في الاتصالات.[4]

كما يمكن تعريف تكنولوجيا الإعلام والإتصال بأنها " خليط من أجهزة الحواسيب الإلكترونية" و وسائل الإتصال المختلفة، مثل الألياف الضوئية والأقمار الصناعية.

ويُعتبر مصطلح تكنولوجيا الإعلام والإتصال أشمل وأدق من الترجمة المتداولة " تكنولوجيا المعلومات والإتصالات" التي ينقصها الشمولية، إذ أن عبارة ICTS تعتمد على عاملين الإعلام INFORMATION والإتصالCOMMUNICATION، وجمع إتصالات يفيد معنى مغاير للمعنى الحقيقي في الكلمة اللاتينية، ومن جهة أخرى هناك فرق بين الإعلام والمعلومة حيث تعتبر المعلومة المادة الخام للإعلاموهذا الأخير هدفه نقل المعلومات.

تحتاج تكنولوجيا الإعلام والاتصال للعمل لدعائم أو مكونات مادية (الأجهزة والمعدات) ولدعائم غيرمادية (البرامج) .

أولا: الدعائم المادية ،الأجهزة والمعدات

تتمثل في أجهزة الحاسب الآلي وشبكات ووحدات الإدخال والإخراج، وهي في الأساس تقوم بحفظ وتخزين ومعالجة البيانات، حيث يقوم جهاز الحاسوب بأخذ البيانات كمدخلات ثم يقوم بتخزينها ومعالجتها حسب أوامر المستخدم ثم يقوم بعرضها كمخرجات، ويتقبل الحاسب الآلي البيانات بكل أشكالها رموز، كلمات، صور، رسائل مسموعة أو مسموعة مرئية .....إلخ.

ثانيا: الدعائم غير المادية البرمجيات

ويقصد بالبرمجيات أو البرامج هي التي تعمل على تشغيل وإدارة المكونات المادية وتقوم بمختلف التطبيقات، وهي برامج التشغيل والبرامج التطبيقية بالإضافة إلى الأفراد المتخصصين في تشغيل وبرمجة وصيانة وتحليل هذه التكنولوجيا بهدف جمع، تخزين، معالجة وإسترجاع ونقل وتحديث المعلومات.[1]

أ- برمجيات التشغيل أو النظام

([1]) كمال عايد، مرجع سابق، ص 31.

وهي البرمجيات الضرورية لتشغيل الحاسوب وتنظيم علاقة وحداته مع بعضها البعض، وتُعَدُّ هذه البرمجيات من قبل الشركة المصنعة للحاسوب وتُخزن فيه داخليا وتعتبر جزء لا يتجزأ من الحاسوب نفسه.

ب- البرمجيات التطبيقية

هي البرامج المُعدَّة لتشغيل عمليات معينة ومعالجة البيانات وتنفيذها، وهذه البرمجيات ضرورية في أداء عمليات منظمات الأعمال.

ج- الأفراد المتخصصون في برمجة وتشغيل التكنولوجيا:

وهم الإختصاصيون المسؤولون عن تشغيل وإستدامة النظام واللذين يقومون بتطوير وتشغيل وإدارة نظام المعلومات فنيًا ومنهم محللو النُظم ومطوروا البرامج ومشغلوا النظام من العاملين.[2)]

المطلب الثاني : خصائص التكنولوجيا الرقمية ووسائل تطبيقها .

تتميز التكنولوجيا الرقمية بالخصائص التالية :

عالمية الإستعمال (تتخطى حدود الدولة الواحدة) .

تتميز تكنولوجيا الإعلام والإتصال بمجموعة من الخصائص يمكن إجمالها فيما يلي:

1- التفاعلية: كان سابقا التدفق الأحادي للآراء، الأفكار والمعلومات هو السائد، أدى ذلك إلى غياب الحوار كأسلوب إتصالي.

أمَّا الآن فأصبح المستعمل للتكنولوجيا يقوم بأدوار مختلفة إذ بإمكانه أن يكون مستقبِلاً ومرسِلاً في نفس الوقتوهو ما يسمح بخلق نوع من التفاعل بين الأنشطة.

2- اللاتزامنية: إمكانية الإطلاع على المعلومة أو إستقبال الرسالة في زمنها غير الحقيقي، أي الوقت الذي يناسب المستخدم دون أن يكون مجبرا بإستخدام النظام في نفس الوقت.

3- اللاجماهيرية:بعد ربط أنظمة الإتصالات بالوسائط الإلكترونية أصبح يمكن توجيه الرسالة أو المعلومة إلى فرد واحد أو جماعة معينة دون أن تكون موجهة إلى جماهير ضخمة، فلم يعد المتلقي مرْغَمًا على متابعة برنامج معين في وقت محدد وهذا ما تطلق عليه بالجماهيرية، بمعنى أن المتلقي هو المتحكم في محتوى الرسالة.

([2]) كمال عايد، المرجع نفسه، ص 34.

4- قابلية التحريك والتحويل

أتاحت تكنولوجيا الإعلام والإتصال الجديدة والوسائطة الإلكترونية الحالية قابلية الحركةوالتنوع للإعلام والإتصال، إذ يمكن للمستخدم الإستفادة من المعلومة في أي مكان كان بإستخدام الحاسب الآلي، الهاتف النقال، .....إلخ. بالإضافة إلى إمكانية تحويل الرسالة المسموعة إلى رسالة نصية أو مقروءة.

5- اللامركزية: هي خاصية تسمح بإستقلالية تكنولوجيا الإعلام والإتصال، إذ تتمتع الأنترنت بإستمرارية عملها في كل الأحوال حول العالم.

6- الذكاء الإصطناعي:

تتميز تكنولوجيا الإعلام والاتصال بإمكانية صنع آلات ذكية تعمل مكان البشر من خلال تزويدها ببرامج وأنظمة ذكية مثل " نظام التموضع العالمي"الإستدلال على طريق الإنتقال من مكان إلى آخر GPS[3]. وقيام هذه الآلات الذكية بالتشخيص الطبي وإبرام عقود إلكترونية في إطار التجارة الإلكترونية والقيام بمحاورة الشخصيات المعروفة عالميا في السياسة، الرياضة والفن، مثل الروبوت "صوفيا" التي تحصلت على الجنسية السعودية.

7- تشغيل، نقل و إيصال المعلومات:ويكون ذلك بمعالجة وتوزيع المعلومات آليا إعتمادًا على تطبيقات الإعلام الآلي. أمّا عملية نقل وإيصال المعلومات بين المواقع المتباعدة للحواسيب بإستخدام تسهيلات الإتصالات عن بعد Télécommunication فهنا تظهر خاصية أخرى لتكنولوجيا الإعلام والإتصال وهي " خاصية الإرتباط مع تكنولوجيا الإتصال السلكية واللاسلكية والسمعي البصري بالجمع بين النص والصوت والصورة".

8- العولمة : ومعناها إحتواء العالم وإنصهار شعوب الدول، وزيادة الإرتباط بينها من خلال إنتقال السلع وتقنيات الإنتاج والأشخاص والمعلومات، وإزداد هذا الإقتراب مع وجود تكنولوجيا الإعلام والإتصال، فالعولمة تجمع **أربعة مفاهيم** ظاهرة إقتصادية، هيمنة القيم الأمريكية وثورة التكنولوجيا وحقبة تاريخية، إذ يعود تاريخ ظهورها مع سقوط الإتحاد السوفياتي وإبرام إتفاقية Gatt.

أما بالنسبة لوسائل تطبيقها فتتمثل فيما يلي :

* جهاز الكمبيوتر .

(3)Global positioning system.

* الهواتف النقالة الذكية .

* مواقع التواصل الاجتماعي .

* الأنترنت .

السبورة الذكية التفاعلية الرقمية البيضاء ، و هي التي تستعمل في التعليم .

الأجهزة اللحية الذكية المتعددة الوسائط .

الكاميرات الرقمية .

*** الاقمار الصناعية:** تسمى بوسيلة الوسائل، وهي ذي عدة وظائف مثل إستلام الموجات الصاعدة من المحطات الأرضية، ثم تغيير ترددتها وتضخيمها وإرسالها مرة أخرى إلى المحطات الأرضية (المستقبل).

ويُعَرّف القمر الصناعي بأنه: " مركبة فضائية تدور حول الكرة الأرضية، لها أجهزة لنقل إشارات الراديو والبرق والهاتفوترسل محطات على سطح الأرض (المحطات الأرضية) الإشارات إلى القمر الصناعي الذي يبث الإشارات بعد ذلك إلى محطات أرضية أخرى" [(4)].

يُفَهمُ من هذا التعريف أنّه يُشترط وجود محطتين، محطة الإرسال ومحطة إستقبال يرسل عبر صاروخ ويقيس قوة الضغط.

وأوّل دولة قامت بإطلاق قمر صناعي هو الإتحاد السوفياتي عام 1964.

ومن إستخدامات الأقمار الصناعية ما يلي:

- نقل المواد الخاصة بالصحف لتصدر من أماكن متعددة في وقت واحد.
- تستخدم لنقل الصورة والصوت.
- تستخدم لنقل ذبذبات الراديو وموجات التلفزيون.
- تستخدم لعقد المؤتمرات عن بعد.
- الربط بين الحاسبات الإلكترونية ونقل البيانات التي تخزنها فيما بينها.
- تستخدم في الإتصال الهاتفي.
- تستخدم في توفير الخدمات البريدية والإلكترونية والمعلوماتية.

([4]) الشافعي منصور، مملكة العلم والتكنولوجيا، ايتراك للنشر، مصر 2000، ص 82 – مرجع مشار إليه في عايد كمال، الميلود سحانين مرجع سابق، ص 23.

- تستخدم كذلك في الدراسات البيئية والفلكية وتنبؤات الأرصاد الجوية.
- تستخدم الأقمار الصناعية في المجال العسكري.

المبحث الثاني : إيجابيات و سلبيات التكنولوجيا الرقمية

تلعب التكنولوجيا دوراً هاماً في حياة الإنسان (المطلب الأول : إيجابيات التكنولوجيا الرقمية) بسوء إستخدامها يؤدي إلى جرائم ذات طابع خاص(المطلب الثاني : سلبيات التكنولوجيا الرقمية) .

المطلب الأول : إيجابيات التكنولوجيا الرقمية

تتمثل فيما يلي :

- وظيفة توثيق المعلومات والإنتاج الفكري:

تلعب وسائل (ت. إ. و. إ) المتمثلة في الحواسيب، الأقراص المضغوطة، الهواتف الذكية، آلات التصوير الرقيمة، Flash disque دورًا هامًا في توثيق المعلومات الذي يساعد في أرشفتها إلكترونيًا ورقميًا.

2- تلعب التكنولوجيا الرقمية دورًا في التحرير الإلكتروني وبالتالي إقتصاد الوقت.

3- تنوع **وسرعة تدفق المعلومات**، إذ ساهمت التكنولوجيا الرقمية بإستخدام الحواسيب وشبكة الأنترنت وشبكات الإتصال في عملية نقل وتبادل المعلومات على وفرتها وكثرتها متخطية حاجزي المكان والزمان وكذا حاجز الحدود، إذ تنتقل البيانات الرقمية بين دول العالم مهما كانت جنسية المستخدم أو المتلقي.

4- وظيفة التسويق و التجارة الإلكترونية: وهذا ما جسده المشرع الجزائري من خلال وتأطير هذه الأخيرة بموجب القانون رقم 18-05 المؤرخ في 2018/05/18.[5]

- تستغل التكنولوجيا الموارد الطبيعية لتحويلها إلى منتجات وخدمات تحقق الرفاهية الإجتماعية.
- تسهيل الإتصال ونقل المعرفة.
- تسهيل التعليم والتعلم (عن بعد).
- تسهيل تسيير الموارد المالية والبشرية والإدارة
- تسهيل وتطوير الإقتصاد.

([5]) الجريدة الرسمية العدد 28 المؤرخ في 2018/05/16.

- تساعد على الإختراعات والتجديدات.
- إختصار المسافات بين دول العالم.
- إختصار للوقت وكذا للمكان.
- تساعد التكنولوجيا على التحاضر عن بعد وعقد الإجتماع عن طريق الفيديو.
- تساهم التكنولوجيا في تقديم خدمات طبية متقدمة خاصة في ظل ما يُعرَفُ بالذكاء الإصطناعيintelligence artificielle
- المساهمة في تحسين الجودة والمراقبة الإلكترونية.
- تساعد التكنولوجيا على تحقيق الميزة التنافسية وكذا المحافظة على البقاء والإستمرارية .
- تساهم التكنولوجيا الرقمية في تطوير قطاع الصحة و الفلاحة و المؤسسات الناشئة.
- للتكنولوجيا عدّة أبعاد زمنية ومكانية، حيث توفر الجهد والوقت اللازمين لأداء الأعمال.

المطلب الثاني : سلبيات التكنولوجيا الرقمية

رغم إيجابيات المعلوماتية في تقريب شعوب العالم وإدخالها في عوالم إفتراضية إلاَّ أن هذه الثورة لها آثار سلبية أثرت على حقوق الأفراد وحرياتهم وحتى على الدول نتيجة استغلال الأفراد والجهات المختلفةللتقنية في غير الغرض الذي أخترعت من أجله.

فسوء إستغلال التكنولوجيا سيؤدي إلى إرتكاب جرائم تعرف بجرائم التكنولوجيا الحديثة .

أساس الجريمة المعلوماتية أو الإجرام المعلوماتي هو المعلومة (معطيات) برامج وكذا التصرفات المحرمة قانونا التي قد تمس بمال الغير أو بالأشخاص والحريات.

ويطلق على الجريمة المعلوماتية عدة مصطلحات منها جرائم الكمبيوتر ، جرائم التقنية العالية ، جرائم الهاكرز ، جرائم الأنترنت، الإجرام في الفضاء الخيالي، الجرائم عبر شبكات الإتصال عن بعد، وكذا السيبركرايم.

و تتميز جرائم التكنولوجيا الرقمية بخصائص غير مألوفة في الجرائم العادية ، يمكن إجمالها فيما يلي :

1- حداثة القوانين المتعلقة بالجرائم المعلوماتية ، فظهر أول قانون في فرنسا عام 1988 قانون رقم 88-19 المؤرخ في 5 جانفي 1988.

أمّا في التشريع الجزائري فأوّل نص قانوني تكلم عن الجرائم المعلوماتية وجرائم الحاسوب هو قانون العقوبات سنة 2001 في المادة 144 مكرر[6] و 144 مكرر 1 والمادة 144 مكرر 2 وم 146، ثم يليه تعديل قانون العقوبات لعام 2004 الذي ضم 8 (ثمانية) مواد من المادة 394 مكرر إلى المادة 394 مكرر 7 في القسم السابع مكرر تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" وقانون الإجراءات الجزئية رقم 06 – 22 المؤرخ في 2006. ثم تم إصدار القانون رقم 04/09 المؤرخ في 5 أوت 2009 [7] ليليه بعد ذلك المرسوم الرئاسي 15 – 261 [8] المؤرخ في 8 أكتوبر 2015 المحدد لتشكيلة وتنظيم سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وقانون العقوبات المعدل عام 2016 (القانون رقم 02/16) ثم قانون التجارة الإلكترونية رقم 05/18[9] المؤرخ في 10 ماي 2018، المرسوم الرئاسي 172/19 المؤرخ في 6 جوان 2019 المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، والنص الأخير هو المرسوم الرئاسي رقم 05/20 المؤرخ في 20 جانفي 2020 [10] المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية.

2- القوانين المتعلقة بجرائم المعلوماتية قليلة التطبيق بالإضافة إلى أنها قوانين نظرية ذات دور محدود.

3 – وسائل إرتكاب الجريمة المعلوماتية مستحدثة يستلزم لارتكابها توافر جهاز الكمبيوتر أو أي جهاز Les Décodeur التي بإمكانه المعالجة الآلية للمعطيات المعلوماتية " كأجهزة فك الرموز المقرصنة يمكن إستعمالها لسرقة الأموال من أجهزة التوزيع الآلي للنقود، وتعتمد هذه الجرائم على الذكاء.

4- صعوبة إكتشاف وإثبات الجريمة المعلوماتية، لأنها لا تترك أثرًا مرئيًا أو كتابيًا، كما يمكن للجاني حذف المعلومات والمعطيات التي يمكن أن تستخدم كدليل ضده، ويصعب على المحقق التقليدي التعامل مع هذه الجريمة لإتسامها بالغموض، والشرطة القضائية لن يكون لها حل وحيد إلا إستعمال نفس الوسيلة التي يستعملها المجرم المعلوماتي

([6]) التي تنص على أنه " يعاقب بغرامة من 100.000 دج إلى 500.000 دج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبًا .....عن طريق الكتابة أو الرسم .....أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى".

([7]) الجريدة الرسمية العدد 47 الصادر بتاريخ 2009/08/16

([8]) الجريدة الرسمية، العدد 53 الصادر بتاريخ 2015/10/08.

([9]) الجريدة الرسمية رقم 28 المؤرخ في 16 ماي 2018.

([10]) الجريدة الرسمية عدد 04 المؤرخ في 26 جانفي 2020.

4- تتسم الجريمة المعلوماتية بالنعومة، لذلك يطلق عليها " الجريمة الناعمة Crimesoft لأنها ترتكب دون إستعمال العنف أو إراقة قطرة دم واحدة ودون بذل جهد عضلي، بل بذل جهد فكري ومعرفة ممتازة بالحاسب الآلي.

5- الجريمة المعلوماتية تتعدى حدود الدولة الواحدة، فلا يشترط أن يكون الجاني والمجنى عليه في مكان واحد أو دولة واحدة عكس الجرائم التقليدية كالقتل أو الإختطاف، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال [11] أدت إلى إختلاف بين البلد الذي إرتكبت منه الجريمة المعلوماتية والبلد الذي يوجد به المجني عليه.

6- يتميز مرتكب الجريمة المعلوماتية (المجرم المعلوماتي) عن غيره من المجرمين بالذكاء والإحتراف، والمهارة والمعرفة الدقيقة للعالم الإفتراضي والحواسيب دون إشتراط مستوى دراسي معين، فأغلبية قراصنة الأنترنت لم يدرسو بالجامعة وإرتكبوا جرائم كبيرة وصلت حتى قرصنة حسابات بنوك دول كبرى وقرصنة مخابراتها.....إلخ

خاتمة :

تبقى التكنولوجيا الرقمية ضرورة ملحة من أجل النهوض بكل القطاعات (التعليم و التعليم العالي و الصحة و الفلاحة و الصحة ....إلخ) .

وظهرت أهمية التكنولوجيات الحديثة بشكل كبير مع إنتشار فيروس كورونا (COVID 19 Corona) خاصة بالنسبة للدول التي لم تكن لها إرادة في رقمنةإقتصادها وجميع المجالات الأخرى ومنها Virus الجزائر التي إضطرت مرغمة إلى التعامل مع الواقع الجديد وإدخال التكنولوجيا في كل المجالات وحتى السياسي أين كان الرئيس عبد المجيد تبون يخاطب الجزائريين عبر تغريداته في تويتر وعبر المحطات الإعلامية بالإضافة إلى إنعقاد مجلس الوزراء والحكومة وحتى الإجتماعات الدولية (أوبيك وأوبيك +) عبر تقنية الفيديو، وكذا رقمنة التعليم والتعليم العالي، وإنجاز مستشفيات إفتراضية .

وقد أظهرت هذه المرحلة عن وجود قدرات هائلة لشباب جزائري شغوب لخدمة هذا الوطن بإستخدام آخر التكنولوجيات وكذا عن طريق إختراعات أبهرت الجميع.

([11]) سليم مزيود، الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها، مقال منشور في المجلة الجزائرية للإقتصاد والمالية، العدد 01 ، افريل 2014، ص 97.

و من التوصيات التي يمكن إدراجها مايلي :

ضرورة تحديد المفاهيم الأساسية (الرقمية ، التكنولوجيا ، الاعلام و الإتصال).

ضرورة رقمنة كل القطاعات تماشيا و التكنولوجيات الحديثة .

ضرورة تفعيل أنظمة الحماية لشبكات الإتصال الداخلية تفادياً للوقوع في الجريمة المعلوماتية .

ضرورة مسايرة القوانين الجزائرية (قانون العقوبات ، قانون مكافحة الجرائم المتعلقة بتكنولوجيا الإعلام و الإتصال) مع العصر الرقمي و مع الإتفاقيات الدولية في مجال حماية حقوق الإنسان .

تكوين العنصر البشري (قضاه ، ضباط الشرطة القضائية ...) متخصصين في مجال مكافحة الجريمة المعلوماتية .

الهوامش و المراجع :

(1) ميمونة مناصرية ، منوبية قاسمية ، إستخدامات تكنولوجيا الإتصال الرقمية في البيئة التربوية ، مجلة الرسالة للدراسات الإعلامية ، المجلد 2 ، العدد 8 ، ديسمبر 2018 ، ص 13

التكنولوجيا الرقمية: المفهوم، المزايا والعيوب، ومتطلبات التوطين

Digital technology: concept, advantages and disadvantages, and localization requirements

بوخملة فوزية دكتوراة في علم المكتبات والتوثيق
جامعة سوق أهراس(كلية العلوم الإنسانية و الإجتماعية) _ الجزائر
Boukhamla.fouzia@gmail.com

ملخص :

تساعدنا التكنولوجيا الرقمية في تحسين حياتنا اليومية، العلمية، والعملية، وتسهيلها من خلال الحصول على المعلومات، التسوق الإلكتروني، التعلم والتعليم عن بعد، التواصل العلمي واللقاءات العلمية الإفتراضية، البحث العلمي، وغيرها من النشاطات اليومية التي تتطلب كثيرا من الجهد والعناء، وهذا ما قدمته هذه التكنولوجيا، فقد اصبح من السهل التنقل عبر العالم بكبسة زر وباستخدام الأجهزة الذكية وتطبيقاتها.

وللحصول على مزايا هذه التكنولوجيا الرقمية لا بد من توفر بعض الشروط والمتطلبات الواجب تحقيقها: كالبنية التحتية الملائمة، الإطار التشريعي الذي ينظمها، توفر الطاقات والقيادات المؤهلة، توافر الموارد المالية. وبالرغم من المزايا التي توفرها التكنولوجيا الرقمية، إلا أنها تتسم ببعض السلبيات التي تتطلب وقفة حقيقية، نذكر منها على سبيل المثال لا الحصر: انتشار العنف والجرائم الإلكترونية، الأمراض التي تصيب الإنسان من الإجهاد والإفراط في استخدام هذه التكنولوجيا، العزلة والإدمان للألعاب والشات، وغيرها.

وتهدف دراستنا الحالية إلى التعريف بالتكنولوجيا الرقمية، والبحث في أصل تسميتها، إضافة إلى التطرق إلى مميزاتها وعيوبها، ومتطلبات توطينها. مع تقديم بعض الحلول والمقترحات للتغلب على عيوبها.

الكلمات المفتاحية: التكنولوجيا الرقمية ؛ المفهوم ؛ المزايا ؛ العيوب ؛ متطلبات التوطين.

Abstract:

Digital technology helps us improve our daily, scientific, and practical lives, and facilitate it through obtaining information, e-shopping, distance learning and education, scientific communication and virtual scientific meetings, scientific research, and other daily activities that require a lot of

effort and effort, and this is what I provided With this technology, it has become easy to move around the world with the push of a button and using smart devices and their applications.

In order to obtain the advantages of this digital technology, some conditions and requirements must be met: such as the appropriate infrastructure, the legislative framework that regulates it, the availability of energies and qualified leaders, and the availability of financial resources. Despite the advantages offered by digital technology, however, it has some negatives that require a real pause, including, but not limited to: the spread of violence and cybercrime, human diseases caused by stress and excessive use of this technology, isolation and addiction to games and chat, and others.

Our current study aims to introduce digital technology, research the origin of its name, in addition to addressing its advantages and disadvantages, and the requirements for its localization. Providing some solutions and suggestions to overcome its shortcomings.

key words: Digital technology ; concept ; advantages ; disadvantages ; localization requirements.

مقدمة:

إن توظيف الأرقام أو الرقمنة في التقنيات الحديثة أدى إلى ثورة جديدة في مجال المعلومات والإتصالات، فظهرت الكاميرا الرقمية والهواتف الرقمية والحواسيب الرقمية...الخ.[1]

وأثرت هذه التكنولوجيا الرقمية على حياة الإنسان سواء العادية، أو العملية، أو العلمية، وفي مختلف المجالات، ومما نلاحظه أن لهذا التأثير جوانب إيجابية: كإختصار الوقت والجهد، والمساعدة في اتخاذ القرارات، والحصول على المعلومات التي يحتاجها بصورة سريعة مستخدما في ذلك النقر على زر فقط ليتمكن من الوصول إلى ما يريده، ورغم الإيجابيات المتعددة للتكنولوجيا الرقمية إلا أنها تتصف بسلبيات وعيوب كثيرة، كالإجهاد الفكري والبدني لمستخدميها والمدمنين عليها، التجسس وتسريب البيانات الشخصية للأفراد

والمواطنين، انتشار الجرائم المعلوماتية والحروب الإلكترونية، السطو على البنوك والمصارف، وغيرها من الأخطار.

إن التكنولوجيا الرقمية وما جاءت به سواء من الناحية الإيجابية أو السلبية تبقى مطلبا للعديد من الدول النامية والفقيرة تكنولوجيا، وتسعى للحصول عليها واستيعابها لتوظيفها التوظيف الصحيح، والإستفادة من مزاياها، ولأجل ذلك لا بد من توفير مجموعة من المتطلبات لتوطينها.

انطلاقا مما سبق ذكره، جاءت هذه الدراسة لتجيب عن التساؤلات الآتية:

_ ماهو مفهوم التكنولوجيا الرقمية؟

_ ماهي مزايا التكنولوجيا الرقمية؟

_ ماهي عيوب التكنولوجيا الرقمية؟

_ ماهي متطلبات توطين التكنلوجيا الرقمية؟

_ كيف يمكن التغلب على عيوب التكنولوجيا الرقمية؟

المبحث الأول: مفهوم التكنولوجيا الرقمية:

للتعرف على مفهوم التكنولوجيا الرقمية لا بد أول من تعريف كل مصطلح على حدا: مصطلح التكنولوجيا ثم مصطلح الرقمية للوصول إلى معنى التكنولوجيا الرقمية.

وينقسم مصطلح التكنولوجيا الرقمية إلى قسمين:

أ. تكنولوجيا:

هي كلمة إنجليزية مشتقة من (Techno) الفن والحرفة، (Logia) الدراسة أو العلم[2] ، وتعرف في اللغة العربية بالتقنية. يعرفها قاموس ويبستر اصطلاحيا على أنها: " التطبيق العملي لمعرفة خاصة في مجال معين".[3] وتعرف بأنها: "مجموعة المعالجات المادية التي تحول المدخلات إلى مخرجات إضافة إلى هيكل النشاطات المستخدمة في عملية التحويل أي الإستعدادات الإجتماعية بشكل صيغ تنظيمية وأساليب إجرائية".[4] بمعنى أنها الطرق والأساليب التي يتم اتباعها لتطبيق المعرفة في مجال معين.

ب. الرقمية:

باللغة العربية و (Digital) بالإنجليزية وهي كلمة مأخوذة من اللغة اللاتينية، وتعني اصبع أو رقم، وتشير إلى واحدة من أقدم أدوات العد. عند تخزين المعلومات أو ارسالها أو إعادة توجيهها بتنسيق رقمي ـ على مستوى الجهاز الأساسي على أنها أصفار أو آحاد.[5]

عند جمع الكلمتين نتحصل على مصطلح التكنولوجيا الرقمية، التي تعرف على أنها: " فرع من فروع المعرفة العلمية أو الهندسية، التي تتعامل مع الإبتكار والإستخدام العلمي للأنظمة والأساليب والأجهزة الرقمية والكمبيوتر وتطبيقات تلك العملية كما في الإتصالات والإنترنت والتواصل الإجتماعي وغيرها".[6]

وتعرف أيضا بأنها: "كل ما يتعلق بالأجهزة الإلكترونية عتادا وبرمجيات التي تقوم بمعالجة المعطيات بعد ترميزها أو تشفيرها إلى إشارات إثنيتية (0،1)، وغالبا ما تكون هذه الأجهزة حواسيب.[7] حسب التعريفات السابقة فإن: التكنولوجيا الرقمية هي استخدام الأجهزة الذكية والوسائل التكنولوجية في انتاج محتويات جديدة، اما بمعالجة بيانات أو بإنشاءها، وذلك بتحويلها إلى لغة الآلة المتمثلة في الصفر والواحد.

المبحث الثاني: مزايا وعيوب التكنولوجيا الرقمية:

إن للتكنولوجيا الرقمية مزايا عديدة كما أن لها عيوب تشوبها وفي هذا المبحث سنتطرق إلى مزاياها وعيوبها.

المطلب الأول: المزايا:

وفرت لنا التكنولوجيا الرقمية سبلا عديدة من الراحة لم يكن الجيل السابق ليتخيلها، فالإنترنت يوفر على الطلبة والمتخصصين ساعات من البحث المرهق في المكتبات، ويتيح التواصل المرئي والشفهي والكتابي الفوري بدون أي تكلفة تذكر ويمكن لأي شخص يمتلك هاتف ذكي أن يستخدم نظام تحديد المواقع العالمي كي لا يفقد طريقة في مدينة غير معروفة له وللعثور على أقرب فرع لمقهى ستاربكس وتوجد خدمات سوق وصيرفة للعملاء عبر الإنترنت، كما توجد أدوات يمكن للأطباء استخدامها في التشخيص باستخدام الكمبيوتر.[8] ويتميز الإتصال الرقمي بـ[9] :

_يتسم الإتصال الرقمي بالنشاط والقوة وخاصة في البيئات التي يكون فيها أسلوب الإشارات التماثلية مكلفا وغير فعال.

_تتسم الشبكات الرقمية بقدر عال من الذكاء حيث يمكن أن يصمم النظام الرقمي لكي يراقي تغيير أوضاع القناة بصفة مستمرة ويصحح مسارها.

_تتميز الشبكة الرقمية بالمرونة، حيث تخضع النظم الرقمية عادة للتحكم من جانب برامج الحاسوب، مما يسمح بتحقيق قدر عال من جودة الإستخدام.

_يتسم الإتصال الرقمي بالشمول حيث يسمح بنقل العديد من المحادثات أو الأصزات المركبة في آن واحد.

_ يتسم الإتصال الرقمي بتحقيق نسبة عالية من تأمين الإتصال حيث سبق استخدامه للأغراض العسكرية ونقل البيانات السرية للحكومات والبنوك.

:المطلب الثاني: العيوب

تتمثل عيوب التكنولوجيا أساسا في:

_وفر انفتاح الشبكات امكانيات أكبر للمسيئين الذين استطاعوا من خلالها الوصول إلى المعلومات الخاصة والسرية، ونسخها وإجراء تعديلات عليها أو حتى اتلافها، إضافة إلى امكانية معرفة كلمة السر، وعناوين الصفحات الإلكترونية وغيرها وحتى الدخول إلى الشبكات بأسماء مسجلة لمستخدمين آخرين، ونتيجة لتلك التصرفات تضررت شركات معروفة بشكل كبير، وتضررت قدرتها التنافسية وعرضتها لفقدان ثقة الزبائن.[10]

_توجد مجموعة أخرى من القضايا لها تأثير خاص في عملية التعليم، وتبعات إجتماعية واسعة وهي تتعلق بنوع الخبرات الرقمية، وأثرها في عقولنا، من هذه القضايا التي تثار كثيرا احتمال تراجع بعض الوظائف الفكرية بسبب طبيعة الخبرة على شبكة الإنترنت ومدتها الطويلة؛ إذ يدعي بعض الباحثين وجود احتمال بأن تكون فضاءات الإنترنت سببا لتقويض قدرتنا على التفكير المستقيم، وتقليل انتباهنا لتسلسل خط أحداث القصص الطويل، وفهم المجادلات المنطقية المطولة المعقدة. أما أشهر الكتب التي تتناول مخاطر النت وآثاره السلبية في الذكاء الإنساني فهو كتاب نيقولاس كار (Nicholas Carr) الموسوم بـ: " ما تفعله الإنترنت بأدمغتنا"[11] .

_لقد انتشر التحرش الجنسي الإلكتروني انتشارا واسعا على شبكة الانترنت ففي الولايات المتحدة الأمريكية وحدها يقدر عدد حالات التحرش الجنسي الإلكتروني بحوالي (850) ألف حالة سنويا. وتنتشر أنساق مشابهة لذلك في دول عدة من مختلف أنحاء العالم.[12]

_التمييز العنصري والعرقي، صحيح أن الوسائط الجديدة هي جديدة في نواح عدة. غير أنها كانت كثيرا جدا تتبع أنماطا قديمة عند تعاملها مع قضايا العنصر والعرق، وعلى هذا فقد عززت الوسائط الجديدة التميز العنصري القديم على اختلاف صوره، وابتكرت أشكالا

أخرى من التمييز العنصري الإفتراضي، ولكنها _ لحسن الطالع _ قدمت أيضا طرائق جديدة لمحاربة هذه القوى.[13]

_تنامي التهديدات العسكرية وهي ذلك النوع من التهديدات الإلكترونية، التي تكون فيه المؤسسات العسكرية الرسمية طرفا في هجوم الكتروني، سواء قامت به هي أو تعرضت له، وأيضا ما يقوم به فاعلون رسميون وغير رسميون من هجمات، وتشكل هذه الهجمات تحديات عن حيث كون الفاعل خفي، وكذلك حجم ومدى الهجوم، ويمكن ابراز أهم نقاط هذه التهديدات في الآتي: سرقة البيانات والمعلومات الاستراتيجية أو التلاعب بها، وتدمير البنى التحتية الإلكترونية للحكومات، والسيطرة على الأنظمة العسكرية.[14]

_تزايد الهوة بين المجتمعات المتقدمة والمتخلفة، ببروز الفجوة الرقمية، والتي خلفت دول غنية معلوماتيا ودول فقيرة معلوماتيا، وانتاج نوع جديد من الفقر، وهو فقر المعلومات والادوات التي تستخدم في جمع واحليل ومعالجة وصياغة وتداول المعلومات وكيفية توظيفها لخدمة الأهداف التنموية.[15]

اضافة إلى: الأمراض التي تصاحب الاستخدام المكثف للأجهزة الرقمية والانترنت: كالإدمان على الألعاب، الإجهاد، تصلب فقرات العمود الفقري، ضعف البصر، وغيرها. التحريض على الإرهاب، العنف والتطرف وتكوين جماعات مسلحة، الإعلام والدعاية المغرضة والأخبار المزيفة والمضللة، توسيع شبكات الإتجار بالأسلحة والمخدرات والإتجار بالرقيق باستخدام الويب المظلم.

المبحث الثالث: توطين التكنولوجيا الرقمية:

تسارع الدول على اختلافها في اكتساب وتوطين التكنولوجيا، وللقيام بهذه العملية لا بد من توفير مجموعة من المتطلبات التي تعتبر أساسية، لذا في هذا المبحث سنتطرق إلى مفهوم توطين التكنولوجيا، والفرق بينها وبين النقل، ومتطلبات التوطين.

المطلب الأول: مفهوم توطين التكنولوجيا الرقمية:

لا بد لنا أولا من التمييز بين نقل التكنولوجيا وتوطينها فالنقل يعني: نقل المصانع (نقل خارجي للتكنولوجيا) يقدم منتجا أو عدة منتجات و التمكن من تشغيله وفق عقد ترخيص يحدد عددا من الممارسات والإجراءات المتعلقة بتعديل عملية الإنتاج والمواد المستعملة ومصادرها.[16] أما التوطين، فهو: مرحلة أكثر تقدما يمكن بلوغها عبر فهم أعمق للتكنولوجيا المنقولة بحيث يمكن تطويرها وتحسينها لتعديل مواصفات المنتج بشكل يظل منافسا. يمكن

أن يطال هذا التطوير وطريقة الإنتاج وهو أمير يستدعي نقلا داخليا للتكنولوجيا ونظام وطني للإبتكار قادر وفعال.[17]

إن توليد التكنولوجيا يكون بإيجاد تكنولوجيات جديدة مبتكرة أو مطورة محليا يمكن بواسطتها تصنيع منتجات مستحدثة منافسة عالميا. أما توطين أو استيعاب التكنولوجيا فيتم عندما يتمكن المتخصمون المحليون أو الوطنيون من فهم عمليات الإنتاج ومواصفات المواد المستعملة مع القدرة على تطويرها وتحسينها لتجاري التطور العالمي لهذه التكنولوجيا وبحيث تبقى الصناعة تجاري التنافس العالمي الحاصل نتيجة التطور التكنولوجي للمواد والعمليات الداخلة في تصنيع هذا المنتج.[18]

نلاحظ أنه هناك فرق بين نقل وتوطين وتوليد التكنولوجيا الرقمية فالنقل عبارة عن استيراد للمصانع بما تحويه من موارد مادية وبشرية وتكنولوجية، أما التوطين فهو محاولة تطوير المنتجات العالمية بأيادي محلية، في حين يظهر أن التوليد هو ابتكار لمنتجات غير موجودة لتسد احتياجات السوق العالمية.

وتتجسد إدارة توطين التكنولوجيا أو استيعابها في العلمليات التالية[19] :

_الهندسة العكسيةReverse Engineering

_التطويع التكنولوجيLocal Development

_فك الحزمة التكنولوجيةUnbundling

_ملائمة التكنولوجيا مع البيئة (ومع عملية التنمية المستدامة)

المطلب الثاني: متطلبات توطين التكنولوجيا الرقمية:

تعتبر عملية التوطين إجراء معقد إلى حدما ويتطلب الإلتزام من القادة وجميع أضحاب المصلحة وذوي الصلة، خاصة عندما يتعلق الأمر بنقل التقنية وذلك من خلال سن القوانين اللازمة ومتابعة الإتفاقيات الخاصة بذلك.[20] كما تتطلب اتفاقا مع الشركاء الأجانب _ مالكي التقنية _ ذات مصداقية لضمان نقل عناصر التقنية. ويمكن إجمال متطلبات توطين التكنولوجيا الرقمية في النقاط الآتية:

_البحث العلمي: إنشاء قاعدة علمية وبنية تحتية تقنية محلية تحدد أنواع التقنية الممكن نقلها وإقامة المؤتمرات والمنتديات العلمية وإجراء البحوث التطبيقية وغيرها.[21]

_التخطيط العلمي والتكنولوجي: إن للتخطيط العلمي والتكنولوجي دور كبير في وضع الخطط والأساليب التي تحدد طرق وأساليب توطين التكنولوجية بما يتلائم والظروف البيئية والاقتصادية والاجتماعية والإمكانات والاحتياجات والجهد المادي والتنظيمي في سبيل

التطوير العلمي والتقاني واكتسابها وتطويعها بشكل يتلائم مع ظروف البلد ويتناول التخطيط العلمي والتقاني. إستراتيجية الخطة العلمية وعلاقاتها بالخطة التنموية وإعطاء الأولوية للبحوث التي لها علاقة مباشرة بمشاريع التنمية لتطوير عملية التقانة وتوطينها.[22]

_مراكز المعلومات: تعتبر من أهم وسائل نقل وتوطين التقانة، إذ تسهل عملية الوصول الى المعلومات العلمية والتقانية في مختلف المجالات، وتسيرها من بنوك معلومات التقانة، إذ تتوفر فيها : أولا. تفاصيل مختلفة عن الأنواع والبدائل التقانية، سواء كانت تقانات تقليدية أو بسيطة أو متوسطة أو متقدمة. ثانيا. توفر كافة المعلومات عن متطلبات وشروط التفضيل عند الاختيار بين البدائل التقانية ومدى ملائمتها لظروف الدول النامية.[23]

_توفير كوادر بشرية مؤهلة: يصاحب هذه العملية (التوطين) تطوير شامل لتخصصات القوى العاملة من ذوي المهارات العالية، التي قد تحتاج وقت للتطوير.[24] وذلك بتخصيص مراكز خاصة بالتأهيل والتدريب لهذه القوى العاملة حتى تكون متمكنة من التعامل مع هذه التكنولوجيا الرقمية و القدرة على توطينها مستقبلا.

_تخصيص الموارد المالية اللازمة: تخصيص ميزانية لدعم الجامعات والمراكز البحثية في مجال البحث والتطوير.[25] فبدون ميزانية كافية لا يمكن لمراكز ومخابر البحث قيامها بمهمة تطوير منظومة البحث في مجال التكنولوجيا الرقمية وتوطينها.

خاتمة:

_**نتائج الدراسة:** توصلت هذه الدراسة إلى النتائج التالية:

_التكنولوجيا الرقمية تشكل ثورة حقيقية في حياة الإنسان وهي كل الأجهزة والوسائل التكنولوجية والشبكات التي تتعامل مع البيانات والمعطيات في شكل أرقام (1.0).

_للتكنولوجيا الرقمية مزايا كثيرة، كسهولة الإتصال وسرعته، تقصير المسافات فقد أصبح العالم قرية صغيرة، ويمكن لأي فرد التنقل عبر قارات العالم بكبسة زر فقط ومن مكانه بإستخدام الأجهزة الذكية والحواسيب، دون عناء وتكلفة غالية، سهلت هذه التكنولوجيا عملية البحث عن المعلومات والحصول على مصادرها للباحثين، وفرت هذه التكنولوجيا أنماطا جديدة للتفاعل بين البشر كشبكات التواصل الإجتماعي وأصبح الإنسان يعيش في عالم رقمي.

_رغم الميزات التي وفرتها هذه التكنولوجيا الرقمية، إلا أنها شكلت تحديات كبيرة للإنسان، نذكر من بين هذه التحديات: انتشار القرصنة الإلكترونية، سرقة حقوق المؤلفين والتعدي على الملكية الفكرية لصانعي المحتوى الرقمي على شبكة الإنترنت، انتهاك

الخصوصية بالنسبة لمستخدمي الإنترنت، انتشار الأخبار الزائفة والمضللة، التهديد الإلكتروني والإبتزاز بإستخدام البيانات الشخصية وصور وفيديوهات الضحايا، انتشار التحرش والإستغلال الجنسي للقصر والأطفال والنساء، انتشار التطرف والعنف والإرهاب الإلكتروني، زيادة العنصرية بين أفراد المجتمعات.

_يتطلب توطين التكنولوجيا: القيادة والسلطة السياسية والتي يتم من خلالها سن قوانين لازمة لتوطين التكنولوجيا ومتابعة الإتفاقيات الخاصة بذلك، التخطيط الإستراتيجي، المراكز والمخابر البحثية الخاصة بتوطين التكنولوجيا الرقمية، الموارد المالية اللازمة لتشجيع البحث العلمي والابتكار في مجال التكنولوجيا، تشجيع الإستثمار وفتح السوق الوطني لتوطين التكنولوجيا، تدريب وتأهيل الكوادر البشرية العاملة في مجال التكنولوجيا.

_توصيات الدراسة:

_سن قوانين لحماية الأفراد من مخاطر التكنولوجيا الرقمية، سواء على مستوى حماية أفكارهم وذلك بوضع اطر قانونية خاصة بحماية الملكية الفكرية وحقوق المؤلف لصناع المحتوى الرقمي، أو من خلال الحماية الجسدية لهؤلاء الأفراد من خلال: مراقبة جماعات الأشرار ومرتكبي الجرائم على شبكة الانترنت: كالإرهاب الإلكتروني، والجماعات المتطرفة، والمتاجرين بالرقيق والبشر.

_توعية الأفراد بضرورة عدم استخدام بياناتهم الشخصية وكلمات السر إلا في المواقع الموثوقة.

_تقليل الوقت وتقنينه أثناء استخدام الأجهزة الرقمية والانترنت وقاية من الأمراض التي تصيب الإنسان جراء الإجهاد، ضعف البصر، تصلب فقرات العمود الفقري، ..الخ.

هذه يخص الأفراد وعلاقته بالتكنولوجيا الرقمية.

_ أما بالنسبة للدول التي تسعى جاهدة لتوطين واستيعاب التكنولوجيا الرقمية، لا بد لها من توفير مجموعة من المتطلبات، من بينها: بيئة تشريعية مناسبة، تمويل مناسب، بنية تحتية قاعدية وهياكل ذات معايير عالمية: مخابر، ومراكز بحث، تدريب وتأهيل القوى العاملة في مجال التكنولوجيا الرقمية لتكون قادرة التعامل مع هذه التكنولوجيا وتوطينها.

---

[1] أحمد علي محمود خالد ، الإستثمار المعرفي وعلاقتها بالآثار السياسية والإجتماعية، دار الفكر الجامعي، الإسكندرية، 2019، ص.59.

[2] خضر إ حيدر.، مفهوم التقنية: دلالة المصطلح، ومعانيه، وطرق استخدامه، الإستغراب 15، 2019، ص.284. متاح على الانترنت على الرابط: https://istighrab.iicss.iq/files/investigations/36v9arj4l.pdf، 05، 04، 2022.

[3] Meriam-Webster Dictionary, Technology Defenition, Available at :https://www.merriam-webster.com/dictionary/technology, 05,04, 2022.

[4] عدنان تايه النعيمي ، تكنولوجيا العمل في المنظمة بين النظرية والتطبيق، دار جليس، عمان ، 2009، ص. 14.

[5] IGIGLOBAL (Publisher og Timely Knowledge), What is Digital Technology ?, Available at : https://www.igi-global.com/dictionary/digital-technology/7723 , 05, 04, 2022.

[6] بن قاصير موسى، عصر الثورة الرقمية... حقبة جديدة في مسار تطور البشرية، العلاقات الدولية في عصر التكنولوجيا الرقمية، تحولات عميقة، مسارات جديدة، مركز الكتاب الأكاديمي،عمان، 2021، ص. 15.

[7] بن قاصير، موسى، مرجع سابق، ص. 15.

[8] ويليش كريس، الجانب المظلم للتكنولوجيا، التمويل والتنمية، سبتمبر 2016، ص. 14. متاح على الإنترنت على الرابط: https://www.imf.org/external/arabic/pubs/ft/fandd/2016/09/pdf/wellisz.pdf ، 06، 05، 2022.

[9] أحمد علي محمود خالد ، مرجع سابق، ص.ص. 58. 59.

[10] عصام الدين مصطفي صالح ، الإعلام الأمن الدولي في الأزمات: بين مكافحة جرائم الحسابات الإلكترونية والتطور التكنولوجي للمعلوماتية وأثر الأجيال الصاعدة في شبكات الإنترنت ومدى تأثيرها على العقل البشري، دار الفكر الجامعي، الإسكندرية، 2020، ص. 21.

[11] ريد تي. في ، نقله ألى العربية كرم الله نشوى ماهر، الحياة الرقمية الثقافة والسلطة والتغير الاجتماعي في عصر الانترنت، مكتبة العبيكان، الرياض ، 2018، ص. 290.

[12] ريد، تي. في، المرجع نفسه، ص. 161.

[13] ريد، تي. في، المرجع نفسه، ص. 170.

[14] بن قاصير موسى، مرجع سابق، ص. 28.

[15] بن قاصير موسى، مرجع سابق، ص. 33.

[16] رفاعيسمير، البحث العلمي وإدارة التكنولوجيا: ضرورة ملحة للعالم العربي، ملتقى الويبو للملكية الفكرية ونقل التكنولوجيا للدول العربية، الرياض، 4_ 6 جوان 2007، ص. 14. متاح على الإنترنت على الرابط: https://arij.net/wp-content/uploads/2015/01/1276766321%D8%A7%D9%84%D8%A8%D8%AD%D8%AB%D8%A7%D9%84%D8%B9%D9%84%D9%85%D9%8A%D9%88%D8%A5%D8%AF%D8%A7%D8%B1%D8%A9%D8%A7%D9%84%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7%D9%81%D9%8A%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85%D8%A7%D9%84%D8%B9%D8%B1%D8%A8%D9%8A.doc، 06، 05، 2022.

[17] رفاعي سمير، المرجع نفسه، ص. 14.

[18] بوعزة خالد ، دور مراكز البحوث التطبيقية والحاضنات التكنولوجية في توطين الصناعة والتكنولوجيا _ كوريا الجنوبية أنموذجا _ ، 2020، ص. 26. 27. متاح على الإنترنت على الرابط: https://www.asjp.cerist.dz/en/downArticle/374/11/2/132299

[19] بوعزة خالد، مرجع سابق، ص. 27.

[20] بوعزة خالد، مرجع سابق، ص. 27.

[21] بوعزة خالد، مرجع سابق، ص. 27.

[22] فياض عبد الله علي، حميد، عذاب مزهر، نقل وتوطين التكنولوجيا وأثرها على الموارد البشرية: دراسة نظرية تطبيقية، مجلة كلية بغداد للعلوم الإقتصادية، 2010، ص. 13. متاح على الإنترنت على الرابط: https://www.iasj.net/iasj/download/64eefc5f3bed8b31، 12، 05، 2022.

[23] فياض عبد الله علي، حميد، عذاب مزهر، المرجع نفسه، ص. 13.

[24] بوعزة خالد، مرجع سابق، ص. 27. (بتصرف).

[25] بوعزة خالد، مرجع سابق، ص. 27.

التكنولوجيا الرقمية: المفهوم والتطبيقات

Digital Technology : concept and applications

خفاش نبيلة، أستاذة محاضرة "ب"
جامعة الجزائر03- الجزائر
Kheffach.nabila@univ-alger03.dz

بحباح فريال، أستاذة متعاقدة
جامعة الجزائر 2 - الجزائر
feriel_bahbah@yahoo.fr

ملخص :

تهدف هذه الدراسة إلى التعريف بالتكنولوجيات الرقمية وأهم تطبيقاتها في ظل الثورة الصناعية الرابعة، التي بدأت مع بداية الألفية الثالثة وساهمت في تنامي التكنولوجيات الرقمية، مغيّرة بذلك طرق عمل وتفاعل الأفراد والمؤسسات والحكومات.

لقد توصلت الدراسة إلى أنّ التكنولوجيا الرقمية، التي أحدثتها الثورة الرقمية في مرحلة أولى والثورة الصناعية الرابعة في مرحلة ثانية، تتسم بالمجال الواسع والتأثير الكبير على كل مناحي الحياة، منتقلين بذلك من تطبيقات مؤتمتة إلى تطبيقات أكثر ذكاء، من خلال تكنولوجيا الذكاء الاصطناعي وأنترنت الأشياء والروبوتيك وغيرها، على غرار الحكومة الذكية والمدينة الذكية والتجارة الذكية.

الكلمات المفتاحية: التكنولوجيا الرقمية؛ الثورة الصناعية الرابعة؛ تطبيقات التكنولوجية الرقمية.

Abstract:

This study aims to present digital technologies and their most important applications in the context of the fourth industrial revolution, which started at the the third millennium and contributed to the growth of digital technologies, changing the ways in which individuals, institutions and governments interact.

The study revealed that digital technology, brought about by the digital revolution in the first phase and the fourth industrial revolution in a second phase, is characterized by a wide range and significant impact on all areas of life, moving from automated applications to smarter applications, through artificial intelligence technology, Internet of Things, robotics and others, such as smart government, smart city, smart commerce.

Keywords: Digital Technology; Fourth Industrial Revolution;Digital Applications.

مقدمة:

تشهد البشرية منذ بداية الألفية الثالثة، تطورات أحدثتها الثورة الصناعية الرابعة والتي هي امتداد للثورة الصناعية الثالثة (أو ما يعرف بالثورة الرقمية)، والتي تمتاز عن الثورات التي سبقتها بالسرعة الفائقة ومجالها الواسع وتأثيرها الكبير على مختلف مجالات الحياة. ليتزايد تِبعا لذلك استخدام التكنولوجيا الرقمية، محسِّنة بذلك ظروف العمل والحياة للكثيرين، لتشكل التكنولوجيا الرقمية الدعامة الأساسية للتكامل بين الأنظمة المختلفة (اقتصادية واجتماعية وتربوية وتعليمية) ولعملية التنمية المستدامة، لكن يبقى هذا المفهوم "التكنولوجيات الرقمية"، رغم استخداماته المتعددة تعريف واسع، إضافة إلى استخدامه إلى جانب مصطلحات كثيرة أخرى كتكنولوجيا المعلومات، تكنولوجيا المعلومات والاتصال، التكنولوجيا الحديثة، التكنولوجيا الجديدة وغيرها.

ضمن هذا السياق تتبادر إلى أذهاننا الإشكالية التالية:

-ما هو مفهوم التكنولوجيات الرقمية وما هي أهم تطبيقاتها؟

وتندرج تحت هذا التساؤل العام عدة تساؤلاتفرعيةكما يلي:

-ما المقصود بالتكنولوجيات الرقمية وما هي خصائص استخدامها؟

-ما هي مختلف أشكال التكنولوجيات الرقمية؟

-ما هي أهم مجالات استخدام هذه التكنولوجيات الرقمية؟

أهمية الدراسة: تنبع أهمية الدراسة من أهمية التكنولوجيا الرقمية والتطورات التي تعرفها، إضافة إلى تنامي استخدامها في مختلف مجالات الحياة.

أهداف الدراسة: تهدف هذه الدراسة إلى البحث في مفهوم التكنولوجيا الرقمية في ظل الزخم الهائل للمصطلحات المستخدمة في هذا المجال، إضافة إلى البحث في أهم تطبيقات هذه التكنولوجية الرقمية.

منهج الدراسة: نستخدم من خلال هذه الدراسة المنهج الوصفي الذي يتلاءم وموضوع الدراسة.

تقسيم الدراسة: للإجابة على إشكالية الدراسة والأسئلة الفرعية ارتأينا تقسيم الدراسة إلى أربعة محاور، نتناول في المحور الأول مفهوم التكنولوجيا الرقمية، أما المحور الثاني فتطرقنا إلى خصائص ومزايا التكنولوجيا الرقمية، لنتناول في المحور الثالث أهم التكنولوجيات الرقمية والتي أنتجتها الثورة الرقمية كمرحلة أولى والثورة الصناعية الرابعة كمرحلة ثانية. أمّا المحور الرابع فلقد تطرقنا فيه إلى أهم تطبيقات التكنولوجيا الرقمية.

أولا: مفهوم التكنولوجيا الرقمية

أحدثت التكنولوجيا الرقمية ثورة في كل مجال من مجالات الحياة البشرية تقريبا خلال السنوات الأخيرة، مُغيّرة بذلك طريقة عمل وتواصل الأفراد،حيث عرف تقدم التكنولوجيات الرقمية تقدما سريعا مدفوعا بثورة العلم.[1] ويرتبط مفهوم التكنولوجيا الرقمية بمفهومين وهما التكنولوجيا والرقمية أو النظام الرقمي والذين سنفصلهما في مايلي:

1-التكنولوجيا

اشتقت كلمة technologie"" من الكلمة اليونانية "techne " والتي تعني فنا أو مهارة، والكلمة "logos "والتي تعني علما أو دراسة، لتعني تبعا لذلك علم المهارات أو الفنون، أي دراسة المهارات بشكل منطقي لتأدية وظيفة محددة.[2]وتفيد القواميس الإنجليزية بأن معنى التكنولوجيا: المعالجة النظامية للفن، أو جميع الوسائل التي تستخدم لإنتاج الأشياء الضرورية لراحة الإنسان واستمرارية وجوده، وطريقة فنية للآداء أو إنجاز أغراض علمية.[3]

وكلمة "تكنولوجيا" معربة لا أصل لها في القواميس اللغوية العربية، ويقابلها في اللغة العربية كلمة "تقنية" والتي تطلق على كلمة "تكنولوجيا"، حيث يمكن استخدام اللفظ ما دام يعطي دلالة المعنى الذي عرِّف به.[4]

و تشمل التكنولوجيا ثلاثة مفاهيم أساسية[5]:

-**التكنولوجيا كعملية**: وهي التطبيق المنظم للمحتوى العلمي أو المعلومات بغرض أداء محدد يؤدي في النهاية إلى حل مشكلة معينة.

-**التكنولوجيا كمنتج**: حيث تكون محصِّلة تطبيق الأساليب العلمية في إنتاج منتجات وتقديم خدمات.

التكنولوجيا كمزيج للأسلوب والمنتج: حيث أن عملية الاختراع تصاحبها عملية إنتاج، وبالتالي لا يمكن فصل التكنولوجيا كأسلوب عنها كمنتج.

ولقد ظهر لفظ استخدام التكنولوجيا في العصور الحديثة بعد ظهور الثورة الصناعية وأخذ الآلة مكانتها البارزة في مجال الإنتاج الصناعي.[6]

2-التحول إلى النظام الرقمي

بدأ تطوير التكنولوجيا الرقمية في منتصف القرن العشرين من طرف مهندسين أمريكيين، عندما حاولا دمج المفاهيم الرياضية التي اقترحها عالم الرياضيات الألماني غوتفريد ويلهامليبنيز Gottfried WilhelemLeibniz في القرن السابع عشر والمتمثلة في نظام الحوسبة الثنائية، ضمن تقنياتهم، حيث تستند النظم الرقمية على عملية أساسية ثنائية، حيث يتم

تسجيل المعلومات الرقمية في رمز ثنائي من مجموعات من الأرقام مكونة من 0 و1، والتي تسمى البيتات، والتي تمثل الصور والكلمات. [7] ليتم الانتقال من الحديث على الذرات إلى الحديث عن البيتات، باعتبارها طريقة لتمثيل البيانات والمعلومات إلى صورة رمزية، ما يسمح بنقلها بسرعة الضوء لتصبح في متناول أي انسان في العالم في نفس اللحظة.[8]

لقد كانت عملية نقل الصوت إلى مسافات بعيدة تعتمد على تحويل الاشارة الصوتية إلى إشارة كهربائية، حيث يتم إرسالها في شكل موجات كهرومغناطيسية (هرتزية)، حيث كلما زادت المسافات تضعف الإشارة على طول مسافة الاتصال، ممّا يتطلب محطات تقوم بتقوية الإشارات الكهربائية لإعادة إرسالها من جديد، حيث يعاني هذا النظام من التشويش الحاصل في نظم الإرسال عند عرض المعلومات في شكل إشارات كهربائية متماثلة، بسبب بعض التداخل أثناء استقبال الإشارة مما يصعِّب التقاطها بشكل مماثل للإشارة الأصلية.[9]

يتضح مما سبق أن النظام الرقمي هو لغة الآلة، فالمعلومة المراد إرسالها يتم تشفيرها في شكل ثنائيات من" 0 و1" حتى يتم ضغطها وتخزينها، وعند استقبالها تقوم الآلة بإزالة التشفير وبذلك يستطيع الإنسان المستقبل فهم مضمون هذه المعلومة سواء كانت حروف أو رموز أو أصوات أو صور أو غيرها. [10]

3-التكنولوجيا الرقمية

ظهرت خلال عقد الثمانينات من القرن العشرين تكنولوجيا حديثة تعتمد على معالجة المعلومات ونقل مواد الاتصال المختلفة باستخدام النظام الرقمي، والتحول من أسلوب التعامل مع المعلومات على أساس تماثلي (تناظري) إلى الأسلوب الرقمي.[11]

تعتمد هذه التكنولوجيا على إرسال النبضات الكهربائية بطريقة التشغيل والإيقاف، حيث يتم تشفير جميع الرموز والحروف والأرقام والأصوات والصور والرسوم في شكل" 0 و1"، ليتم ضغط هذه المعطيات بهدف ربح الحيز المكاني بما يؤهل من تخزين عدد كبير من المعلومات، ليتم بعد استقبال الرسائل إزالة الضغط ويتم بذلك إزالة التشفير [12]من أجل قراءته أو سماعه أو مشاهدته أو غيرها. لتقتضي الرقمنة تبعا لذلك تحويل كل البيانات والمعلومات التي أنتجت أو حفظت في شكل تماثلي إلى الشكل الرقمي ممّا يسهل عملية إرسالها وتخزينها ومعالجتها وضغطها ويصبح استغلالها من الأجهزة الرقمية ممكنا.[13]

لقد سمح التطور المستمر لتكنولوجيا المعلومات وتكنولوجيا الاتصالات وتكنولوجيا الشبكات بالاندماج بين مختلف وسائلها، وبتنامي هذا الارتباط والتداخل بصفة

مستمرة،تجسّدت التكنولوجيا الرقمية التي جمعت بين تلك الوسائل في نظام رقمي وتقنية رقمية ذكية جدا[14].

تتعدَّد المصطلحات المستخدمة في العصر الرقمي حيث نجد تكنولوجيات المعلومات والاتصال، التكنولوجية الجديدة، التكنولوجية الحديثة، التكنولوجية الرائدة وغيرها، حيث يعكس كل مصطلح مرحلة معينة من مراحل تطور تكنولوجيا المعلومات والاتصال.

وضمن هذا السياق ومع الثورة الصناعية الرابعة والتي كانت مع بداية الألفية الثالثة، ومع التطورات التي عرفتها تكنولوجيا المعلومات والاتصال، ومع تنامي استخدام الشاشات التي تعمل باللمس سواء تعلق الأمر بالحواسيب الشخصية أو الهواتف الذكية أو غيرها، اكتسب مصطلح التكنولوجيا الرقمية نموا كبيرا.

ممّا سبق يمكن أن نعرف التكنولوجيا الرقمية بأنها **مختلف الموارد والأجهزة والشبكات والتطبيقات وغيرها والتي من شأنها جمع، معالجة، تخزين، نقل، تحليل، تبادل البيانات أو المعلومات رقميا سواء كانت صوت، كتابة، أو صورة أو غيرها، كما تسمح بالتفاعل بين الأشخاص أو بين الأشخاص والأجهزة أو بين الأجهزة فيما بينها.**

ثانيا:مز ايا وآليات التكنولوجية الرقمية

أصبحاستخدام التكنولوجيا الرقمية محوريا في حياتنا اليومية، لما تتمتع به من مزايا ولما يتيحه استخدامها من آليات والتي من شأنها المضي قدما نحو تيسير أو تسريع تحقيق أهداف التنمية المستدامة.

1-مز ايا التكنولوجيا الرقمية

تتمتع التكنولوجيات الرقمية بالعديد من المزايا المرتبطة بمزايا النظام الرقمي المعتمد كلغة للتكنولوجيا المستخدمة، والتي يمكن ذكر أهمها في[15]:

-تحسين مستوى الخدمات باعتبار الإشارة الرقمية أقل عرضة للتشويش والضوضاء والتداخل.

-المقدرة العالية من الذكاء في التعامل مع المعلومات والبيانات أياّ كان نوعها، والتحكم في أوضاعها واستخداماتها؛ كتصحيح الأخطاء إلكترونيا والحفاظ على قوة الإشارة على طول خط الاتصال ومقاومة التشويش والتداخل أثناء انتقال المعلومات والبيانات.

-القدرة على التخزين والاسترجاع للمعلومات والبيانات في مساحة ذاكرة صغيرة نسبيا.

-تقليص حجم المعدات وخفة وزنها وقلة تكاليفها وتنوعها.

-توفير النقاء والدقة للصوت والصورة ولا تقل جودتها مع إعادة استخدامها.

-يتسم النظام الرقمي بالشمول بحيث يمكنه نقل البيانات في شكل نصوص وأصوات وصور ورسوم بقدر عال من الدقة كما يمكنه نقل المحادثات أو الأصوات المركبة في وقت واحد.
-المرونة التي تسمح بتحقيق قدر عال من جودة الاستخدام وذلك بخضوع النظم الرقمية من جانب برامج soft ware بالحاسب الإلكتروني أو غيره.

- إضافة إلى[16]**:**

-أخذ المعلومات في ظل استخدام التكنولوجيات الرقمية صفة الرقمية، والتي تجعلها تتميز بمجموعة من الخصائص تميزها عن المعلومات المادية أو الأنالوجية، وهي إمكانية التحويل والتخزين (ضمن مساحات سحابية) والتشفير والاستفادة منها سواء في شكلها الخام أو بربطها مع بيانات ومعلومات أخرى.

2-آليات التكنولوجيات الرقمية

حققت التكنولوجيا الرقمية انتشارا ونموا سريعين، حيث أصبح بإمكان الأفراد والمؤسسات والحكومات التواصل بشكل أكبر من أي وقت مضى، متضمنة بذلك مكاسب يجب اغتنماها والتي من شأنها دعم عملية التنمية باعتبارها حق من حقوق الانسان، وذلك من خلال الآليات الرئيسية التي تتمتع بها التكنولوجيات الرقمية والمتمثلة في:[17]

- **<u>الاحتواء أو الشمول الاجتماعي</u>:** تعزّز التكنولوجيا الرقمية الاحتواء الاجتماعي من خلال حصول الأفراد وخاصة الفئات الهشة (الشباب والنساء وذوي الاحتياجات الخاصة) على مختلف الخدمات التي كانوا محرومين منها من خلال الشبكة العالمية للاتصالات، كتعزيز فرص العمل وتكافؤ فرص الوصل إليها،وتدعيم فرص التواصل والمشاركة بين مختلف الأفرادلتحقيق أهداف مشتركة، والوصول إلى التجارة ومختلف الخدمات.

ضمن هذا الإطار يعتبر العمل على اتاحة الانترنت للجميع بتكلفة ميسورة والشمول المالي (وصول الخدمات المالية الرسمية لمختلف فئات المجتمع وفي مختلف المناطق) والتمكين الاقتصادي (من خلال خلق فرص عمل للفئات الهشة)، من الأولويات التي تعمل عليها الحكومات من أجل تعزيز الاحتواء الاجتماعي والتي تعتبر التكنولوجيا الرقمية أحد الحلول أو الدعائم التي يمكن العمل من خلالها.

- **<u>تعزيز الكفاءة</u>:** سمحت التكنولوجيا الرقمية بأتمتة مختلف الأنشطة والخدمات ما يجعلها أقل تكلفة أو أسرع إنجازا أو أيسرا حصولا من ذي قبل. كما تدعم عملية الأتمتة تخفيض تكلفة الحصول على المعلومات أو المعاملات سواء للشركات أو الأفراد أو مؤسسات القطاع العام والحصول على معلومات على شكل شفاف. لهذا تعتبر التجارة الإلكترونية

والحكومة الإلكترونية والإدارة الإلكترونية وغيرها إنجازات لا يمكن التخلي عنها لما حققته من نتائج.

- **تحفيز الابتكار**: تعتبر الميزة التي تتمتع بها أو توفرها التكنولوجيات الرقمية من تخفيض تكلفة المعاملات إلى صفر تقريبا، حافزا للبحث عن تقنيات جديدة للقيام بنشاطات أو تقديم خدمات أخرى.

ثالثا: الثورة الرقمية وبداية التكنولوجيا الرقمية

يشهد العالم تطورات تكنولوجية متعددة منذ الثورة الصناعية الثالثة والتي يطلق عليه الثورة الرقمية، لتستمر مع الثورة الصناعية الرابعة والتي بدأت مع بداية الألفية الثالثة كما يوضحه الجدول رقم (1)، والتي يطلق عليها البعض تسونامي التقدم التكنولوجي، والتي غيرت وستغيّر تفاصيل كثيرة في الحياة البشرية.[18]

ويوضح الجدول التالي مراحل الثورة الصناعية، حيث تتصل الثورات الصناعية الثلاثة الأولى، حيث بدأت الأولى بمكننة الإنتاج والثانية بتضخيم الإنتاج في حين اتسمت الثالثة بأتمتة العملية الإنتاجية. وتواصل المرحلة الصناعية الرابعة في عملية الأتمتة إلاّ أنها دخلت مراحل غير مسبوقة من التطور التكنولوجي حيث تقوم بدمج التقنيات التي ظهرت من قبل بالشكل الذي تمحي به الحدود الفاصلة بين المجالات الفيزيائية والرقمية والبيولوجية.

الجدول رقم (1): مراحل التطور التكنولوجي عبر مراحل تطور الثورة الصناعية

الثورة	أهم الخصائص
الثورة الصناعية الأولى 1760	-الاعتماد على المحركات البخارية في الإنتاج والنقل والمواصلات (ظهور الآلة)
الثورة الصناعية الثانية 1900	-اختراع محرك الاحتراق الداخلي. -استخدام الطاقة الكهربائية في تعزيز الإنتاج الضخم. (الكهرباء وسلاسل الإنتاج الآلي الضخم)
الثورة الصناعية الثالثة 2000-1960	استخدام الحواسيب والروبوتات في معظم مناحي الحياة وعرفت هذه المرحلة بالثورة الصناعية الثالثة.
الثورة الصناعية الرابعة بداية الألفية إلى يومنا هذا	-مجموعة من التطورات التقنية المتصلة التي توفر أساسا لزيادة رقمنة بيئة الأعمال. -ثورة مدفوعة بعدة محركات وتقنيات قائمة على بعضها البعض لخلق تحول اقتصادي واجتماعي وسياسي. واتسمت هذه الثورة بظهور تقنيات مبتكرة كالروبوتات والذكاء الاصطناعي وتقنية النانو والحوسبة الكمية والتقنية الحيوية وانترنت الأشياء والطباعة

	الثلاثية الأبعاد والمركبات الذاتية القيادية وغيرها.

المصدر: من إعداد الباحثتين بالاعتماد على:

-شركة برايس ووترهاوس كوبرز(PWC)، القمة العالمية للصناعة والتصنيع(GMIS)، استطلاع الثورة الصناعية الرابعة(Industry 4.0) في الشرق الأوسط لعام 2016: الثورة الصناعية الرابعة: بناء المؤسسات الصناعية الرقمية، تاريخ الإطلاع: 2022/05/10، الموقع: https://www.pwc.com/m1/en/publications/documents/middle-east-industry-4-0-survey-ar.pdf

-محمد عبد القادر الفقي، الثورات الصناعية الأربع: إطلالة تاريخية، مجلة التقدم العلمي، العدد 103، أكتوبر 2018، تاريخ الإطلاع: 2022/05/20، الموقع: https://taqadom.aspdkw.com/wp-content/uploads/2019/01/taq-103-october-2018.pdf

لقد تطورت التكنولوجيات الرقمية منذ الثورة الصناعية الثالثة (الثورة الرقمية)، من مواقع الويب وأجهزة الحاسوب بأنواعها إلى الهواتف الذكية ومختلف وسائل التواصل الاجتماعي وغيرها، والتي كانت القوة الدافعة نحو استخدام هذه التكنولوجيات لتعرف أنوا ع أخرى من التكنولوجيا الرقمية أكثر تقدما مع الثورة الصناعية الرابعة كالذكاء الاصطناعي وشبكات الجيل الخامس للهواتف المحمولة والحوسبة السحابية وانترنت الأشياء والطابعة الثلاثية الأبعاد والواقع المعزز وسلسلة الكتل "البلوك تشين" والروبوتات والطائرة دون طيار وغيرها، لننتقل من عالم شديد الاتصال إلى عالم الاقتصادات والمجتمعات الرقمية.[19]

ضمن هذا الإطار تجدر الإشارة إلى أنّ إتاحة شبكة الانترنت والشبكة العالمية للاتصالات (الويب) على جانب كبير من الأهمية، دونها تصبح التكنولوجيات الرقمية دون أهمية .

ويوضح الجدول التالي أهم التكنولوجيات الرقمية منذ الثورة الصناعية الثالثة وصولا إلى الثورة الصناعية الرابعة، حيث تجدر الإشارة أنّ استخدام الهواتف باعتباره أحد التكنولوجيات الرقمية قدّم دفعة قوية لتطور هذه التكنولوجيات.

الجدول رقم (2): أهم أشكال التكنولوجية الرقمية

التكنولوجية الرقمية	التعريف
مواقع الويب	-هي من أكثر أجزاء الانترنت استخداما للوصول إلى الانترنت. - تعرف بأنّها أجزاء متعددة من التكنولوجيا الرقمية. -تزود مستخدميها بأنواع كبيرة ومتعددة من المعلومات. -أصبحت تفاعلية بوصول الجيل الثالث من الويب.

	- المواقع التالية الأكثر زيارة على الويب: غوغل و يوتوبوالفايس بوك. -المتصفح كروم هو الرائد بين المتصفحات بنسبة 64.06 % وسفاري بنسبة 19.22 % وميكرو سوفت ايدج بنسبة 4.19% و 3.91 %لفاير فوكس*.
الهواتف الذكية	-ظهور الهواتف الذكية هو قوة دافعة لنمو التكنولوجيا الرقمية: 92.1 % من مستخدمي الانترنت يستخدمون الهواتف الذكية من أجل تصفح الانترنت، مقابل 71.2 % لأجهزة الكمبيوتر بأنواعها المكتبية والمحمولة، 27.2 % للأجهزة اللوحية. - غيرت الهواتف المحمولة طريقة التواصل (شفهيا أو رسائل نصية وحتى صوتية). تحتوي على تكنولوجيات رقمية كالكاميرات والآلات الحاسبة وغيرها من تطبيقات الهواتف الذكية والتي يمكن تحميلها.
أجهزة الكمبيوتر	-تشمل أجهزة الكمبيوتر المحمولة و المكتبية، والتي أصبحت أقل حجما وأخف وزنا وأكثر سرعة. -تتضمن هذه الأجهزة برامج وتطبيقات يمكن تحميلها أو العمل بها مباشرة من مواقع سحابية والتي يمكن من خلالها انجاز العديد من المهام.
وسائل التواصل الاجتماعي	-تشمل منصات التواصل الاجتماعي: Facebookو LinkedIn و Twitter وInstagram و Tik Tok. -تجمع بين تقنيات مختلفة للتكنولوجيا الرقمية للسماح للمستخدمين بالتواصل من خلال النصوص والصور والفيديو وغيرها. -تعتمد تطبيقات الوسائط الاجتماعية بشكل كامل تقريبا على المحتوى الذي ينشئه المستخدم. -وصل عدد مستخدمي الشبكات الاجتماعية إلى 4.62 مليار شخص في جانفي 2022، ما نسبته 58.4 % من عدد سكان العالم؛ 53.9 % رجال و 46.1% منهم نساء. مع قضاء ما مدته 2سا و27 د. -تعتبر واتساب المنصة المفضلة لمستخدمي الانترنت بنسبة 15.7 بالمئة مقابل 14.8 % للانستغرام و 14.5 %للفيسبوك. ويعتبر الفايسبوك منصة التواصل الاجتماعي الأكثر استخداما في العالم فيما يعادل 60 % من مجمل سكان العالم.
الجيل الخامس للأنترنت	-يوفر الجيل الخامس من تكنولوجيا شبكات الاتصالات نظاما لشبكات لاسلكية أفضل وأكثر ذكاء وأسرع وأكثر ثباتا -يحفز التحسينات في العديد من التطورات الأخرى مثل الأجهزة الأكثر ارتباطا وتدفقات البيانات الضخمة الأكثر ثراء.
انترنت الأشياء	-شبكة تربط بين الأجهزة والمركبات والأدوات المنزلية التي تشمل على مكونات إلكترونية وبرامج ومحركات، بالإضافة إلى خاصية اتصال تتيح لها إمكانية التواصل فيما بينها والتفاعل وتبادل البيانات.
الحوسبة	- هي نظام يتم فيه تسجيل البيانات الضخمة وتخزينها على معالجات أخرى واسترجاعها عبر

السحابية	الإنترنت.
الطباعة الثلاثية الأبعاد	-استخدام أساليب التصنيع الإضافي صناعة منتجات ثلاثة الأبعاد بطريقة طباعة طبقات متتالية من المادة الخام فوق بعضها البعض.
الذكاء الاصطناعي	-يدعى أيضا بالذكاء الآلي: مجموعة خوارزميات حاسوبية مهيأة للتعلم وقادرة على آداء مهام تحتاج إلى ذكاء بشري وإدراك بصري والتعرف على الكلام واتخاذ القرار. -يعمل من خلال الخوارزميات على محاكاة عملية الذكاء البشري بواسطة الآلات التي تعمل وتتفاعل مثل الإنسان. -يعتبر القوة المؤثرة وراء العديد من حركات التكنولوجيا الرقمية الأخرى التي ظهرت والتي يمكن أن تظهر.
أجهزة الصراف الآلي	.تم تطويرها في لندن في عام 1967 ومنذ ذلك الحين أصبحت عالمية. - تعتبر طريقة سريعة وبسيطة، تسهل وصول الأشخاص إلى حساباتهم المصرفية. -يمكن استخدام أجهزة الصراف الآلي الحالية لأنشطة مثل السحب النقدي أو إيداع الأموال أو التحقق من الأرصدة المصرفية أو الهواتف المحمولة الائتمانية.
مواقع الجهاز	-تشير إلى الجمع بين التكنولوجيا الرقمية والأقمار، مثل الهاتف الذكي أو جهاز GPS أو نظام متصل بالإنترنت، يمكن قياسه بشكل صحيح للغاية. يمكن بعد ذلك استخدام هذه البيانات مع التطبيقات الرقمية الأخرى، مثل تقنية رسم الخرائط، لتزويد المستخدمين بالمعلومات ذات الصلة وفقا لموقعهم.
الواقع المعزز	تقنية تضيف معلومات رقمية إلى معلومات مأخوذة من البيئة المحيطة، فتعرضها معا عبر صورة مركبة غنية بالمعلومات. وعلى عكس تقنية الواقع الافتراض لا تعرض تقنية الواقع المعزز بيئة اصطناعية بالكامل وإنما تدمج المعلومات الجديدة مع المعلومات المستقاة من الواقع.
سلسلة الكتل الرقمية أو قواعد البيانات المتسلسلة **"Blockchain"**	-منصة عمل عامة لا مركزية تعمل كدفتر حساب لجميع العمليات والمعاملات. - تخزن سجلات تتبع المعاملات لعامة الناس في سجلات مختلفة، تسمى"السلسلة"، وفق نظام مرتبط. عادة، يعرف هذا التخزين باسم "دفتر الأستاذ الرقمي". -يتم اعتماد كل معاملة في هذا الدفتر من خلال التوقيع الرقمي لحاملها، والذي يتحقق من المعاملة ويحميها من التلف. لذلك، فإن البيانات التي يتكون منها دفتر الأستاذ الرقمي آمنة للغاية.
الطائرات دون طيار	- هي استخدام مسلح للتكنولوجيا الرقمية: تقاتل مع المركبات الطائرة والصواريخ الموجهة وتدمج التكنولوجيا الرقمية من أجل الأداء بنجاح. -يتم توجيه الطائرات بدون طيار في الوقت الفعلي بواسطة عنصر تحكم بشري بعيد. تستخدم الصواريخ التكنولوجيا الرقمية لإدارتها وتوجيهها وهياكل طيرانها.

الكاميرات الرقمية	-تتمتع بمرونة أفضل بكثير من الكاميرات القديمة، خاصة عند استخدامها مع التقنيات الرقمية الأخرى. -الصور الرقمية أبسط في التخزين والإنشاء والتحرير والطباعة والبريد الإلكتروني. يمكن للعديد من الكاميرات الرقمية أيضا إنشاء مقاطع فيديو أيضا.
الروبوتات	-آلات كهربائية ميكانيكية أو حيوية أو هجينة يوظف فيها الذكاء الاصطناعي لتنفيذ أنشطة بشرية آليا، أو تعزيزها أو المساعدة في تنفيذها، سواء عبر التشغيل الآلي أو باتباع توجيهات محددة. -يعمل خبراء التكنولوجيا على روبوتات نانوية صغيرة من خلال التكنولوجيا النانوية، يمكن إدخالها في جسم البشر لإجراء تحقيقات وتدابير طبية.

المصدر: من إعداد الباحثتين بالاعتماد على:

-Kevin JOHNSON, What is Digital Technology ? 25 Best Examples, consulté le: 10/06/2022, Site: https://honestproscons.com/what-is-digital-technology-25-best-examples/

-دائرة الشؤون الخارجية للاتصالات، مسرد الثورة الصناعية الرابعة: انجليزي-عربي، شركة تنمية نفط عمان، عمان، جانفي 2019، تاريخ الاطلاع: 2022/06/15، الموقع: https://www.pdo.co.om/en/news/publications/Publications%20Doc%20Library/4IR%20Glossary.pdf

-claraLOUISET , Digital report 2022 : les chiffres clés d'internet et des réseaux sociaux, consulté le :10/05/200, site : https://www.influenth.com/digital-report-2022-les-chiffres-cles-dinternet-et-des-reseaux-sociaux/

ضمن هذا السياق تجدر الإشارة أن الميزة التي تتمتع بها التكنولوجيات الرقمية وهي في مرحلتها الحالية –الثورة الصناعية الرابعة- هي إمكانية الجمع بين عدة تقنيات، حيث بشكل الترابط بين هذه الابتكارات عالية التقنية بيئة فيزيائية إلكترونية تتطلب ضرورة إعادة التفكير في كيفية استخدام هذه الموارد والتقنيات.ليطلق عليها اسم التكنولوجيات الرائدة أو التكنولوجيات الجديدة، للإمكانية التي تتمتع بها هذه التكنولوجيات للاستفادة من أساليب الرقمنة والاتصال الإلكتروني، حيث يمكنها الجمع بين هذه التكنولوجيات ومضاعفة آثارها.[20]

رابعا: تطبيقات التكنولوجيا الرقمية

أصبحت عملية الأتمتة في ظل الثورة الصناعية الرابعة تتم بطريقة أكثر ذكاءا من خلال استخدام تكنولوجيا الذكاء الاصطناعي وانترنت الأشياء والروبوتيك وغيرها، حيث أصبحنا نتكلم عن الأشياء الذكية والتي تشمل التعلم الذكي والعملات المشفرة والتجارة الذكية والمدن الذكية والحكومة الذكية والبني التحتية الذكية وغيرها. حيث تشير الأشياء الذكية إلى المجالات التي يمكن استخدام تكنولوجيا الثورة الصناعية الرابعة ضمنها، والتي

ستكون لهذه التقنيات تداعياتها على النمو الاقتصادي والقدرة على المنافسة والسياسة والتماسك الاجتماعي وغيرها.[21]

من هنا أصبحت التكنولوجيا الرقمية تقوم بالعديد من الوظائف والعمليات التي كانت موكلة للإنسان، حيث تؤكد ضمن هذا الإطار بحوث الاتحاد الدولي للاتصالات أن فرص العمل ستكون لذوي المهارات المتقدمة في السنوات القادمة (حيث يقصد بالمهارات المتقدمة القدرة على التعامل مع الواقع الافتراضي والبيانات الضخمة والذكاء الاصطناعي والأمن السيبيراني وانترنت الأشياء وغيرها[22]).

تتعدد مجالات تطبيق التكنولوجيا الرقمية، حيث تشمل جميع المجالات (الصحة والتعليم والاقتصاد والثقافة وغيرها)، من خلال ما توفره من فرص ومكاسب بشكل أكثر سرعة وكفاءة وأمان ودقة. ويعتبر الاقتصاد من خلال الاقتصاد الرقمي الأوفر حظا في استخدام التكنولوجيات الرقمية الناتجة عن الثورة الصناعية الرابعة، كما تؤثر التكنولوجيا الرقمية من خلال مختلف المنصات الرقمية (التي تستخدم الذكاء الاصطناعي وتكنولوجيا البلوكتشينو غيرها) المستخدمة في أسلوب عمل الحكومات والمؤسسات ومشاركة المواطنين في مختلف أوجه الحياة.

من هذا المنطلق جعلت التكنولوجيا الرقمية مختلف العمليات الروتينية ذات المعاملات المتعددة أسهل وأسرع وأكثر ملاءمة وراحة ودقة ومتعة نتيجة لكل هذه التطورات. وسنركز فيما يلي على بعض التطبيقات الذكية للتكنولوجية الرقمية.

1-الحكومة الذكية

مر تطور الحكومة الإلكترونية بمجموعة من المراحل انتقالا من حكومة إلكترونية عام 1999 إلى حكومة ذكية مع حلول عام 2013 [23]، كاتجاه لتطوير خدمات الحكومة الإلكترونية والذي ارتبط ظهورها بثورة تكنولوجيا المعلومات والاتصال خاصة الانترنت ضمن العمل الحكومي، حيث وصل عدد الدول الأعضاء في الأمم المتحدة والتي تملك موقعا إلكترونيا حكوميا 193 دولة ولكن بنسب متفاوتة من تقديم الخدمات الإلكترونية.[24]

وتعتبر الحكومة الذكية التطور الطبيعي للحكومة الإلكترونية مستغلة الأجهزة الذكية لتسهيل النفاذ للخدمات الحكومية لأكبر عدد من المستفيدين في أي وقت ومن أي مكان، متجاوزة بذلك الحدود الزمانية والمكانية، والاقتراب أكثر من المواطن وانشغالاته ومتطلباته

من خلال التفاعل المباشر والمتزامن مع مختلف البيانات المنتشرة في المجتمع وبمختلف مكوناته. وتتميز الحكومة الإلكترونية بأربعة خصائص[25]:

-**مطاطة**: من خلال القدرة على استيعاب الطلب المتزايد على الطاقة الحاسوبية ومتطلبات التخزين بطريقة ديناميكية.

-**جوالة**: من خلال نشر مختلف الخدمات الحكومية على الأجهزة الذكية من هواتف ذكية ولوحات إلكترونية بطريقة فعالة وأمنة.

-**اجتماعية**: حيث تتفاعل الحكومة الذكية مع جمهورها بشفافية وتشارك في الحراك الإلكتروني الاجتماعي.

-**حساسة**: من خلال التقاط مختلف البيانات المنتشرة حولها من مختلف القطاعات كالصحة والطاقة والبيئة وغيرها من خلال أجهزة الاستشعار الذكية المرتبطة بشبكة انترنت الحكومة.

2-المدينة الذكية

عرّف الاتحاد الدولي للاتصالات ولجنة الأمم المتحدة الاقتصادية لأوروبا في 2015 المدينة الذكية بأنها: "مدينة مبتكرة تستخدم تكنولوجيا المعلومات والاتصالات لتحسين نوعية الحياة، وكفاءة العمليات والخدمات الحضرية، والقدرة على المنافسة، وتلبي في نفس الوقت ذاته احتياجات الأجيال الحالية والقادمة فيما يتعلق بالجوانب الاقتصادية والاجتماعية والبيئية، والثقافية".[26]

لا توجد لحد اليوم مدن ذكية بشكل تام ولكنها في طريقها إلى تحقيق ذلك، حيث تعتمد هذه المدن على التكنولوجيات الرقمية لتنظيم حركة المرور ولتعزيز كفاءة استهلاك الطاقة وإدارة المخلفات، تحسين الإسكان والرعاية الصحية، تحسين تدفق حركة المرور والسلامة، الكشف عن جودة الهواء، تنبيه الشرطة إلى الجرائم التي تحدث في الشوارع وتحسين شبكات المياه والصرف الصحي.

تعتبر التطورات التي تعرفها التكنولوجيات الرقمية في ظل الثورة الصناعية الرابعة (استخدام تكنولوجيا الذكاء الاصطناعي، التوأمة الرقمية: الواقع الافتراضي والواقع المعزز، الروبوتات ومختلف شبكات الجيل الثالث والرابع من الانترنت وغيرها) داعما لتطوير هذا النوع من المدن، حيث تمكن الأجهزة المجهزة بأجهزة الاستشعار الذكية من التواصل فيما بينها وجمع المعلومات في الوقت الفعلي وإرسال هذه البيانات عبر الاتصالات اللاسلكية إلى أنظمة التحكم المركزية، كما تستخدم تقنيات الذكاء الاصطناعي في تحليل البيانات من أجل

الكشف عن الأنماط التي تستخدم من أجل صنع القرار وتعزيزه[27]. ويروج الاتحاد الدولي للاتصالات منذ 2021 في جعل المجتمعات الريفية أكثر ذكاءا واستدامة من خلال القرى والجزر الذكية.[28]

ويصدر المعهد الدولي للتنمية الإدارية في سويسرا بالتعاون مع جامعة سنغافورة للتكنولوجيا والتصميم، مؤشرا للمدن الذكية والتي كان عددها 118 مدينة في 2021، حيث تحتل سنغافورة (سنغافورة)، زيوريخ (سويسرا)، أوسلو (النرويج)، تايبيه (تايوان)، لوزان (سويسرا) المراتب الخمسة الأولى بهذا الترتيب من بين 118 مدينة ذكية.في حين تحتل أبو ظبي (الإمارات)، دبي (الإمارات)، الرياض (السعودية)، المدينة المنورة (السعودية)، المدينة المنورة (السعودية) المراتب: 28، 30،29، 73، 103 على التوالي[29].

3-التجارة الذكية

تعتبر التجارة الذكية أو التجارة عبر الهواتف الذكية الجيل الثاني من التجارة الإلكترونية، أين يتم استخدام الأجهزة المحمولة كالهواتف الذكية واللوحات الذكية وغيرها في البيع والشراء وغيرها. مغيرة بذلك الطريقة التي تتعامل بها الشركات مع عملائها، أو الموردون مع زبائنهم، وهي أنواع مثلها مثل التجارة الإلكترونية حيث نجد: مؤسسات لمؤسسات (B2B)أو فرد مقابل فرد (P2P) أو فرد لمؤسسة (P2B) وغيرها.وتشمل التجارة الذكية توفير مواقع الويب والتطبيقات المجهزة خصيصا للهواتف الذكية، والتي من شأنها القيام بالتسوق الإلكتروني أو تقديم الخدمات المصرفية أو القيام بالمدفوعات عبر الهاتف الذكي...إلخ[30].

كما أدى تنامي استخدام انترنت الأشياء وتكنولوجيا الذكاء الاصطناعي وتكنولوجيا البلوكتشين وغيرها لتنامي الحديث عن المصانع الذكية والمستودعات الذكية والجرد الذكي من خلال استخدام الرفوف الذكية وغيرها.

4-التعلم الذكي

يعتبر التعليم الذكي مرحلة لاحقة لإدخال التكنولوجيا في المؤسسات التعليمية، حيث يمكِّن التعليم الذكي من:توفير الوقت وزيادة الإنتاجية وقدرة لتجاوز حدود الزمان والمكان وفي استيعاب الأعداد الكبيرة للمتعلمين. ويعتبر المتعلِّم محور عملية التعليم الذكي من خلال التفاعل والمشاركة الفاعلة في التعلم، حيث تضطلع فيه التكنولوجية الرقمية بدور فاعل وأساسي.[31]

يعرّف التعليم الذكي بأنه: "منظومة تعليمية لتقديم البرامج التعليمية أو التدريبية للمتعلمين أو المتدربين في أي وقت وفي أي مكان باستخدام المستحدثات التكنولوجية

وتكنولوجيا المعلومات والاتصالات التفاعلية، مثل: الويب،والسبورة الذكية، وقنوات اليوتوب، والبريد الإلكتروني، وأجهزة الحاسوب، والمؤتمرات الصوتية والمرئية عن بعد لتوفير بيئة تعليمية تفاعلية متعددة المصادر بطريقة متزامنة في الفصل الدراسي أو غير متزامنة عن بعد. دون الالتزام بمكان محدد، واعتمادا على التعلم الذاتي والتفاعل بين المحاضر والمتعلم".[32]

ومنه يسمح التعليم الذكيبالتواصل الفعال بين مكونات العملية التعليمية وما تحدثه من تغيير في المنهجية التقليدية للتعلم وفي بيئات التعلم، متجاوزا بذلك الحدود الجغرافية والزمانية للعملية التعليمية.

خاتمة:

توصلت الدراسة إلى النتائج التالية:

1-باعتبار التغير أو التوجه نحو التكنولوجيات الرقمية لا رجعة فيه، يصبح الاستثمار في التكنولوجيا الرقمية ضروري لما تحققه من إمكانية للنمو وتوفير فرص للعمل والخدمات وكل تأخر في فهمها ومن ثم استخدامها يزيد من تكلفة الفرصة الضائعة حيث تصبح تكلفة اللحاق بالركب كبيرة.

2- التكنولوجيا الرقمية وهي في مرحلتها الحالية انتقلت إلى تطبيقات أكثر فأكثر ذكاءا حيث أصبحنا نتكلم عن الحكومة الذكية، والتجارة الذكية والمدن الذكية والتعلم الذكي وغيرها.

3-التكنولوجيا الرقمية وهي في مرحلتها الحالية تتميز بالقدرة على دمج مجموعة من التكنولوجيات فيما بينها، الأمر الذي سينتج عنه ظهور تكنولوجيات أكثر فأكثر ذكاءا من خلال استخدام تكنولوجيا الذكاء الاصطناعي وانترنت الأشاء وسلسلة الكتل وغيرها.

3-التطور المستمر للتكنولوجيات الرقمية يفرض ضرورة التعلم مدى الحياة للمهارات الضرورية للتعامل معها.

4-إن الاستفادة من المزايا التي توفرها التكنولوجيا الرقمية تفرض بنية تحتية متاحة وبأسعار معقولة ومستقرة وآمنة وموثوقة.

5-تعرف التكنولوجيا الرقمية منذ الثورة الصناعية الرابعة تطورا متناميا عرف بتسونامي التكنولوجيا، يستدعي فهمها والإحاطة بها حتى لا نصبح خارج الركب.

6--أصبحت البيانات الضخمة -الناتجة عن التكنولوجيا الرقمية- **تشكل قوة اجتماعية**، نتج عنها عدة مشكلات اجتماعية تثير مخاوفا على عدة مستويات: أخلاقية، اجتماعية، ثقافية، سياسية... الخ.

توصيات الدراسة:

1-ضرورة الاستثمار في التكنولوجيات الرقمية لما تحققه من فرص للاحتواء وتحقيق الكفاءة والابتكار.

2-ضرورة توفير الانترنت للجميع وبتكلفة ميسورة، دونها تعتبر الاستفادة من مزايا استخدام التكنولوجيات الرقمية غير ذي أهمية.

3-التطور المستمر للتكنولوجيات الرقمية يفرض ضرورة التعلم مدى الحياة للمهارات الضرورية للتعامل معها.

---

[1] Kevin JOHNSON, What is Digital Technology ?25 Best Examples, consulté le: 10/06/2022, Site: https://honestproscons.com/what-is-digital-technology-25-best-examples/

[2] لبنى جلال سكيك، "استخدام التكنولوجيا الرقمية في النشرة الإخبارية التلفزيونية: "نشرة الأخبار الرئيسية في التلفزيون الجزائري نموذجا"، مذكرة ماجستير، تخصص: الإعلام والاتصال، جامعة الجزائر بن يوسف بن خدة، كلية العلوم السياسية والإعلام، قسم علوم الإعلام والاتصال، 2007-2008، ص11.

[3] نفس المرجع السابق، ص11.

[4] نفس المرجع السابق، ص11.

[5] نفس المرجع السابق، ص ص 11،12.

[6] نفس المرجع السابق، ص12.

[7] Degital Technology,consulté le : 25/06/2022, Site : https://www.encyclopedia.com/history/dictionaries-thesauruses-pictures-and-press-releases/digital-technology

[8] نيكولاس نيجروبونت، ترجمة : سمير إبراهيم شاهين، التكنولوجيا الرقمية: ثورة جديدة في نظم الحاسبات والاتصالات، الطبعة الأولى، مكتبة الإسكندرية، القاهرة، 1998، ص ص 9،10.

[9] لبنى جلال سكيك، مرجع سبق ذكره، ص 108.

[10] نفس المرجع السابق، ص13.

[11] نفس المرجع السابق، ص 108.

[12] نفس المرجع السابق، ص12.

[13] نفس المرجع السابق، ص 109.

[14] نفس المرجع السابق، ص27.

[15] نفس المرجع السابق، ص ص 110، 111.

[16] فريد راغب النجار، الاستثمار بالنظم الالكترونية للاقتصاد الرقمي، مؤسسة شباب الجامعة، مصر، 2004، ص 34.

[17] مجموعة البنك الدولي، تقرير عن التنمية في العالم 2016: العوائد الرقمية (عرض عام)، البنك الدولي، 2016، ص 05، تاريخ الاطلاع: 2022/05/10، الموقع: https://documents1.worldbank.org/curated/en/198711468001491553/pdf/102724-ARABIC-Revised-WDR2016Overview-PUBLIC.pdf

[18] محمد قيس عادل القنبري، أثر التقنيات الحديثة للثورة الصناعية الرابعة على المحاسبة والمراجعة، Third international conference on technical sciences (ictst 2020).28-30 novembre 2020, Tripoli, Libya, p205, consulté le : 10/05/2022, site :https://unctad.org/system/files/official-document/tir2020overview_ar.pdf

[19] نفس المرجع السابق، ص 208.

[*] claraLOUISET , Digital report 2022 : les chiffres clés d'internet et des réseaux sociaux, consulté le :10/05/200, site : https://www.influenth.com/digital-report-2022-les-chiffres-cles-dinternet-et-des-reseaux-sociaux/

[20] مؤتمر الأمم المتحدة للتجارة والتنمية، الأونكتاد، "تقرير التكنولوجيا والابتكار 2021: اللحاق بركب موجات التقدم التكنولوجي (التوفيق بين الابتكار والانصاف)، الأمم المتحدة، جنيف، 2021، ص 7.

[21] محمد قيس عادل القنبري، مرجع سبق ذكره، ص 208.

[22] الاتحاد الدولي للاتصالات، مجموعة أدوات المهارات الرقمية، جنيف، سويسرا، 2018، تاريخ الإطلاع: 2022/05/12، الموقع: https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/Digital-Skills-Toolkit_Arabic.pdf

[23] سالم زغبي، تعزيز المدن الذكية في برامج الحكومة الذكية، اجتماع افتراضي لمديري الحكومة الإلكترونية في المنطقة العربية، الاسكوا، الأمم المتحدة، ديسمبر 2021، تاريخ الإطلاع: 2022/06/25، الموقع: https://www.unescwa.org/sites/default/files/event/materials/4-Smart-city-support-Saleem-Zoughbi-Ar.pdf

[24] لونيس نادية، الحكومة الذكية كاتجاه حديث لتطوير الخدمات الحكومية الإلكترونية، مجلة دراسات في الاقتصاد والتجارة والمالية، مخبر الصناعات التقليدية لجامعة الجزائر 03، المجلد 06، العدد03، 2017، ص ص 1061، 1066.

[25] نفس المرجع السابق، ص 1068.

[26] الاتحاد الدولي للاتصالات، المدن الذكية، تاريخ الإطلاع: 2022/06/30، الموقع: https://www.itu.int/ar/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx

[27] نفس المرجع السابق.

[28] نفس المرجع السابق.

[29] IMD and all, Smart City Index 2021 : A tool for action, an instrument for better lives for all citizens, Consulté le : 15/06/2022, Site : www.smartcityindex2021.pdf

[30] LjupchoAntovski, MarjanGuesv, M-commerce sevices, janvier 2003, consulté le :20/06/2022, site : https://www.researchgate.net/publication/228851169_M-Commerce_Services(بالتصرف)

[31] عبد الرحمن تلي، علياء قاسمي الحسني، التطبيقات التربوية لذكاء الاصطناعي –التعليم الذكي نموذجا-، مجلة التربية والصحة النفسية، المجلد السادس، العدد 02، جامعة الجزائر 02، 2021، ص102.

[32] سليمان أحمد حرب، محمود محمد فؤاد برغوت، درجة توافر متطلبات التعلم الذكي بمؤسسات التعليم العالي التابعة لوزارة التربية والتعليم العالي الفلسطينية"، مجلة تاريخ العلوم، العدد 12، جانفي2019، صص 59، 60.

قائمة المراجع:

1-الكتب:

- فريد راغب النجار، الاستثمار بالنظم الالكترونية للاقتصاد الرقمي، مؤسسة شباب الجامعة، مصر، 2004.

-نيكولاس نيجروبونت، ترجمة : سمير إبراهيم شاهين، التكنولوجيا الرقمية: ثورة جديدة في نظم الحاسبات والاتصالات، الطبعة الأولى، مكتبة الإسكندرية، القاهرة، 1998.

2-المجلات:

- سليمان أحمد حرب، محمود محمد فؤاد برغوت، درجة توافر متطلبات التعلم الذكي بمؤسسات التعليم العالي التابعة لوزارة التربية والتعليم العالي الفلسطينية"، مجلة تاريخ العلوم، العدد 12، جانفي 2019.

-لونيس نادية، الحكومة الذكية كاتجاه حديث لتطوير الخدمات الحكومية الإلكترونية، مجلة دراسات في الاقتصاد والتجارة والمالية، مخبر الصناعات التقليدية لجامعة الجزائر 03، المجلد 06، العدد03، 2017.

-عبد الرحمن تلي، علياء قاسمي الحسني، التطبيقات التربوية للذكاء الاصطناعي –التعليم الذكي نموذجا، مجلة التربية والصحة النفسية، جامعة الجزائر 02، المجلد السادس، العدد 02، 2021.

3-الرسائل الجامعية:

- لبنى جلال سكيك، "استخدام التكنولوجيا الرقمية في النشرة الإخبارية التلفزيونية: "نشرة الأخبار الرئيسية في التلفزيون الجزائري نموذجا"، مذكرة ماجستير، تخصص: الإعلام والاتصال، جامعة الجزائر بن يوسف بن خدة، كلية العلوم السياسية والإعلام، قسم علوم الإعلام والاتصال، 2007-2008.

4-مراجع إلكترونية:

-باللغة العربية:

-الاتحاد الدولي للاتصالات، المدن الذكية، تاريخ الإطلاع: 2022/06/30، الموقع: https://www.itu.int/ar/mediacentre/backgrounders/Pages/smart-sustainable-cities.aspx

–الاتحاد الدولي للاتصالات، مجموعة أدوات المهارات الرقمية، جنيف، سويسرا، 2018، تاريخ الإطلاع: 2022/05/12، الموقع: https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/Digital-Skills-Toolkit_Arabic.pdf

-سالم زغبي، تعزيز المدن الذكية في برامج الحكومة الذكية، اجتماع افتراضي لمديري الحكومة الإلكترونية في المنطقة العربية، الاسكوا، الأمم المتحدة، ديسمبر 2021، تاريخ الإطلاع: 2022/06/25، الموقع: https://www.unescwa.org/sites/default/files/event/materials/4-Smart-city-support-Saleem-Zoughbi-Ar.pdf

-دائرة الشؤون الخارجية للاتصالات، مسرد الثورة الصناعية الرابعة: انجليزي-عربي، شركة تنمية نفط عمان، عمان، جانفي 2019، تاريخ الاطلاع: 2022/06/15، الموقع: https://www.pdo.co.om/en/news/publications/Publications%20Doc%20Library/4IR%20Glossary.pdf

-شركة برايس ووترهاوس كوبرز(PWC)، القمة العالمية للصناعة والتصنيع(GMIS)، استطلاع الثورة الصناعية الرابعة(Industry 4.0) في الشرق الأوسط لعام 2016: الثورة الصناعية الرابعة: بناء المؤسسات الصناعية الرقمية، تاريخ الإطلاع: 2022/05/10، الموقع: https://www.pwc.com/m1/en/publications/documents/middle-east-industry-4-0-survey-ar.pdf

-مجموعة البنك الدولي، تقرير عن التنمية في العالم 2016: العوائد الرقمية (عرض عام)، البنك الدولي، 2016، تاريخ الاطلاع: 2022/05/10، الموقع: https://documents1.worldbank.org/curated/en/198711468001491553/pdf/102724-ARABIC-Revised-WDR2016Overview-PUBLIC.pdf

-محمد عبد القادر الفقي، الثورات الصناعية الأربع: إطلالة تاريخية، مجلة التقدم العلمي، العدد 103، أكتوبر 2018، تاريخ الإطلاع: 2022/05/20، الموقع: https://taqadom.aspdkw.com/wp-content/uploads/2019/01/taq-103-october-2018.pdf

-محمد قيس عادل القنبري، أثر التقنيات الحديثة للثورة الصناعية الرابعة على المحاسبة والمراجعة، Third international conference on technical sciences (ictst 2020).28-30 novembre 2020, Tripoli, Libya, consulté le : 10/05/2022, site : الموقع: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3910850

-مؤتمر الأمم المتحدة للتجارة والتنمية، الأونكتاد، "تقرير التكنولوجيا والابتكار 2021: اللحاق بركب موجات التقدم التكنولوجي (التوفيق بين الابتكار والانصاف)، الأمم المتحدة، جنيف، 2021، الموقع: https://unctad.org/system/files/official-document/tir2020overview_ar.pdf

-باللغة الإنجليزية:

_clara LOUISET , Digital report 2022 : les chiffres clés d'internet et des réseaux sociaux, consulté le :10/05/200, site : https://www.influenth.com/digital-report-2022-les-chiffres-cles-dinternet-et-des-reseaux-sociaux/

_ Kevin JOHNSON, What is Digital Technology ? 25 Best Examples, consulté le: 10/06/2022, Site: https://honestproscons.com/what-is-digital-technology-25-best-examples/

[-]LjupchoAntovski,MarjanGuesv, M-commerce sevices, janvier 2003, consulté le :20/06/2022, site : https://www.researchgate.net/publication/228851169_M-Commerce_Services)

-DegitalTechnology,consulté le : 25/06/2022, Site : https://www.encyclopedia.com/history/dictionaries-thesauruses-pictures-and-press-releases/digital-technology

-Kevin JOHNSON, What is Digital Technology ? 25 Best Examples, consulté le: 10/06/2022, Site: https://honestproscons.com/what-is-digital-technology-25-best-examples/

دور التكنولوجيا الرقمية في إدارة الموارد البشرية

The role of digital technology in human resource management

بوغـولـة فطيمة طالبة دكتوراه حقوق
كلية الحقوق جامعة الجــزائـــــر- 1- بن
يوسف بن خدة -سعيد حمدين- الجزائر.
lamtww32@gmail.com

ملخص :

في ظل التغيرات التي يمر بها الاقتصاد العالمي إلى جانب التغيرات التقنية التي أتاحتها الرقمنة و التحول الرقمي من خلال تكنولوجيا المعلومات وخاصة الانترنت والتطور في الفكر الإداري، فإن إدارة الموارد البشرية تتعرض لتغيير جذري في مفاهيمها وسياساتها واستراتيجياتها وممارساتها، و يعتبر تطبيق الإدارة الإلكترونية ضرورة حتمية لمواكبة التطورات الحاصلة في مختلف المجالات، وفي هذا المقال، سوف يتم التطرق إلى دراسة دور التكنولوجيا الرقمية في إدارة الموارد البشرية.

الكلمات المفتاحية : تكنولوجيا المعلومات ؛ الأنترنيت ؛ الرقمنة ؛ التحول الرقمي ؛ الإدارة الإلكترونية .

Abstract:

Lack of management in light of the changes that the global economy is going through, in addition to the technical changes made possible by digitization and digital transformation through information technology, especially the internet and the development in management thought, the management of human resources is subjected to a radical change in its concepts, policies, strategies and practices and the application of electronic management is an absolute necessity to keep pace with developments in various fields, and in this interventions, The study the role of digital technology in human resources management will be addressed.

Keywords: Information technology ; the internet ; digitation ; digital transformation ; electronic management.

مقدمة:

إن إدارة الموارد البشرية في ذلك النشاط الإداري المتعلق بتحديد احتياجات المؤسسة من القوى العاملة، والعمل على توفيرها بالأعداد والكفاءات التي تتناسب مع احتياجات المؤسسة، والعمل أيضا على استخدام تلك الموارد استخداما فعالا في تحقيق الإنتاجية، وتواجه إدارة الموارد البشرية في عصرنا الحالي تحديات كبيرة في العام والخاص، كالتغيرات السياسية والاقتصادية والاجتماعية والتكنولوجية والحضارية، وهي تغيرات سريعة ومعقدة.

و في ظل هذه التغيرات التي يمر بها الاقتصاد العالمي إلى جانب التغيرات التقنية التي أتاحتها تكنولوجيا المعلومات وخاصة الانترنت والتطور في الفكر الإداري، فإن إدارة الموارد البشرية تتعرض لتغيير جذري في مفاهيمها وسياساتها واستراتيجياتها وممارساتها، و بالتالي فبظهور الانترنت وتطور تكنولوجيا المعلومات وأساليب الاتصال، وتحويل وظائف التسويق والمحاسبة والعمليات المختلفة إلى أعمال إلكترونية، ومع زيادة التحول التكنولوجي الرقمي للمؤسسات، أصبح من الضروري تحويل الوظائف والملفات الورقية إلى ملفات إلكترونية، وأصبحت العلاقات بين الإدارة العمومية والمؤسسات والنقابات والعاملين والزبائن تتم عن طريق الشبكات الداخلية والخارجية والانترنت.

وظهر إلى الوجود مصطلحات جديدة مثل الإدارة الالكترونية-الأعمال الإلكترونية، التسويق الإلكتروني إدارة الموارد البشرية إلكترونيا(E-HRM) ، الاستقطاب الإلكتروني، التعليم الإلكتروني والعديد من المسميات الجديدة التي تتعلق كلها بهذا التطور، و يطلق على استخدام التكنولوجيا في إدارة الموارد البشرية أو إدارة الموارد البشرية إلكترونيا مصطلح(E-HRM) ، ويعني تطبيق التقنيات المعتمدة على الويب في النظم المرتبطة بالموارد البشرية ووظائفها.

و من خلال ما سبق ذكره، تم طرح التساؤل والإشكالية التالية:

- ما هو دور التكنولوجيا الرقمية في إدارة الموارد البشرية؟

للإجابة على هذه الإشكالية تم انتهاج كلا من المنهج الوصفي، من خلال معرفة تعاريف عن الإدارة الإلكترونية، و عن الموارد البشرية، و كذا المنهج التحليلي من خلال تحليل المعلومات المتعلقة بالتحول الرقمي و الرقمنة و التكنولوجيا، و هذا من خلال وضع خطة منهجية بمبحثين، المبحث الأول بعنوان: مفهوم الإدارة الإلكترونية، و المبحث الثاني: استخدام التكنولوجيا الرقمية في تسيير الموارد البشرية، ليتم ختام هذا المقال بمجموعة من النتائج و التوصيات الهامة.

المبحث الأول: مفهوم الإدارة الإلكترونية

يعتبر تطبيق الإدارة الإلكترونية ضرورة حتمية لمواكبة التطورات الحاصلة في مختلف المجالات وهذا ما يستدعي تدعيم تطبيقها والاطلاع الدائم على التطورات و التقنيات الحديثة التي يفرضها العالم اليوم، وتوظيفها من أجل تحسين الأداء وتقديم الخدمات وفق المعايير التي تحقق الرضا التام للمستفيدين،

المطلب الأول: تعريف الإدارة الإلكترونية

الإدارة لغة: مشتقة من الفعل "أدار" وأدار الشيء أي تعاطاه تولى السهر على حسن عمله "أدار المؤسسة".

والإدارة (Management) يقصد بها:" عملية التسيير، وهي تنسيق الموارد الكلية للمؤسسة وذلك بغرض تحقيق الأهداف المطلوبة لتلك المؤسسة من خلال تنفيذ مجموعة من الوظائف المتعلقة ببعضها مثل التخطيط، التنظيم، تدبير الأفراد، والتوجيه والمراقبة". وهو ما يؤكد حقيقة أن الإدارة هي المحرك الفعلي للوظائف داخل النظام.

ورغم حداثة مصطلح الإدارة الإلكترونية فقد تنوع تعريفها بين المفكرين والمهتمين الذين تعرضوا لهذا المفهوم. يعرفها البنك الدولي بكونها:" مفهوم ينطوي على استخدام تكنولوجيا المعلومات والاتصالات، بتغيير الطريقة التي يتفاعل من خلالها المواطنين والمؤسسات التجارية مع الحكومة للسماح بمشاركة المواطنين في عملية صنع القرار، وربط طرق أفضل في الوصول على المعلومات، وزيادة الشفافية، وتعزيز المجتمع المدني".

ويبين هذا التعريف أثر الإدارة الإلكترونية في تغيير طريقة التواصل بين مختلف الفواعل داخل الدولة[1].

كما يمكن تعريفها على أنها "نظام إلكتروني متكامل يعتمد على تكنولوجيا المعلومات والاتصالات، لتحويل كافة الأعمال الإدارية التقليدية إلى أعمال إلكترونية تعتمد على التكنولوجيا الرقمية والحديثة".

أما بالنسبة إلى الإدارة الإلكترونية في القطاع العام فيمكن القول أنها "رؤية جديدة لمفهوم الإدارة العامة في عصر المعلومات، تعمل على تمكين جميع المؤسسات والوزارات والهيئات العامة من ممارسة كافة أعمالهم وتعاقداتهم وتقديم أفضل الخدمات للجمهور مع أفضل استغلال للوسائل

---

[1] عروسى وداد، الإدارة الإلكترونية وتطبيقاتها في الخدمة العمومية نموذج قطاع العدالة، مذكرة ضمن متطلبات نيل شهادة الماستر في العلوم السياسية تخصص سياسات عامة، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور –الجلفة، 2019-2020، ص 11.

الحديثة المتاحة للتكنولوجيا والاتصال، من خلال توظيف ما هو متاح معنويا وبشريا وماديا في المجال الإلكتروني الحديث لاستغلال الوقت والجهد والمال على أفضل وجه لتحقيق المصلح العامة"[2].

المطلب الثاني: خصائص وأهداف الإدارة الإلكترونية.

للإدارة الإلكترونية مجموعة خصائص و أهداف، و هو ما تم التطرق له في فرعين منفصلين فيما يأتي.

الفرع الأول: خصائص الإدارة الإلكترونية

تنصف الإدارة الالكترونية بمجموعة من الخصائص التي تميزها عن الإدارة التقليدية، وتنعكس هذه الخصائص على المؤسسات التي تمارس الأعمال الإدارية الكترونيا، ومن هذه الخصائص:

1-السرعة والوضوح في تحقيق الأهداف

يؤدي تطبيق الإدارة الالكترونية إلى إمكان تحقيق أهداف المؤسسة بصورة عالية من خلال الاعتماد على الوسائل الالكترونية الحديثة، وما تقدمه تكنولوجيا المعلومات والاتصالات من دعم ومساندة تساهم في وصول السريع للأهداف ومتابعة هذه الأهداف.

2-عدم التقيد بالزمان والمكان

إمكانية المراجعة طوال ساعات اليوم، فمواقع الإدارة متاحة عبر الانترنت ويقوم الحاسوب بالإجابة على أسئلة المراجع ويتلقى منه معاملاته بيسر عبر قائمة من الخيارات والأوامر التي يتيحها.

3- إدارة المعلومات لا الاحتفاظ بها.

وذلك عبر توفير برامج للمراجع تمكنه من انجاز معاملاته عبر شاشاتها وأزرارها وتبسيطها له بدرجة شبه تعليمية.

---

[2] قادة يزيد، اعمر مولاي، تطبيقات الإدارة الإلكترونية في القطاع العمومي خلال جائحة كورونا، دراسة تطبيقية بمديرية الإدارة المحلية بولاية سعيدة، مجلة دراسات في الاقتصاد وإدارة الأعمال، مخبر إدارة وتقييم أداء المؤسسات، جامعة سعيدة - مولاي الطاهر-، المجلد 04، العدد 01 ، جوان 2021، ص 692.

4-المرونة.

وذلك بسبب الاستجابة السريعة للأحداث والتجاوب معها ، متعدية بذلك حدود الزمان والمكان وصعوبة الاتصال مما يعين الإدارة على تقديم الكثير من الخدمات لم تكن متاحة في السابق بسبب عوائق الإدارة التقليدية[3].

الفرع الثاني: أهداف الإدارة الإلكترونية

الإدارة الإلكترونية هي الرغبة في زيادة كفاءة وفعالية نشاط المنظمات، وذلك عن طريق الانتقال من الأساليب التقليدية الورقية إلى أساليب حديثة ومعاصرة، تعتمد على تكنولوجيا المعلومات والاتصال قصد تحقيق جملة من المكاسب والأهداف ونذكر منها:

1- تكريس الشفافية في الأداء والقضاء على البيروقراطية من حيث خفض فرص الفساد الإداري والتقليل من التعقيدات الإدارية.

2- تحقيق مبدأ العدالة في تقديم الخدمة بنفس الدقة والتكلفة والجودة والوقت، إلى جانب المساواة في المعاملة والتقدير والاحترام.

3- سهولة الوصول إلى الخدمة من خلال شبكات الاتصال من أي مكان وفي أي وقت[4].

4- تبسيط الإجراءات داخل الإدارات، وهذا ينعكس إيجابا على مستوى الخدمات التي تقدم إلى المواطنين، ومنه اختصار وقت تنفيذ إنجاز المعاملات الإدارية المختلفة.

5- تسهيل اجراء الاتصال بين المصالح الإدارية المختلفة.

6- الدقة والموضوعية في إنجاز العمليات المختلفة داخل المصالح المختلفة.

7- تقليل استخدام الورق بشكل ملحوظ، وهذا ما يؤثر إيجابيا على عمل الإدارة، ويعالج مشكلة تعاني منها أغلب الإدارات في عملية الحفظ والتوثيق، مما يؤدي إلى عدم الحاجة إلى أماكن التخزين، حيث يتم الاستفادة منها في أمور أخرى.

---

[3] توفيق حناشي، فارس قاطر، واقع الإدارة الالكترونية والمعيقات التي تقلل من تطبيقها مجلة روئ الاقتصادية، جامعة العربي التبسي، تبسة الجزائر، المجلد09، العدد 02، ص 334.

[4] الشيكر أيوب الإدارة الإلكترونية في الجزائر تطبيقات وتحديات، مجلة الإدارة والتنمية للبحوث والدراسات، بمخير تسيير الجماعات المحلية ودورها في تحقيق التنمية، جامعة لونيسي علي، البليدة2، الجزائر، المجلد 08، العدد01 ، 2019، ص 285.

8- سرعة الوصول إلى الوثائق والمعلومات بوجود نظام متكامل في أي وقت و أي زمان لتخفيف تكاليف الجودة وخدمتها[5].

9- تخفيض تكاليف أداء الخدمة مع ميزة السرعة في إنجازها (توفير الجهد والوقت والنفقات).

10- ربط القطاع العام بالقطاع الخاص تحت مظلة واحدة بفضل البنية الإلكترونية التي تجمع القطاعين، فالقطاع العام بحاجة للقطاع الخاص ليحصل على حاجياته من السلع والخدمات، وهذا التواصل بين القطاعين يتم بصورة إلكترونية.

11- قدرة الحكومة الإلكترونية على توفير خدمات عامة متكاملة إلكترونيا.

12- السرعة في بناء الاقتصاد المبني على المعرفة وتكوين مجتمع المعرفة.

13- كفاءة الأداء الحكومي والإعداد للاندماج في النظام العالمي لمواكبة نظم المعلومات الحديثة المتبعة.

14- الارتقاء ثقافة المواطنين من خلال تشجيعهم على استخدام وسائل التكنولوجيا الحديثة.

المبحث الثاني: استخدام التكنولوجيا الرقمية في تسيير الموارد البشرية.

في ظل التغيرات التي يمر بها الاقتصاد العالمي إلى جانب التغيرات التقنية التي أتاحتها تكنولوجيا المعلومات وخاصة الانترنت والتطور في الفكر الإداري، فإن إدارة الموارد البشرية تتعرض لتغيير جذري في مفاهيمها وسياساتها واستراتيجياتها وممارساتها، و من هنا تم تقسيم المبحث لمطلبين، مطلب أول تم تناول فيه مفهوم التحول الرقمي، و مطلب ثان تم تخصيصه لكيفية مساهمة التطور التكنولوجي في إدارة الموارد البشرية.

المطلب الأول: مفهوم التحول الرقمي.

الفرع الأول: تعريف التحول الرقمي

إن التحول الرقمي ليس مجرد استخدام التكنولوجيا الرقمية في مجال الأعمال وريادة الاستثمار فيها، فالتكنولوجيا تعتبر أداة تمكن التحولات الرقمية فيما يجب على المؤسسات التي تسعى لخوض تجربة التحولات الرقمية أن تعرف كيف و كم تستثمر في التكنولوجيا من اجل استغلال الفرص المتاحة ، وعليه فقد تم تعريف التحول الرقمي على أنه التغيير الجذري و المتسارع

[5] بن مبارك ماية، دور المشرع الجزائري في تفعيل الإدارة الإلكترونية، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، المجلد 8، العدد02، ص 74.

في الشطة الأعمال و الممارسات و الكفاءات و نماذج الاعمال من الاستغلال الأمثل للتغيرات و الفرص الناتجة عن التكنولوجيات الرقمية و تأثيرها في المجتمع.

الفرع الثاني: أركان التحول الرقمي.

بنت الدراسات أن كل الشركات الرقمية اتبعت استراتيجيات محددة في مسارها الانتقالي إلى العالم الرقمي بحيث تشير النتائج إلى وجود خمسة أركان يجب توفرها من أجل إحداث التحول الرقمي و التي يمكن تلخيصها فيما يلي:

1-استراتيجية الأعمال الرقمية.

2-الارتباط بين الموظفين و العملاء .

3-ثقافة الإبداع .

4-التقنية أو التكنولوجيا الحديثة.

5-البيانات و التحليل.

الفرع الثالث: خصائص التكنولوجيا الرقمية.

تتميز التكنولوجيا الرقمية بمجموعة من الخصائص أهمها ما يلي:

1- **تقليص الوقت:** فالتكنولوجية تجعل كل الأماكن – إلكترونيا – متجاوزة الوقت .

2- **تقليص المكان:** تتيح وسائل التخزين التي تستوعب حجما هائلا من المعلومات المخزنة والتي يمكن الوصول إليها بيسر وسهولة.

3- **اقتسام المهام الفكرية مع الآلة:** نتيجة حدوث التفاعل والحوار بين الباحث والنظام.

4- **الذكاء الاصطناعي**: أهم ما يميز التكنولوجية الرقمية هو تطوير المعرفة وتقوية فرص تكوين المستخدمين من أجل الشمولية والتحكم في عملية الإنتاج.

5- **التفاعلية:** أي أن المستعمل لهذه التكنولوجية يمكن أن يكون مستقبل ومرسل في نفس الوقت، فالمشاركين في العملية التكنولوجية الرقمية يستطيعون تبادل الأدوار وهو ما يسمح بخلق نوع من التفاعل بين الأنشطة[6].

[6]واعروسيلة، دورالحكومة الإلكترونية في تحسين جودة الخدمات الحكومية ، حالة وزارة الداخلية والجماعات المحلية، الجزائر، ورقة مقدمة ضمن الملتقى الدولي إدارة الجودة الشاملة بقطاع الخدمات، كلية العلوم الاقتصادية وعلوم التسيير،جامعة منتوري، قسنطينة، يومي 10 و11 ماي 2011 ،ص5.

6- **اللاتزامنية:** وتعني إمكانية استقبال الرسالة في أي وقت تناسب المستخدم، فالمشاركين غير مطالبين باستخدام النظام في نفس الوقت.

7- **اللامركزية:** وهي خاصية تسمح باستقلالية التكنولوجيا، فالانترنيت مثلا تتمتع باستمرارية عملها في كل الأحوال، فلا يمكن لأي جهة أن تعطل الانترنيت على مستوى العالم بأكمله.

8- **قابلية التواصل:** وتعني إمكانية الربط بين الأجهزة الاتصالية المتنوعة الصنع، أي بغض النظر عن الشركة أو البلد الذي تم فيه الصنع.

10- **قابلية التحرك و الحركية:** أي أنه يمكن للمستخدم أن يستفيد من خدمات أثناء تنقلاته، أي من أي مكان عن طريق وسائل اتصال كثيرة مثل: الحاسب الآلي النقال ، الهاتف النقال... إلخ.

13- **الشيوع و الانتشار:** وهو قابلية هذه الشبكة للتوسع لتشمل أكثر فأكثر مساحات غير محدودة من العالم ، بحيث يكون الانتشار انتشارا منهجيا.

14- **العالمية و الكونية** : وهو المحيط الذي تنشط فيه هذه التكنولوجيات، حيث تأخذ التكنولوجيات الرقمية مسارات مختلفة ومعقدة تنتشر عبر مختلف مناطق العالم، وهي تسمح لرأس المال بأن يتدفق إلكترونيا ، فيسمح لها بتخطي عائق المكان والانتقال عبر الحدود الدولية[7].

المطلب الثاني: كيفية مساهمة التطورالتكنولوجي في إدارة الموارد البشرية .

شهد تطور إدارة الموارد البشرية عدة مراحل نتيجة للتطور التكنولوجي، إذ يمكن تقسيمها إلى مايلي:

الفرع الأول: النظام الورقي

في البداية كانت أنظمة الموارد البشرية قائمة على الورق ابن كانت تعمل بشكل مستقل و غير متكامل مع مختلف الوظائف الأخرى حيث كان يتم تخزين البيانات عادة على أجهزة الكمبيوتر[8] ،

---

[7] واعروسيلة، المرجع السابق ، ص6.

[8] ليلي ، دور التدريب في تحسين أداء الموارد البشرية في ظل اقتصاد المعرفة، دراسة حالة، ، في مؤسسة الاسمنت بباتنة، مجلة الباحث الاقتصادية ، العدد 03، 2013، ص 123.

المركزية كما كانت تعد التقارير الأولية بأساليب بدائية للغاية ، وكانت إدارة الموارد البشرية هي الجهة الوحيدة المسؤولة عن البيانات.

الفرع الثاني: بداية الكمبيوتر الشخصي.

في هذه المرحلة تم تحويل البيانات من الأنظمة الورقية إلى الكمبيوتر الشخصي و الشبكات المحلية و مع التقدم التكنولوجي تم إنشاء قواعد البيانات، كما طورت هذه التكنولوجيا أساليب كتابة التقارير و كشف الرواتب و تتبع مسار الموظفين.

الفرع الثالث: نظام قواعد البيانات الإلكترونية.

ظهرت هذه المرحلة مع ظهور تكنولوجية قواعد البيانات المترابطة و التي تعلى تخزين مجموعة من البيانات في ملفات مختلفة ، بحيث كل صنف من الملفات يحوي أنواع محددة من البيانات و التي يمكن ربطها و بالتالي استخدام مختلف البيانات من مختلف الملفات من أماكن مختلفة و في هذه المرحلة أصبح استخدام الانترنت في تزايد و مع تزايد هذه التكنولوجيا تمكنت المنظمات من استغلالها في إعداد التقارير المعقدة و زيادة الاندماج مع باقي الأقسام الأخرى.

أولا: تكنولوجيا شبكات الانترنت.

في هذه المرحلة بدأت العديد من الشركات تسعى لاحتضان تكنولوجيا الموارد البشرية أين تحت مزايا التشغيل الآلي معروفة على نطاق واسع للموارد البشرية والمناطق الأخرى من العمل، كما تحول التركيز إلى جعل أكثر المعاملات أوتوماتيكية لتحقيق الفعالية والكفاءات، إضافة إلى ذلك أصبحت مراكز الاتصال تستخدم أنظمة الاستجابة الصوتية على نطاق واسع إضافة إلى استخدام التطبيقات التي تمكن المستخدم الى الوصول إلى قاعدة البيانات من أي مكان و في أي وقت.

ثانيا: التحولات الرقمية لإدارة الموارد البشرية .

تسعى المؤسسات إلى الاستفادة القصوى من تجربة العملاء لضمان تقتهم و ولاتهم و رفع علامة المؤسسة ، الأمر الذي أصبح يستوجب على المؤسسات أن تعمل على إدماج موظفيها و خلق بيئة عمل مجدرة تؤدي إلى خلق الرضي الوظيفي ، حيث أثبتت الدراسات أن الشركات ذات القوى العاملة عالية الأداء تتفوق على نظيراتها بنسبة 147 في المائة في الأرباح لكل سهم و أن أفضل الشركات هي التي تتحرك بسرعة التقديم تجربة فائقة للموظفين يمكنها من خلالها دفع الابتكار والإنتاجية ورضا العملاء .

اتجهت إدارة الموارد البشرية إلى تحول جذري باعتبارها إحدى أهم الوظائف في المعلمات فهي مصدر توفير العنصر البشري و عنصر فعال في رحلة التحول الرقمي الذي تشهده المنظمات حيث بيت الدراسات أن التحولات الرقمية تؤدي إلى تغيير ثلاث مجالات رئيسية في إدارة الموارد البشرية[9].

1- رقمنة القوى العاملة : و التي تمثل كيفية قيادة المنظمة للإجراءات الإدارية الجديدة، بحيث تشمل ثقافة الإبداع و تعزيز المشاركة و الممارسات الإبداعية التي تشكل شبكات عمل جديدة داخل المنظمة.

2- رقمنة مكان العمل : حتى يمكن للمنظمة من إنشاء بيئة عمل جديدة التي تعزز الإنتاجية، في ظل استعمال أدوات التواصل الحديثة و تعزيز روح المبادرة و الرغبة في المشاركة و الحس الهادف.

3- رقمنة المورد البشري : حيث يمكن للمنظمة من تحويل وظائف الموارد البشرية إلى وظائف يمكن ممارستها بطريقة رقمية و أدوات رقمية و إبداع مستمر، إذ أن إدارة الموارد البشرية الآن مطالبة بإعادة صياغة ممارساتها من التوظيف إلى القيادة و الأداء الوظيفي و هذا بالاستفادة من التطبيقات الرقمية و تجارب العمال المقنعة، و كل هذا يجب أن يتم بالتركيز على إعادة هندسة المنظمة على أساس ثقافة فرق العمل و الاعتماد على تكنولوجيا تحليل البيانات لا سيما في مجال اتخاذ القرارات إضافة إلى التركيز على التنوع في الثقافات و التعلم و المسارات المهنية، و ممارسات إدارة الموارد البشرية التي تبنى على خبرة الموظفين القدامى و إبداع المواهب الشابة حديثة العهد بالمؤسسة باعتبار أن القاعدة العمالية عبارة عن مزيج من الشباب و كبار السن الذين يمتلكون الخبرة في ميدان العمل و بالتالي مثل هذه المقاربات مطلوبة تقريبا في كل الشركات ، كما أن إدارة الموارد البشرية الرقمية تتطلب خبرة في مجال التكنولوجيات الرقمية، و بالرغم من أن إدارة الموارد البشرية المبنية على الحوسبة السحابية أصلت قيمة هائلة للمنظمات، إلا أن هذا لم يعد يكفي في الوقت الراهن حيث بات يفكر الخبراء في إنشاء فرق عمل خاصة بالتصميم الرقمي داخل قسم الموارد البشرية، و بالتالي تكون السحابة عبارة عن قاعدة العمل، و يقوم فريق التصميم الرقمي بهندسة الأعمال على حسب احتياجات الشركة، كما يجب وضع استراتيجية فعالة للتحول إلى إدارة موارد بشرية رقمية[10] .

الخاتمة:

---

[9] حمد، س و سعيدة، ب ، البعد الاستراتيجي لتنمية و إدارة الموارد البشرية في ظل تحديات العولمة ، مجلة اقتصاديات المال و الأعمال ، 2017 ،ص166- 169.

[10] حمد، س و سعيدة، ب، المرجع نفسه، ص 179-180 .

من خلال هذا المقال الموسوم بـ : " دور التكنولوجيا الرقمية في إدارة الموارد البشرية "، تم التوصل لمجموعة من النتائج، لم تستثني تداعيات التحولات الرقمية إدارة الموارد البشرية التي باتت تلعب دورا مركزيا في بناء استراتيجيات إعمال المؤسسات، و مع تزايد أهميتها بات لزاما عليها تبني أسلوب العمل الجماعي لأن قطاع البنوك من القطاعات الخدماتية فعمليات التحول الرقمي تصبح أكثر من ضرورة من أجل المنافسة و ضمان المكانة السوقية ، إلا أن اعتمادها المطلق على التكنولوجيا الحديثة لا يعني بالضرورة نجاح مساعي التحول الرقمي و تطوير ممارسات إدارة الموارد البشرية حيث يجب على المؤسسات إنشاء كفاءات قيادية قادرة على استغلال هذه التكنولوجيا لأجل تطوير ممارسات إدارة الموارد البشرية، و في الأخير تم اقتراح مجموعة من **التوصيات الهامة**، و التي من شأنها أن تساهم و تساعد الإدارة على استخدام التكنولوجيا الرقمية، نذكر أهمها :

1- تحسين خدمة الانترنت ومحاولة الرفع من عدد مشتركيها ومستخدميها.

2- العمل على إنشاء موقع للأنترنت لتقديم المعلومات وتعريف الجمهور بخدمات كل إدارة على حدى، ونشر الوعي بين المواطنين وتعليمهم الإلكتروني.

3- العمل على إدخال معلومات وبيانات إدارية دقيقة على الانترنت.

4- السهر على وضع تشريعات قانونية فعالة لتحديد تعاملات الإدارة الالكترونية مع المواطنين بما يؤدي الى تحقيق رضا الطرفين وأهدافهم.

5- لابد من الاعتماد في كل الإجراءات و الأنشطة الإدارية على الحاسب الآلي.

6- ضرورة الرد على استفسارات وشكاوى المواطنين بالاعتماد على الانترنت.

7- استخدام البريد الإلكتروني كوسيلة اتصال حديثة وسريعة في كل الإدارات.

8- محاولة استخدام النماذج الإلكترونية في الموقع لتقديم وتلقي الطلبات.

9- لابد من توفير العمالة المدربة على المعلوماتية و تكنولوجيا الاتصال الحديثة، بالإضافة إلى العمل على رفع مستوى قدرة المواطنين على التعامل مع التقنيات الحديثة.

10- توفير التمويل اللازم لتغطية التكاليف الخاصة بالتقنيات التكنولوجية في جميع القطاعات.

11- ضرورة القيام بإعداد برامج تكوينية للموظفين في الإدارات و هذا في مجال التكنولوجيا الرقمية.

12_ إعادة النظر في برامج التعليم والتكوين في مجال التكنولوجيا الرقمية، و تلقين التكنولوجيات الرقمية لجميع الفئات الاجتماعية.

13- التركيز على استقطاب الكفاءات ذات المهارات الرقمية في عمليات التوظيف.

14- تبني أسلوب فرق العمل داخل المؤسسات من أجل تبادل المهارات بين مختلف الموظفين.

15- وضع استراتيجية فعالة للتحول الحقيقي و الفعلي إلى إدارة موارد بشرية رقمية.

قـائـمة المـراجـع:

- عروسي وداد، الإدارة الإلكترونية وتطبيقاتها في الخدمة العمومية نموذج قطاع العدالة، مذكرة ضمن متطلبات نيل شهادة الماستر في العلوم السياسية، تخصص سياسات عامة، كلية الحقوق و العلوم السياسية، جامعة زيان عاشور –الجلفة-، 2019-2020.
- قادة يزيد ،اعمر مولاي، تطبيقات الإدارة الإلكترونية في القطاع العمومي خلال جائحة كورونا، دراسة تطبيقية بمديرية الإدارة المحلية بولاية سعيدة، مجلة دراسات في الاقتصاد وإدارة

الأعمال، مخبر إدارة وتقييم أداء المؤسسات، جامعة سعيدة - مولاي الطاهر-،المجلد 04، العدد 01 ، جوان 2021.

- توفيق حناشي ، فارس قاطر، واقع الإدارة الالكترونية والمعيقات التي تقلل من تطبيقها مجلة روئ الاقتصادية، جامعة العربي التبسي، تبسة الجزائر، المجلد09، العدد 02.
- الشيكر أيوب، الإدارة الإلكترونية في الجزائر- تطبيقات وتحديات، مجلة الإدارة والتنمية للبحوث والدراسات بمخبر تسيير الجماعات المحلية ودورها في تحقيق التنمية،جامعة لونيسي علي، البليدة2، الجزائر، المجلد 08، العدد: 01 ، 2019.
- بن مبارك ماية، دور المشرع الجزائري في تفعيل الإدارة الإلكترونية، مجلة الحقوق والعلوم السياسية بجامعة خنشلة، المجلد 8، العدد02.
- ليلى، دور التدريب في تحسين أداء الموارد البشرية في ظل اقتصاد المعرفة دراسة حالة ، في مؤسسة الإسمنت بباتنة ، مجلة الباحث الاقتصادي ، العدد 03 ، 2013.
- حمد، س و سعيدة، ب، البعد الاستراتيجي لتنمية و إدارة الموارد البشرية في ظل تحديات العولمة ، مجلة اقتصاديات المال و الأعمال، 2017.

أهمية التكنولوجيا الرقمية في المجال المصرفي

The importance of digital technology in banking

عرورة فتيحة – أستاذة محاضرة أ –

كلية الحقوق – جامعة الجزائر 1 –.

البريد الإلكتروني: fatiha.aroura8@gmail.com

ملخص:

شهدت السنوات الأخيرة من القرن الماضي ثورة هائلة في تكنولوجيا الاتصال والمعلومات أثّرت على جميع مجالات الحياة بما فيها المجال التجاري، حيث أصبحت الصفقات التجارية تتم عبر شبكات الاتصال الإلكترونية، وظهر ما يسمى بالتسوق الآلي، الدفع الإلكتروني والتجارة الإلكترونية. هذه الأخيرة فرضت نفسها بقوة في جميع المجالات، بما فيها المجال المصرفي، مما نتج عنه تغير في المفاهيم السائدة في المعاملات المدنية والتجارية، الأمر الذي يستوجب البحث حول أهمية التكنولوجيا الرقمية في المجال المصرفي، وبصفة خاصة بيان تأثير العمل المصرفي الإلكتروني على حقوق الانسان في إطار العصر الرقمي.

الكلمات المفتاحية: التكنولوجيا الرقمية، القطاع المصرفي، العمليات المصرفية الالكترونية، العميل، البنوك.

Abstract:

The last few years of the last century have witnessed a huge revolution in communication and information technology that has affected all areas of life, including business, as business transactions were conducted via electronic communication networks. Thus, so-called automated purchasing, electronic payments and electronic transactions emerged.The latter has become a strong feature in all areas, including banking, which has led to a change in the dominant concepts in civil and commercial transactions, necessitating research in terms significance of digital technology in banking, and in particular the impact of electronic banking on human rights in the digital era.

Keywords: digital technology ,banking, electronic banking ,customer, banks.

مقدمة:

شهدت الصناعة المصرفية تقدمًا ملموسًا في مجال العمليات المصرفية الإلكترونية، هذا ما أتاحته الابتكارات التقنية المتواصلة والتنافس الشديد بين المؤسسات المصرفية. وقد كان القطاع المصرفي من أبرز القطاعات التي تأثرت بثورة المعلوماتية والاتصالات، التي شكلت عاملاً مساعدًا لتنمية العمل المصرفي منذ أوائل السبعينات من القرن العشرين.

أدّى نمو التجارة الإلكترونية إلى تطور كبير في مختلف المجالات الاقتصادية المعاصرة بسبب التطورات التكنولوجية المتسارعة انعكست بصورة واضحة على أداء مختلف القطاعات الاقتصادية، خاصة القطاع المصرفي الذي توسعت وتعددت خدماته بشكل كبير جدًّا، جعلت البنوك قادرة على إيصال خدماتها إلى زبائنها من خلال التكنولوجيا الرقمية و مختلف التقنيات الإلكترونية الحديثة التي تمكّنهم من القيام بكافة العمليات المصرفية التي يحتاجونها بواسطة الانترنت التي لعبت دورًا ملحوظًا في تنويع الخدمات المصرفية المقدمة للعملاء، وزادت من كفاءة وكمية المعلومات المقدَّمة للمصارف وللزبائن على حد سواء.

وهذا ما أتاح زيادة حجم المنتجات المصرفية المترتبة على هذه المستجدات التقنية العالية، بعد إزالة حواجز الزمان والمكان، كما ساهمت في تقديم أسعار تنافسية وخفض النفقات.

إنّ الاعتماد على التكنولوجيا الرقمية ومختلف الأدوات الإلكترونية لتسوية المعاملات المصرفية، بين البنوك والمتعاملين معهم، ينبغي أن تتوفر لها البيئة الإلكترونية اللازمة لأداء دورها على النحو المرجو، ذلك أنّ عدم توفر التقنية الكافية والمتطورة سيعيق حتمًا البنوك في تطوير إستراتيجيتها المصرفية القائمة على الخدمة الذاتية للعميل.

ويمكن القول بأنّ متطلبات العمل المصرفي الإلكتروني اللازمة لمواكبة التحول المتزايد نحو الحصول على الخدمة المصرفية الإلكترونية تدور حول توفر البيئة الإلكترونية المناسبة التي تستجيب مع متطلبات التكنولوجيا الرقمية. وعليه نطرح الاشكالية التالية: **إلى أي مدى يمكن للقطاع المصرفي الاستفادة من التكنولوجيا الرقمية؟ وبعبارة أخرى ما أهمية التكنولوجيا الرقمية في المجال المصرفي؟**

إنّ تفاعل القطاع المصرفي مع مستجدات التكنولوجيا الرقمية ومتطلباتها يستوجب تفاعل وتطوير البيئة التي يتحرك في إطارها هذا القطاع مثل البنية القانونية، الإدارية، التقنية، الإجرائية، الإعلامية، الثقافية، بالإضافة إلى ما يحتاجه هذا التطور في القطاع المصرفي من تأهيل البنية

البشرية وتدريبها على المنتجات والخدمات الإلكترونية الجديدة وعلى استخدام مختلف الوسائل الإلكترونية الحديثة في مجال المعاملات المصرفية **(المبحث الأول)**.

وكذلك وضع الحلول اللازمة لمواجهة مختلف التحديات والصعوبات القانونية التي تواجه التكنولوجيا الرقمية في المجال المصرفي **(المبحث الثاني)**.

هذا ما سنحاول توضيحه أكثر من خلال هذه المداخلة:

المبحث الأول: تطوير الخدمات المصرفية الإلكترونية

أدّت ثورة الاتصالات والمعلومات والتطورات المتلاحقة إلى ظهور تغيرات جوهرية في طبيعة الخدمات المصرفية، خاصة مع وجود مؤسسات مصرفية عملاقة، مما دفع بالبنوك إلى إعادة النظر في الدور التقليدي لها – البنوك – الذي يقوم على قبول الودائع ومنح الائتمان.

فقد باتت التطورات التكنولوجية المتسارعة في عصر الرقمنة تشكل تحديًا حقيقيًا في قطاع الخدمات المالية بشكل عام والمصرفية بشكل خاص، بعد أن تجاوزت شبكة الاتصالات العالمية – الانترنت – المفهوم الجغرافي للعمليات المصرفية. وأصبحت مسألة اللحاق بركب التكنولوجيا الإلكترونية الرقمية وتطورها أمرًا ضروريًا لا بديل له للاستمرار والبقاء في سوق الصناعة المصرفية والقدرة عل المنافسة ضمن المحافظة على السلامة والأمان والسمعة والثقة، خاصة في العالم العربي[1]، ومن ضمنه الجزائر التي تبذل جهدًا حثيثًا من أجل مواكبة هذا التطور.

وعليه، يمكن القول في هذا الصدد أنّ تفعيل دور التكنولوجيا الإلكترونية الحديثة يكون بالدرجة الأولى من خلال تطوير الخدمات المصرفية بصفة عامة. وهذا يتطلب التحديث والتطوير على عدّة مستويات منها **التقنية والمالية (المطلب الأول)** ومنها **البشرية والقانونية (المطلب الثاني)**.

المطلب الأول: التحديث من الناحية التقنية والمالية

إنّ استخدام التكنولوجيا الرقمية الحديثة في المجال المصرفي يتطلب مواكبة التطورات الإلكترونية، الأمر الذي يستوجب بدوره تطوير وتحديث البنية التحتية اللازمة لتطوير شبكات الاتصال على المستوى المحلي والخارجي لتسهيل وتسريع ربط المعلومات داخليا ودوليا.

فعلى سبيل المثال نجد أنّ استخدام الانترنت أو الهاتف الخلوي كأحد الوسائل التكنولوجية لإجراء عملية مصرفية إلكترونية معينة، مثل سحب أو تحويل أموال أو غيرها، يستوجب تطوير شبكة وأنظمة الاتصالات التي تعمل من خلالها لتسهيل وتسريع العملية المصرفية الإلكترونية ونجاحها.

وعليه، عدم توفر التقنية التكنولوجية الكافية والمتطورة سيعيق البنوك في إستراتيجيتها المصرفية التي تهدف إلى تسهيل عمليات التجارة الإلكترونية، وتوفير أدوات ووسائل إلكترونية لتسوية هذا النوع من المعاملات.

ومن ثم فإنّ الإدخال الناجح للعمل الإلكتروني إلى القطاع المصرفي يقتضي إنجاز مجموعة من الإجراءات تتمثل أهمها فيما يلي[2]:

أولاً: في مرحلة أولى ينبغي أن يتوافر لكل من البنك والعميل أجهزة كمبيوتر ومجموعة من البرمجيات تمثل البنية التحتية للاتصالات مع الصيانة المستمرة للأجهزة والمعدّات، والتطوير الدائم لملاحقة التطورات المستمرة، بحيث يتوافق ذلك مع تحديث البيانات لتمكين العملاء من الإطلاع على أحدث العروض التجارية التي تقدمها البنوك في هذا المجال.

ثانيًا: إنجاز البنك موقعا مدروسا على شبكة الانترنت (Net Bank) بهدف تعريف أو توسيع معرفة العملاء بخدماته، ثم في مرحلة موالية يمكن أن يتطور هذا الموقع إلى موقع لتقديم خدمات مصرفية فورية ومتنوعة، وذلك حتى يستطيع العميل الدخول إلى هذا الموقع من خلال جهاز الكمبيوتر الشخصي الخاص به، والاستفادة من الخدمات المصرفية للبنك الإلكتروني[3].

في كل الأحوال يجب على البنك أن يتخذ كل التدابير التي تكفل أمن العمليات التي تتم عبر الانترنت، وذلك درءًا أو تقليلاً من المخاطر الكبيرة المترتبة عن سوء استخدام الشبكة.

ثالثًا: توفير متطلبات البيئة الأساسية للاتصالات وشبكات المعلومات، يتحقق ذلك عن طريق:

- ✓ ضرورة تحسين مستوى الخدمات الاتصالية وتوفيرها في جميع الأنحاء.
- ✓ زيادة دور شركات القطاع الخاص في تقديم خدمات أساسية للاتصالات بإنشاء وتطوير الشبكة الرقمية.
- ✓ الاستمرار في خفض تكاليف استخدام شبكات الاتصالات الرقمية.
- ✓ العمل على تطوير قطاع الاتصالات[4] ومساعدة المشروعات والأفراد على الاشتراك في العمل البنكي الإلكتروني، وذلك من خلال ضمان استمرار عمل شبكات المعلومات بصفة سريعة ومستقرة

حتى تسمح بنقل البيانات بالصوت والصورة في نفس الوقت وبجودة عالية، ذلك أنّ ضعف شبكة الاتصالات وانعدام الأمن للبرامج المطروحة عبر الانترنت من شأنه أن يعرقل نمو التجارة الإلكترونية وبالتالي يضعف دور البنوك في استخدام وسائل التبادل الإلكترونية.

أما من يجب **من الناحية المالية** على السلطات النقدية في الدولة أن تجد حلولاً ناجعة لقضايا أساسية مثل:

- ✓ أصول وأشكال منح الائتمان الإلكتروني.
- ✓ شروط إصدار البطاقات الإلكترونية.
- ✓ إجراءات الأمن والوقاية خاصة فيما يتعلق بمراقبة وضبط مسألة إصدار أو خلق النقود الإلكترونية كأداة لتسوية المعاملات التجارية الإلكترونية.

بصفة عامة يجب على الدولة أن تعمل على إقامة الإطار التشريعي والتقني المناسب لنمو العمل المصرفي الإلكتروني، ولمنع الغش والتحايل في مجال التكنولوجيا الرقمية .

المطلب الثاني: التحديث من الناحية البشرية والقانونية

من الناحية البشرية: يلعب العنصر البشري دورًا مهمًّا في إنجاح أي تطور ضمن أي قطاع، لاسيما في القطاع المصرفي الذي يسعى دائما لمواكبة التطور التكنولوجي المتسارع في العالم وما يرافقه من ثورة إلكترونية في كافة المجالات، إذ أنّ الاستثمار في الإنسان هو الاستثمار المولد للثروة المتجددة[5].

لذلك يقتضي رفع كفاءة العنصر البشري في كافة الأجهزة التشغيلية، الإنتاجية، الخدماتية والرقابية لمواكبة التطور الذي تشهده العمليات المصرفية الإلكترونية. و في هذا الإطار ينبغي إلمام العاملين في القطاع المصرفي بالقوانين والضوابط الرقابية التي تنظم علميات التجارة الإلكترونية، والعمليات المصرفية التي تتم عبر الحدود، وعليه يجب أن يتوافر لدى البنك الإطار الوظيفي القادر على الإلمام بالتقنيات الفنية، الإدارية والقانونية ذات الصلة.

كما ينبغي على البنك أن يعمل على تطوير قدراته الذاتية بما يكفل استيعاب العاملين فيه للتكنولوجيا الحديثة في مجال الاتصالات الإلكترونية الحديثة من خلال التطوير المستمر لأنشطة التدريب، ويتطلب ذلك من ناحية أخرى العمل على زيادة مستخدمي شبكة الانترنت من خلال إتباع مجموعة من الإجراءات من بينها:

- خفض تكلفة الاتصال بالشبكة[6].
- خفض أثمان الحواسيب الإلكترونية والأجهزة اللازمة للربط مع الشبكة.
- العمل على سرعة تبادل المعلومات عبر الشبكة.

تجدر الإشارة إلى أنّه من أجل ضمان الحصول على ممارسة بنكية صحيحة، قد يضع البنك تحت تصرف العميل كتيب أو دليل يحتوي على معلومات وضوابط حول العديد من القضايا الخاصة بالتعاملات البنكية الإلكترونية التي تربطه بالعميل، والتي قد تشمل على:

- الحقوق والواجبات التي تنتج عن علاقة البنك بالعميل.
- إجراءات فتح الحساب.
- واجبات البنك بخصوص ضمان سرية معاملات العميل.
- تحديد نظام إصدار الشيكات الإلكترونية، البطاقات البنكية وغيرها من التقنيات الإلكترونية الحديثة بالنسبة للعميل.
- طريقة معالجة البنك لأي شكوى ترد إليه من العميل.
- أهمية مبادرة العميل إلى إعلام البنك سريعا إذا ما تعرض لأي أزمة مالية أو عارض معين.
- أهمية قيام العميل بالتعرف على كافة ما يطرحه البنك من خدمات مصرفية للعملاء،... الخ.

أما من الناحية القانونية: فمن المعلوم أن التجارة الإلكترونية هي جملة العمليات التجارية التي تتم بين المستهلك والمنتج عبر وسائط إلكترونية، إلاّ أنّ هذه العمليات تتطلب إطارًا قانونيًا يضمن حماية كل الأطراف التجارية. كما أنّ التشريعات ملزمة على متابعة كل العمليات التجارية داخل حدودها الجغرافية أولاً ثم جعلها تتماشى مع التشريعات الدولية في آن واحد. فقدرة المستهلك على طلب سلعة معينة من أي موقع جغرافي من العالم يجعل القضاء أمام تحدي حقيقي هو إيجاد إطار قانوني موحد للتجارة الإلكترونية بين حكومات الدول.

نستنتج من ذلك أنّ هناك أساسين قانونين تقوم عليهما التجارة الإلكترونية بصفة عامة هما[7]: توحيد الإطار القانوني وإيجاد تشريعات محلية مرنة تتماشى مع خصائص التجارة الإلكترونية.

في هذا السياق تعتبر القواعد القانونية الإطار التشريعي لأي عمل وإعطائه الآثار المرجوة منه، وهذه القواعد تمثل الضمانة التي تحمي حقوق جميع المتعاملين في أي عمل شرعي.

وعليه، فإنّ العمليات المصرفية الإلكترونية تحتاج إلى بيئة قانونية تثبتها وتعطيها مفعولها، وتكرس حقوق وواجبات كافة الأطراف فيها سواء البنوك والمؤسسات المصرفية أو العملاء، مما يقتضي تحديث البنية القانونية لمواكبة التطورات التكنولوجية والتجارة الإلكترونية، وإعطاء كل من السند والتوقيع الإلكترونيين حجتهما الثبوتية ضمن شروط واضحة ومحدّدة، مما يؤدي إيجابا إلى تطوير العمليات المصرفية الإلكترونية التي تحتاج إلى قوانين خاصة ترعاها وتضمن عدم التعرض لها أو الاعتداء عليها ضمن ما يسمى بقرصنة المعلوماتية الإلكترونية.

واعترافا بأهمية البنية القانونية، أصدرت اللجنة الاقتصادية والاجتماعية للاتحاد الأوروبي في عام 1997 وثيقة بعنوان "المبادرة الأوروبية في التجارة الإلكترونية **European Initiative in Electronic Commerce** تهدف إلى تشجيع نمو التجارة الإلكترونية، ومن بين المواضيع التي اهتمت بها هذه المبادرة الأوروبية هي ضرورة اعتماد نظام قانوني خاص لمقدمي الخدمات الإلكترونية في السوق الأوروبية وحماية وسائل الدفع الإلكتروني، وكل التقنيات الإلكترونية بمختلف أنواعها، إضافة إلى حماية النظم الإلكترونية التي تقوم عليها، مثل التوقيع الإلكتروني والوثائق الرقمية.

وفي الجزائر نجد أن هناك جهود تبذل وإجراءات تُعتمد من أجل النهوض بالاقتصاد الرقمي[8]، تجسدت في الأطر القانونية والتشريعية المتمثلة خاصة في قانون التجارة الالكترونية رقم 18- 05 المؤرخ في 10ماي2018 [9] ذلك أن أنشطة التجارة الالكترونية والعلاقات القانونية الناشئة في بيئتها تثير العديد من التحديات القانونية حول أثر استخدام الوسائل الالكترونية في تنفيذ المبادلات الالكترونية .

المبحث الأول: تحديات العمل المصرفي الإلكتروني

إنّ التنظيم القانوني لكافة العمليات الإلكترونية، ومن ضمنها العمليات المصرفية الإلكترونية تواجهه الكثير من التحديات بالنظر إلى خصوصية هذه العمليات التي تمتاز بالطبيعة الدولية والشمولية وكثرة المسائل التي تنظمها، والتي تتجاوز تنظيما تشريعيًا محليًا، إضافة إلى مسائل الملكية الفكرية للعناصر الرقمية الإلكترونية، وأحكام التقاضي وإجراءاته. وغيرها الكثير من التحديات والإشكالات التي لا تزال محل جدل ونقاش، نتعرض لأهمها **(المطلب الأول)** ثم الحلول القانونية المطلوبة لنجاح العمليات المصرفية الإلكترونية وبالتالي تفعيل دور وسائل التبادل المصرفي الإلكترونية باعتبارها موضوع الدراسة **(المطلب الثاني)**.

المطلب الأول: التحديات القانونية أمام العمل المصرفي الإلكتروني

أولاً: ينشأ عن إجراء العمليات المصرفية الإلكترونية بالدرجة الأولى صعوبة تحديد القواعد القانونية الواجبة التطبيق على هذا النوع من الأعمال،خاصة فيما يتعلق بالجوانب التالية:

- حجية التوقيع الإلكتروني بالمقارنة مع التوقيع التقليدي.
- إثبات شخصية الأطراف المتعاقدين أو المتعاملين عبر وسائل الاتصال الحديثة، خاصة شبكة الانترنت.
- القوة الثبوتية للمراسلات والعقود والصفقات المصرفية الإلكترونية.
- أنظمة الدفع النقدي وماهية النقد الإلكتروني.
- سرية المعلومات وأمنها من مخاطر الجرائم الإلكترونية.
- الاختصاص القضائي ، أحكام التقاضي وإجراءاته في النزاعات الناشئة عن العمليات المصرفية الإلكترونية، فهل يستطيع القضاء أن يتعامل إيجابيا مع تلك الوسائل الإلكترونية؟.
- القانون الواجب التطبيق على المسؤولية عن الأخطاء والمخاطر.
- حماية الملكية الفكرية للبرامج المصرفية الإلكترونية.

ثانيًا: كما يواجه استخدام تقنيات الاقتصاد الإلكتروني عدّة عقبات أهمها ما يلي:

- انتشار ظاهرة القرصنة على الوسائل الإلكترونية من خلال عصابات المافيات الدولية التي ترتكب جرائم منظمة[10]، وتستثمر أموالها في عدّة نشاطات من خلال تبييض الأموال مما ينتج عنه خسارة مالية فادحة وما يتبعه من سلبيات مباشرة على الاستثمار والاقتصاد بشكل عام.
- عدم نضج الوعي لدى العملاء[11] بشكل كاف لمواكبة التطور المتسارع في مجال التجارة والعمليات المصرفية الإلكترونية.
- ضعف شبكة الاتصالات التي تواجه البنوك وخشيتها من احتمال فقدان الاتصال عند القيام بعملية مصرفية معينة، مما يهدد فرص تسويق الخدمات المصرفية الحديثة.
- ضعف عملية تطوير وسائل الحماية والسرية والأمان لكل العمليات المصرفية والمعلومات المرتبطة بها عند استخدام مختلف وسائل التبادل المصرفي الإلكترونية، كالبطاقات

البنكية، الشيكات الإلكترونية، التحويل الإلكتروني للأموال،... الأمر الذي يهدد ثقة العملاء في استعمالها.

- عدم تأمين التمويل الذي تحتاجه الاستثمارات الضخمة في مجال تطوير البنية التقنية، التشريعية والبشرية للعمليات المصرفية الإلكترونية بصفة عامة واللازمة لتعميم ونجاح وسائل التبادل المصرفي الإلكترونية بصفة خاصة.

ثالثًا: كذلك من التحديات المهمة التي تثور في مجال العمل المصرفي الإلكتروني نجد قضية وسائل التبادل المصرفي الإلكترونية والإشكاليات الضريبية على النحو التالي:

1) إشكاليات وسائل الدفع الإلكترونية:

إنّ الاتجاه السائد نحو المال الإلكتروني بديلاً عن المال الورقي، يجعل المعايير والقواعد والنظريات تتغير تدريجيا لتصبح أكثر ملائمة مع المفاهيم الجديدة للمال ووسائله، وصولاً إلى بناء قانوني يسهل على إدارات البنوك التعامل مع تحديات العمليات المصرفية الإلكترونية، خاصة التي تتمثل في مشاكل وسائل الدفع والوفاء بالالتزامات الناتجة بين الأطراف وتقديم الخدمات وغيرها، مع مراعاة خصوصيات العمليات المصرفية الإلكترونية.

2) الإشكالية الضريبية والرسوم الجمركية:

إنّ طبيعة العمليات المصرفية الإلكترونية تطرح إشكالية تحديد النظام الضريبي الواجب التطبيق على تلك الأنشطة، بسبب عدم إمكانية تحديد مكان إجراء تلك العمليات ليتم على أساسه تحديد القانون الواجب التطبيق على هذه العمليات.

فقد ظهرت عدّة مشاكل مالية تتعلق بكيفية تحصيل الرسوم الجمركية والضرائب المفروضة على التبادل التجاري الإلكتروني، وهذه الإشكالية ذات أهمية كبرى بالنسبة للدول النامية التي تعتبر هذه الرسوم والضرائب من أهم مواردها المالية التي تمكّنها من تحقيق التوسع وتنفيذ المشروعات لخدمة التنمية والاستثمار. الأمر الذي يقتضي وضع قواعد واتفاقيات دولية تضمن حقوق هذه الدول دون حرمانها من مزايا التجارة الإلكترونية.

في هذا السياق قرّرت الولايات المتحدة الأمريكية[12] عدم فرض ضرائب على الأنشطة التجارية الإلكترونية، في حين تجري الدول الأوروبية دراسات وأبحاث حول أهمية هذا التوجه وآثاره، لأنّ فرض الضرائب على هذا النوع من الأنشطة يتطلب أنظمة ضريبية مختلفة عن الأنظمة التقليدية، من ناحية تحديد المكلفين بها وتحقق الضريبة ، تأديتها ومراقبتها، بالإضافة إلى ضرورة التعاون والتنسيق الإقليمي والدولي في مجال الأنظمة الضريبية[13].

المطلب الثاني: الحلول القانونية لتفعيل دور التكنولوجيا الرقمية في المجال المصرفي

إضافة إلى ضرورة سن تشريعات خاصة بالعمليات المصرفية الإلكترونية، بعد وضع القوانين الخاصة بالإثبات، التجارة الإلكترونية والتوقيع الإلكتروني، تتطلب العمليات المصرفية الإلكترونية أيضًا إزالة النقص والعقبات القانونية، الأمر الذي يستلزم ما يلي:

- ✓ أجهزة قضائية متخصصة في الأمور الاقتصادية والمالية والمصرفية الإلكترونية، تكون قادرة على التعامل مع مختلف القضايا المرتبطة بهذه التطورات التكنولوجية الإلكترونية.
- ✓ دراسة الآثار القانونية للتطورات التكنولوجية، خاصة في مجال المعلومات وتقنية وسائل التبادل المصرفي الإلكترونية وتحدياتها.
- ✓ ضرورة التعاون بين البنوك وشركات تكنولوجية[14] من أجل تطوير الوسائل الإلكترونية لخدمة العمليات المصرفية في إطار التجارة الإلكترونية، ومن ثم خلق آليات تكنولوجية جديدة على مستوى البنوك تهدف إلى تفعيل دور الرقمنة في مختلف العمليات المصرفية التي تقدمها البنوك لعملائها.
- ✓ ضرورة توفير الحماية التقنية للعمليات المصرفية الإلكترونية وأمن المعلومات التي لا يمكن أن تتحقق إلاّ بتوفير الحماية القانونية من خلال وضع إستراتيجية شاملة لأمن المعلومات، تتناول البنك وموقعه ونظم الحماية الداخلية، بالإضافة إلى إستراتيجية الحماية من الاختراقات الداخلية والخارجية للأنظمة المصرفية وما تختزنه من معلومات سرية خاصة بالبنوك وبالعملاء[15].
- ✓ ضرورة توسيع ثقافة الزبائن أو العملاء في إطار العمل المصرفي الإلكتروني، ذلك أنّ قبول العملاء بمواكبة التغير الحاصل في العمليات المصرفية يشكل عنصرًا جوهريًا وحيويًا لإنجاح سياسة البنك في استثمار التكنولوجيا الإلكترونية، مما يفرض توفر ثقافة لدى الزبائن لاستخدام هذه الوسائل المتطورة في إنجاز عملياتهم المصرفية.

هذا يتطلب حتما توعية العميل أو المستهلك بشكل مستمر عن الخدمات المصرفية الجديدة وعن الوسائل والتقنيات الإلكترونية المقترحة من طرف البنوك، وعن إجراءات حل الأخطاء المتعلقة بها، مما يساهم في حماية العميل واحترام خصوصية المعلومات.

خاتمة:

في الأخير بالنسبة للجزائر ووفقا لما هو ملاحظ في الواقع العملي، نجد أنّ العمل المصرفي الإلكتروني لا يزال متأخرًا جدًّا مقارنة مع الدول المتقدمة التي عرفت تطورًا كبيرًا في هذا الجانب، وأنّ مختلف التحديات التي تواجه التكنولوجيا الرقمية أو العمل المصرفي الإلكتروني تنطبق بالكامل على واقع البنوك الجزائرية، بالنظر إلى مختلف المشاكل والمعوقات التي تواجهها.

الأمر الذي يستلزم حتمًا الأخذ بمختلف الحلول القانونية المقترحة من أجل النهوض بالقطاع المصرفي بصفة عامة وتفعيل دور التكنولوجيا الرقمية الإلكترونية بصفة خاصة، ومن ثم تحسين نوعية الخدمات ومختلف العمليات المصرفية المقدّمة من طرف هذه البنوك لعملائها.

الأمر الذي يعود بالنفع للطرفين معا:

- ✓ بالنسبة للبنوك زيادة أرباحها ومداخيلها المالية.
- ✓ أمّا بالنسبة للعملاء: تسهيل مختلف معاملاتهم المالية وربح الوقت وقلّة التكلفة، إضافة إلى الاستفادة من مزايا العمل المصرفي الإلكتروني.

الهوامش:

[1] نادر عبد العزيز شافي: **المصارف والنقود الإلكترونية**، المؤسسة الحديثة للكتاب، لبنان، الطبعة الأولى، 2007، ص108.

[2] خنفوسي عبد العزيز: **الآثار القانونية والاقتصادية للعولمة على الجهاز المصرفي الجزائري**، أطروحة دكتوراه في القانون العام، جامعة الجزائر 1، كلية الحقوق، 2013/2012، ص182-183.

[3] **البنك الإلكتروني** لا يعني فقط أن هناك بنكًا بالمفهوم التقليدي له مقر فيه إدارة وموظفون، تكتسي عملياته البنكية طابعا إلكترونيا حيث يتم استلام الأوامر وتنفيذها بطرق إلكترونية، وإنما يحمل كذلك البنوك الافتراضية التي تقدّم خدماتها من خلال شبكة الانترنت لمشتركين فيها، دون أن يكون لها مبنى مادي أو إداري وفقًا لما هو معروف.

[4] لقد تنبّه الاتحاد الأوروبي لأهمية تنظيم قطاع الاتصالات الإلكترونية، حيث باشر منذ عام 2000 بإعداد إطار تنظيمي لهذا القطاع عبر مجموعة إرشادات أوروبية (Directives) تهدف إلى خلق إطار تنظيمي متناغم لشبكة الاتصالات الإلكترونية، وتوفير تطبيق منسجم لهذا الإطار على مستوى الاتحاد الأوروبي.
راجع في ذلك: نادر عبد العزيز شافي: مرجع سابق، ص109.

[5] أحمد سفر: **العمل المصرفي الإلكتروني في البلدان العربية**، المؤسسة الحديثة للكتاب، طرابلس، لبنان، بدون طبعة، 2006، ص27.

[6] خنفوسي عبد العزيز: مرجع سابق، ص183.

[7] شافع بلعيد عاشور: **العولمة التجارية والقانونية للتجارة الإلكترونية**، دار هومة للطباعة والنشر والتوزيع، الجزائر، بدون طبعة، 2006، ص46 وما بعدها.

[8] حمري نجود وحمري نوال: **واقع التجارة الالكترونية في الجزائر وفق مقتضيات قانون رقم 18- 05 (قانون التجارة الالكترونية)** ، مقال منشور في مجلة البحوث القانونية والاقتصادية، المجلد 4، العدد 01، السنة 2021، ص 03.

[9] القانون المتعلق بالتجارة الالكترونية رقم 18- 05 المؤرخ في 10 ماي 2018 ، جريدة رسمية عدد 28 الصادرة بتاريخ 2018/05/16.

[10] نادر عبد العزيز شافي: مرجع سابق، ص115.

[11] أحمد سفر: **العمل المصرفي الإلكتروني في البلدان العربية**، مرجع سابق، ص35.

[12] راجع في تفصيل ذلك: بوعمرة آسيا: **النظام القانوني للتجارة الإلكترونية – دراسة مقارنة –**، أطروحة دكتوراه علوم تخصص قانون الملكية الفكرية، جامعة الجزائر 1، كلية الحقوق، 2013/2012، ص50؛ نادر عبد العزيز شافي: مرجع سابق، ص151.

[13] تتجه منظمة التجارة العالمية (WTO) إلى عدم فرض رسوم جمركية على التبادل الإلكتروني، راجع في ذلك: أحمد سفر: مرجع سابق، ص105-106.

[14] لا تعتبر التكنولوجيا هدفا بحد ذاتها، وإنما هي أحد العناصر التي تمكن البنوك من تنفيذ أعمالها بكفاءة وفاعلية، وتعزيز إنتاجيتها وزيادة أرباحها.

[15] أحمد سفر: **العمل المصرفي الإلكتروني في البلدان العربية**، مرجع سابق، ص104؛ نادر عبد العزيز شافي: مرجع سابق، ص128-129.

ملتقى وطني موسوم ب: حقوق الإنسان في العصر الر قمي

مداخلة بعنوان: المواطن و الموظف أمام المفاهيم الحديثة: الإدارة الإلكترونية و الحكومة الإلكترونية

Le citoyen et le fonctionnaire face aux nouveaux concepts : la e-administration et le e-gouvernement

د/ سلاماني ليلى : أستاذة محاضرة قسم أ / كلية الحقوق جامعة الجزائر (1)/ الجزائر

البريد الإلكتروني: leila.slamani@hotmail.fr

ملخص المداخلة:

تعمل العديد من الدول منذ الألفية الثانية على تحديث الإدارات العمومية مستعينة بالآلة أو بالتكنولوجيا الحديثة في إطار موجة الإصلاحات التي باشرتها ،و التي شملت العديد من القطاعات الاقتصادية و الاجتماعية و السياسية و حتى الإدارية بغية تحسين الخدمات و نيل رضا المواطنين أيضا.

إن الإدارة هي أداة الحكومات في تسيير الشأن العام، لهذا تحول الفضاء الإداري بعد الاستعانة بالآلة إلى افتراضي، إلا أن التعقيدات التي تصاحب هذا الفضاء حولت النقاش في الإصلاحات من الرقمنة كأداة في خدمة المستخدمين إلى غاية تريد الحكومات الوصول إليها.

إن الإدارة الإلكترونية كإدارة تابعة للدولة لا يمكنها أن تسير بعيدا عن الأطر القانونية ، كما لا يمكنها أن تستبعد الإمكانات المذهلة التي توفرها التكنولوجيا الحديثة، و بجمع الفكرتين قد يجد المواطن أو المتعامل مع الإدارة ضالته في خدمة حسنة و لكنه في المقابل قد يواجه صعوبات في الحفاظ على حقوقه ،و كذلك الأمر بالنسبة للموظف الذي يجد هو الأخر ضالته في تخفيف للأعباء و لكنه في المقابل أيضا قد يستعص بل يستحيل الأمر عليه للدفاع عن حقوقه ، و في جميع الأحوال سيفرض نقاش جديد نفسه في المستقبل و يتعلق الأمر بأنسنة المرفق العمومي .

كلمات مفتاحية: الموظف، المواطن، الإدارة الإلكترونة، الحكومة الإلكترونية ، العصرنة

Résume

Plusieurs pays œuvre à moderniser leurs administrations publiques en utilisant la nouvelle technologie dans le cadre des réformes entreprises par ces derniers dans différents secteurs, économique, social, et politique et même administratif en vue d'améliorer la prestation des services et obtenir la satisfaction des citoyens.

L'administration est l'outil de l'Etat dans la gestion des affaires publiques, et la transformation de la sphère administrative en un monde virtuel avec toutes les complications que cela comporte a transformé le débat d'une numérisation au service des usagers à une numérisation objectif gouvernemental.

L'administration électronique comme administration de l'Etat ne peut fonctionner en dehors des lois, ni loin des nouveautés technologiques, ces deux paramètres permettent au citoyen de trouver son gain dans une bonne prestation, mais il trouvera des difficultés à conserver ces droits ,aussi le fonctionnaire trouvera son gain étant délivre de la charge professionnelle, mais il trouvera des difficultés à défendre ses droits .en final un nouveau débat s'imposera dans le prochain futur celui de l'humanisation du service public

Mots clés. Fonctionnaire , citoyen administration, électronique gouvernement électronique , modernisation

---

مقدمة

يعد الإنترنيت أحد الابتكارات الرئيسية لهذا القرن ، فبعدما أحدثه من تغييرات بالنسبة لتواصل الأفراد فيما بينهم وصل الأمر في الآونة الأخيرة إلى العمل عن بعد سواء كان ذلك في القطاع العمومي

أو كان على مستوى القطاع الخاص .كما تغيرت ،مع هذا التحول ، بعض الإدارات العمومية إذ اختارت إنشاء مواقع إلكترونية(site web)و أخرى بوابات إلكترونية (portail web) إلى غير ذلك من الابتكارات.فلم يعد يقتصر الأمر على التواصل فقط بل تطور إلى تقديم الخدمات كما مكّن بعض الأفراد في بعض الدول من دفع الضرائب عن بعد و في دول أخرى من الاستشارة عن بعد[1].

كل هذا التطور جعل حديث الباحثين في جميع المجالات و حتى في المجال القانوني، و كذلك حديث القائمين على تسيير الشأن العمومي، و على جميع المستويات في الدولة، يرتكز على مفاهيم جديدة من إدارة إلكترونية و حكومة إلكترونية و عن كيفية استخدام الآلة لتحسين أداء الخدمات العمومية الموجهة للفرد سواء كان مواطنا أو موظفا و هنا يُطرح التساؤل هل تحسين الخدمة العمومية عن طريق الآلة كفيل بتحسين و تدعيم حقوق الأفراد؟

قبل الإجابة عن هذا التساؤل يجب التعريج على هذه المفاهيم الجديدة من إدارة إلكترونية و حكومة إلكترونية قبل مناقشة الأثر الذي تحدثانه على حقوق الأفراد سواء كانوا مواطنين أو موظفين.و هذا ما يدفعنا لمناقشة و تحليل الموضوع من خلال النقاط التالية.

1- الإدارة الإلكترونية و الحكومة الإلكترونية:مفاهيم قيد الإنجاز

1-1 جهود علمية مسارعة لتحديد مضمون المفاهيم الجديدة

2-1 تبني المفاهيم الإلكترونية في إطار الإصلاح في الجزائر

2- أثر الإدارة الإلكترونية و الحكومة الإلكترونية على حقوق الأفراد: نعمة أم نقمة

1-2 القيمة المضافة لتكنولوجيا الإعلام و الاتصال على حقوق الأفراد

2-2 مصير الحقوق المتحولة للصيغة الإلكترونية.

.....

1- الإدارة الإلكترونية و الحكومة الإلكترونية: مفاهيم قيد الإنجاز

[1] H. Belrahali –Bernard :la pratique des consultations sur Internet par l'administration ,RFAP ,n°137,138,2011,p182.

لا يمكن للفرد أن يعيش في مجتمع غير منظم لا تحكمه ضوابط و قواعد حتى و إن كان في المجال الافتراضي ، لهذا فإن عصر التكنولوجيا الذي يهيمن على العالم أجبر الدول و الحكومات على مسايرة هذا التطور و لكن دون أن تتخلى عن أدوارها الاجتماعية و الاقتصادية و السياسية تجاه الأفراد سواء بإقرار الحقوق أو العمل على حمايتها، غير أن سرعة التكنولوجيا جعلت الجهود العلمية لا تستقر على مفهوم محدد للإدارة الإلكترونية و الحكومة الإلكترونية (1)

أما على المستوى الجزائري فقد تناول الخطاب الرسمي مفاهيم الإدارة الإلكترونية و الحكومة الإلكترونية في العديد من المناسبات [2] ثم تجسد في النصوص القانوني و التنظيمية(2)

1-1 جهود علمية مسارعة لتحديد مضمون المفاهيم الجديدة.

اعتمد الباحثون في العلوم القانونية على مقاربة بسيطة [3] لتعريف الإدارة الإلكترونية تتمثل في إضافة عبارة" استعمال أنظمة الاتصال" للتعاريف الفقهية للإدارة ، و من هذه التعاريف ما جاء به الكاتب شاتييون [4] أن الإدارة الإلكترونية هي "إدارة تسيير المرافق العمومية و تنظيم العلاقات فيما بينها و بين المواطنين باستعمال أنظمة الاتصال للبيانات من أجل توفير الخدمة بتكاليف و وقت أقل" .

إن هذا الاتجاه في تعريف الإدارة الإلكترونية يعتمد على معايير عديدة، المعيار المادي و يتعلق بإدارة و تسيير المرفق،و المعيار الوظيفي و يتعلق بتنظيم العلاقات بين الإدارة و المواطنين و المعيار الغائي أو معيار الهدف و هو توفير الخدمات بأقل تكلفة.

أضاف التعريف عنصرا جديدا و ليس معيارا [5] و يتعلق بالمجال المالي للحديث عن تكلفة خدمات المرافق العمومية.

---

[2] خطاب الرئيس بوتفليقة سنة 2008 ثم تلته الخطابات الرسمية الأخرى على جميع المستويات

عشور عبد الكريم :دور الإدارة الإلكترونية في ترشيد الخدمة العمومية في الولايات المتحدة الأمريكية و في الجزائر ،مذكرة لنيل شهادة [3] الماجستير ،جامعة منتوري ،قسنطينة ،2010،ص12

[4] G.Chatillon : l'administration électronique, RIDC, n°2, 2006, p673.

المعيار هو أساس المنطق القانوني و منطلق التفكير القضائي في كشف القواعد و استنباط الحلول ، بينما العنصر هو جزء من مجموعة ، [5] للمزيد من المعلومات أنظر القواميس المتخصصة .

إذا كانت كل المعايير السابقة قد نوقشت من طرف الفقه القانوني في مجلدات القانون الإداري [6] فإن العنصر المالي عادة ما يمثل أحد المعايير التي يعتمد عليها القاضي الإداري للبث في النزاعات التي تعرض عليه ، و يُقصد به مصدر الأموال فإذا كانت عمومية فإن النزاع إداري ،بينما التكلفة التي أوردها التعريف لا تعني المرافق العمومية فقط بل و حتى الإدارات الخاصة و هي عبارة محاسبية.

الحقيقة أن هذه المحاولة لتعريف الإدارة الإلكترونية تركز على الجوانب الإجرائية "توفير الخدمات بأقل وقت و بأقل تكلفة " و هي إجراءات باشرت الحكومات بوضعها و تنظيمها عن طريق المراسيم و التعليمات ،كما هو الشأن في فرنسا مابين سنة 1998 و سنة 2003 [7] و كذلك فعلت الجزائر منذ الألفية الثانية لتحديث مجمل مرافقها العمومية ، و شملت هذه الإجراءات

-تبسيط الإجراءات الإدارية ، تقليص الوثائق الإدارية ، تعميم استخدام الإعلام الآلي.....إلخ.

إن تعريف الإدارة الإلكترونية يبقى نفسه التعريف الذي قام الفقه الإداري بوضعه، أما إضافة عنصر التكنولوجيا للتعريف فلا يجعل الإدارة الإلكترونية تنفرد بتعريف خاص بها.لهذا السبب نجد جهودا علمية في ميدان المناجمت تسارع لوضع قواعد و مبادئ [8] لكل ما هو إلكتروني و بالأخص للإدارة الإلكترونية، و قد تلت هذه الجهود عملية استقبال و قبول قانونيين في العديد من الكتابات لكل ما هو إلكتروني ، و تحول النقاش إلى كيفية استخدام الآلة في المجال القانوني [9] و مزايا و عيوب الإدارة الإلكترونية مستبعدا البحث في عناصر تعريفها.

المفهوم الأخر و الذي يلازم مفهوم الإدارة الإلكترونية و هو الحكومة الإلكترونية هو الآخر ظهر حديثا في الخطابات الرسمية و يُنسب للرئيس الأمريكي "كلينتون" في حملته الانتخابية سنة 1992[10] و قد ارتبط بمفهوم الإصلاح في العديد من الدول ، غير أن التعريف الذي حظيت به الحكومة الإلكترونية يشوبه غموض كبير .

---

[6] قائمة كتب القانون الإداري طويلة ، سواء باللغة العربية أو باللغة الأجنبية

[7] G.Chatillon, Op Cite p 673.

[8] R Fakhouri et B Aubert :l'e-administration à du chemin à faire ,l'Expansion Management review,juin2013,p36.

[9] L. Mehl :informatique juridique et Droit comparé,RIDC,n°4,1968,p618.

[10] R Fakhouri et B Aubert :Op Cite p 36.

تتجه بعض التعاريف إلى ربط مفهوم الحكومة الإلكترونية بالإصلاح كما سبقت الإشارة إليه و قد عرَّف أحدهم الحكومة الإلكترونية على أنها" استخدام تكنولوجيا الإعلام و الاتصال لتحويل الحكومة و جعلها ممكنة الوصول من طرف المواطنين و أكثر فعالية و أكثر مسؤولية "[11]

« le e-gouvernement est l'usage des TIC pour transformer le gouvernement en le rendant plus accessible aux citoyens , plus efficace et plus responsable »[12]

يركز التعريف على الدور الجديد للدولة و علاقته بتكنولوجيا الإعلام و الاتصال و هو يتضمن عناصر لا تحمل نفس المفاهيم التي يحملها القانون، إذ يشير لعنصر اتصال المواطنين بالحكومة (ممكنة الوصول) و لا يُعنى به وضع أو إضافة أجهزة كمبيوتر في المكاتب الإدارية للتواصل مع المواطنين ، بل يقصد به إنشاء علاقات بين الموظفين و المواطنين ، كما لا يعنى بمفهوم المسؤولية ذلك التعريف الذي يحدده القانون، و إنما يُقصد به أن تتحول العمليات بين الموظفين الحكوميين و المواطنين إلى عمليات شفافة.

يشير تعريف أخر للحكومة الإلكترونية [13] صدر عن دولة تكساس الأمريكية يفيد بأن الحكومة الإلكترونية هي" أنشطة حكومية تتم عن طريق عمليات رقمية في إطار شبكة اتصال ،عادة ما تكون عبر الإنترنيت بين الإدارة و عناصر من العامة ،و أيضا بين الإدارة و كيانات خاصة من القطاع الخاص و بالأخص المنظمة منها .

تتضمن الأنشطة في غالب الأحيان التبادل الإلكتروني للمعلومات بهدف الاستحواذ أو تقديم السلع أو الخدمات ، إجراء طلبيات ، تقديم أو الحصول على المعلومات ، أو القيام بمعاملات مالية"[14]

Activités gouvernementales qui s'opèrent par des processus numériques dans le cadre d'un réseau informatique, généralement l'Internet, entre l'administration et

---

[11] ترجمة الكاتبة

[12] El.Megder et autres :le e-gouvernement et la modernisation du secteur public, **SETIT 2005** 3rd International Conference: **S**ciences of **E**lectronic **T**echnologies of **I**nformation and **T**elecommunications March 27-31, 2005 – TUNISIA.p2

[13] D.Brown :le gouvernement électronique et l'administration publique ,RISA2005, p252.

[14] ترجمة الكاتبة

des membres du public ainsi que des entités du secteur privé, en particulier des entités réglementées. Ces activités concernent généralement l'échange électronique d'informations dans le but d'acquérir ou de fournir des produits ou des services, de passer ou de recevoir des commandes, de fournir ou d'obtenir des informations, ou de réaliser des transactions financières

لم يخل التعريف لا من الإجراءات و لا من العناصر التي أوردتها التعاريف الأخرى ، كما يركز على إنشاء العلاقات عن طريق الآلة بين المواطنين و الموظفين الحكوميين و في إطار منظم.

جميع التعاريف التي تناولت كل من الإدارة الإلكترونية و الحكومة الإلكترونية تركز على العنصر الخاص بعلاقة المواطن بالإدارة وهذه هي الميزة الوحيدة التي تجعل من المفهومين منفصلين عن المفاهيم التقليدية ،و هي الميزة أيضا التي تجعل كل الأنظمة و كذا الباحثين يسارعون لوضع قواعد و مبادئ للمفاهيم الجديدة، الأمر الذي جعل البحوث متواصلة في جميع المجالات بما فيها المجال القانوني لتحديد و حصر كل ما يتعلق بالإدارة الإلكترونية و الحكومة الإلكترونية فسرعة التكنولوجيا لم تسمح لهؤلاء حتى الاستقرار على مصطلح موحَّد فمنهم من ربطها بمحيط الإدارة داخل النظام و يتعلق الأمر بالديمقراطية الإلكترونية [15] و آخرون وضعوا مصطلحات جديدة على غرار(Levy : l'hyper-république,2002 ,Steiner : cyberdémocratie ,cyberadministration [16](2002

1-2 تبني المفاهيم الإلكترونية في إطار الإصلاح في الجزائر:

نظمت الجزائر علاقة الإدارة بالمواطن في أطر قانونية مختلفة غير أن أدوات تفعيل هذه العلاقة لم تحدد بصفة واضحة إلا من خلال المرسوم 88-131 [17] ، لأن الخدمة السيئة التي تقدمها المرافق العمومية أرّقت الحكومات المتتالية، و في الألفية الثانية لجأت الدولة لإدخال الإعلام الآلي في الإدارات العمومية وفي قطاعات مختلفة من أجل تجسيد الإدارة الإلكترونية.

---

[15] H. Belrahali –Bernard :Op Cite pp 182-183.

[16] El.Megder et autres :Op Cite.p3.

[17] المرسوم 88-131 المؤرخ في 1988/7/4 ينظم العلاقات بين الإدارة و المواطن، جريدة رسمية رقم.27

أولى الخطوات التي تبنت فيها الدولة الجزائرية المفاهيم الإلكترونية هي برنامج الحكومة لسنة 2000 الذي نص على تقليص الهوة الرقمية بين الجزائر و الدول التي تحولت للفضاء الرقمي في تسيير الشؤون العمومية ، ثم تلت هذه الخطوة مبادرة من وزارة البريد و تكنولوجيا الإعلام و الاتصال بمشروع أ-الجزائر الإلكترونية قدمته الحكومة للمجلس الوطني الاقتصادي و الاجتماعي لإبداء الرأي حوله[18].

تضمن المشروع الجديد جميع الجوانب المادية و البشرية التي يتوجب على الدولة استغلالها من أجل التحول الرقمي، و قد تفادى مصممو المشروع الحديث عن الحكومة الإلكترونية و اكتفوا بتسمية المشروع باسم الدولة " أ-الجزائر 2013 "من جهة ، و جهة ثانية فقد أوصى المجلس الوطني الاقتصادي و الاجتماعي بعد طلب رأيه حول المشروع بضرورة التكفل بتكوين العنصر البشري و التركيز على الجوانب الأمنية للتحول الرقمي لحماية الأفراد [19]

في مرحلة موالية لمشروع أ-الجزائر ما بين 2009 و 2013 ، صدر مرسوم تنفيذي13-381 يحدد صلاحيات الوزير المنتدب لدى الوزير الأول مكلف بإصلاح الخدمة العمومية[20] ليتبنى الإدارة الإلكترونية في المادة 09 الفقرة الثانية "تولي الوزير المنتدب التشجيع على تطوير الإدارة الإلكترونية بإدخال التكنولوجيا الحديثة للإعلام الآلي و تعميمها".

تكفل نص تنظيمي أخر بالإدارة الإلكترونية و هو المرصد الوطني للمرفق العمومي[21] الذي أنشئ سنة 2016 و كُلف هو الآخر "بتحفيز و تطوير الإدارة الإلكترونية بإدخال التكنولوجيا الحديثة للإعلام و الاتصال و تعميمها "[22] ، و لم يكتف النص بالإدارة الإلكترونية فقط و إنما أضاف مفهوما جديدا ليواكب التطورات الحاصلة في علاقة الإدارة بالمواطن في المجال التكنولوجي و ذلك بالحديث

---

[18] رأي حول مشروع أ-الجزائر2013، المجلس الوطني الاجتماعي و الاقتصادي، جريدة رسمية عدد 54 سنة2009.

[19] أنظر النقطة 8 و 9 من رأي المجلس ، مرجع سابق

[20] المرسوم التنفيذي 13-381 الموافق ل19 نوفمبر سنة2013 يحدد صلاحيات الوزير لدى الوزير الأول المكلف بإصلاح الخدمة العمومية ، ج ر عدد 59

[21] المرسوم الرئاسي 16-03 المؤرخ في 7 يناير 2016 ، جريدة رسمية عدد 02 .

[22] المادة 5 فقرة 3 نفس المرجع

عن أنسنة العلاقات بين أعوان المرفق العمومي و مستعمليه [23] و لكن دون أن يُبين الآليات المرتبطة بهذا المفهوم و لا تحديد مفهومه.

و كما أوصى به المجلس الوطني الاقتصادي و الاجتماعي أن قابلية المجتمع لتكنولوجيا الإعلام و الاتصال تستلزم تواصلا مستمرا، فيجب أن لا يقتصر ذلك على الإدارات فقط ، و من هذا المنطلق أشار المجلس لمفهوم جديد في المجال الرقمي وهو دمقرطة الاستفادة من تكنولوجيا الإعلام و الاتصال[24] .

صدر نص تنظيمي أخر سنة 2020 يتضمن مفاهيم الإدارة الإلكترونية و مفاهيم أخرى مرتبطة به و يتعلق الأمر بالمرسوم التنفيذي الخاص بصلاحيات وزير الرقمنة و الإحصائيات [25].

أنُشئ المنصب الوزاري بعد التطورات الحاصلة في المجال الرقمي ليُشكل حسب اختصاصات الوزير التي وردت في النص حلقة وصل بين مختلف القطاعات الوزارية و ذلك "بوضع و بالتشاور مع القطاعات الوزارية الآليات المتعلقة بإعداد خطط العمل القطاعية في مجال الرقمنة ، و المصادقة عليها ، و متابعتها"[26] ، كما أُسند للقطاع صلاحية تقديم الاستشارة للحكومة حول أية مسألة تطلب منها في مجال الرقمنة [27].

لم يكتف تنظيم الوزارة و لا صلاحيات الوزير بالمفاهيم الخاصة بالإدارة الإلكترونية و تفصيل مهامها ،بل أضاف مفهوما جديدا يتوجب على القطاع المشاركة فيه و هو مفهوم الحوكمة الإلكترونية [28]. إذ يقر النص أنها مفهوم يجب أن يوضع في البيئة الملائمة له أو بمعنى أخر مفهوم يحتاج لتطوير التكنولوجيا في إستراتيجية شاملة.

خلاصة القول أنه إذا كانت البحوث العلمية لم تستقر على مضمون المفاهيم المتعلقة بالإدارة الإلكترونية و الحكومة الإلكترونية فإن دولا عديدة انتقلت لاستخدام تكنولوجيا الإعلام و الاتصال

---

[23] المادة 6 الفقرة 3 نفس المرجع

[24] توصيات المجلس الوطني الاقتصادي و الاجتماعي النقطة 19، مرجع سابق

[25] المرسوم التنفيذي 20-363 المؤرخ في5 ديسمبر2020 يحدد صلاحيات وزير الرقمنة و الإحصائيات، ج ر عدد 74

[26] المادة3/فقرة6 المرسوم التنفيذي 20-363 مرجع سابق

[27] نفس المرجع فقرة17 .

[28] المادة 2 /فقرة5 نفس المرجع

لتحسين خدماتها لمواطنيها ،و كذلك فعلت الدولة الجزائرية في العديد من القطاعات، و قد بات الحديث في الألفية الثانية عن قياس درجة رقمنة الخدمات في مختلف القطاعات و لم ينتقل بعد النقاش إلى ما تخلفه هذه التكنولوجيا من آثار على حقوق الأفراد و الموظفين.

2- أثر الإدارة الإلكترونية و الحكومة الإلكترونية على حقوق الأفراد: نعمة أم نقمة.

إن اهتمام حكومات العديد من الدول بتحسين خدماتها عن طريق تكنولوجيا الإعلام و الاتصال في تزايد مستمر، و ذلك بسبب الآثار الجيدة التي مكنتها من التواصل مع الأفراد و امتصاص التذمر الاجتماعي

إن الأفراد و باختلاف الوضعية القانونية التي يشغلونها داخل المجتمع يتطلعون دائما لما هو سهل و واضح في التعامل مع الدولة و مؤسساتها، لهذا نجد العديد من الدول كرست حقوقا لهم، و مع التحول لرقمنة المعاملات في قطاعات عديدة كانت النتيجة أن دعمت بعض الحقوق، و لكن البعض الأخر لم يدخل في دائرة اهتمام الحكام أو أنه أُرجئ لأسباب مختلفة .

يبقى المواطن هو المُتلقي الأول للخدمات الإلكترونية أما الموظف في المرافق العمومية فيستخدم الآلة لتساعده على تقديمها، و كلاهما يستفيد من مزايا التكنولوجيا (1).و لكن كلاهما أيضا يتساءل حول مصير حقوقه (2)

2-1 القيمة المضافة لتكنولوجيا الإعلام و الاتصال على حقوق الأفراد.

إن ظهور تكنولوجيا الإعلام و الاتصال له العديد من المزايا ،خاصة و أنه أتى بعد أن نظمت القوانين و التنظيمات حقوق الأفراد ، إذ كرست المبادئ في النصوص الأساسية ،أي الدساتير ثم تلتها القوانين و فصّلتها التنظيمات، غير أن المجال التكنولوجي لم يعرف هذا المسار فقد تولت الحكومات التكفل بكل ما هو تكنولوجي عن طريق المناشير و التعليمات ،ثم المراسيم و بعد ذلك تدخل القانون[29] لوضع ضوابط أخرى ،فما هي الإضافة التي أضافها المجال التكنولوجي لحقوق الأفراد.

[29] G.Chatillon, Op Cite p 673

كرس الدستور الجزائري[30] العديد من الحقوق من مساواة و حياد و حق في الإعلام و غيرها من الحقوق و في ظل التحول الرقمي فإن البعض من هذه الحقوق تدعم و الآخر بقي من الناحية القانونية محل نقاش.

أول ما يرتبط بعلاقة المواطن بالإدارة أو بالدولة هي الحق في الإعلام بالنسبة لجميع المواطنين، و قد نظم بشكل جديد مع ظهور عصر تكنولوجيا الإعلام و الاتصال، حيث يجد المواطن كل ما يريد معرفته عبر الانترنيت حتى النصوص القانونية. ، و من مزايا هذه التكنولوجيا أن مواطن أية دولة يستطيع الاطلاع على قوانين و أخبار دول أخرى بسهولة ،و يستطيع بذلك تكوين فكر و وعي قانوني لا يكلفه جهدا كبيرا ، و قد كانت هذه المسألة قبل ظهور تكنولوجيا الإعلام و الاتصال تنظمها القواعد التي تقرها الدساتير و القوانين و التي لا يطلع عليها العديد من المواطنين إلا إذا كانت الحاجة إليها مطلوبة.إلى هنا تبقى المسألة جيدة ،و لكن ماذا عن الأنظمة التي تزاوج بين النمطين التقليدي و المعاصر في تنظيم إعلام المواطنين بين ما هو مادي و ما هو لا مادي ؟ و حتى لا نذهب بعيدا في التحاليل يمكننا الانطلاق من الأمثلة القريبة منا و من بينها المثال الجزائري، إذ ينص الدستور الجزائري على وجوب نشر القوانين و التنظيمات في الجريدة الرسمية [31] لكي يلتزم المواطنون بها، و في موضع أخر يقرر الدستور قاعدة دستورية تضمن الاستقرار و تتمثل في مقولة يعرفها العام و الخاص و هي "لا يعذر أحد بجهل القانون"[32] . فمع وصول إلى علم المواطن وجود قاعدة قانونية بعد النشر لا يمكنه أن يتذرع بأية حجة. إن هذه القواعد التي كرسها الدستور تفرض إلزامية القوانين و تضع ضمانات للمواطنين و هذا ما تؤكده المادة .04 من القانون المدني[33]التي تنص "تطبق القوانين في تراب الجمهورية الجزائرية الديمقراطية الشعبية ابتداء من يوم نشرها في الجريدة الرسمية"

---

[30] المرسوم الرئاسي 20-442 الموافق ل30ديسمبر2020 يعل بإصدار التعديل الدستوري ، جريدة رسمية عدد82.

[31] المادة 78/فقرة 2 نفس المرجع

[32] نفس المرجع فقرة1

[33] أمر 75-58 الموافق ل 26 سبتمر 1975 يتضمن القانون المدني المعدل و المتمم.

- تكون نافذة في الجزائر العاصمة بعد مضي يوم كامل من تاريخ نشرها و في النواحي الأخرى في نطاق كل دائرة بعد مضي يوم كامل من تاريخ وصول الجريدة الرسمية إلى مقر الدائرة و يشهد على ذلك ختم الدائرة الموضوع على الجريدة "

إن إضافة النسخة الإلكترونية و نشرها على الموقع الإلكتروني للأمانة العامة للحكومة مع الإبقاء على النسخة الورقية يجعل مفهوم النشر أشمل و مفهوم الوصول إلى علم المواطن أوسع مما كان عليه، حيث لا يتطلب الأمر من المواطنين وقتا طويلا لمعرف مضمون الجريدة و لكنهم لا يستطيعون التذرع بعدم وجودها بعد التحول الرقمي .

إن هذه النتيجة تحتاج من الباحثين تسليط الضوء عليها في العصر الحالي لأن نص المادة 04 من القانون المدني لم يطرأ عليها أي تعديل ، و في جميع التعديلات التي خضع لها القانون المدني، و هي تشير إلى مدة زمنية محددة بيوم كامل بعد النشر أي النشر للنسخة الورقية ، بينما الفضاء الإلكتروني الذي أصبح حقيقة قانونية لا يعرف هذا التحديد الزمني هذا من جهة ، و من جهة ثانية تلزم الفقرة الثانية من نص المادة 04 كل دائرة إدارية بوضع ختم على النسخة الورقية كدليل على وصولها إلى علم المواطنين. هذه المسألة يجب أن تفتح النقاش على مصراعيه في ظل التحول الرقمي و الحقوق المترتبة عليه ،لأنه إذا كان الأمر غير ذلك فما الجدوى من التحول و تقليص الهوة بين دولتنا و الدول المتقدمة في المجال الرقمي إذا كانت الاستعانة بالآلة من الأطراف القضائية و حتى الإدارية لا تؤخذ بعين الاعتبار .

حق أخر يمنحه الدستور و القوانين للمواطنين في إطار ممارسة الديمقراطية و هو الحق في التصويت ، و أخر ما أصبح يدور في الخطابات السياسية هي فكرة الديمقراطية الإلكترونية التي تتم عن طريق التصويت عن بعد أي عبر الانترنيت ، هذه العملية و إن كانت ذات محاسن كثيرة في اختصار الوقت و في تعزيز الشفافية و الحياد و كذا المساواة في التعامل و كذا توسيع دائرة الناخبين ،غير أن بعض الباحثين يرون فيها عبارة سحرية [34] تحمل من المخاطر ما قد يقطع بل يبتر الثقة بين المواطن و الدولة لأنها تحتاج لوعي شعبي و لثقافة إلكترونية ، كما تتطلب تقنيات متطورة في هذا المجال من أجل ضمان و حماية العملية الانتخابية.

---

[34] E.Neuveux

تعرف بعض الدول الغربية الديمقراطية الإلكترونية و قد أشادت بها العديد من التقارير [35]التي أنجزتها هيئات دولية ، و كذلك التحقت الجزائر بالركب من خلال تجربة التسجيل الإلكتروني للقوائم الانتخابية عن بعد إثر التعديل الدستوري لسنة 2020[36] . و قد تكون هذه البداية لتعميم و توسيع العملية لتشمل جميع المناسبات الانتخابية و في جميع مراحلها و تساهم في تكريس مبادئ الشفافية و النزاهة و المساواة. غير أن مسألة قانونية ملحة يجب أن تعكف عليها الحكومات الجزائرية في ظل المعطيات الواقعية و هي تصويت البدو الرحل ؟

لم يعكف الباحثون و لا السياسيون بعد على مناقشة جوانب أخرى أفرزتها الممارسة حول تنظيم الحملة الانتخابية أو الاسفتائية التي ينظمها القانون بقواعد صارمة [37]،غير أن الفضاء الإلكتروني شهد إثر التعديل الدستوري الجزائري لسنة 2020 حملة "إلكترونية" -إن صح التعبير – تضمنت تدخلات عديدة عبر مواقع التواصل الاجتماعي لأطراف مختصة في المجال السياسي و القانوني و الدولي و الاقتصادي و غيرها، و أكثرها غير مختصة ، و ذلك بالموازاة مع الحملة الإستفتائية الرسمية .وقد نتج عن هذه التدخلات سوء فهم لبعض المواد[38] نظرا لتأثير الفئة الثانية من غير المختصين، فإذا كان الفضاء الإلكتروني يتيح حرية التعبير فإن الأمر يختلف عندما يتعلق الأمر بالنص الأساسي للبلاد أو بالنسبة للمناسبات الرسمية التي تقرر مصير المؤسسات ،و الذي يجب على المواطن أن يفهمها فهما صحيحا يُمكّنه من تقدير مدى تطابق النص و ميوله السياسية أو الاجتماعية و حتى الاقتصادية لكي يستطيع التصويت بالإيجاب أو بالسلب. فإذا كان القانون يحدد فترة للحملة فهو يترك للمواطن فترة زمنية ليُكَون موقفا تجاه المسألة و ليس الأمر كذلك على المستوى التكنولوجي.

ظهرت في خطابات سياسية و قانونية أيضا فكرة الديمقراطية الإلكترونية عن طريق مشاركة المواطنين في إعداد القوانين و قد كان المثال الذي قدمه تقرير المجلس الوطني الفرنسي سنة 2015

---

[35] Promesses et limites de la démocratie électronique ,OCDE 2003.

[36] http://ina-élections.dz *تقرير السلطة الوطنية المستقلة للانتخابات*

[37] تختلف هذه المسألة في الدول الغربية و لا يسع هذا المقال مناقشتها

[38] تصريح رئيس لجنة الخبراء أحمد لعرابة لجريدة" ليبرتي"بتاريخ 8 جوان 2020 حول المواطنة و الذي أولته العديد من الأطراف رغم حداثة النقاش حول الموضوع.

[39] أشار إلى إمكانية منح المواطنين فرصة المشاركة في إعداد القوانين عن طريق الولوج إلى منصة إلكترونية لهذا الغرض، و أضاف أنه بإمكانهم أيضا اقتراح تعديلات على القانون . و لكن سرعان ما تبين من خلال التقرير وجود عوائق عملية لتجسيد مثل هذه المقترحات ، منها أن العملية تعد لصالح الأشخاص الذين يتحكمون في تكنولوجيا الإعلام و الاتصال ، و هم الوحيدين الذين يستطيعون المشاركة في النقاش حول القانون، أما البقية قد يحرمون من المشاركة لأسباب تقنية و حسب .هذا ، وقد توصل البحث ذاته حول المسألة لأرقام تؤكد مخاوف مصممي التقرير.[40]

يشير الدستور و القوانين و التنظيمات في الجزائر لمشاركة المواطنين في صنع القرار في عدة مجالات عن طريق المجالس الانتخابية و الاستشارية و غيرها من الآليات المكرسة، و يبقى اللجوء لتفعيل المسألة من الناحية الإلكترونية في جدول أعمال الحكومات المستقبلية عندما تصل الدولة إلى المستوى المطلوب من الرقمنة كما صرح به وزير الرقمنة و الإحصائيات [41]

إن إقرار الحقوق الأخرى في قائمة طويلة في الدساتير و في المقابل إقرار العديد من القوانين لتفصيل و وضع ضوابط لهذه الحقوق ما هو إلا ردة فعل طبيعية على سرعة التكنولوجيا فبعد إقرار حرية التعبير و حق إنشاء صحافة إلكترونية و غيرها من الحقوق ،ها هو المشرع يسارع لوضع قوانين لحماية البيانات الشخصية [42] و يسارع لحماية حرية الإبداع الفكري بأبعاده العلمية و الفنية و بتحديد شروط بيع الكتاب الإلكتروني[43] و غيرها من القوانين.

إن المواطن يواجه أوضاعا جديدة في عصر تكنولوجيا الإعلام و الاتصال كما أن جميع الجهود الحكومية و في جميع الدول منصبة عليه ،غير أن التكنولوجيا التي تسهل المعاملات تحتاج هي الأخرى إلى مواطن أخر يكون في خدمته عن طريق استخدام الآلة و هو الموظف الذي يجب أن تراعى الحكومات حقوقه في المجال الرقمي ، و هذا ما ظهر من خلال توصية المجلس الوطني الاقتصادي و

---

[39] L. El Badawi :L'accessibilité numérique au droit", Le Dossier : De l'accès au droit à l'exercice de la citoyenneté, Actes du colloque de Clermont-Ferrand des 24-25 septembre 2015, textes réunis par F. Faberon et A. Habrial, La Revue du Centre Michel de l'Hospital [édition électronique], 2017, n° 12, pp. 33-44

[40] Ibid.

[41] مداخلة وزير الرقمنة و الإحصائيات، يوم دراسي حول موسوم بالتحول الرقمي من أجل مرفق عمومي فعال، المجلس الشعبي الوطني 06/جوان 2022.

[42] قانون 18-07 المواف ل10يونيو2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي

[43] المرسم التنفيذي 22-271 الموافق ل18 يوليو2022 يحدد كيفيات بيع الكتاب الإلكتروني جريدة رسمية عدد49.

الاجتماعي من أجل تكوينه من جهة ،و من جهة أخرى فتح باب التوظيف لكل متخصص في المجال التكنولوجي [44] . فللتكنولوجيا مزايا على المواطن و على من يقدم له الخدمة أيضا

2-2 مصير الحقوق المتحولة للصيغة الإلكترونية.

ليست الجهود العلمية فقط هي التي تريد مواكبة التكنولوجيا فالمشرع أيضا يرى وجوب تنظيم العديد من الحقوق التي تحولت للمجال الرقمي من أجل ضمان السلامة القانونية للمعاملات.

كتب بعض المؤلفين [45]عن حقوق الأفراد تجاه المرفق العمومي أنه حسب أشهر مؤلفات القانون العام يعتبر المرفق العمومي خطر على الحريات العامة[46] ، حتى و إن كانت المسألة فقهية و محل نقاش فإنها لا تخلو من الاهتمام بالنسبة للموظف الذي يتمتع بجميع الحقوق و الحريات كمواطن ،و لكنه في مقابل ذلك يصطدم بموانع لهذه الحقوق فرضتها القوانين و التنظيمات ، و في ظل تكنولوجيا الإعلام و لاتصال يمكن التساؤل .هل تزول هذه الموانع أم أنها تحتاج لتنظيم مختلف؟

يرتبط الموظف بالإدارة العمومية بعلاقة قانونية و نظامية تمنحه العديد من الحقوق و تلزمه بالعديد من الواجبات و من بين الحقوق التي يتمتع بها الحق في التوظيف و الحق في الراتب بعد تأديته للخدمة و الحق في الترقية و الحق في الراحة و الحق في التكوين.....إلخ. كما يتمتع بالحريات العامة التي يتمتع بها المواطن من حرية التعبير و حرية التنقل و غيرها .....إلخ. و بالإضافة إلى هذه الحقوق و الحريات فإن الموظف مطالب باحترام الواجبات المفروضة عليه من واجب الطاعة و واجب احترام مبدأ السرية و واجب التحفظ و غيرها.

إن المعادلة التي تجمع بين الحقوق و الحريات و الواجبات للموظف هي محل أبحاث توصل المشرع في القانون المقارن و كذا في القانون الجزائري من خلالها إلى تنظيم البعض منها، و لكن دون أن يتوصل إلى توازن معقول، و المثال على ذلك هو نص المادة 26 من قانون الوظيفة العمومية الجزائرية [47] التي تمنح حرية الرأي للموظف و تلزمه بواجب التحفظ ، فإذا كان الأمر كذلك في

---

[44] رأي حول مشروع أ-الجزائر13 ، مرجع سابق.

[45] A.Antoine ;E.Fraysse :service public ,libertés et approche contemporaine du droit administratif,RDLFn°83,2020,http//www.revuedlf.com.

[46] P.Devolvé, Ibid.

[47] أمر 06-03 الموافق ل15 يوليو 2006 يتضمن القانون الأساسي العام للوظيفة العمومية ، جريدة رسمية عدد

الحالات العادية فما هو مصير هذا المنع في الفضاء الإلكتروني؟ خاصة و أن تكنولوجيا الإعلام و الاتصال تتيح الفرصة لكل فرد سهولة نشر المعلومات التي بحوزته[48] ،كما أن هذه الأخيرة تتيح له أيضا عدم الإفصاح عن هويته أو انتمائه المهني الأمر الذي ينتج عنه الإضرار بمصالح الأشخاص و المؤسسات أيضا ، و يتطلب إعادة تنظيم المجال الإلكتروني بما يحفظ التوازن.

بالإضافة لإقرار العديد من الحريات للموظف كمواطن فإن له العديد من الحقوق أقرها قانون الوظيفة العمومية ، غير أن التعداد الذي ورد في القانون ليس حصريا حسب موقف القضاء الجزائري في العديد من القضايا .

الحق في الحماية من التهديد و الإهانة و الشتم و الاعتداء ، الحق في الراتب ، الحق في الأقدمية و الحق النقابي، و كذا الحق في الإضراب و الحق في التكوين و تحسين المستوى ،و الحق في العطل ،كلها حقوق وردت ضمن قانون الوظيفة العمومية و هي تمارس بصفة عادية من طرف الموظف و مع ظهور تكنولوجيا الإعلام و الاتصال صار مفهوم و أثر كل حق من هذه الحقوق حسب الوضعية التي تعترض الموظف مختلفا عما كان عليه من قبل .

قبل سرد مجمل الحقوق في زمن التكنولوجيا يجب الوقوف عند مفهوم جديد للوظيفة أو العمل الذي ينجز عن طريق تكنولوجيا الإعلام و الاتصال و هو العمل عن بعد (le télétravail) ،و الذي يقصد به اللجوء لوسائل تكنولوجيا الإعلام و الاتصال من هواتف ذكية و لوحات إلكترونية و الكمبيوتر للقيام بالأعمال خارج مكان العمل [49] .كما يكون العمل عن بعد محل اتفاق بين صاحب العمل و العمال أو الموظفين ، و يُشترط فيه تحديد موضوع العمل و الوسائل المستخدمة و آليات الرقابة و طرق الإبلاغ عن العمل المنجز.

يستخدم هذا النمط من العمل عن بعد في الدول المتقدمة بالشروط المذكورة آنفا ،و قد تضاعف اللجوء إليه خلال جائحة 2020 في جميع دول العالم ،غير أن تطبيقه في الجزائر ، خاصة في الوظيفة العمومية ، لم يخضع للشروط التي ذُكرت من قبل ، كما لم تُثر حوله المسائل القانونية

---

[48] J.M.Sauvé : la protection des droits fondamentaux à l'ère du numérique ,CE dec 2017, www.conseil-etat.fr.

[49] OIT : le télétravail durant la pandémie de covid19 et après ; guide pratique 1ère éd 2020 ترجمة. الكاتبة

المرتبطة بحقوق الموظفين من حيث الراتب و أوقات العمل و ما إلى ذلك ، مع أن اللجوء إلى هذا النمط من العمل لم يعد مرتبطا بالظروف الاستثنائية.

لمناقشة الحقوق الخاصة بالموظف تستوقفنا المادة 30 من قانون الوظيفة العمومية [50] و التي تقرر حماية الموظف من الشتم و التهديد و الإهانة ، فإذا كانت المسألة سهلة التطبيق في الحياة الإدارية العادية ، فإن الأمر قد يأخذ وقتا طويلا عندما يتم الاعتداء عبر وسائل الإعلام و الاتصال و قد ينجر عنه تبعات نفسية للموظف ربما تغير تعامله تجاه المرتفقين أو ترتب آثار أخرى تؤدي إلى تعطيل المرفق العمومي و الأهم من ذلك ما هي الوسيلة الإلكترونية التي تقي الموظف من الإهانة.

حق أخر من أهم الحقوق التي يطالب بها الموظفون باستمرار هو التكوين و تحسين المستوى ، فمع الدخول في عصر تكنولوجيا الإعلام و الاتصال تغيرت المعطيات، فقبل أن تتسع رقعة الرقمنة في الوظيفة العمومية، كان المجلس الوطني الاقتصادي و الاجتماعي الجزائري قد لاحظ في تقرير مشروع أ الجزائر 2013 أن هناك نقص في المورد البشري المتخصص، كما أوصى بتوظيف واسع لكل من يحمل المؤهلات التقنية لتسريع عملية رقمنة الخدمات العمومية ،و في هذا الإطار أصبحت جميع القطاعات تشمل على فئات متخصصة من الموظفين في المجال التكنولوجي.

إن النتيجة القانونية المترتبة عن تطبيق المادة 38 من قانون الوظيفة العمومية تؤدي إلى أن تكوين الموظف العادي في مجال تكنولوجيا الإعلام و الاتصال يصبح غير ملح ، كما أنه يزيد من كلفة التكوين .أما النتيجة الأخرى و التي تنبأت لها بعض الكتابات [51] في مثل هذه الأوضاع هي أن الآلة قد تكون سببا في التخلي عن بعض الموظفين و تسريحهم ، لأن الخدمة لا تحتاج لعدد كبير من الموظفين.

تساؤلات أخرى قانونية لم تر النور بعد في العصر الرقمي مثل كيفية ممارسة الحق النقابي و ممارسة حق الإضراب في نمط العمل عن بعد، و الحق في العطل، غير أن الوتيرة التي تسير عليها معظم الدول في رقمنة خدماتها ستجبرها يوما ما التفكير فيها لإيجاد الحلول المناسبة.

---

[50] أمر 06-03 مرجع سابق

[51] T.Perroud : droits des administrés internautes et téléservices publics, RFSP2013,p 3.

و على مستوى أخر ينظم قانون الوظيفة العمومية المسار المهني للموظف إذ تلتزم الإدارة بتكوين ملف إداري يتضمن مؤهلات الموظف و وثائق أخرى ، و كما تحدده لمادة 38 من قانون الوظيفة العمومية فإن للموظف الحق في الترقية .غير أن ممارسة هذا الحق في العصر الرقمي لا يتيح له الاطلاع على ملفه الإداري عبر تكنولوجيا الإعلام و الاتصال، و إنما يُبلّغ بقرار الترقية و غيره من القرارات بالطريقة التقليدية المادية [52] مع أن العديد من القطاعات العمومية تتوفر على وسائل تكنولوجية لحماية بياناتها. هذا و قد أدرج التنظيم في إطار العصرنة معايير جديدة لتقييم الموظف ذكرها المرسوم التنفيذي 19-165 [53] و التي لا يجد البعض منها تفسيرا واضحا له في ظل استخدام تكنولوجيا الإعلام و الاتصال ، بل لا يمكن للمسئول الإداري أخذها بعين الاعتبار لتقييم الموظف ، على غرار ما ورد في المادة 05 من المرسوم و التي تحدد قدرات التعبير الكتابية و الشفاهية للموظف بينما تسعى التكنولوجية في العديد من الخدمات لاستغلال الآلة عن طريق برامج محددة للغرض و الاستغناء عن العنصر البشري ، بالإضافة إلى ذلك فإن قدرات الموظف في الاستباق و التكيف و الابتكار قد تصلح في بعض المجالات و قد لا يكون لها مكان في مجالات تقنية لا يتحكم فيها الموظف ،و بالتالي قد تصلح كمعايير للتقييم في البعض و قد لا تستخدم في البعض الأخر.

آخر ما أشار إليه المرسوم التنفيذي 19-165 في المادة 5 منه يتعلق بروح العمل الجماعي و القدرة على التواصل و روح المبادرة و الديناميكية. و ترتبط هذه المعايير بالمبدأ الذي جاء ضمن المرسوم المنظم للمرصد الوطني للمرفق العمومي حول أنسنة المرفق العمومي[54]، غير أن تقييم روح العمل الجماعي في المجال التكنولوجي ليس بالأمر اليسير . أما القدرة على التواصل فهي من صميم البرامج التي يعدها المختصون في المجال الآلي لتسهيل العمل على الموظفين

خلاصة القول أن الموظف مثله مثل المواطن العادي دخلت تكنولوجيا الإعلام و الاتصال في حياته المهنية لكي تسهل عليه العمل، و تسهل عليه الاستفادة من حقوقه المهنية أيضا .فإذا كان تسهيل العمل موجها في بداية الأمر للمواطن من طرف الحكومات، فإنه خلق أيضا آثارا إيجابية

---

[52] لم يرد إلينا و لو مثال واحد من الإدارات العمومية يخرج عن هذه الممارسة

[53] المرسوم التنفيذي 19-165 الموافق ل 27 مايو 2019 يحدد كيفيات تقييم الموظف ، جريدة رسمية عدد 37.

[54] المرسوم الرئاسي 16-03 مرجع سابق

لدى الموظف ،أهمها تقليل الضغط عليه. و مادون هذه الآثار يُنتظر أن تتحول جهود القوانين و التنظيمات إلى تنظيم حقوقه المهنية إلكترونيا لكي تكتمل فكرة عصرنة المرفق.

خاتمة.

إن ظهور تكنولوجيا الإعلام و الاتصال في حياة الأفراد العادية و المهنية أيضا أعطت نتائج مبهرة على مستوى المفاهيم و على مستوى التطبيق، و قد ساعدت على إنتاج لغة رقمية متخصصة في مجالات عديدة ،منها المجال القانوني ، كما غيرت طرق التسيير التقليدية على المستوى الإداري إلى طرق تعتمد مبادئ جديدة حتى أضحت عنصرا هاما في إرساء الإصلاحات.

كما استفاد المواطن و الموظف من تكنولوجيا الإعلام و الاتصال بات من الضروري التفكير في تجسيد المبادئ التي وردت في القوانين و التنظيمات من أنسنة للمرفق العمومي و من ديمقراطية إلكترونية و غيره حتى تتدعم مكانة الفرد في العالم الافتراضي أو بعبارة أخرى ،إضافة للاهتمامات الحكومية المتعلقة بتحسين الخدمة العمومية اهتمامات أخرى تتعلق بحقوق الأفراد في الفضاء الرقمي.

الحق في الولوج إلى الأنترنت

The right of access to the internet

يبدة ليلى، أستاذة محاضرة أ

كلية الحقوق-جامعة الجزائر1-الجزائر

yebdaleila@yahoo.fr

ملخص :

تتميز الأنترنت بطبيعتها العالمية والمفتوحة بصفتها قوة دافعة إلى التنمية بمختلف أشكالها، كما أن الولوج إلى الأنترنت شرط أساسي لممارسة الحقوق والحريات والمشاركة في العملية الديموقراطية، إلا أنه إلى حد الآن ليس حقا موثقا من حقوق الإنسان، لكن المشاركة الفعالة في مجتمع المعلومات تتطلب الولوج إلى الاتصال الرقمي.

ويكمن الهدف من هذه الدراسة تحديد الأساس القانوني للحق في الولوج إلى الأنترنت بإعتبار أن مجتمع المعلومات فرض ضمانه للجميع من أجل التمتع الأحسن بحقوقهم.

الكلمات المفتاحية: حقوق الإنسان، الأنترنت، التحديات، الفجوة الرقمية.

Abstract :

The internet is characterized by its global and open nature as a driving force for development in its various forms, and access to the internet is a prerequisite for the exercise of rights and freedoms and participation in the democratic process, but so far it is not a documented human right, but effective participation in the information society requises access to communication digital.

The aim of this study is to determine the legal basis for the right to access the internet , considering that the information society imposes a garantee for all in order to better enjoy their rights.

Keywords : Human rights , internet, challenges, digital divide.

مقدمة:

تطال الثورة الرقمية كل أوساط الحياة العامة والخاصة، بحيث تتزايد المعلومات الشخصية والعامة التي تجمع، تخزن وتتقاسم عبر الأنترنت، كما يتميز المجال الرقمي بالتعقيد والحساسية بشكل خاص، وذلك بسبب طابعه عبر الوطني ومتعدد الأبعاد، وهذا ما دفع بمجلس حقوق الإنسان إلى التأكيد على الطبيعة العالمية والمفتوحة للأنترنت بصفتها قوة دافعة إلى التنمية بمختلف أشكالها، وتؤدي إلى بلوغ أهداف التنمية المستدامة، كما دعا جميع الدول إلى تشجيع محو الأمية الرقمية وتيسير الوصول إلى الأنترنت، بإعتبار أن الولوج إلى الأنترنت شرطا أساسيا مهما لممارسة الحقوق والحريات والمشاركة في العملية الديموقراطية، وهو إلى حد الآن ليس حقا موثقا من حقوق الإنسان، إلا أنه في مجتمع المعلومات تتطلب المشاركة الفعالة الولوج إلى الاتصال الرقمي.

كما أن هناك حقوق ذات الصلة بتداول المعلومات مثل حرية الرأي والتعبير، حرية تداول المعلومات، الحق في الخصوصية، الحق في الأمان الرقمي، الحق في المعرفة، الحق في التعليم، الحق في التطوير والاستفادة من فوائد التقدم العلمي، وغيرها من الحقوق، وعليه نطرح الإشكالية التالية:" إلى أي مدى يمكن ضمان الحق في الولوج إلى الأنترنت بإعتباره حق إنساني؟".

اتبعنا في دراستنا على المنهج الوصفي من خلال سرد محتلف التعاريف للحق في الولوج إلى الأنترنت، وعلى المنهج الاستقرائي من خلال تحليل مختلف النصوص القانونية المكرسة لهذا الحق واستنباط مختلف التحديات التي تواجهه.

ولقد قسمنا دراستنا إلى قسمين الأول تناولنا فيه ماهية الحق في الولوج إلى الانترنت والثاني التحديات التي تواجهه.

المبحث الأول: ماهية الحق في الولوج إلى الأنترنت

سنتناول في هذا المبحث نشأة وتعريف الأنترنت ثم نبين الأساس القانوني لهذا الحق

المطلب الأول: مفهوم الحق في الولوج إلى الأنترنت

تعتبر الأنترنت هي العنصر الأساسي المكون لهذا الحق لهذا سنقوم بالتحدث عن نشأتها ثم تعريفها، لنبين فيما بعد تعريف الحق في الولوج إلى الأنترنت وأساسه القانوني وذلك في الفرعين التاليين:

الفرع الأول: مفهوم الأنترنت

سنبين في هذا الفرع نشأة الأنترنت ثم نقوم بتوضيح مختلف تعريفاتها

أولا/-نشأة الأنترنت وأهميتها:

يعود نشأة الأنترنت إلى أواخر الستينات، وهي نتاج الثورة التكنولوجيا، ولقد تطور استعمالها لشمل كل مجالات الحياة، وعليه سنوضح فيما يلي، نشأة الأنترنت ثم نبين أهميتها.

1/-نشأة الأنترنت:

تعد الأنترنت من نتائج الثورة المعلوماتية والتكنولوجية، وهي من أهم الإنجازات التقنية التي شهدتها البشرية في العقد الأخير من القرن العشرين، حيث أصبحت شبكة الانترنت بمثابة دائرة معارف ومعلومات عالمية الانتشار، وظاهرة اجتماعية تمس حياة الإنسان في مختلف الميادين حتى الأكثر خصوصية منها[1].

ويرجع تاريخ ظهور الأنترنت إلى عام 1969 مع أربانتARPANET، وهي شبكة كمبيوتر أسستها مشروعات الأبحاث المتطورة التابعة لوزارة الدفاع الأمريكية، أما الخطوة الثانية نحو نشأة الأنترنت بفكرة ربط شبكة أربانت بشبكات الكمبيوتر الأخرى الممكنة، وبدأت هذه المحاولات بشبكات الإتصال التي تديرها أربانت، وفي عام 1973 تم وضع أول بروتوكول موحد للاتصالات وفي عام1983 قررت الوزارة الدفاع الأمريكية تقسيم الشبكات حسب أغراض الاستخدام إلى مجتمعات عسكرية وأخرى بحثية غير عسكرية، وتم إنشاء شبكة MILNET للأغراض العسكرية وتحويل أربانت ARPANETإلى ARPA-INTERNET لتدعيم الأغراض البحثية، ومع إطلاق الإنترنت خارج المجال العسكري، قامت الولايات المتحدة بتمويل مؤسسة العلوم الوطنية الأمريكية، وفي 1985 أعلنت هذه الأخيرة عن نيتها في خدمة مجتمع التعليم العالي[2].

2/-أهمية الأنترنت:

يمثل الأنترنت قفزة هائلة إلى الأمام باعتباره واسطة تفاعلية، فبظهور خدمات web 2.0، أو المنصات الوسيطة التي تسهل تبادل المعلومات القائم على المشاركة والتعاون في إنشاء المحتويات، لم يصبح الأفراد متلقين، وإنما ناشرين فاعلين للمعلومات، كما تكتسي تلك المنصات قيمة خاصة في البلدان التي لا توجد فيها وسائط إعلام مستقلة لأنها تمكن الأفراد من تبادل الآراء النقدية ومن إيجاد المعلومات الموضوعية، كما تتيح الأنترنت الحصول على المعلومات والمعارف التي كانت في السابق بعيدة المنال، فهي تمكن الأفراد من تبادل المعلومات والأفكار عبر الحدود الوطنية آنيا وبكلفة رخيصة، وهذا ما يساهم في الكشف عن الحقيقة وفي تقدم المجتمع ككل[3].

ثانيا/- تعريف الأنترنت:

سنوضح مختلف التعريفات اللغوية، الفنية والقانونية

1/-التعريف اللغوي:

كلمة أنترنت ترجمة حرفية لمصطلح '« Internet، بالأنجليزية، ولقد اختلف الفقهاء في تحديد المصطلحات الأصلية التي اشتق منها هذا الإسم، فهناك جانب من الفقه يرى بأن مصطلح الأنترنت هو اختصار للتسمية الإنجليزية Inter connection network والتي يقصد بها شبكة الترابط أو الإتصال، أما جانب من الفقه يرى بأن أصل كلمة ,Internet بالإنجليزية هو اختصار للمصطلحات International Network والذي يقصد به الشبكة العالمية[4].

2/-**التعريف الفني للأنترنت:**

الأنترنت هو النظام العالمي لشبكات الكمبيوتر المترابطة التي تستخدم مجموعة بروتوكول أنترنت(TCP/IP)لارتباط المليارات من الأجهزة في جميع أنحاء العالم، فالأنترنت شبكة الشبكات التي تتكون من ملايين الشبكات الخاصة والعامة والأكاديمية والتجارية، والحكومة المحلية على النطاق العالمي مرتبط بمجموعة واسعة من تقنيات الشبكات اللاسلكية والإلكترونية والضوئية[5].

3/-التعريف الفقهي:

حاول بعض فقهاء القانون وشراحه خاصة المهتمين منهم والمتخصصين في مجال تكنولوجيا الإعلام و الاتصال والتجارة الإلكترونية تحديدا إيجاد بعض التعريفات القانونية لشبكة الأنترنت نذكر منها تعريف الفقيه يونس عرب الأنترنت هي:" أكبر شبكة اتصالات، فهي البديل النظري للعالم الجغرافي، وهي مجموعة شبكات اتصالات فردية وجماعية ومجموعة كمبيوترات متناثرة وموزعة عبر جميع أرجاء العالم مرتبطة معا في كتلة لم يتبلور شكلها حتى الآن، إنها اتحاد كونفيدرالي مفكك الأوصال على الرغم من أنها لم تبدأ بالأصل كذلك، وهي ليست مملوكة لأحد وليس ثمة هناك جمعية إدارية مركزية أو تحكم، وإن كانت دول الشمال هي من سعت وتسعى للتحكم فيها"[6].

4/-التعريف القانوني للأنترنت:

سنبين فيما يلي تعريف الحق في الولوج إلى الأنترنت حسب ما جاء في التشريعات الوطنية الجزائرية، والتعريف الدولي.

أ/-التعريف القانوني الوطني:

بالرجوع إلى التشريعات الوطنية الجزائرية نجد المرسوم التنفيذي رقم98-257[7]، في المادة 2 منه عرفت الأنترنت من خلال خدماتها، كما عرف القانون 18-04[8]في المادة 10 منه الأنترنت بأنها:"شبكة معلوماتية عالمية تتشكل من مجموعة شبكات وطنية وإقليمية وخاصة، موصولة فيما بينها عن طريق بروتوكول الاتصالIP وتعمل معا بهدف تقديم واجهة موحدة لمستخدميها".

ب/-التعريف الدولي:

لقد بينا أعلاه مختلف التعريفات التي تضمنتها القوانين الجزائرية المتعلقة بالأنترنت والتي عرفت هذه الأخيرة دون أن تنص على الحق في الولوج إلى الأنترنت ولم تعرفه، وعليه سنتناول فيما يلي التعريف الدولي للحق في الولوج إلى الأنترنت الذي ورد في تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير:" وهو حق الأفراد في الوصول إلى الأنترنت وإتاحته بشكل يمكنهم من ممارسة هذا الحق والتمتع بالحقوق المترتبة عليه من حرية التعبير على الأنترنت وبقية الحقوق التي تعتبرها الأمم المتحدة حقوق أساسية للأفراد، بحيث تتحمل الدول مسؤولية ضمان إتاحة الوصول إلى الأنترنت، في نفس الوقت لم يعد ضروريا على الدولة تحمل مسؤولية تقييد وصول الأفراد إلى الأنترنت[9]، ويؤكد المقرر الخاص على أن الحصول على خدمة الأنترنت بعدان الأول: هو الوصول إلى محتويات الأنترنت دون أي قيد ما عدا في حالات قليلة محدودة يجيزها القانون الدولي لحقوق الإنسان، أما البعد الثاني، فيتمثل في: توفر الهياكل الأساسية وتكنولوجيات الاتصال والمعلومات الضرورية للولوج للأنترنت، كالكابلات وأجهزة المواديم والحواسيب والبرامج المعلوماتية[10].

الفرع الثاني: الأساس القانوني للحق في الولوج إلى الأنترنت.

هناك جدل حول اعتبار الولوج إلى الانترنت حق إنساني، لابد من ضمانه للجميع بحكم طبيعتهم الإنسانية، إلا أن الوصول إلى الأنترنت ليست متأصلة في الطبيعة البشرية، وإنما التطور التكنولوجي هو الذي فرض اعتباره حق إنساني، وعليه نبحث في النصوص الدولية عن وفي التشريعات الوطنية عن أساس هذا الحق، فيما يلي:

أولا/- التكريس الدولي للحق في الولوج إلى الأنترنت:

أصبح من الضروري الاعتراف بحق الولوج إلى الأنترنت كحق من حقوق الإنسان، لأنه في العصر الرقمي هناك العديد من حقوق الإنسان التي لا يمكن التمتع بها بشكل كاف دون الوصول إلى الأنترنت خاصة في البلدان النامية، على سبيل المثال تسهيل الوصول إلى الأنترنت يسهل الوصول إلى الخدمات الصحية، ولقد أظهرت جائحة كورونا أساسية وجود هذا الحق، إلا أن هناك من يرى بأنه لا يمكن اعتبار الاتصال بالأنترنت أو الاتصال الرقمي مطلبا متأصلا في الجنس البشري[11]،

ويرى آخرون أن الوصول إلى الأنترنت حق ثانوي بإمكانه تسهيل الحقوق الأساسية، لكن لا يمكن اعتباره حق إنساني ، رغم اتصال الحقوق الأساسية بالأنترنت، وفي هذا الشأن يقول الأستاذ مارك كويكلبيرج من جامعة فيينا بأن:" الذين ليس لديهم الأنترنت سيتمتعون بحماية أقل لحقوق معينة، ويضيف أنه من المهم الاعتراف بالوصول إلى الأنترنت في إطار قانوني يضمن التمتع به، لكن

لا يملك صفة حقوق الإنسان، ولقد أيدت الأمم المتحدة هذا الرأي في قرار صدر عام 2016، الذي أقر بأهمية الأنترنت لممارسة حقوق مثل حرية التعبير والتعليم وحرية الضمير"[12].

1/-تكريس الحق في الولوج إلى الأنترنت في النصوص الدولية الصادرة عن الأمم المتحدة:

لقد نصت المادة 15 من العهد الدولي المتعلق بالحقوق الاقتصادية والاجتماعية والثقافية على حق كل فرد في المشاركة في الحياة الثقافية، والتمتع بفوائد التقدم العلمي وتطبيقاته، وألزمت الدول الأطراف في العهد باحترام الحرية التي لا غنى عنها للبحث العلمي والنشاط الإبداعي، كما نصت المادة 19 من الإعلان العالمي لحقوق الإنسان والعهد الدولي المتعلق بالحقوق المدنية والسياسية على حق كل شخص في التماس الأنباء والأفكار وتلقيها ونقلها إلى الآخرين بأية وسيلة.

يتبين لنا من المادة 15 أعلاه أنها تضمنت بشكل ضمني الاستفادة من التكنولوجيات الحديثة بما فيها الأنترنت، لكنها لم تنص عليها صراحة، أما المادة 19 المبينة أعلاه صيغت بطريقة تتماشى مع التطورات التكنولوجية المستقبلية بما فيها الأنترنت[13].

كما أقرت الجمعية العامة للأمم المتحدة بموجب القرار رقم 198/68[14] بأن الأنترنت عنصر أساسي في بنية مجتمع المعلومات ومرفق عالمي في متناول الجميع، ضف إلى أن مجلس حقوق الإنسان دعى في القرار رقم 8/20[15] جميع الدول إلى تعزيز وتيسير الوصول إلى الأنترنت والتعاون الدولي الرامي إلى تطوير وسائط الإعلام ومرافق المعلومات والاتصالات في جميع البلدان، وفي هذا الشأن أشار المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير "فرانك لا رو": "أنه ينبغي أن يكون تيسير حصول جميع الأفراد على خدمة الأنترنت أولوية بالنسبة لجميع الدول، مع فرض أقل قدر ممكن من القيود على الوصول إلى محتوياته"[16].

ولقد دعت الغاية8/و من الأهداف الإنمائية للألفية الدول إلى إتاحة فوائد التكنولوجيا الجديدة بالتعاون مع القطاع الخاص، وتم التأكيد على ضرورة تحقيق هذه الغاية في خطة العمل لعام 2003 التي اعتمدت أثناء مؤتمر القمة العالمي لمجتمع المعلومات المنعقد في جنيف، والتي حددت الأهداف والغايات من أجل بناء مجتمع معلومات يشمل الجميع[17].

بالإضافة إلى هذه النصوص الدولية المكرسة للحق في الولوج إلى الأنترنت، فقد أعلنت الحكومات والشركات ومنظمات المجتمع المدني في القمة العالمية الأولى لمجتمع المعلومات عام 2003 عن رغبتهم والتزامهم المشتركين ببناء مجتمع معلومات مركز وشامل وموجه نحو التنمية، بحيث يمكن للجميع إنشاء المعلومات والمعرفة والوصول إليها واستخدامها وتبادلها وتمكين الأفراد والمجتمعات والشعوب من تحقيق إمكاناتهم الكاملة في تعزيز تنميتهم المستدامة وتحسين نوعية حياتهم ويشكل هذا أثرا حاسما للتأكيد على أهمية الصلة بين الأنترنت وحقوق الإنسان[18].

2/-تكريس الحق في الولوج إلى الأنترنت في التشريعات والقضاء الوطنيين:

أقرت عدد من الدول في تشريعاتها أو بموجب قرارات قضائية الحق في الوصول إلى الأنترنت فعلى سبيل المثال نص قانون الاتصالات الإستوني لعام 2000على الحق في الوصول إلى الأنترنت ونص الدستور اليوناني لعام 2001 في المادة 5أ منه على أن :" لجميع الأفراد حق المشاركة في مجتمع المعلومات، والدولة ملزمة بتسهيل الوصول إلى المعلومات إلكترونيا، فضلا عن إنتاجها وتبادلها ونشرها...."، كما أن فلندا أقرت الحق الأساسي للوصول إلى النطاق الواسع سنة 2010 بعد تعديل قانون سوق الاتصالات، أما اسبانيا فقامت في 2011 بضمان الوصول إلى النطاق الواسع إلى الخدمة الشاملة للإنترنت بموجب القانون المتعلق بالاقتصاد المستدام[19].

كما أصدرت أحد المحاكم البريطانية قرار بعدم حجب الأنترنت كلية على الأفراد لاستحالته أولا ولأهمية الوصول إلى الأنترنت الحيوية، التي أصبحت تغذي كل مجالات الحياة تقريبا، وهو نفس الاتجاه الذي ظهر في استطلاع الرأي العالمي الذي أجرته BBC في 2010في أكثر من 26 دولة الذي كانت نتيجته أن أكثر من 80 ٪يرون الأنترنت أحد الحقوق الإنسانية الأساسية[20].

وبالرجوع إلى التشريعات الجزائرية انطلاقا من التعديل الدستوري لسنة 2020 نجد أن المادة 55 منه لم تشر إلى الحق في الولوج إلى الأنترنت، بحيث نصت فقط على حق كل مواطن في الوصول إلى المعلومات والوثائق والإحصائيات دون أن تحدد وسائل الوصول إلها، كما أن المرسوم التنفيذي رقم2000-307المؤرخ في 2000/10/14المعدل للمرسوم التنفيذي رقم 98-257 لم ينص على الحق في الولوج إلى الأنترنت، نفس الشيء بالنسبة للقانون رقم 18-04[21]، لم ينص على الحق في الولوج إلى الأنترنت، وإنما نص في المادة 1 منه على تقديم خدمات البريد والاتصالات الإلكترونية دون تمييز .

المبحث الثاني: التحديات التي تواجه التمتع بالحق في الولوج إلى الأنترنت

لقد أشرنا سابقا إلى أن المقرر الخاص إن تأمين الحق في الوصول إلى الانترنت يتطلب أمران وهما: الوصول إلى محتويات الأنترنت دون أي قيد إلا في حالات استثنائية، وتوفير الهياكل الأساسية وتكنولوجيات الاتصال والمعلومات الضرورية للولوج للأنترنت، وهذا ما أكده المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير [22]، وعليه يمكن تقسيم أهم التحديات التي تواجه التمتع بالحق في الولوج إلى الأنترنت إلى قسمين، الأول يتعلق بالفجوة الرقمية، والثاني يتعلق بقطع الأنترنت، وهذا ما ستناوله بالتفصيل في المطلبين التاليين:

المطلب الأول: الفجوة الرقمية

سنتناول في هذا المطلب تعريف الفجوة الرقمية، ونوضح كيف بإمكان الفجوة الرقمية أن تحد من الوصول إلى الأنترنت،

الفرع الأول: تعريف الفجوة الرقمية

الفجوة الرقمية مصطلح مركب من كلمتين، الأولى يفصد بها الفرق التقني في الوسائل والثانية تقنية سريعة تنقل المعلومات بسرعة وبكميات ضخمة جدا وغير محددة، كما يرى البعض أن الفجوة الرقمية هي الفجوة الني خلفتها ثورة المعلومات والاتصالات بين الدول المتقدمة والنامية.

وجاء في تقرير الاستراتيجية العربي تعريف للفجوة التقنية بأنها:"المسافة بين حالة إنتشار استخدام الشبكة العنكبوتية في الدول المتقدمة[23].

يقصد بالفجوة الرقمية، أو الهوة الرقمية، الثغرة التي تفصل بين الأشخاص الذين تتوفر لديهم إمكانية الحصول فعلا على التكنولوجيات الرقمية وتكنولوجيات المعلومات، خاصة الأنترنت، وبين أولئك الذين لا يحصلون عليها إلا بدرجة محدودة جدا أو لا يحصلون عليها بتاتا[24].

الفرع الثاني: الفجوة الرقمية كعائق للوصول إلى الأنترنت

بينت الإحصائيات أن مستخدمي الأنترنت في الدول المتقدمة لا يتجاوز 71,6 مستخدم أنترنت لكل 100 نسمة من السكان، في حين يزداد هذا الفرق في المنطقة الإفريقية، بحيث لا يتعدى عدد المستخدمين 9,6 مستخدم لكل 100 نسمة[25]، و3,5 مليون نسمة يستخدمون الأنترنت في الوطن العربي من أصل 275 مليون نسمة في العالم[26]

كما تتفاوت الفجوة الرقمية حسب درجة الغنى أو نوع الجنس أو المنطقة الجغرافية أو الطيقة الاجتماعية داخل نفس الدولة، بحيث غالبا ما يكون الحصول على خدمة الأنترنت متاحا لدى نخب اجتماعية واقتصادية، خاصة في البلدان التي تنخفض فيها نسبة نفاذ الأنترنت، وعليه فإن التفاوت في الوصول إلى الأنترنت يكون لا يقتصر داخل الدول، إنما يكون أيضا بين الدول ضف إلى أن سكان الأرياف لا يتمتعون بخدمة الأنترنت بالشكل الكافي لعدة أسباب كقلة توفر التكنولوجيا، أو بطء الاتصال بالأنترنت أو ارتفاع التكاليف[27].

كما أن هناك فئات من الأشخاص تحرم من الحق في الوصول إلى الأنترنت، حتى وإن كان الاتصال بهذه الأخيرة متسيرا، كالأشخاص ذوي الإعاقة، والأشخاص المنتمين إلى الأقليات[28].

ضف إلى أن النظام الدولي الجديد يعمل على زيادة قوة الدول المتقدمة وإضعاف الدول النامية، مما يؤدي إلى تحويل الفجوة التقنية والمعلوماتية إلى فجوة اقتصادية لها إنعكاساتها السلبية على إقتصادات الدول النامية، وعدم تحول اقتصادات هذه الأخيرة إلى الاقتصاد الرقمي

سيؤدي إلى تقزيم اقتصاداتها مقارنة بالاقتصادات المتقدمة، بالإضافة إلى عدم التبني الجاد للدول النامية للمشاريع المدعمة للرقمنة كالحكومة الإلكترونية، التجارة الإلكترونية، الصيرفة الإلكترونية نتيجة الفقر الاقتصادي والمعلوماتي[29].

وسعيا من الدول إلى ضمان الوصول إلى الأنترنت، قامت بمجهودات من أجل كسر هذه الفجوة الرقمية التي تحول دون تمتع الأشخاص بهذا الحق، ومن بين أهم هذه الجهود إطلاق مشروع ربط العالم في عام 2005 من طرف الاتحاد الدولي للاتصالات، بالإضافة إلى مشروع 'حاسوب محمول لكل طفل ' في البلدان النامية المدعم من طرف برنامج الأمم المتحدة الإنمائي بحيث يوزع هذا المشروع حواسيب محمولة بسعر زهيد والتي تكون مهيأة لتيسير تعلم الأطفال وبناءا عليه وزع سنة 2006، 2400000 حاسوب محمول على الأطفال والمدرسين في جميع أنحاء العالم وأستفاد من المشروع في أوروغواي 480000طفل ، ووزع في رواندا نحو 56000 حاسوب محمول، بالإضافة الى الجهود الوطنية للتصدي للفجوة الرقمية، فعلى سبيل المثال أنشأت الحكومة الهندية مراكز الخدمة العامة أو ما يسمى ب"الأكشاك الإلكترونية" العامة بالتعاون مع القطاع الخاص في إطار الخطة الوطنية للإدارة الإلكترونية لعام 2006، كما أطلقت الحكومة البرازيلية برنامج"الحواسيب للجميع "، الذي يقدم معونات مالية لشراء حواسيب، وأنشئ أكثر من 100000مركز للتزويد بخدمة الأنترنت، تعرف باسم "دور شبكة المنطقة المحلية"[30].

ولقد سعت الأمم المتحدة إلى تضيق الفجوة الرقمية بين دول العالم، بحيث قدرت حاجة الدول النامية لتضييق هذه الفجوة سنة 2004 ب 2مليار دولار ، وتعهدت من أجل ذلك بإقراض 500دولار ، كما أطلق البنك الدولي برنامجا عالميا في الأنترنت هو InfoDEV كوسيط إلكتروني مباشر بحيث يقوم البنك من خلاله بتوفير خبرات ودراسات من مصادر عالمية، ويقوم بدعم مجموعة من الأنشطة المحلية والإقليمية والمشاريع المشتركة في مجال الأنترنت ومحو الأمية الرقمية في الدول النامية، وفي 2005 صدرت توصية في قمة تونس للمعلوماتية بإنشاء صندوق التضامن الرقمي لبناء مجتمع المعلومات في الدول النامية للدعم الفني والمالي لتضييق الفجوة الاقتصادية[31]

المطلب الثاني: قطع الأنترنت أو تقييدها

غالبا ما تلجأ الدول إلى قطع الأنترنت نهائيا كوسيلة لتقييد حرية الرأي، أو للرقابة، كما تلجأ في أحيانا أخرى إلى تقييدها من خلال تقييد المحتوى على شبكة الأنترنت، وهذا ما سنفص فيه فيما يلي:

أولا/-تقييد المحتوى على شبكة الأنترنت:

تتعدد أسباب وطرق تقييد المحتوى على شبكة أنترنت، هذا مل سنوضحه فيما يلي:

1/-أسباب تقييد المحتوى على شبكة الأنترنت:

تقوم معظم الدول بالعمل على منع أو الحد من الوصول إلى محتوى ما على الأنترنت بحجة تأمين حقوق الملكية الفكرية، وحماية الأمن القومي، والحفاظ على المعايير الثقافية والقيم الدينية، وحماية الأطفال من المواد الإباحية والاستغلال الجنسي، وغيرها من الحجج التي تلجأ الحكومات إلى استخدامها في بعض الأحيان من أجل تقييد حرية المعارضين من الأفراد أو الجماعات في التعبير عبر الأنترنت[32].

2/-طرق تقييد المحتوى عبر الأنترنت:

تتعدد طرق تقييد المحتوى عبر الأنترنت، نبين أهمها فيما يلي:

أ/-الحجب التقني:

الحجب هو التدابير التي تتخذ لمنع محتويات معينة من الوصول إلى المستخدم النهائي[33]، وهناك ثلاث تقنيات عادة ما تستخدم لحجب الوصول إلى مواقع الأنترنت والمتمثلة في : حجب بروتوكول الأنترنت IP، التلاعب بخوادم إسم النطاق DNS، الحجب باستخدام وسيط Proxy، بحيث تستخدم هذه التقنيات لحجب الوصول إلى صفحات إلكترونية معينة، أو نطاقات، أو عنوان لبروتوكولات الأنترنت، وغالبا ما تستخدم هذه الطرق من طرف السلطة القضائية[34].

كما قد تلجأ الحكومات إلى الحجب المحدد التوقيت لمنع المستخدمين من الوصول إلى المعلومات أو نشرها في أوقات سياسية هامة كالانتخابات وفترات الاضطراب الاجتماعي أو إحياء ذكرى أحداث هامة، والتي يتم خلالها حجب مواقع أحزاب المعارضة ووسائط الإعلام المستقلة ومنتديات التشبيك الاجتماعي كالتويتر والفيسبوك[35].

ب/-إزالة نتائج البحث:

تكون من خلال قيام الشركات التي توفر خدمات البحث على الأنترنت بالتعاون مع الحكومات بناءا على قوانين وضعتها هذه الأخيرة بشأن تنظيم الأنترنت، من أجل قيام هذه الشركات بحذف المواقع غير القانونية أو غير مرغوب فيها من نتائج البحث[36].

ج/-جعل المحتوى غير مرئي:

يكون ذلك في حالة ما إذا طلب منظمي الأنترنت من مضيفي محتوى الأنترنت بحذف المواقع الإلكترونية ذات المحتوى غير اللائق أو غير القانوني، فيقومون بإزالته وجعله غير مرئي[37].

د/-الحث على الرقابة الذاتية:

وهي طريقة فعالة لتقييد المحتوى، تتم من عن طريق التحكم في عادات التصفح أو في اختيار المحتوى الذي يتم نشره على شبكة الأنترنت[38].

ثانيا/-قطع الأنترنت:

إذا كانت تدابير الحجب تمنع الوصول إلى محتويات معينة على الأنترنت، فقد تلجأ الدول إلى تدابير لقطع الاإتصال بالأنترنت تماما، وقد درات نقاشات حول وضع وسيلة مركزية للتحكم في تصفح الأنترنت "بكبسة زر"، بالإضافة إلى الاقتراحات الموضوعة بشأن قطع اتصال المستخدمين بالأنترنت في حالة انتهاكهم حقوق الملكية الفكرية، ومن بين تلك الاقتراحات وجود تشريع يستند إلى مفهوم "الرد المتدرج" الذي يفرض سلسلة من العقوبات على منتهكي حقوق الطبع قد تؤدي إلى تعليق خدمة الأنترنت،من قبيل الإجراء المسمى"قانون الضربات الثلاث في فرنسا، وقانون الاقتصاد الرقمي في المملكة المتحدة عام 2010[39].

خاتمة:

أضحت الأنترنت أداة ضرورية لا غنى عنها في إعمال حقوق الإنسان ومكافحة عدم المساواة وتسريع التنمية والتقدم الإنساني، ورغم هذه الأهمية التي تكتسيها، ورغم تكريسه ضمنيا في المواثيق الدولية المتعلقة بحقوق الإنسان، ونص بعض صراحة في تشريعاتها على ضرورة توفيره للجميع باعتباره حق من حقوق الإنسان، إلا أن هناك العديد من التحديات توفير الحق في الحصول على الأنترنت، وعليه خلصنا من خلال هذه المداخلة إلى أهم الاستنتاجات:

1/-الحق في الوصول إلى الأنترنت حق إنساني فرضته الحياة المعاصرة.

2/-صعوبة ضمان الحق في الوصول إلى الأنترنت للجميع في الوقت الحالي، تحقيقه يتماشى مع تضييق الفجوة الرقمية.

كما نقترح أهم التوصيات التالية:

1/-السعي إلى ضمان الحق في الوصول إلى الأنترنت للجميع.

2/-ضرورة التعاون الدولي من أجل تضييق الفجوة الرقمية.

3/-الحد من حالات قطع الأنترنت وتقييدها، مع ضرورة اللجوء إليها في حالات استثنائية ينص عليها القانون.

الهوامش:

[1] زخمي الطاهر ، اثر تطور وسائل الاعلام على حقوق الإنسان، ص7 ، متوفر على الموقع الالكتروني:-http://dspace.univ-ouargala.dz/jspui/handale/123456789/14202، 2017/06/15، تاريخ الاطلاع2022/06/20.

[2] الشريف سارة ، حق النفاذ الحر إلى الأنترنت-دراسة مقارن_مركز دعم لتقنية المعلومات، القاهرة،2015،ص7.

3فرانك لا رو، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، 2011/05/16، ص ص7،A/HRC/17/27.8 .

4بن عزة حمزة محمد، المسؤولية القانونية لمتعاملي الأنترنت: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، 2018،ص24.,

sمركز هردو لدعم التعبير الرقمي، الأنترنت1989، القاهرة، 2016،ص4.

6محمد حمزة بن عزة، مرجع سابق، ص ص27،28.

[7] المرسوم التنفيذي رقم98-257المؤرخ في 25غشت 1998 والمتعلق بضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها المعدل بموجب المرسوم التنفيذي رقم2000-307المؤرخ في 2000/10/14، ج ررقم 63 المؤرخة في 1998/08/23.

[8] ا القانون 18-04المؤرخ في 2018/05/10 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر رقم 27 المؤرخة في 2018/05/13.

[9] فينت كيرف،حق النفاذ الحر إلى الأنترنت، دراسة مقارنة،بمركز دعم لتقنية المعلومات القاهرة، 2015ص19.

[10] فرانك لا رو، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، 2011/05/16، ص ص4،A/HRC/17/27.5 .

[11] وفي هذا الشأن يقول "نيث دانو' مدير آسيا لمجموعة عمل ETC المعنية بالتكنولوجيا:"إن الحقوق والخدمات الأساسية التي يجب أن يحصل عليها الناس أكثر أهمية من الأنترنت، كما يتساءل عن إمكانية الشعوب البدائية في المناطق النائية الذين ليس لديهم حتى إمكانية الحصول على الكهرباء إعطاء الأولوية للوصول إلى الأنترنت، على الصحة والتعليم والغذاء؟، ويضيف قائلا أنه إذا تم الاعتراف بالوصول على الأنترنت كحق من حقوق الإنسان، فإن على الحكومات أن تضمن الوصول إلى الأنترنت قبل أن تتمكن من تغطية احتياجات الحياة الأساسية، ولا يمكن توفير الأنترنت من طرف الحكومات فبل الكهرباء أو الطعام أو التعليم"، أنظر لورا فردياجو، الإنترنت حق من حقوق الإنسان، جسور بوست، متواجد علة الموقع الالكتروني:lwww.jusoorpost.com/postsL1993، تاريخ الإطلاع2022/06/25,

[12] لورا فردياجو، الإنترنت حق من حقوق الإنسان، جسور بوست، متواجد على الموقع الالكتروني:www.jusoorpost.com/postsL1993تاريخ الإطلاع2022/06/25..

[13] فرانك لا رو، مرجع سابق، ص8..

[14] الجمعية العامة قرار رقم 198/68 المؤرخ في 2013/12/20، ص6،A/RES/68/198

[15] مجلس حقوق الإنسان، قرار رقم 8/20 المؤرخ في 2012/07/5،A/HRC/RES/20/8

[16] فرانك لا رو، مرجع سابق ص4.

17نفس المرجع، ص23.

[18] غانية بن كرويدم، مرجع سابق،ص ص2044،2043.

[19] فينت كيرف، مرجع سابق،ص ص21،22، 23..

[20] نفس المرجع، ص 22..

[21] القانون رقم 18-04المؤرخ في 2018/05/10 المحدد للقواعد العامة المتعلقة بالبريد والإتصالات الإلكترونية،جريدة رسمية رقم27.

[22] فرانك لا رو، مرجع سابق، ص ص4،5..

[23] النجار إخلاص ياقر، حسين مصطفى مهدي، فياس وتحليل الفجوة الرقمية في الوطن العربي، مجلة العلوم الاقتصادية، المجلد 6 العدد26، ص191.

[24] فرانك لا رو،مرجع سابق ص 22،

[25] نفس المرجع ص22..

[26] النجار إخلاص ياقر، مرجع سابق، ص193.

[27] فرانك لا رو،مرجع سابق، ص 22.

[28] نفس المرجع، ص 22.

[29] النجار إخلاص ياقر، مرجع سابق، ص195.

[30] فرانك لا رو،مرجع سابق، ص ص 23،24،

[31] النجار إخلاص ياقر، مرجع سابق، ص197.

[32] نفس المرجع، ص30.

[33] فرانك لا رو،مرجع سابق، ص11.

[34] فينت كيرف، مرجع سابق،ص 31.

[35] فرانك لا رو،مرجع سابق، ص12.

[36] فينت كيرف، مرجع سابق، ص 22.

[37] نفس المرجع، ص 31.

[38] نفس المرجع، ص 31.

[39] فرانك لا رو،مرجع سابق، ص18.

قائمة المراجع:

أ/-الكتب:

1/-الشريف سارة ، حق النفاذ الحر إلى الأنترنت-دراسة مقارن_مركز دعم لتقنية المعلومات، القاهرة،2015.

2/-فينت كيرف،حق النفاذ الحر إلى الأنترنت، دراسة مقارنة،بمركز دعم لتقنية المعلومات القاهرة، 2015ص19.

3/-مركز هردو لدعم التعبير الرقمي، الأنترنت1989، القاهرة، 2016.

ب/-الرسائل الجامعية:

1/-بن عزة حمزة محمد، المسؤولية القانونية لمتعاملي الأنترنت: دراسة مقارنة، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي ليابس، سيدي بلعباس، 2018.

ج/-تقاريروقرارات دولية:

ج1/-تقارير دولية:

فرانك لا رو، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، A/HRC/17/27.8،7 ص ص، 2011/05/16

ج2/-قرارات دولية:

1/-قرار رقم 8/20 المؤرخ في A/HRC/RES/20/8،2012/07/5

2/-قرار رقم 198/68 المؤرخ في A/RES/68/198، 2013/12/20

د/-التشريعات الوطنية:

1/- المرسوم التنفيذي رقم98-257المؤرخ في 25غشت 1998 والمتعلق بضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها المعدل بموجب المرسوم التنفيذي رقم2000-307المؤرخ في 2000/10/14، ج ر رقم 63 المؤرخة في 1998/08/23.

2/-القانون 18-04المؤرخ في 2018/05/10 المحدد للقواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر رقم 27 المؤرخة في 2018/05/13.

ن/-مراجع إلكترونية:

1/-زخمي الطاهر ، اثر تطور وسائل الاعلام على حقوق الإنسان، متوفر على الموقع الالكتروني:http://dspace.univ-ouargala.dz/jspui/handale/123456789/14202، 2017/06/15، تاريخ الاطلاع2022/06/20.

استمارة المشاركة

المشارك الأول

الاسم و اللقب : بن عوفية قادة

الرتبة العلمية : طالب دكتوراه (سنة رابعة)

التخصص: قانون إداري متخصص

الهيئة المستخدمة : مخبر المرافق العمومية و التنمية، كلية الحقوق و العلوم السياسية 19 مارس 1962- جامعة جيلالي ليابس – سيدي بلعباس .

الهاتف: 0672689504

البريد الإلكتروني:kada.benaoufia@univ-sba.dz

المحور المختار: دور التكنولوجيات الرقمية في إعمال و تعزيز حقوق الإنسان (المحور الثاني)

عنوان المداخلة: استعمال وسائل الاتصال الحديثة في في الحصول على المعلومة .

المشارك الثاني

الاسم و اللقب: دويني مختار

الرتبة العلمية: دكتور – أستاذ محاضر – قسم أ-

الهيئة المستخدمة: كلية الحقوق والعلوم السياسية، جامعة سعيدة

البريد الإلكتروني : mokhtar.douini@univ-saida.dz

رقم الهاتف: 0664075733

مقدمة:

يعد الحق في الحصول على المعلومة حقا شموليا يخترق باقي حقوق الإنسان المختلفة والمتعددة، ذلك أن التمتع به يعزز إمكانية اكتساب حقوق الإنسان الأخرى كحرية التعبير والإعلام والرأي.

فالتركيز على حقوق الإنسان في العصر الرقمي أساسي. فجمع البيانات يجري في الواقع على نطاق واسع عبر مختلف وسائل الاتصال الحديثة، بسبب تقدّم التكنولوجيا الرقمية التي في الواقع لها العديد من الفوائد، فقيمتها بالنسبة إلى حقوق الإنسان والتنمية لا تُقدّر بثمن، فهي تمكّننا من التواصل والترابط مع الناس و المرافق العامة في جميع أنحاء العالم بشكل غير مسبوق، و بالمقابل يتم رصد العديد من جوانب حياتنا الخاصة و الاطلاع عليها وتخزينها وإساءة استخدامها رقميًا.

لذا فقد أولى المشرع الجزائري أهمية بالغة للحق في الحصول على المعلومة بتنظيمه بموجب العديد من النصوص القانونية، وعزز ذلك بتكريسه بموجب التعديل الدستوري لسنة 2020 و في نصوص أخرى تشريعية منها و تنظيمية، ليمنحه بذلك قدسية منيعة ويضفي عليه الحماية الدستورية.

نسعى من خلال هذه الدراسة إلى تسليط الضوء على أهمية وسائل الاتصال الحديثة لتكريس الحق في الحصول على المعلومة ، وذلك بالتساؤل حول الحق في الحصول على المعلومة رقميا؟

من خلال هذه الاعتبارات و أخرى مرتبطة بالموضوع، ولبلوغ الهدف من هذه الدراسة فقد قسمنا العمل إلى اربعة محاور، تناولنا في المحور الأول التعريف بوسائل الاتصال الحديثة أما المحور الثاني فقد خصصناه في الحق للحصول على المعلومة وفق القانون الجزائري و القانون الدولي، و المحور الثالث تناولنا فيه العلاقة بين الإدارة و المواطن في مجال الحصول على المعلومة و أخيرا المحور الرابع أبرزنا فيه أهمية الحق في الحصول على المعلومة للإجابة عن الإشكالية اتبعنا المنهجين الذين يتوافقان مع طبيعة الموضوع وهما: المنهج الوصفي الذي يتجلى في تحديد مفهوم الحق في الحصول على المعلومة و مجالاتها

و التعريف بوسائل الاتصال الحديثة ، أمّا التحليلي فيظهر من خلال تحليل النصوص القانونية المستحدثة في نفس المغزى.

المحور الأول : وسائل الاتصال الحديثة

شهد العالم خلال الفترة الأخيرة اتساعاً كبيراً في الكثير من المجالات، حيث أصبح العالم أكثر تطوراً، حيث أصبح التواصل بين الناس في كافة أنحاء العالم، عبر وسائل التواصل الاجتماعي بكل سهولة.

كذلك الفرد لم يكن وحده هو المستفاد من وسائل الاتصال الحديثة، بل المجتمع أيضاً مستفاد لأنه يمكن استخدام وسائل الاتصال الحديثة، في العديد من الأعمال في المجتمع.

تعريف وسائل الاتصال الحديثة ومخاطرها

تعد وسائل الاتصال الحديثة، هي الوسائل التي من خلالها يتمكن الإنسان للتواصل مع العالم بأكمله، حيث أصبحت من أهم الضروريات التي لا يمكن العيش بدونها أو التخلي عنها، كما إن هذه الوسائل سهلة على الإنسان الحياة، لأنها تقرب بين المسافات و تعريف وسائل الاتصال الحديثة.

و تعرف الوسائل الاتصال الحديثة على أنها تلك الطرق و الوسائل التي يمكن من خلالها إيصال الأفكار و الآراء و المعلومات إلى جمهور عريض من الأشخاص في أماكن بعيدة و متفرقة، لا رابط مكاني بينهم في الغالب من خلال شبكة واسعة من الأنظمة و التقنيات المتعددة و المتنوعة و المتطورة منها على سبيل المثال الانترنت و البث و النشر التي تؤدي دورا مهما في ربط الجماهير بعضهم ببعض الآخر عبر إرجاء العالم[1]

المحور الثاني : الحق في الحصول على المعلومة

اعتبر الحق في الوصول إلى المعلومة العامة أمر أساسي لسير الديمقراطية في المجتمعات ورفاه كل فرد. وهو حق من الإعلان العالمي لحقوق الإنسان[2]، مكرس في المادة

---

[1] أحمد عبد العزيز الشيخ، الحماية القانونية لمشترك تكنولوجيا الاتصالات، دار الجامعة الجديدة، الإسكندرية، مصر ، 2022، ص28

[2] الإعلان العالمي لحقوق الإنسان المؤرخ في 1948/12/10.

19 يساعد على تعزيز المشاركة المواطنة وممارسة الحقوق الاجتماعية والاقتصادية والسياسية، الأمر الذي يعزز التنمية والأداء الاقتصاديين ويجعل من السلطات الوطنية محاسبة عن أعمالها وعن إدارتها المالية العامة. إن الحق في الحصول على المعلومة أمر حتمي أيضا بالنسبة للأفراد والمجتمعات ومؤسسات المجتمع المدني في سعيها لدى الحكومات لتحسين الخدمات العامة.،

يعد الحق في الإطلاع على المعلومات أو الحصول عليها أو الولوج إليها من أكثر الحقوق أهمية في العقود الأخيرة باعتباره حجر الزاوية للعديد من الحقوق الأخرى كحرية التعبير والإعلام والرأي، ومن الوسائل التي تضمن وتكفل للمواطن الديمقراطية التشاركية، لذا فقد أولى له المشرع الجزائري أهمية بالغة بتنظيمه بموجب العديد من النصوص منها، المادة 55 من التعديل الدستوري لسنة 2020 [32] ، حيث جاء فيها :" يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والإحصائيات، والحصول عليها وتداولها".

لا يمكن أن تمس ممارسة هذا الحق بالحياة الخاصة للغير وبحقوقهم، وبالمصالح المشروعة للمؤسسات، وبمقتضيات الأمن الوطني.

ركز المشرع على تحسين مستوى التمكين من الحصول على المعلومات العمومية من خلال التوعية والتثقيف ودعم استخدام الوسائط العالمية الجديدة والتكنولوجيا من أجل نشر المعلومات العمومية وتداولها، خاصة في مجال مكافحة الفساد كونها أداة قوية للتمكين من وضع المسئولين موضع المساءلة. عندما يتسنى الحصول عليها بشكل حر، . الحصول على المعلومات أمر ضروري لا غنى عنه لأنه يعزز الشفافية ويمهد الطريق للمساءلة في المجتمع بأسره ..

---

[3] **دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996** ، المنشور بموجب المرسوم الرئاسي رقم 96-438 مؤرخ في 1996/12/07 ،ج ر ج ج ، العدد 76 المؤرخ في 08 ديسمبر 1996 ، معدل و متمم بالقانون رقم 02-03 مؤرخ في 2002/04/10، ج ر ج ج ، العدد 25 المؤرخ في 14 افريل 2002 ، و القانون رقم 08-19مؤرخ في 2008/11/15، ج ر ج ج ، العدد 63 المؤرخ في 16 نوفمبر 2008، و القانون رقم 16-01 مؤرخ في 06 مارس 2016، ج ر ج ج ، العدد 14 المؤرخ في 07 مارس 2016، و المرسوم الرئاسي رقم 20-442 مؤرخ في 30 ديسمبر لسنة 2020، يتعلق بإصدار التعديل الدستوري، مصادق عليه في استفتاء أول نوفمبر سنة 2020، ج ر ج ج ، العدد 82 المؤرخ في 30 ديسمبر 2020

و تجدر الملاحظة أن قانون الولاية رقم 12-07[4] جاء فيه أن مداولات المجلس الشعبي ألولائي يجب أن تكون في جلسات علنية مع إلزامية إلصاق جدول أعمال المجلس الشعبي ألولائي فور استدعاءه عند مدخل قاعة المداولات و في أماكن الإلصاق المخصصة للجمهور و في الموقع الالكتروني للولاية أو المجلس و في مقر الولاية و البلديات التابعة لها.

و عملا بأحكام المادة 11 من القانون رقم 11-10 المتعلق بالبلدية جاء فيها:" ضرورة اتخاذ المجلس الشعبي البلدي كل التدابير لإعلام المواطنين بشؤونهم باستعمال الوسائط الإعلامية المتاحة "[5].

و في هذا الإطار، يمكن للمواطن الاطلاع و نسخ مستخرجات مداولات المجلس الشعبي البلدي و كذا القرارات البلدية استنادا إلى المادة 14 من نفس القانون و يظهر جليا من قانون البلدية على أن تكون الجلسات العلنية، و على إلزامية لصق جدول أعمال دورة المجلس الشعبي البلدي في قاعة الاجتماعات وفي أماكن المخصصة للجمهور، و تم تنظيمها بموجب المرسوم تنفيذي رقم 16-190 يحدد كيفيات الإطلاع على مستخرجات مداولات المجلس[6].

على ضوء المرسوم رقم 88-131 المنظم للعلاقة بين الإدارة و المواطن، جاء في المادة 08 منه، على ضرورة قيام الإدارة بإطلاع المواطنين بالتنظيمات و التدابير التي تقوم بها وذلك باستعمال الأسانيد المناسبة للنشر و الإعلام، و أضافت المادة 09 من نفس

---

[4] القانون رقم 12-07 المؤرخ في 21 فبراير 2012 ، يتعلق بالولاية، ج ر، ج ج ، ع 12، الصادر في 29 فبراير 2012 .

[5] القانون رقم 11-10 المؤرخ في 22 يونيو 2011، يتعلق بالبلدية، ج ر، ج ج ، ع37،الصادر في 03 يوليو 2011 .

[6] المرسوم التنفيذي رقم 16-190 مؤرخ في 30 يونيو 2016، يحدد كيفيات الاطلاع على مستخرجات مداولات المجلس الشعبي البلدي و القرارات البلدية، ج ر ، ج ج ، ع 41، الصادر في 12 يوليو 2016

المرسوم على التزام الإدارة نشر بانتظام للتعليمات و المناشير المذكرات و الآراء التي تهم المواطن، ناهيك على المادة 09 من القرار المؤرخ في 04سبتمبر1988[7].

فمن خلال المرسوم التنفيذي رقم 13-381[8] المحدد لصلاحيات الوزير لدى الوزير الأول المكلف بإصلاح الخدمة العمومية، في المادة 02 فقرة 09 منه نص على تولي الوزير المنتدب التشجيع على تطوير الإدارة الالكترونية بإدخال التكنولوجيات الحديثة للإعلام والاتصال و تعميمها، مما يشكل مكسبا من مكاسب مبدأ الشفافية، و يجعل الشفافية عنصرا بارزا لإصلاح الإداري .و نذكر انه صدرت تعليمة عن الوزير المكلف بإصلاح الخدمة العمومية بتاريخ 11 نوفمبر 2013 تخص تطبيق تدابير إصلاح الخدمة العمومية، إذ تشكل التدابير الاستعجالية و المشتركة بين جميع القطاعات بالنسبة للمواطن إشارات قوية لإرادة الحكومة لتحديث المرفق العمومي و التغيير النوعي في كيفيات تنظيمه و سيره، وأكدت التعليمة على انه تتمحور التدابير حول عمليات استراتيجية رئيسيه منها على وجه الخصوص، في مجال تبسيط الإجراءات الإدارية منها على الخصوص، نشر بطريقة واضحة و مفهومة قائمة الوثائق المكونة للملفات المطلوبة لكل إجراء أو خدمة عمومية، و توفير الوسائل العصرية للاتصال و الإعلام و توجيه المواطنين (الهاتف الأخضر ،الموقع الالكتروني ،البريد الالكتروني ....) قصد تجنيبهم تنقلات غبر المجدية و العراقيل التي لا طائل منها .

---

[7] انظر المادة 09 من المرسوم رقم 88-131 مؤرخ في 4 يوليو 1988 ينظم العلاقة بين الإدارة و المواطن، ج ر، ج ج ، ع 27 الصادر في 06 يوليو 1988 تنص على انه : " يتعين على الإدارة أن تنشر بانتظام التعليمات و المناشير و المذكرات و الآراء التي تهم علاقتها بالمواطنين إلا إذا وردت أحكام مخافة في التنظيم الجاري به العمل..."".

و أيضا محتوى المادة 09 من القرار المؤرخ في 04 سبتمبر 1988 يحدد شروط استقبال المواطنين في مصالح الولايات و البلديات و توجيههم و إعلامهم، ج ر،ج ج ،ع 39، الصادر في 28 سبتمبر 1988 حيث جاء فيها: " يضبط الولاة و رؤساء المجالس الشعبية كل إجراء يرمي تحسين إعلام الجمهور...".

[8] المرسوم التنفيذي رقم 13-381 المؤرخ في 19 نوفمبر 2013 ، يحدد صلاحيات الوزير لدى الوزير الأول المكلف بإصلاح الخدمة العمومية ، ج ر،ج ج ،ع 59 الصادر في 20 نوفمبر 2013.

إن المرسوم الرئاسي 15-247 [9] المتضمن تنظيم الصفقات العمومية و تفويضات المرفق العام نص في المادة 05 منه على مبادئ الصفقات العمومية منها المساواة في معاملة المرشحين و شفافية الإجراءات

و تظهر جليا صور مبدأ الشفافية في الصفقات العمومية بداية من إلزامية إشهار الصحفي لإعلان طلب العروض حتى يتسنى للجميع من سحب الدفتر الشروط، بالإضافة إلى تمكين المتعهدين من حضور عملية فتح الاظرفة، و هدف من إعلان الإشهار الصحفي و الحضور عملية فتح الاظرفة هو ضمان اكبر قدر من شفافية.

أما بالنسبة لأهمية مبدأ الشفافية في الصفقات العمومية فله أهمية بالغة في الحفاظ على المال العام ومكافحة الفساد في قطاع الصفقات العمومية باعتباره أكثر القطاعات العامة إنفاقا للمال العام، لهذا فهو أكثر المجالات استقطابا للفساد المالي والإداري[10]. غير أن وضوح وعلانية إجراءات ومراحل عقد الصفقة العمومية يحقق الغاية المرجوة وهي الحفاظ على المال العام وإنفاقه في ما يحقق المصلحة العامة [11] هذا و تكمن أهمية مبدأ الشفافية ايضا في علاقته بالمبادئ الأخرى للصفقات العمومية.

فمبدأ حرية المنافسة لا يتحقق إلا بتوفير أكبر قدر ممكن من الشفافية في إبرام الصفقات العمومية[12] و بالتالي أن الإعلان عن شروط المنافسة مسبقا يجعل الراغبين في

---

[9] مرسوم رئاسي رقم 15-247 مؤرخ في 16 سبتمبر 2015 يتضمن تنظيم الصفقات العمومية و تفويضات المرفق العام ، ج ر،
ج ج ، ع 50،الصادر في 20 سبتمبر 2015.

[10] قانون رقم 06-01 مؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد و مكافحته، ج ر ،ج ج ، ع 14 الصادر في 08 مارس 2006، نصت المادة 01 منه على انه :"... دعم التدابير الرامية إلى الوقاية من الفساد و مكافحته و تعزيز النزاهة
و المسؤولية و الشفافية في تسيير القطاعين العام و الخاص...".

[11] نصت المادة 05 من المرسوم الرئاسي 15-247 على انه : " لضمان نجاعة الطلبات العمومية و الاستعمال الحسن للمال العام، يجب أن ترعى في الصفقات العمومية مبادئ حرية الوصول للطلبات العمومية و المساواة في معاملة المرشحين و شفافية الإجراءات، ضمن احترام أحكام هذا المرسوم".

[12] تنص المادة 14 من المرسوم الرئاسي 15-247 على انه : " جثت المصلحة المتعاقدة بوجوب البحث عن الإشهار الملائم

التعاقد مع الإدارة على قدم المساواة في تقديم عطاءاتهم دون تمييز وفقا لمبدأ المساواة،كما يمكنهم الاطلاع على العروض في الصحف و الجرائد[13] أو عن طريق المواقع الالكترونية[14]

-المحور الثالث : التزامات الإدارة تجاه المواطن في مجال إيصال المعلومة

يعد المرسوم رقم 88-131 بمثابة دفتر شروط، على الإدارة أن توفي به في علاقتها مع المواطن، حيث افرد جزءا هاما إلى استعراض واجبات الإدارة تجاه المواطن، نذكرهم في ما يأتي[15]:

- واجب إعلام المواطن :

يشمل أساسا حقه في معرفة التنظيمات و لتدابير التي تتخذها الإدارة، خاصة تلك المتعلقة بعلاقتها مع المواطن، وحقه أيضا في تلقى مبرر مكتوب في حالة وجود سبب يحول دون تمكينه من هذا الحق[16].

و في هذا الخصوص أن الإدارة ملزمة بانتظام بنشر التعليمات و المناشير و المذكرات و الآراء التي تهم علاقتها بالمواطنين[17] و دائما و في إطار إعلام المواطن صدرت نصوص قانونية متفرقة و ذات الصلة منهار نصوص تشريعية و أخرى تنظيمية تصب كلها في إعلام المواطن و توصيل المعلومة إليه و اغلبها تلك المواد جاءت بصيغة الإلزام (يتعين ،

---

[13] تنص المادة 61 من المرسوم الرئاسي 15-247 على انه : " يكون اللجوء إلى الإشهار الصحفي إلزاميا ...".

[14] تنص المادة 203 من المرسوم الرئاسي 15-247 على انه": تؤسس بوابة الكترونية للصفقات العمومية ".

[15] نصت المادة 06 من المرسوم رقم 88-131 تنص على انه :"تسهر الإدارة دوما على تكييف مهامها و هياكلها مع احتياجات المواطنين، و يجب أن تضع تحت تصرف المواطن خدمة جيدة و تليها المادة : يجب على الإدارة أن تمارس رقابة صارمة في جميع مستويات المراتب السلمية على سلوك أعوانها و انضباطهم. و يجب أن تتأكد دوما بأنهم يضطلعون بمهامهم في كنف احترام حقوق المواطنين احتراما دقيقا ".

[16] نصت المادة08 من المرسوم 88-131 عل ما يلي :" يتعين على الإدارة أن تطلع المواطنين على التنظيمات و التدابير التي تسطرها.و ينبغي، في هذا الإطار، أن تستعمل و تطور أي سند مناسب للنشر و الإعلام ".

[17] نصت المادة 09 من المرسوم 88-131 : " يتعين على الإدارة أن تنشر بانتظام التعليمات و المناشير و المذكرات والآراء التي تهم علاقاتها بالمواطنين إلا إذا وردت أحكام مخالفة في التنظيم الجاري به العمل، و إذا لم يتقرر هذا النشر صراحة في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، فانه ينجز في النشرة الرسمية للإدارة المعنية التي يتم إعدادها و نشرها وفقا لأحكام التنظيم الجاري به العمل".

الحق في الإعلام ، يجب ...)، حتى إن بعض القرارات الإدارية في مجال نزع الملكية تكون قرارات باطلة إن لم تشهر في المكان المخصصة لإعلام المواطنين أو إشهار في الجرائد الوطنية اليومية أو النشر في مجموع القرارات الإدارية للولاية، و من أهم الواجبات التي تقع على عاتق الإدارة هي إعلام المواطن بكل الطرق و هو ما يعبر عنه بالإشهار الواسع، وقد صدرت قوانين تلزم الإدارة بإعلام المواطن و نأخذ على سبيل المثال القانون رقم 01-14 يتعلق بتنظيم حركة المرور عبر الطرق و سلامتها و أمنها، معدل و متمم نصت المادة 63 منه :" ... الفقرة الأولى تربية و إعلام المواطن من اجل ترقية الانضباط في استعمال المسالك العمومية الكفيلة بضمان أمنه"[18].

و جاء القانون رقم 02-09 الذي يتعلق بحماية الأشخاص المعوقين و حمايتهم حيث نصت المادة 30 منه : الفقرة الخامسة : "تسهيل استعمال و صائل الاتصال و الإعلام." و تضمن القانون رقم 03-10 يتعلق بحماية البيئة في إطار التنمية المستدامة [19] في مادته 03 :"...لكل شخص الحق في أن يكون على علم بحالة البيئة و المشاركة في الإجراءات المسبقة عند اتخاذ القرارات تضر بالبيئة و بموجب المادة 07 منه : "لكل شخص طبيعي أو معنوي يطلب من الهيئات المعنية معلومات متعلقة بحالة البيئة، الحق في الحصول عليها"[20].

و في نفس السياق اصدر المشرع مراسيم تنظيمية مختلفة تلزم فيها الإدارة كذلك بواجب إعلام المواطن نذكر منها المرسوم التنفيذي رقم 93-186 يحدد كيفيات تطبيق القانون رقم 91- 11 الذي يحدد القواعد المتعلقة بنزع الملكية من اجل المنفعة العمومية و جاء في المادة 06 منه : "يفتح التحقيق المسبق بقرار من الوالي، يذكر فيه وجوبا ما يأتي " الفقرة

---

[18] القانون رقم 01-14 مؤرخ في 19 أوت 2001، ج ر ، ج ج ، ع 46، الصادر في 19 أوت 2001 ، يتعلق بتنظيم حركة المرور عبر الطرق و سلامتها و أمنها ، معدل و متمم .

[19] القانون رقم 02-09 مؤرخ في 8 مايو 2002، ج ر ، ج ج ، ع 34 الصادر في 14 مايو 2002 يتعلق بحماية الأشخاص المعوقين و حمايتهم .

[20] القانون رقم 03-10 مؤرخ في 19 يوليو 2003 يتعلق بحماية البيئة في إطار التنمية المستدامة ، ج ر ، ج ج ، ع 43 الصادر في 20 يوليو 2003 .

04 – كيفيات عمل اللجنة (أوقات استقبال الجمهور و أماكنه، و دفاتر تسجيل الشكاوى و طرق استشارة ملف التحقيق) و الفقرة 07 : يجب أن يكون هذا القرار قبل خمسة عشر (15) يوما من تاريخ فتح التحقيق : مشهر بمركز البلدية، منشور في يوميتين وطنيتين.

كما ينشر في مجموع القرارات الإدارية للولاية"[21]. إضافة إلى المرسوم التنفيذي رقم 93-123 المتعلق بتأسيس السجل العقاري ونصت المادة 09 منه : "يكون محضر التسليم ، المنصوص عليه في المادة السابقة، محل إشهار واسع..."[22] .و بناءا عليه فالمواطنون لهم الحق في الإعلام و أيضا لهم الحق في الاطلاع على الوثائق و المعلومات الإدارية إلا تلك المعنية و المحمية بالسر المهني[23]

المحور الرابع : أهمية الحق في الحصول على المعلومة .

أولا- تجسيد مبدأ الديمقراطية الإدارية .

لقد عني لمبدأ الديمقراطية الإدارية بعدة تعاريف، منها ما عرفه بأنه تهيئة السبل و الآليات المناسبة للمواطنين المحليين كالأفراد و الجمعيات قصد المساهمة و المشاركة في عمليات صنع و اتخاذ و تنفيذ القرارات الإدارية، بطريقة مباشرة أو غير مباشرة من خلال المجالس المنتخبة[24].

إضافة إلى ذلك يعرف مبدأ الديمقراطية الإدارية بأنها مشاركة و مساهمة المواطنين في الإدارة و التسيير بمشاركتهم في اتخاذ القرارات ليس بصفتهم كموظفين في الإدارات

---

[21] المرسوم التنفيذي رقم 93-186 مؤرخ في 27 يوليو 1993، يحدد كيفيات تطبيق القانون رقم 91- 11 المؤرخ في 27 ابريل 1991، الذي يحدد القواعد المتعلقة بنزع الملكية من اجل المنفعة العمومية، ج ر ،ج ج، ع 51 الصادر في 01 أوت 1993.

[22] المرسوم التنفيذي رقم 93-123 مؤرخ في 19 مايو 1993، يعدل و يتمم المرسوم رقم 76-63 المؤرخ في 25 مارس 1976 و المتعلق بتأسيس السجل العقاري، ج ر ،ج ج ، ع 34 الصادر في 23 مايو 1993.

[23] نصت المادة 10 على انه : " من المرسوم رقم 88-131 يمكن المواطنين أن يطلعوا على الوثائق و المعلومات الإدارية...."

[24] عمار بوضياف، شرح قانون الولاية، الجسور للنشر و التوزيع، الجزائر، 2012، ص180.

العمومية، و إنما كالمترفقين أو كالمستعملين للمرافق العمومية، باعتبارهم عنصرا مكونا للإدارة الحكومية حتى تكون قراراتها معبرة و مترجمة عن حاجات و رغبات المواطنين[25].

فهذين المفهومين لمبدأ الديمقراطية الإدارية يعبران عن المشاركة الخارجية للمجتمع المدني، الذي يعبر عن إرادة المواطنين بما يمثل انشغالاتهم التي يجب على الإدارة تحقيقها و تلبيتها و التي تعد من روافد الإصلاح الإداري[26].

ثانيا – تفعيل الديمقراطية التشاركية.

تعتبر البلدية الإطار المؤسساتي لممارسة الديمقراطية على المستوى المحلي، أن هذا القانون قد أقر جملة من الصلاحيات لرئيس المجلس الشعبي البلدي منها اتخاذ كل التدابير اللازمة لإعلام المواطنين و استشارتهم[27]، و له إمكانية تقديم عرض عن نشاطه السنوي أمام المواطنين.

و خصص المشرع في القانون رقم 11-10 المنظم للبلدية كهيئة إقليمية لامركزية بابا بأكمله لمبدأ مشاركة المواطنين في تسيير الشؤون البلدية، بحيث ورد ذلك في الباب الثالث المتضمن أربع مواد بدأ بالمادة11 إلى المادة 2814، و ما يلاحظ على هذا القانون أنه

---

[25] إن ذلك ما يستنتج من بعض النصوص المنظمة للإدارة المحلية في الجزائر و تحديدا نص المادة 02 من قانون البلدية الحالي على انه : " البلدية هي القاعدة الإقليمية للامركزية، و مكان لممارسة المواطنة، و تشكل إطار مشاركة المواطن في تسيير الشؤون العمومية ..." ينظر في ذلك، حبشي لزرق، الجوانب النظرية و التطبيقية للإدارة المحلية في الجزائر، مرجع سابق، ص 41 و 42.

[26] بلحاجي احمد، علاقة المواطن بالإدارة، دراسة قانونية، المرجع السابق، ص75 .

[27] ينظر في ذلك إلى المادة 02 من المرسوم التنفيذي رقم 16-190 يحدد كيفيات الاطلاع على مستخرجات مداولات المجلس الشعبي البلديو القرارات البلدية .

[28] قانون رقم 11-10 جاء في المادة 11 منه الفقرة 01 و 02 :"تشكل البلدية الإطار المؤسساتي لممارسة الديمقراطية على المستوى المحلي و التسيير الجواري. يتخذ المجلس الشعبي البلدي كل التدابير لإعلام المواطنين بشؤونهم و استشارتهم حول خيارات و أولويات التهيئة و التنمية الاقتصادية و الاجتماعية و الثقافية حسب الشروط المحددة في هذا القانون."

و يمكن في هذا المجال استعمال، على وجه الخصوص الوسائط و الوسائل الإعلامية المتاحة.كما يمكن المجلس الشعبي البلدي تقديم عرض عن نشاطه السنوي أمام المواطنين." ضف إلى ذلك المادة 12: "قصد تحقيق أهداف الديمقراطية

جاء صريحا و معبرا عن حق المواطن في المشاركة. لقد أضحى موضوع المشاركة الشعبية من أهم الموضوعات التي تشغل علماء الاجتماع و السياسة والاقتصاد والإدارة، ذلك على صعيد الدول المتقدمة و كذا تلك النامية.[29]

حضور المداولات في المجلس الشعبي البلدي : Délibération

يجري المجلس الشعبي البلدي خلال دواته مداولات[30] و أهم ما يحكمها :

العلانية : القاعدة العامة، أن مداولات المجلس علنية، إلا أنها تكون – استثناء – مغلقة في حالتين

1- فحص حالات المنتخبين الانضباطية.

2- فحص المسائل المرتبطة بالأمن و المحافظة على النظام العمومي.

و في هذا السياق، فان الجمهور يتمتع بحق الاطلاع على مداولات المجلس سواء :

- بحضوره إلى الجلسات المادة 26[31]، أي فتح الجلسات للجمهور : الأصل في جلسات المجلس أنها علنية و يجوز أن تكون مغلقة . و الجلسة المفتوحة تخول لكل مواطن في البلدية و كل مواطن معني

المحلية في إطار التسيير الجواري المذكور في المادة 11 أعلاه، يسهر المجلس الشعبي البلدي على وضع إطار ملائم للمبادرات المحلية التي تهدف إلى تحفيز المواطنين

و حثهم على المشاركة في تسوية مشاكلهم و تحسين ظروف معيشتهم. يتم تنظيم هذا الإطار طبقا للتشريع و التنظيم المعمول به."

[29] مسعد الفاروق حمودة، التنمية و المجتمع، مدخل نظري لدراسة المجتمعات المحلية، المكتب الجامعي الحديث،مصر،2001، ص240.

[30] نصت المادة 52 من القانون 11-10 على انه: "يعالج المجلس الشعبي البلدي الشؤون التي تدخل في مجال اختصاصه عن طريق المداولات."

موضوع المداولة من حضورها،و يحضر الجمهور طبقا للمادة 14 من المرسوم التنفيذي رقم 13-105[32] المخصص له و هذا في حدود الأماكن المتوفرة، إذ يلزم الجمهور بالصمت طيلة مدة الجلسة و لا يمكن لأي شخص من الجمهور المشاركة في المناقشات أو تعكيرها أو القيام بأي تصرف من شانه المساس بالسير الحسن لأشغال المجلس تحت طائلة الطرد من قاعة المداولات و الفضاءات المحيطة بها[33]، أو عن طريق تعليقها بمقر البلدية، خلال الأيام الثمانية الموالية للدورة (المادة 30)، أو الاطلاع المباشر على محاضر المداولات، أو أخد نسخة منها[34].

و في ظل القانون رقم 12-07، متعلق بتنظيم الولاية، نجد أن المشرع لم يتوانى عن إقرار مبدأ المشاركة ذلك بموجب المواد 13، 18، 32 و 36 منه، بحيث يشدد في كل مرة على ضرورة إعلام الجمهور من خلال نشر الإعلانات و ذلك بموجب المواد 18 و31 ، أما بشأن المادة 32 نجد أن المشرع قد أجاز لأي شخص ذو مصلحة الإطلاع على محاضر مداولات المجلس الشعبي ألولائي و الحصول على نسخة كاملة أو جزئية لكن على نفقته، و بحكم الخبرة و المؤهلات فنجد أن لجان المجلس الشعبي ألولائي مؤهلة بدعوة أي شخص

---

[31] نصت المادة 26 من القانون 11-10 على انه : "جلسات المجلس الشعبي البلدي علنية، و تكون مفتوحة لمواطني البلدية و لكل مواطن معني بموضوع المداولة، غير أن المجلس الشعبي البلدي يداول في جلسة مغلقة من اجل : دراسة الحالات التأديبية للمنتخبين – دراسة المسائل المرتبطة بالحفاظ على النظام العام".

[32] نصت المادة 14 على انه: " يحضر الجمهور جلسات المجلس في الفضاء المخصص له على مستوى قاعة المداولات في حدود الأماكن المتوفرة..."من مرسوم تنفيذي رقم 13-105 مؤرخ في 17 مارس 2013، يتضمن النظام الداخلي النموذجي للمجلس الشعبي البلدي، ج ر، ج ج ،ع 15 الصادر في 17 مارس 2013.

[33] عمار بوضياف، الوجيز في القانون الإداري، مرجع نفسه، ص 387- 388.

[34] محمد الصغير بعلي، القانون الإداري، مرجع سابق، ص 166 و بالرجوع إلى المادة 14 من القانون 11-10: "يمكن كل شخص الاطلاع على مستخرجات مداولات المجلس الشعبي البلدي و كذا القرارات البلدية، و يمكن كل شخص ذي مصلحة الحصول على نسخة منها كاملة أو جزئية على نفقته ...".

من شأنه أن يقدم أي معلومة مقيدة لأشغال اللجنة مما يفسح مجال لإشراك المواطن وهذا ما أكدته المادة 36 .

فقد جاء في المادة 36 من قانون الولاية[35] إمكانية الاستعانة بأشخاص ذوي خبرة في مختلف المجلات للاستفادة من خبراته، و من خلال هذه المادة حاول المشرع أن يدفع اللجنة و أعضائها المنتخبين من أن تمد يدها لأشخاص من خارج المجلس و تطلب منهم مساعدتها في أمر محدد.كان تطلب لجنة الاقتصاد و المالية من خبير مالية محافظ حسابات مثلا أن يمدها بمعلومات تخص ميزانية المجلس.أو كأن تطلب لجنة الصحة و النظافة و حماية البيئة من جمعية تنشط في مجال البيئة معلومات محددة تساعدها على إعداد تقريرها.

و لا شك أن لجوء لجنة المجلس الشعبي ألولائي لطلب مساعدة شخص أو أشخاص من خارج المجلس يترجم من جهة أخرى تجسيد مبدأ المشاركة و هو احد أهم مؤشرات الحكم الراشد كما رأينا. علما أن ذات التقنية كانت مقررة في قانون 1990بموجب المادة 24 منه[36].

و أضحت البلدية من خلال المادة 175 من القانون 11-10 : تشجع البلدية و تدعم كل نشاط أو مساهمة أو مبادرة فردية أو جماعية تهدف إلى انجاز مشاريع ذات منفعة عامة.

حضور المداولات في المجلس الشعبي الولائي: Délibération

الأصل في جلسات المجلس أنها علنية و يجوز أن تكون مغلقة[37]. و الجلسة المفتوحة تخول لكل مواطن في الولاية و كل مواطن معني بموضوع المداولة من حضورها. و يحضر

---

[35] نصت المادة 36 من القانون رقم 12-07 على انه :"يمكن لجان المجلس دعوة كل شخص من شانه تقديم معلومات مفيدة لأشغال اللجنة بحكم مؤهلاته أو خبرته ".

[36] عمار بوضياف، الوجيز في القانون الإداري، مرجع سابق، ص 238.

[37] نصت المادة 16 من المرسوم التنفيذي رقم 16-190على انه : "تجري دراسة المسائل المتعلقة بالنظام العام و الحالات التأديبية لأعضاء المجلس في جلسات مغلقة".

الجمهور طبقا للمادة 16 من المرسوم في الفضاء المخصص له و هذا في حدود الأماكن المتوفرة. و لا يسمح بالدخول للفضاء المخصص لأعضاء المجلس لغير الأعضاء و الموظفين الملحقين بالديوان أو أي موظف آخر مفوض من الوالي . و لا يمكن لأي شخص غير عضو الجلوس في المقاعد المخصصة لأعضاء المجلس .

و لا يمكن للجمهور المشاركة في المناقشات أو تعكيرها أو القيام بأي تصرف من شانه المساس بالسير الحسن لأشغال المجلس تحت طائلة الطرد من قاعة المداولات و الفضاءات المحيطة بها[38].

ثانيا – تفعيل مكافحة الفساد.

فبعد الوقوف عند كل من تعريف الحق في تداول المعلومة وتحديد الإطار القانوني له، توصلت كل الابحاث إلى أن الحق في النفاذ إلى المعلومة يساهم بدرجة كبيرة في مكافحة الفساد ، وذلك من خلال الكشف عن جوانب الإهدار والاحتيال وعدم الكفاءة والعجز ، وتبيان الأخطاء والتجاوزات التي تقع فيها الحكومات ، فيكون بوسع الأفراد أو الصحافيين من خلال الحصول والوصول إلى المعلومات كشف الأخطاء وكشف بؤر الفساد واستغلال السلطة لتحقيق الأغراض الشخصية. ، وتوفير حماية أساسية ضد عمليات إساءة استخدام السلطة وسوء الإدارة والفساد. وهو ما يعتبر رادعا للفساد – وغيره من المساوئ– خوفا من الكشف والمحاسبة فقد جاء في المادة **المادة** (9) معدلة : "يجب أن تؤسس الإجراءات المعمول بها في مجال الصفقات العمومية على قواعد الشفافية والنزاهة والمنافسة الشريفة وعلى معايير موضوعية"[39].

---

[38] عمار بوضياف، الوجيز في القانون الإداري، مرجع سابق، ص 292 ، و تأكيدا لذلك نصت المادة 15 من المرسوم التنفيذي رقم 16–190على انه :"يلتزم الجمهور الصمت طيلة مدة الجلسة. و لا يمكن أي شخص من الجمهور، بأي حال من الأحوال، المشاركة في المناقشات أو تعكيرها أو القيام بأي إشارة من شانها المساس بالسير الحسن لأشغال المجلس، تحت طائلة الطرد من قاعة المداولات و الفضاءات المحيطة بها".

[39] القانون رقم 06_01 المؤرخ في 20 فيفري 2008 المتعلق بالوقاية من الفساد و مكافحته،ج ر ج ج ، العدد 14المؤرخ في 08 مارس 2006 .

ويجب أن تكرس هذه القواعد على وجه الخصوص: -علانية المعلومات المتعلقة بإجراءات إبرام الصفقات العمومية، و التي عدلت بموجب المادة 2 من الأمر رقم 10-05[40]،

و جاء أيضا في المادة 11 من قانون مكافحة الفساد:" لإضفاء الشفافية على كيفية تسيير الشؤون العمومية، يتعين على المؤسسات والإدارات والهيئات العمومية أن تلتزم أساسا: باعتماد إجراءات وقواعد تمكن الجمهور من الحصول على معلومات تتعلق بتنظيمها وسيرها، وكيفية اتخاذ القرارات فيها،

بتبسيط الإجراءات الإدارية، بنشر معلومات تحسيسية عن مخاطر الفساد في الإدارة العمومية، بالرد على عرائض وشكاوى المواطنين،.....

و من أهم مظاهر مكافحة الفساد مشاركة المجتمع المدني ، و الذي اقرته المادة 15من قانون مكافحة الفساد و الذي فحواها :" يجب تشجيع مشاركة المجتمع المدني في الوقاية من الفساد ومكافحته بتدابير مثل :اعتماد الشفافية في كيفية اتخاذ القرار وتعزيز مشاركة المواطنين في تسيير الشؤون العمومية، عداد برامج تعليمية وتربوية وتحسيسية بمخاطر الفساد على المجتمع، وتمكين وسائل الإعلام والجمهور من الحصول على المعلومات المتعلقة بالفساد، مع مراعاة حرمة الحياة الخاصة وشرف وكرامة الأشخاص، وكذا مقتضيات الأمن الوطني والنظام العام وحياد القضاء.

خاتمة:

في النهاية، يمكن القول بأن العلاقة بين الإدارة والمواطن في مجال تيسير الحصول على المعلومة خصوصا في الجزائر– هي محل تأثيرات لعوامل متعددة :نفسية، اجتماعية، تاريخية وسياسية أيضا، بالتالي– فهي مجرد صورة عاكسة لواقع المجتمع بمختلف جوانبه.

ومن ثم فإن هذه الدراسة لا تعدو أن تكون مجردة نظرة واحدة ذات بُعدٍ واحد، معنى هذا أن هذه العلاقة هي في حاجة إلى نظرات أخرى وبأبعاد متعددة حتى يتم الإلمام بها من

[40] الأمر رقم 10-05، المؤرخ في 26 غشت سنة 2010، ج ر ج ج، عدد 50، صفحة 16.

شتى الزوايا ، إنها ببساطة علاقة تعكس هذه " الطبقية السياسية في المجتمع :" بعبارة أخرى هي إنها تعكس وجود الدولة ذاتها، علاقة ليس أدل على تلازمها من مقولة أدام سميث: لا يمكن الحديث عن مجتمعات متطورة اقتصاديا وأخرى متخلفة، بل هناك مجتمعات متطورة إداريا وأخرى متخلفة".

الاقتراحات

بداية يجب على الطرفين(الإدارة و المواطن) فهم وقبول الطرف الآخر كواقع، وضرورة التعامل معه على هذا الأساس خاصة في مجال تسهيل الحصول على المعلومة.

– إصباغ السلوك الإنساني للإدارة في تعاملها مع المواطن على اعتباره أنه الطرف الضعيف في هذه العلاقة.

– إعطاء الانطباع لدى المواطن بأنه هو غاية وجودها، وهذا من خلال متابعة انشغالاته و تزويده بالمعلومات الضرورية.

– حماية أصحاب الشكاوى و التظلمات من انتقام الإدارات المشكو منها، حتى يُعمم سلوك الشكوى لدى المواطن ليكون بذلك مصدرا من مصادر المعلومة لدى الإدارة.

– حماية الموظف من تأثيرات القوى الضاغطة في المجتمع والمحيط على حد سواء، و ذلك من خلال صيانة كرامته وحمايته من التجاوزات التي قد تلحق بشخصه .... . بحزم مع

– تعميم استعمال وسائل الاتصال الحديثة توصيل شبكات الانترنت عبر مختلف مناطق الوطن خاصة في مناطق الظل.

– رقمنة القطاعات العمومية و في هذا الصدد نشكر الديوان الوطني لمكافحة المخدرات الذي أتاح لنا حرية الوصول إلى المعلومات و كل الإحصائيات المطلوبة في أبحاثنا.

– وضع ضوابط لحسن استعمال المعلومة و عدم التعدي على الخصوصيات.

– تجريم استعمال المعلومة لإلحاق الضرر بالمصالح العليا للدولة.

حقوق المؤلف على شبكة الانترنت

Copyright Online

حواس فتحية، أستاذة محاضرة أ
جامعة الجزائر1، الجزائر
houesfethia@gmail.com

الملخـص:

إن تقدم ورقي الإنسان في مختلف المجالات لا يأتي إلا إذا استخدم فكره لتحقيق هدف ما، فإنتاجه الذهني هو الأساس في توفير حياة أفضل له ولمن يحيط به.

ولكن هذا الإنتاج الفكري يمكن أن يكون محل اعتداء من الغير وخاصة مع التطور الهائل الذي يشهده العالم، وبالتحديد في مجال الشبكة العنكبوتية.

حيث تسببت الانترنت في نشوء اعتداءات جديدة على المؤلف تمس بحقوقه المعنوية والمالية.

هذه المداخلة هدفها تسليط الضوء على بعض الانتهاكات التي تطال هذه الحقوق وتبيين أسبابها.

الكلمات المفتاحية:

المؤلف، الأنترنت، الإعتداءات، الحقوق، الحماية

Abstract :

The progress and advancement of man in various fields does not come unless he uses his thought to achieve a goal, as his mental production is the basis for providing a better life for him and those around him.

But this intellectual production can be subject to aggression from others, especially with the tremendous development that the world is witnessing, specifically in the field of the Internet.

The Internet has caused new attacks on the author, affecting his moral and financial rights.

This intervention aims to shed light on some violations of these rights and to explain their causes.

Keyword :

Author, Internet, Attacks, Rights, Protection.

المقدمـة:

تبنى المشرع الجزائري في تنظيمه لحقوق المؤلف عبر جميع تشريعاته المتلاحقة النظرية الثنائية لحقوق المؤلف والتي مفادها أن المصنف الذهني ينشأ عنه مركز قانوني مختلط يتكون من عنصرين هما : العنصر المعنوي والعنصر المادي .

وإذا كان العنصر المعنوي يهدف إلى ضمان استمرار التوافق بين شخصية المؤلف وأثره الفني، فإن العنصر المادي يهدف إلى جعله يستغل ماديا مصنفاته عبر منحه امتيازات تجعل له الحق في إمكانية استنساخها وإبلاغها إلى الجمهور .

ولقد كان لظهور وانتشار شبكة الانترنت أثر كبير على سرعة وسهولة التواصل فيما بين مستخدميها عبر كافة أنحاء العالم بشكل لم يسبق له مثيل وذلك بفضل ما أتاحته لهم من خدمات وتطبيقات متعددة ومتنوعة ساهمت بشكل كبير في إطلاق حرية التعبير وسهولة الحصول على المعلومات و مختلف ضروب و أنواع المصنفات الفكرية .

وبقدر ما كان لشبكة الأنترنت من مزايا فإنها و في الوقت نفسه لم تخلو من بعض السلبيات الناتجة عن استخدامها السيئ وغير المشروع خاصة في مجال حقوق الملكية الفكرية بوجه عام وحقوق المؤلف على الوجه الخصوص عن طريق نسخ المصنفات وإتاحتها وتحميلها عبر الشبكة دون الحصول على إذن مؤلفها أو ذوي حقوقه ، مما أدى إلى إهدار حقوق المؤلف والتسبب في حرمانه من استغلالها ماليا.

فكيف أثر استخدام شبكة الانترنت على حقوق المؤلف المعنوية والمادية؟

المبحث الأول : الحقوق المعنوية للمؤلف على شبكة الأنترنت

إن الحقوق المعنوية تهدف أساسا إلى حماية الشخصية الفكرية للمؤلف وضمان احترامها باعتباره مبدعا لمصنف يشكل مرآة تعكس شخصيته وأفكاره، ولقد استقر الفقه والقانون على أنها تتضمن مجموعة من الحقوق الفرعية التي قام بتنظيمها المشرع في المواد من 22 إلى 26 من الآمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة والمتمثلة في حق

الكشف عن المصنف، الحق في أبوة المصنف، الحق في سحب المصنف من التداول، والحق في احترام سلامة المصنف .

المطلب الأول: الحق في الكشف عن المصنف

تتمثل أغلب صور الاعتداء على الحقوق المعنوية المقررة للمؤلف، قيام الغير بنشر المؤلف قبل أن يقرر المؤلف نشره، أو أن تتم عملية النشر بصورة تختلف عن تلك التي عينها المؤلف[1].

على الرغم من المزايا والإيجابيات التي حققتها تقنيات النشر الرقمي الحديثة للمؤلفين من انتشار كبير وسريع لمصنفاتهم عبر العالم أجمع، إلاّ أنّها مع ذلك تتضمن سلبيات باتت تهدد الحق الأدبي للمؤلفين في إتاحة مصنفهم للجمهور لأول مرة، وتؤثر بشكل واضح على حقهم في تقرير النشر وتحديد موعد هذا النشر وكيفيته، ومن ذلك ما يقوم به قراصنة الأنترنت من نسخ تسجيلات أغاني لم يتم طرحها للجمهور بعد، ومن ثم بثها على موقع الواب، وهو الأمر الذي يشكل خرقا وانتهاكا لحقوق المؤلف في تقرير نشر مصنفه[2].

ويستلزم النشر عبر شبكة الأنترنت تحوير المصنف ليتلاءم مع طريقة النشر الإلكترونية، وكذا دمج مصنفات محمية مع بعضها البعض لإخراجها في صورة معلومات جديدة أو بيانات رقمية. وتشكل جميع هذه الحالات اعتداء صارخا على الحق المعنوي للمؤلف ما دام أنّها أجريت دون علم المؤلف.

وتكمن خطورة نشر المصنفات عبر شبكات الأنترنت في أنها تفتح المجال أمام الاستعمال الجماعي للمصنفات المحمية. ولعل هذا المثال يوضح جانبا من المشكلات القانونية التي ترتبط بكيفية حماية حقوق المؤلف عبر شبكة الأنترنت[3].

المطلب الثاني : الحق في الأبوة : le droit de paternité

يقصد بحق الأبوة حق المؤلف في المطالبة بالاعتراف بأن المصنف الذي أبدعه هو من إنتاجه، وإيصال هذا المصنف إلى الجمهور مقرونا باسمه ولقبه ومؤهلاته العلمية، وذلك بشكل بارز على كل نسخة من نسخ المصنف الذي ينشره بنفسه أو بواسطة غيره[4].

---

[1] نصير صبار لفته، "أثار عقد التأليف"، مجلة القانون المقارن، ع 42، 2006، العراق، ص22.

[2] رامي ابراهيم حسن الزواهرة، النشر الرقمي للمصنفات وأثره على الحقوق الأدبية والمالية للمؤلف: دراسة مقارنة في القوانين الأردني والمصري والإنجليزي، دار وائل للنشر، عمان، الأردن، 2013، ص 336.

[3] خالد ممدوح إبراهيم، جرائم التعدي على حقوق الملكية الفكرية، الدار الجامعية، الإسكندرية، مصر، 2010، ص 238.

[4] نواف كنعان، حق المؤلف (النماذج المعاصرة لحق المؤلف ووسائل حمايته) دار الثقافة للنشر و التوزيع، الأردن ، الطبعة الأولى ،2009.، ص105.

كما يعني حقه في أن يعلن عن اسمه في حالة الأداء العلني أو إذاعة للمصنف، أو في حالة الاقتباس من المصنف، وحقه في أن ينشر مصنفه تحت اسم مستعار أو بدون اسم، وفي أن يحظر على الغير القيام بنشر مصنفاته تحت اسم آخر[1].

ويترتب على حق المؤلف في نسبة مصنفه إليه أن يدافع ضد أي اعتداء يقع على اسمه وعنوان مصنفه، وقد يتخذ هذا الاعتداء صورا أو أشكالا مختلفة، كأن يتم تحريف اسم المؤلف أو أن يتم انتحال اسم المؤلف وجعله مقرونا بمصنف آخر غير الذي أبدعه.

وبذلك حق الأبوة يطبق على المصنفات المنشورة على شبكة الأنترنت حتى في فرضية كون المؤلف يكون قد تنازل عن حقوق الاستغلال للغير. إذ أن كل مصنف منشور على الشبكة يجب أن يذكر عليه اسم مؤلفه، ويكون مساسا بالحق المعنوي للمؤلف على شبكة الأنترنت عندما تستعمل إشهادات من مصنفات الغير دون أن يذكر عليها اسم المؤلف.

كما أنّ حق الأبوة يطرح مشاكل تطبيقية على شبكة الأنترنت، وهذا لكون احترام هذا الحق يختلف عن ما هو عليه في الدعامة المادية، إذ أن المجلات والمصنفات المتعددة الوسائط قد تحتوي على أكثر من 500.000 صورة، واسم المؤلف لا يوضع عليها إنّما يوضع على ملف (fichier) يكون في متناول مستعمل الأنترنت عند الطلب، وهذا أمر غير صائب.

إن نشر المصنفات على شبكة الأنترنت يمس بحق المؤلف في أبوة مصنفه، فما هو منشور على الشبكة يمكن الوصول إليه بكل بساطة وبشكل مجاني. والأمر الذي زاد من تكرار صور وأشكال الاعتداء على هذا الحق هو انتحال اسم المؤلف ونسبته إلى مصنفات لم يقم بإيداعها، أو القيام باقتباس أجزاء كبيرة من المصنفات دون ذكر اسم مؤلفها ودمجها مع أجزاء من مصنفات أخرى بشكل يشوه من المصنف الأصلي ويسيء إلى سمعة مؤلفه.

إن الأمر وصل إلى حد السرقات الأدبية الكاملة لمصنفات ونسبتها إلى شخص غير مؤلفها، وهو الأمر الذي يستطيع أي باحث متخصص التيقن منه لكثرة الأبحاث والمقالات التي يدعي ناشروها عبر صفحات ومواقع الواب العديدة بأنهم مؤلفوها في حين أنها تعود لمؤلف آخر.

إن هذا المزج والتفاعل بين مصنف أدبي وفني لمؤلفين مختلفين يثير مشكلة ملكية المصنف الناتج من هذا المزج أو التفاعل بين المصنفات. كما أنه من شأنه أن يهدر حق المؤلف

[1] Mirielle Buydens, Droits d'auteurs et Internet: Problèmes et solutions pour la création d'une base de données en ligne contenant des images ou, texte, Université catholique de lonvain, Faculté de droit, Belgique, 2001, disponible sur : [http://www.droit-technologique.org], la dernière consultation le : 28/12/2007, p22.

في أن ينسب مصنفه إليه، لكون المصنف الهجين قد يشكل مصنفا مختلفا عن المصنفات الأصلية الداخلة في تكوينه، وبالتالي لا يعتبر انعكاسا لفكر وذوق المؤلف الأصلي لأي من المصنفات الأصلية[1].

ويتم المساس بهذا الحق في إطار البيئة الرقمية عندما يتم الكشف عن المصنف على شبكة الانترنت مثلا دون الإشارة إلى اسم مؤلفه ، فلقد أدانت محكمة الدعوى الكبرى لباريس مثلا في حكم لها بتاريخ 09 أكتوبر 2009 محرك البحث قوقل نظرا لقيامه بنشر صور فوتوغرافية دون الإشارة إلى اسم ملتقطها.[2]

كما قضي في هذا الخصوص أيضا بأن التقنية التي تعرف بالروابط المنطقية الداخلية "hyperliens profonds " التي تعد كاشفة مباشرة للصفحات الداخلية لموقع أخر دون إظهار لأصل المصنف الذي يظهر على شاشة الحاسب الآلي يعد مساسا بحق الأبوة.[3]

كما قضت محكمة الدعوى الكبرى في باريس في حكم لها بتاريخ 28 /2004/01 بأن الإشارة إلى اسم المؤلف لا بد أن يكون بشكل وثيق الصلة بمصنفه، وأنه لا يكفي. احتراما لهذا الحق. وضع روابط تحيل إلى الموقع الذي يظهر في اسم المؤلف[4].

المطلب الثالث : الحق في احترام المصنف:

يقصد بالحق في احترام المصنف الحق في الحفاظ على سلامة المصنف ودفع أي اعتداء يؤدي إلى تشويه أو تحريف أو الإضرار بسمعة صاحبه. كذلك الحق في منع أي تغيير أو تشويه لأدائه، سواء ما يتعلق بأدائه السمعي الحي أو أدائه المثبت في تسجيل صوتي[5].

وفي هذا الصدد يمكن القول أن أكثر أشكال الاعتداء على حق المؤلف في سلامة مصنفه هو ما تتعرض له المصنفات من تشويه واعتداء عند نشرها رقميا عبر مواقع وصفحات الواب، وذلك من خلال قيام مصممي صفحات ومواقع الواب بإنشاء روابط ووصلات تشعبية ضمن المصنفات التي يقومون بنشرها على صفحاتهم الخاصة، بحيث تشير وتقود هذه الوصلات والروابط إلى مصنفات أخرى منشورة على مواقع أخرى، الأمر الذي

---

1 حسام الدين كامل الأهواني، مرجع سابق، ص 35.

2 - TGI Paris 3éme ch. ,9 oct2009 , H /K ,André R. c / Google ,CCE2010 ,chron n1,voir ,WWW.legalis.net.

3 . TGI Paris , réf 10 juin 1997 Queneau / Mygale, Expertises juin 1997 p 242 , voir , LARRIEU Jacques , Droit de l'internet, Ellipses , coll. Mise au point 2 éme édit , 2010 p 43

4 - CA 28 janvier 2004 ,SARL Société de la presse internationale / SARL TELFUN , voir WWW.legalis.net ,

5 نواف كنعان، مرجع سابق، ص409.

يؤدي إلى تشويش القارئ بالمضمون الحقيقي للمصنف وبالتالي تشويه المصنف وتحريفه، وبالتالي الاعتداء على حق المؤلف في احترام وسلامة مصنفه1.

وتجدر الإشارة أنّ، التخزين أو التثبيت البسيط للمصنفات على دعائم أو في ذاكرة أجهزة الحاسب أو على مواقع الأنترنت لا تثير أية مشاكل بالنسبة للحقوق الأدبية للمؤلف ومنها حق الاحترام، ما دام الناشر قد التزم بما يجب عليه نحو عدم إضافة أو حذف أو تعديل أي شيء في المصنف أو إليه بما يؤثر على قيمته الأدبية أو الفنية. أما إذا أضاف الناشر للمصنفات أو ألحق بها ما يؤثر على مضمونها كالصور والرسومات مثلا فإن هذا قد يثير بعض المؤلفين ويجعلهم يطالبون بحق احترام مصنفاتهم.

كما ان نشر المصنفات الموسيقية أو غيرها على شبكة الأنترنت بدون أخذ إذن من صاحبها فعل يشكل جنحة التقليد، خاصة إذا رافقه تعديلات أو تغيرات على مصنفات الغير، الأمر الذي من شأنه أن يمس بتكامل المصنفات.

ولعرض نموذج من نماذج الصعوبات التي صادفت أصحاب حق المؤلف والحقوق المجاورة بسبب نشر وإعادة نشر وتوزيع المصنفات محل الحماية عبر الإنترنت دون موافقتهم، فإننا نذكر القضية الشهيرة المعروفة باسم "نابستر" وهي قضية حدثت في أمريكا. وتتمثل حيثيات القضية في قيام إحدى الشركات المعروفة لخدمات الأنترنت في الولايات المتحدة، وهي شركة "Napster" التي تملك موقع على الأنترنت بتوزيع برامج حاسوب يسهل الحصول على ملفات موسيقية "MP3" (وهي ملفات موسيقية مضغوطة) على الأنترنت.

قامت هذه الشركة بتوفير الكتالوج الغنائي الموسيقي لأحدى الفرق الموسيقية وهي فرقة "Matallica" في موقعها على الشبكة بدون الحصول على إذن بهذا منها.

أقامت الفرقة بتاريخ 13 أفريل 2000 برفع دعوى قضائية ضد الشركة متهمة إياها بانتهاك حق المؤلف في ملكيتها الفكرية للموسيقى موضوع الكاتالوج2. وهذا لأن شركة "Napster" تركت الملايين ينسخون أو يحملون موسيقاهم مضيعة عليهم العوائد المالية المستحقة لهم في مقابل هذا النسخ أي التحميل المجاني.

إن شركة "Napster" دافعت على نفسها بقولها أنّها سهلت الاتصال ما بين الناس المهتمين بالموسيقى، وأنّها اتبعت المنهج الأصلي بالأنترنت في توفير المشاركة في المعلومات.

---

1 رامي إبراهيم حسن الزواهرة، مرجع سابق، ص429.

2 أنظر تفاصيل القضية على الموقع: [http://www.juriscom.net/int/dpt/dpt29.htm]، تاريخ آخر تصفح: 2012/02/02.

وفي 28 جويلية 2000 حكم القضاء الأمريكي لصالح الفرقة الموسيقية، أين أمر بإغلاق موقع شركة "Napster" على الأنترنت كعقاب لها لانتهاك حق المؤلف للفرقة في المادة موضوع الكتالوج الموسيقى الخاص بها.

إنّ المخاطر الأكثر التي تتعرض إليها المصنفات المنشورة على الأنترنت هي التبديل والتشويه والتحريف، وهي أفعال تدخل في جريمة التقليد التي يعاقب عليها قانون العقوبات، لذلك يجب تفادي مثل هذه التصرفات التي من شأنها تغيير من صورة المصنف، فلا يصبح هذا الأخير يعكس شخصية مؤلفه[1].

طبقا لذلك يكون كل تعديل أو تغيير في المصنفات يشكل مساسا بالحق المعنوي للمؤلف، وهذا ما أكدته المحاكم الفرنسية في كثير من المرات. أمّا القضاء الجزائري فلا يوجد به دعاوى في هذا الموضوع.

وفي قضية وقعت في فرنسا تم تعديل صورة منشورة على شبكة الأنترنت، وهذا بإزالة العناصر التي تحيط بها، فأدانت المحكمة المدعى عليه لكونه مس بالحق المعنوي للمؤلف[2].

ونفس الحكم كان في قضية تم فيها وضع الصورة في إطار[3]، وفي قضية أخرى تم فيها تلوين رسم بعد أن كان منشور بالأبيض والأسود[4].

وبذلك كل استغلال للمقالات أو الكتب أو الكتابات الأدبية والعلمية المنشورة على الشبكة العنكبوتية إمّا بتحريفها، أو بتعديل محتواها، ونشر معلومات مغلوطة ونسبها إلى أشخاص آخرين مع عدم ذكر المصدر، يمس بسلامة المصنف المنشور على شبكة الأنترنت.

والأمر كذلك بالنسبة إلى زراعة الفيروسات على الشبكة لتدمير المعطيات والملفات المخزنة أو تعديلها.

وقد يقع المساس كذلك من ربط المصنف بصفحة تحتوي على كلمات أو رسومات مما قد يشوه المصنف أو يسيء إليه (Liens Hypertexts)، أو وضع المصنف في إطار سياسي أو دعائي يتعارض مع فكرة المؤلف5.

المطلب الثاني: الحق في سحب المصنف من التداول

---

1 Jolie Jacob et Benjamin Jacob, "Les enjeux de la musique numérique", Petites affiches, 1999, N° 242, p 8.

2 TGI Paris, 26 Juin 1985, Dexhame c / le figaro, D 1986, somm 184.

3 C.A. Paris, 11 Juin 1990, D 1990, p 191.

4 C.A. Paris, 31 1988, Express Oct c/ Deveria, D 1989, N° 15, p 22.

5 حسام الدين كامل الأهواني، مرجع سابق، ص11.

وقد اعترف المشرع بهذا بحق سحب وتعديل المصنف في المادة 24 من أمر 03_05 المتعلق بحقوق المؤلف والحقوق المجاورة إذ نص على أنه:" يمكن *للمؤلف الذي يرى أن مصنفه لم يعد مطابقا لقناعته أن يوقف صنع دعامة إبلاغ المصنف إلى الجمهور بممارسة حقه في التوبة أو أن يسحب المصنف الذي سبق نشره من جهة الإبلاغ للجمهور عن طريق ممارسة حقه في السحب*".

إنّ التشريعات التي تسمح للمؤلف بحق سحب مصنفه من التداول قيدته بشروط منها أن يكون هناك أسباب جدية للسحب، وكذا تعويض عادلا للناشر يراعى فيه ما فاته من كسب عن الفرص المالية التي ضاعت عليه نتيجة سحب المؤلف للمصنف، وما تحمله من مصاريف كان يتوقع تغطيتها من بيع نسخ المصنف[1].

يعتبر حق المؤلف في سحب المصنف أو تعديله من أكثر السلطات أو الامتيازات الأدبية للمؤلف تأثيرا بالتطورات التكنولوجية في العصر الحديث، إذ أن التقنيات الرقمية المتطورة لوسائل وأساليب نشر وإتاحة المصنفات عبر الأنترنت قد أدى إلى الحد من هذا الحق وتقييده، إلى درجة أصبح يمكن معها القول بأن النشر الرقمي قد أدى إلى إلغاء أو تعطيل حق المؤلف في سحب مصنفه أو تعديله ولا سيما فيما يخص بالمصنفات ذات الطابع الرقمي والتكنولوجي الحديث[2].

فقد أصبحت النصوص القانونية التي تنص على هذا الحق مستحيلة التطبيق في ظل الواقع العملي الذي تفرضه صناعة النشر الرقمي للمصنفات بما تتطلبه من استثمارات اقتصادية هائلة، فمن الناحية الواقعية النشر عن طريق الأنترنت يكاد يقضي على الحق في سحب أو تعديل المصنف، فبعد أن تم النشر عبر العالم فأي سحب أو تعديل قد يتحقق[3].

فضلا عن ذلك فإن المؤلف قد يكون من الصعب عليه -إن لم يكن مستحيلا- سحب المصنف من التداول وذلك لعدم قدرته على دفع التعويض المالي العادل للناشر، فمثل هذا التعويض قد يشكل مبلغا كبيرا جدا خاصة إذا تعلق الأمر بمصنفات تكبد الناشر أموالا طائلة في سبيل وضعها على دعامات رقمية وطرحها للتداول رقميا، ناهيك عن أن الانتشار الواسع للمصنفات المنشورة رقميا عبر شبكة الأنترنت يزيد من قيمة هذا التعويض العادل[4].

---

[1] نصت على حق التعويض المادة 2/24 من أمر05/03 المتعلق بحقوق المؤلف والحقوق المجاورة.

[2] رامي ابراهيم حسن الزواهرة، مرجع سابق، ص 362.

3حسام الدين كامل الأهواني، المرجع السابق، ص12.

4 رامي ابراهيم حسن الزواهرة، مرجع سابق، ص 364.

يواجه المؤلف صعوبات بالغة لحماية حقه إذا نشرت مصنفاته على شبكة الأنترنت بدون إذنه، وهذا لأنه يتعذر عليه إيقاف الاعتداء على المصنف، وكذا منع استمرار إتاحته للجمهور عبر الشبكة، بالإضافة إلى صعوبة وعقبات اللجوء إلى التقاضي نظرا لتعدد القوانين الوطنية واختلافها وتنازع الاختصاص فيما بينها.

ولعل خير مثال على ذلك، قضية "السر الكبير"، وتتمثل وقائع هذه القضية فيما حدث في أعقاب وفاة الرئيس الفرنسي "ميتران" سنة 1996، فبعد أيام من وفاته نشر طبيبه الخاص مذكراته التي تتكون من 190 صفحة وسمّاها السر الكبير، وقد تناولت المذكرات أسرار فاضحة عن حياة الرئيس الشخصية وعلاقته الجنسية[1].

وعندما علمت عائلة الرئيس "ميتران" بإقدام طبيبه على نشر المذكرات، رفعت دعوى ضده أمام القضاء الفرنسي، الذي أمر بمنع نشر المذكرات استنادا إلى أن ما تحتويه يعد انتهاكا للحق في الخصوصية. وتنفيذا لهذا الأمر تمّ سحب المذكرات قبل أن تطرح في السوق.

ولكن، ما حدث بعد ذلك أنّ أحد أصحاب مقاهي الأنترنت في فرنسا تحصل على نسخة من المذكرات، وقام بتحويلها إلى مصنف رقمي أخذ شكل ملف إلكتروني، ووضعه على موقع للأنترنت من جهاز حاسوب في فرنسا. وبعد مدة قصيرة أزال هذا الشخص الملف الذي يحتوي على المذكرات من الموقع خشية تعرضه للبطش والتنكيل من عائلة "ميتران".

لكن، سرعان ما ظهرت المذكرات في مواقع أخرى على شبكة الأنترنت، إذ نسخها بعض مستعملي الشبكة أثناء الفترة القصيرة التي أتيحت فيها على الشبكة، حيث تم بثها من مواقع أخرى خارج فرنسا كائنة في كندا والولايات المتحدة الأمريكية وإنجلترا.

المبحث الثاني: الحقوق المالية للمؤلف على شبكة الأنترنت

تقوم جميع التشريعات المنظمة لحقوق الملكية الفكرية خاصة في شقها المتعلق بالملكية الأدبية و الفنية على تكريس مبدأ رئيس مفاده بأنه يحق للمؤلف الحصول مقابل مالي نتيجة انتفاع الجمهور بإبداعه ، وقد ورد النص على هذه الحقوق بموجب المادة 27 من الأمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، والذي حدد أهم الخصائص التي

[1] Arrêt de la Cour Européenne de droits l'homme dans l'affaire Plon contre la famille Mittérand, disponible sur:[http://www.denistouret.fr/eurodroits/affaire_Gubler.html], consulté le 30/10/2010.

تقوم عليها هاته الحقوق منها أنها يمكن التصرف فيها والحجز عليها ناهيك عن طابعها المؤقت وقابليتها للانتقال إلى الورثة .[1]

ويتجلى من نص المادة المشار إليه أعلاه أن مدلول الحقوق المادية ينصرف إلى منح صاحبها المبدع امتيازات ذات طابع مالي، تتمثل في إمكانية نقل المصنف بطريق غير مباشر عن طريق نسخ صور منه (الحق في الاستنساخ) ، و كذا حقه في نقل المصنف بطريق غير مباشر عن طريق الأداء العلني.[2]

المطلب الأول: الحق في الاستنساخ . le droit de reproduction

مقتضى الحق في الاستنساخ هو إمكانية نقل المصنف في شكله الأصلي أو المعدل بفضل التثبيت المادي له على أية دعامة أو بكل وسيلة تسمح بإبلاغه و بالحصول على نسخة أو أكثر من كامل المصنف أو جزء منه ، أو كما عرفه المشرع الفرنسي في نص المادة ل 3.122" التثبيت المادي للمصنف بكل طريقة تسمح بنقله إلى الجمهور بطريقة غير مباشرة ".[3]

يتمثل الاستنساخ غير المشروع للمصنف في نشر مصنف محمي عبر أجهزة الحاسب أو شبكة الانترنت أو غيرها من الوسائل دون إذن مسبق من المؤلف، وتسمى هذه الجريمة بالمساس بحق الاستنساخ، وهو بدوره يأخذ عدة صور على الأنترنت وهي:

أ- ترقيم المصنفات المحمية:

إنّ الفقه والقضاء الجزائريين لم يدرسا هذا الأمر، وبالرجوع إلى الاجتهاد القضائي الفرنسي نجده أعتبر ترقيم المصنف يشكل فعل استنساخ. وأوّل قضية عرضت عليه في هذا

---

1. بالنسبة لخاصية التأقيت في حقوق المؤلف المادية فمفادها بأن الحماية لهذه الحقوق تعطي للمؤلف طوال حياته ، و لفائدة ذوي حقوقه من بعده لمدة زمنية قدرها 50 سنة إبتداءا من مطلع السنة المادية التي تلي وفاته بحسب نص المادة 55 من الآمر 05.03.

[2].عبد الرزاق السنهوري ، الوسيط في شرح القانون المدني الجديد (حق الملكية، مع شرح مفصل للأشياء و الأموال)
، منشورات الحلبي الحقوقية ، بيروت ، لبنان طبعة 2000 ص362361 ، فرحة صالح زراوي ، الكامل في القانون التجاري ، الحقوق الفكرية ، حقوق الملكية الصناعية و التجارية ، حقوق الملكية الأدبية و الفنية ، إبن خلدون للنشر و التوزيع ، الجزائر ، ص 52.
فضلا عن الحقوق الوارد ذكرها أعلاه هناك حق يطلق عليه الحق في التتبع(le droit de poursuit) وهو عبارة عن امتياز مالي أحدته التشريع المتعلق بحقوق المؤلف لصالحه و لصالح ورثته من بعده ليمكنهم من نسبة معينة عبارة عن حاصل عمليات إعادة بيع المصنف الأصلي و يتعلق الأمر خاصة بالنسبة لمصنفات الفنون التشكيلية ، و نظرا لكون هذا الحق لا يشهد انتهاكات عبر شبكة الانترنت أو بواسطتها ، لذا لن يتم التطرق إليه خلال هذه الدراسة .

[3].لم يعرف المشرع الجزائري الحق في الاستنساخ و إنما اقتصر في نص المادة 27 من الآمر 05.03 على عبارة " استنساخ المصنف بأية وسيلة كانت " و هو بذلك يتبني وجهة نظر اتفاقية برن التي تركت المجال مفتوحا للمؤلف في التمتع بكافة الصلاحيات في ممارسة حقه الإستئثاري بوضع عدة نسخ من المصنف .

المجال هي قضية "Jacque Brel" أين قام طلبة بترقيم أغانيه، وبعدها تم نشرها على موقعهم الخاص على الأنترنت وهذا دون أن يؤخذ الإذن منه1.

فجاء في حكم المحكمة الإستعجالي أن: "ترقيم المصنفات الموسيقية المحمية ووضعها في متناول جمهور متصفحي شبكة الأنترنت بدون إذن من ذوي الحقوق يشكل فعل إستنساخ"2.

ونفس الحكم جاء به الاجتهاد القضائي البلجيكي في قضية رقمت فيها مقالات صحفية ووضعت على قاعدة بيانات ثم نشرت بعدها على شبكة الأنترنت دون أخذ إذن من المؤلفين أصحاب المقالات الصحفية3.

ب- استنساخ مصنف من الأنترنت على دعامة مادية (Off line):

هذه الحالة هي فرضية معاكسة للسابقة (ترقيم المصنف ووضعه على شبكة الأنترنت). فالمصنف هنا موجود على شبكة الأنترنت ويستنسخ بعدها على دعامة مادية. وهذا الفعل يشكل مساسا بحق الاستنساخ لأنه تم فيه استنساخ مصنف كان منشورا على شبكة الأنترنت، وثُبّت بعدها على دعامة مادية قد تكون ورقا أو قرصا مضغوطا (CD ROM). لذلك يجب أن يؤخذ إذن من المؤلف.

وتجدر الإشارة هنا، أنّ إرادة المؤلف ليست ضرورية إذا كان الاستنساخ للاستعمال الخاص والذّي يشكل بدوره استثناء النسخة الخاصة، أو كان لأهداف التعليم أو البحث العلمي. ولكن لا يوجد ما يمنع أن يقوم هذا الشخص بطبع العديد من النسخ والتصرف فيها ببيعها أو إهدائها إلى الغير بمجرد الضغط على كبسة واحدة مما يؤثر على حقوق المؤلفين.

فعلى شبكة الأنترنت، يكثر استنساخ المؤلفات الموسيقية سواء أكانت مصحوبة أو غير مصحوبة بكلام، وأدت الشبكة إلى انتشار كبير للمواقع المتخصصة في نشر المؤلفات السمعية والبصرية وذلك بسبب استخدام تقنيات مبتكرة في تكثيف (ضغط) الملفات الموسيقية وتخزينها وتبادل الآلاف منها عن بعد.

إن تقنية "mp3" و"mp4"، هما من التكنولوجيات التي ساهمت في نسخ الموسيقى من شبكة الأنترنت بشكل غير مشروع، إذ تمتاز على الحفاظ على الجودة العالية للتسجيلات

1 TGI Paris, réf, 14 Août 1996, D 1996, p 90.

2 André Kerever, Droit d'auteur et Internet, Bull de droit d'auteur, 1997, N°3, p 40.

3 Trib, 1ère instance, Bruxelles, 16 Oct 1996, Rida Avril 1997, p 238.

الصوتية، وقد تم إدانة مزودي الخدمة لقيامهم بتوفير هذه التقنيات، حيث اعتبروا ماسين بحق الاستنساخ1.

كما أنه ظهرت العديد من التقنيات والبرمجيات التي تسهل تحميل الأفلام والقطع الموسيقية وحتى مقاطع فيديو عن بعد، والتي طرحت مشكلة فيما يخص حماية هذه المصنفات، ومن بينها برنامج "Naster" سنة 1999، وهو برنامج قادر على شحن الموسيقى والأغاني عن بعد، ويمكن الإحتفاظ بها داخل ملفات "mp3". وهو يشبه كثيرا تقنية "البلوتوت" في الهواتف المحمولة والحواسيب المحمولة. ويوزع مجانا عبر شبكة الأنترنت ويتضمن فهرسا بعناوين ملايين الأغاني التي تظهر على شاشة الحاسوب مجرد أن يتصل بواحدة من المكتبات الموسيقية الإلكترونية الموصولة بشبكة الأنترنت.

يشكل هذا العمل تعدي على حقوق المؤلف والموزع، خاصة في شقه المالي مما إستدعى ضرورة حماية هذه المصنفات خاصة في هذا الفضاء الرقمي الافتراضي.

ج- إستنساخ مصنف من الأنترنت في إطار موقع آخر من الأنترنت:

هذه الفرضية تكون في حالة ما إذا كان الموقع يشتمل على مصنفات محمية بموجب قانون حق المؤلف، كتاب مثلا، فيقوم مستعمل الأنترنت بإعادة نشره على موقع آخر من شبكة الأنترنت -يكون عادة خاص به-، ويعتبر هذا الفعل أنه استنساخ ما دام أن المصنف في ذاكرة حاسوب المستنسخ.

وأكدت المعاهدة العالمية للملكية الفكرية بشأن حق المؤلف في مادتها 08 على ما سبق، وحثّت المؤلفين على أن يمنعوا إيصال مصنفاتهم إلى الجمهور دون أخذ إذن منهم.

وهكذا يكون نشر المصنفات المحمية على شبكة الأنترنت يؤدي إلى إيصالها إلى جمهور مستعملي الأنترنت، والذين يشكلون أفرادا متواجدين في كل أقطار العالم.

إن نشر المصنفات المحمية على شبكة الأنترنت فعل يتطلب أخذ الإذن من مالكي الحقوق على هذه المصنفات، وأنّ هذا التصرف يشكل مساس بالحق المالي للمؤلف، وبالتالي المساس بحق الإستنساخ وحق إيصال المصنف إلى الجمهور[2].

المطلب2 : الحق في إبلاغ المصنف إلى الجمهور

---

1 عطوي مليكة، الحماية القانونية لحقوق الملكية الفكرية على شبكة الأنترنت، أطروحة لنيل درجة دكتوراة في علوم الإعلام والإتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر، 2010، ص245.

[2] Alain bensoussan , Internet aspect juridique,2ème édition, éd Hermès , Paris, 1998. p99.

يعرّف حق التمثيل على أنّه إيصال المصنف إلى الجمهور بأي طريقة كانت[1]. وبذلك إذا اعتبرنا الموقع وسيلة اتصال فإن كل نشر للمصنفات المحمية بموجب حق المؤلف على مواقع الأنترنت بدون أخذ إذن من أصحاب الحقوق فعل يمس بهذا الحق.

وأكد على هذا المساس الاجتهاد القضائي البلجيكي في قضية نشرت فيها المقالات الصحفية المحمية بموجب قانون حق المؤلف على شبكة الأنترنت دون أن يؤخذ الإذن من مؤلفيها. فجاء في حكم محكمة بروكسل أنه: "يوجد مساس بحق الاتصال بالجمهور وهذا لأن الدخول إلى قاعدة البيانات أمر مسموح به لكل شخص متصل بشبكة الأنترنت وقام بتصفح الموقع الذي نشرت فيه المقالات الصحفية"[2].

وصدر في هذا الشأن كذلك، حكم استعجالي عن المحكمة التجارية بباريس بتاريخ 1997/03/03 قضى على أنه: "يوجد مساس بحق التمثيل بصفة واضحة عندما تم وضع برامج الإعلام الآلي على مواقع "الواب" دون أخذ الإذن من صاحبها"[3].

وبناء على ما سبق، فإن الترقيم يعتبر وسيلة من وسائل النسخ أو النشر شأنه شأن الكتابة و غيرها، بذلك فإن وضع المصنف على شبكة الأنترنت عن طريق موقع "الواب" يعتبر أداء علنياً لهذا المصنف، والنشر والأداء يستلزمان الحصول على إذن المؤلف بالنشر والأداء العلني. ولكن يلاحظ أحياناً أن المؤلف يلجأ إلى وضع المصنف تحت تصرف الجمهور من خلال الأنترنت "Free ware"، هو بهذا يتنازل عن حقه المالي مقابل ما يحصل عليه أدبياً من انتشار مصنفه عبر العالم[4].

إن طرق النشر الإلكترونية - خاصة الرقمية منها - قد تكون سببا في الحد من الحق المالي للمؤلف، إذ أن ما يجنيه الناشر الإلكتروني من أرباح يتجاوز بكثير ما يجنيه المؤلف، كما لا يوجد أي ضابط قانوني فعال يمنع من قيام الناشر باستغلال مصنف لم يرخص باستعماله.

لقد أثرت التقنية الحديثة ليس فقط على وسيلة العرض على الجمهور من خلال الشبكة ، و إنما أيضا على مفهوم الجمهور نفسه ، فلم يعد مفهوما تقليديا يشير إلى أولئك الأشخاص المجتمعين في مكان واحد و قد عرض المؤلف لمصنفه عليهم ، بل تغير بفعل البيئة الرقمية

---

[1] Mirielle Buydens, Op.cit, p 40.

[2] Trib, 1ère instance, Bruxelles, 16 Oct 1996, Rida, Avril, 1997, p 2.

[3] Trib. com. Ord. réf. 3 Mars 1997, JCP (G), II, 22 840, note. Frédérique Olivier.

[4] حسام الدين الأهواني، المرجع السابق، ص 17.

ليشمل أشخاصا متواجدين في أماكن مختلفة و في أزمنة متفرقة ، عبر مختلف أنحاء العالم .**الخاتمة** :

سهلت تكنولوجيا الأنترنت توزيع نسخ مصنفات المؤلفين بطرق غير مكلفة وملائمة إلى عدد كبير من الجمهور .غير أنها شكلت في نفس الوقت تهديدات حقيقية بروح الإبداع والمبادرة، هذا التطور قابله نمو مذهل لأنظمة القراصنة، وتطور آلات النشر والطبع والنسخ، والتحميل غير المشروع للمصنفات المحمية. كما قابله نمو مخيف لنشاطات التقليد والتزييف والسرقات الأدبية.

فقد فرضت هذه التطورات سهولة في الإعتداء على حقوق المؤلف المعنوية كالحق في الكشف عن المصنف، والحق في أبوة المصنف، والحق في السلامة المصنف، والحق في ممارسة حق التوبة وسحب المصنف من التداول، وبذلك يمكن القول أن الحقوق المعنوية للمؤلف لا تطبق على شبكة الأنترنت.

إن الأمر لا يختلف بالنسبة للحقوق المالية للمؤلف التي أصبحت مهددة على شبكة الأنترنت بسبب التحميل غير المشروع للمصنفات، والنشر غير المشروع لها دون رضا المؤلف صاحب المصنف، الأمر الذي يمس بحق الإستنساخ وحق التمثيل. ويحرم فيه المؤلف من ثمرة جهده والسماح للقرصنة من سرقة ذلك الجهد أو استغلاله غير المشروع.

ولقد جاءت هذه الدراسة بالتوصيات التالية:

–نشر الوعي بحقوق المؤلف في المحيط الرقمي للمؤلفين ومستخدمي شبكة الأنترنت.

- تنظيم دورات تكوينية في مجال التكنولوجيا لسلك العدالة والقضاء والأجهزة المختصة.

-ضرورة تطوير التشريعات المتعلقة بحقوق المؤلف بما يواكب مستجدات العصر ووجوب التعاون بين الدول العربية والإسلامية، واستحداث مؤسسات علمية متخصصة تحمي الأعمال في نطاق منظومة تكنولوجيا المعلومات والاتصال من التقليد أو السرقة بشتى صورها.

-تدريس مادة الملكية الفكرية في جميع الجامعات لإبراز أهميتها، وتبيان العقوبات المقررة للاعتداءات عليها.

-تشديد العقوبات في حالة إنتهاك حقوق المؤلف على شبكة الأنترنت.

-تعزيز الحماية القانونية للمؤلف بحماية تقنية لها، معاقبة المنتهكين على الحماية التقنية.

-ايجاد أنظمة عربية موحدة تتبنى وضع تدابير تقنية تمنع وتجرم التحايل عليها لحماية حقوق المؤلف في هذه الشبكة الرقمية.

-تفعيل الأقطاب المتخصصة في مجال الملكية الفكرية.

قائمة المراجع باللغة العربية :

أ-**الكتب**:

- محمد حسنين ، الوجيز في الملكية الفكرية ، المؤسسة الوطنية للنشر و الكتاب ، الجزائر ، بدون طبعة.

- رامي ابراهيم حسن الزواهرة، النشر الرقمي للمصنفات وأثره على الحقوق الأدبية والمالية للمؤلف: دراسة مقارنة في القوانين الأردني والمصري والإنجليزي، دار وائل للنشر، عمان، الأردن، 2013.

-خالد ممدوح إبراهيم، جرائم التعدي على حقوق الملكية الفكرية، الدار الجامعية، الإسكندرية، مصر، 2010.

-عبد الرزاق السنهوري ، الوسيط في شرح القانون المدني الجديد (حق الملكية، مع شرح مفصل للأشياء و الأموال) ، منشورات الحلبي الحقوقية ، بيروت ، لبنان طبعة 2000 .

-نواف كنعان، حق المؤلف (النماذج المعاصرة لحق المؤلف ووسائل حمايته) دار الثقافة للنشر و التوزيع، الأردن ، الطبعة الأولى ،2009.

ب-المقالات:

- حسام الدين كامل الأهواني، "الأنترنيت كوسيلة للإستغلال المصنفات وحقوق المؤلف"، متاح على الموقع: [http://www.alecso.org.tn/images/stories/fichiers/thakafa/01H_Ahwani.pdf].

- نصير صبار لفته، "أثار عقد التأليف"، مجلة القانون المقارن، ع 42، 2006، العراق

ج-الرسائل الجامعية:

-عطوي مليكة، الحماية القانونية لحقوق الملكية الفكرية على شبكة الأنترنت، أطروحة لنيل درجة دكتوراة في علوم الإعلام والإتصال، كلية العلوم السياسية والإعلام، جامعة الجزائر، 2010.

قائمة المراجع باللغة الفرنسية

-Mirielle Buydens, Droits d'auteurs et Internet: Problèmes et solutions pour la création d'une base de données en ligne contenant des images ou, texte,

Université catholique de lonvain, Faculté de droit, Belgique, 2001, disponible sur : [http://www.droit-technologique.org], la dernière consultation le : 28/12/2007,
-Jolie Jacob et Benjamin Jacob, "Les enjeux de la musique numérique", Petites affiches, 1999, N° 242, p 8.
-André Kerever, Droit d'auteur et Internet, Bull de droit d'auteur, 1997, N°3, p 40.
-Alain bensoussan,Internet aspect juridique,2ème édition, éd Hermès , Paris, 1998. p99.

التعليم الرقمي
أي مصير للحق في التعليم في ظل الرقمنة

digital education
What is the fate of the right to education in light of digitalization

د. بوثلجي أمينة ،أستاذة مؤقتة
كلية الحقوق ،جامعة الجزائر-1-
BOUTELDJI_AMINA@hotmail.com

د. كروش نعيمة ، أستاذة محاضرة
كلية الحقوق جامعة الجزائر-1-
kerouchenaima@gmail.com

الملخص :

التعليم الرقمي نمط من أنماط التعليم المستحدثة في مجال العلوم والمعرفة باعتباره أسلوب أكثر توافقا والتطور التكنولوجي من جهة ،وكحل بديل لضمان استمرار التعليم في مختلف المؤسسات التربوية في العالم في ظل الكوفيد لضمان صحة الأفراد وتجنب انتقال العدوى ، وذلك بالاعتماد على وسائط إلكترونية تقتضي وسائل مادية وتقنية وتطرح العديد من التساؤلات بخصوص حق الإنسان في التعليم في ظل الرقمنة .

Summary :

Digital education is a type of education developed in the field of science and knowledge as a more compatible method and technological development on the one hand and as an alternative solution to ensure the continuity of education in various educational institutions in the world in light of the covid-19 to ensure the health of individuals and avoid transmission of infection, by relying on electronic media that require physical and technical means and introduce Many questions regarding the human right to education in light of digitalization.

الكلمات المفتاحية :

التعليم الرقمي ، الوسائط الإلكترونية ، حق الإنسان في التعليم .

key words :

Digital education, electronic media, the human right to education.

مقدمة :

الحق في التعليم أحد الحقوق المهمة ضمن السلسلة القانونية لحقوق الإنسان لدوره الكبير في التطلع لمختلف الحقوق والتمتع بها ، والذي حضي بإجماع النصوص والصكوك الدولية لحقوق الإنسان بالنص على حق الفرد في التعليم ،وفرض التزام الدول بتجسيده ضمن سياساتها التشريعية من خلال عملها على إتاحة فرص التعليم للجميع تبعا لما تفتضيه إمكانياتها ،إذ عملت العديد منها على تطوير سبل التعليم انتقالا من التعليم النظامي الحضوري إلى التعليم الرقمي ، فلقد تزايد الإقبال في السنوات الأخيرة خاصة على البيئة الرقمية في التحصيل العلمي ، باستعمال وسائل ووسائط التواصل الإلكترونية ، وذلك في إطار متطلبات ودوافع تعددت مبرراتها منها ما صنف ضمن مبررا ت مواكبة التطور التكنولوجي وتحسين مستوى التعليم ، ومنها ما فرضته الجائحة الأخير التي عرفها العالم " جائحة الكوفيد- 19، إذ في إطار تطبيق التدابير الصحية لمنع انتشار جائحة الكوفيد اعتمد التعليم عن بعد كأحد الحلول المثلى لتعميم الحق في التعليم ، و هو ما حقق نقلة نوعية في الانتقال بالحق في التعليم من الأسلوب العادي البسيط إلى تعليم رقمي يفرض ضرورة توفير ميزانية خاصة لاقتناء بعض الأدوات الخاصة من حاسوب وغيرها ، وضرورة إتقان الكثير من الجوانب التقنية للولوج إلى منصات التعليم الرقمية ، وهو يطرح العديد من التساؤلات بخصوص التعليم المجاني وإتاحة الحق في التعليم وتعميمه وفقا لما تكرسه الصكوك الدولية لحقوق الإنسان ،و الدساتير والتشريعات الوطنية ، و مصير الحق في التعليم في ظل رقمنة قطاع التعليم ؟

وهو ما يتم معالجته من خلال :

المبحث الأول: طبيعة وخصائص التعليم الرقمي

المبحث الثاني : مصيرحق الإنسان في التعليم في ظل التوجه نحو رقمنة قطاع التعليم

المبحث الأول: طبيعة وخصائص التعليم الرقمي

لم يقتصر التطور التكنولوجي على مجالات محددة من حياة الإنسان إنما امتد بدوره إلى قطاع التعليم ، حيث تزايد الإقبال في السنوات الأخيرة على التعليم الرقمي ضمن متطلبات متعددة منها تحسين جودة التعليم ومواكبة التطور التكنولوجي (المطلب الأول) ، ولخصوصيته في ضمان سرعة نشر المعرفة دون تكلفة (المطلب الثاني) .

المطلب الأول : المقصود بالتعليم الرقمي

التعليم الرقمي واحد من الأنماط التعليمية الحديثة التي أصبحت أكثر اعتمادا في العصر الحالي(الفرع الأول) ، بالنظر إلى خصوصيته للاستجابة إلى التطور التكنولوجي وكأحد الحلول المهمة التي اعتمدت خلال الأزمات الصحية كتلك الخاصة بجائحة الكوفيد19 (الفرع الثاني)

الفرع الأول: تعريف التعليم الرقمي

انتشر التعليم الرقمي في العصر الحالي ضمن تسميات متعددة منها : التعليم الإلكتروني ، التعليم عن بعد وغيرها ، تعددت أساليب ومحتوى تعريفه من بين أهم ه ذه التعاريف ذكر بأنه : " تقديم للمتعلم محتوى تعليمي عبر الوسائط المعتمدة على الأجهزة الذكية، يمكنه من التواصل مع غيره في أي مكان وزمان من دون اشتراط الحضور المادي أو تحديد زماني "[1]، كما عرف بالنظر إلى الوسائط الرقمية المستعملة على أنه :" طريقة للتعليم باستعمال آليات الاتصال الحديثة من حاسوب و شبكاته ووسائطه المتعددة من صوت وصورة ورسومات وآليات بحث ومكتبات إلكترونية عن بعد أو في القاعة الدراسية باستعمال التقنية بأنواعها [2]، وهو كذلك :" طريق للتعليم باستعمال آليات التعليم الحديثة من حاسوب ، وشبكة ، ووسائط وغيرها .."[3]

الفرع الثاني : خصائص التعليم الرقمي:

للتعليم الرقمي جملة من الخصائص التي تميزه عن التعليم الحضوري أو التعليم العادي لما يوفره من ضمان جودة وسرعة نشر العلم والمعرفة على نطاق واسع من المتعلمين، وذلك في ظل الإتاحة المادية للوسائط الإلكترونية و الأجهزة الذكية، من ضمن هذه الخصائص يمكن ذكر منها :

أولا – نشر وتحقيق لا مركزية التعليم دون اشتراط الحضور المادي للمتعلم : يسمح التعليم الرقمي وصول العلم والمعرفة إلى جمهور واسع من المتعلمين أو من يرغبون في ذلك أينما تواجدوا ،و متى سمحت شبكة التواصل والأنترنت ، من دون اشتراط الحضور المادي للمتعلم مقارنة لنمط التعليم السابق الذي أضحى يعرف بالتعليم التقليدي ، إذ يتلقى هذا الأخير العلم والمعرفة أينما تواجد بمجرد تواصله بمنصة تعليمة تزوده بها مؤسسة من مؤسسات التعليم الافتراضية منها أو العادية ، كما يعفي بعض الفئات المحرومة من التنقل إلى المدارس والمؤسسات النظامية كالمرضى المتواجدون في المستشفيات والمحرومون من الالتحاق بها كالمتواجدون بالسجون والمناطق النائية وغيرها .

ثانيا- تعميم التعليم الرقمي لمجابهة أزمة الكوفيد : ظهر التعليم الرقمي كأحد الحلول المهمة لتعميم التعليم على مستويات متنوعة وذلك لمجابهة العديد من الأزمات الصحية كأزمة الإيبولا و خصوصا خلال الثلاث السنوات الأخيرة بسبب انتشار أزمة الكورونا [4]،وذلك لحماية الأفراد من انتقال وانتشار المرض ، إذ اعتمدت دولا عديدة انماطا بديلة للتعليم الحضوري ، وبدور ها لجأت الجزائر إلى التعليم عن بعد لضمان استمرارية التعليم وديمومته بموجب القرار الوزاري رقم 915 المؤرخ في 11 أوت 2021. والذي يحدد الأحكام الاستثنائية المرخص بها في مجال التنظيم والتسيير البيداغوجي في ظل فترة جائحة الكوفيد 19 ، و للسنة الجامعية 2021 2022 .

ثالثا- التعليم الرقمي أداة من أدوات تطوير البيئة التعليمية : يتميز التعليم الرقمي بكونه أداة مهمة من أدوات تطوير المجال العلمي والمعرفي لاعتماده على أدوات تساهم بشكل كثير في تسهيل وسرعة الحصول على المعلومات العلمية من جهة ، و إنجاز البحوث العلمية من جهة أخرى[5].

المطلب الثاني: أدوات التعليم الرقمي

يختلف أسلوب ونظام التعليم الرقمي عن التعليم الحضوري في اعتماده على أدوات ووسائط إلكترونية (الفرع الأول) ، تتضمن مناهج تربوية وتعليمية ترد ضمن هذه الوسائط الإلكترونية (الفرع الثاني)

الفرع الأول : اعتماد التعليم الرقمي على أجهزة وسائط إلكترونية:

يعتمد التعليم الرقمي على أدوات وأجهزة ذكية تعرف بالوسائط الإلكترونية تختلف أنواعها وطاقتها في تخزين ونقل المحتوى الرقمي للبرامج التعليمية من حاسوب، وهواتف ذكية وغيرها ، وعلى الرغم من أن هذه الأجهزة أصبحت جد متطورة ومنتشرة بين الشرائح الاجتماعية المختلفة إلا أنها معقدة نوعا ما بالنسبة لغير المتعود لها ، وتقتضي من المتعلم ضرورة إتقان بعض نظم عملها بخصوص البرامج التعليمية . من الأدوات المعتمدة في هذا الإطار يعد جهاز الحاسوب وشبكة الأنترنت [6]حجر الزاوية في التعليم الرقمي ، إذ دون حاسوب لا يمكن ربط التواصل مع أي منصة خاصة في ظل انعدام شبكة الأنترنت أو ضعف تدفقها ، فضلا عن هذه الأدوات خدمة البريد لتحقيق التواصل بين المعلم والمتعلم ، ولا يقتصر الأمر على هذا وحسب إنما يشهد الواقع الرقمي اليوم انتشارا واسعا للكتاب الإلكتروني الذي يتم اقتناؤه وتصفحه وفقا لبروتوكول تحدده المنصة التعليمية الرقمية .

الفرع الثاني : اعتماد المناهج الدراسية على الوسائط الإلكترونية

يختلف التعليم الرقمي في أدواته عن نمط التعليم التقليدي وذلك لعرض محتواه المعروف بالمنهج الدراسي ضمن بيئة رقمية و على وسائط وأدوات إلكترونية أدت إلى تصميم المناهج الدراسية وفقا لمحتوى رقمي جعل من المعلم والمتعلم محصور ضمن جملة من المسائل الفنية والتقنية أصبح أكثر انشغالا بها عن محتوى ومضمون المناهج التربوية والتعليمية ، إذ كثيرا ما تعترض عملية عرض الدرس الانقطاع التقني لشبكة الأنترنت ،أو ضبط لوحة التفاعل وغيرها . تقتضي هذه الوسائط من المعلم بالدرجة الأولى ضرورة بدل المزيد والكثير من المهارات في عرض محتوى المناهج التعليمية المدمجة ضمن الأسطوانات أو المعروضة على صفحات الواب أو المواقع الإلكترونية ،وخاصة بالنسبة للمناهج التقنية نظرا لعنصر التواصل غير المباشر، أو التواجد عن بعد بين المعلم والمتعلم والذي يؤثر بدوره على حق الإنسان في الحصول على العلم أو في إتاحته وتعميمه ، إذ قد يتعذر على الفرد حل هذه المشاكل الرقمية خلال متابعته للدرس الرقمي ، نظرا لكون المدرس أو الأستاذ في ظل هذه البيئة التعليمية الرقمية ليس مختص في هذه الجوانب التقنية ، بل حتى أنه لم يساهم في وضع هذه المناهج في شكل رقمي مما يقتضي ضرورة تكوينه التقني ومساهمته في إعداد محتوى البرامج التعليمية الرقمية.[7]

المبحث الثاني : مصيرحق الإنسان في التعليم في ظل التوجه نحو رقمنة قطاع التعليم

الحق في التعليم حق من الحقوق المكفولة للإنسان بموجب الصكوك والنصوص القانونية الدولية نظرا لدوره المهم في التطلع للتمتع بحقوق الإنسان الأخرى لذا اكدت النصوص والوثائق الدولية على ضرورة العمل على تجسيد هذا الحق وترقيته (المطلب الأول) و ضرورة الإتاحة المادية لهذه الأدوات وتعلم استعمالها تجسيدا لحق الإنسان في التعليم أيا كان نوعه والتعليم الرقمي يرتبط بضرورة إتقان نظم عمل الوسائط الإلكترونية و المنصات الرقمية التي تعرض البرامج التعليمية ضمنها والتي تختلف عن تلك التي اعتمدها المعلم والأستاذ والطالب والتلميذ في مراحل تعليمه السابقة (المطلب الثاني)

المطلب الأول : حق الإنسان في التعليم في النصوص والبرامج الدولية

الحق في التعليم من الحقوق التي حضيت بمكانة هامة في مختلف الصكوك والنصوص الدولية سواء تلك الخاصة بحقوق الإنسان نظرا لكونه مقوما أساسيا لبناء

شخصية الإنسان [8] (الفرع الأول) ،أو البرامج الدولية كبرنامج التنمية المستدامة (الفرع الثاني)

الفرع الأول : حق الإنسان في التعليم في الصكوك الدولية لحقوق الإنسان والقانون الدولي الإنساني

حضي الحق في التعليم باهتمام واسع ضمن النصوص والصكوك الدولية ، التي أجمعت في مضمونها على ضرورة تكريس هذا الحق في كل الأحوال ومختلف الظروف ،إذ لم تقتصر على الدول الغنية منها دون الفقيرة ، ولا على المستقرة منها دون تلك التي تشهد حروبا ونزاعات ، بل أكدت على استمرار تعزيز الحق في التعليم حتى في أماكن النزاعات المسلحة ، فلق نصت مختلف الصكوك الدولية لحقوق الإنسان على حق الفرد في التعليم العالمية منها والإقليمية العربية والأوروبية ، إذ نص الإعلان العالمي لحقوق الإنسان لسنة 1948 [9] في المادة السادسة والعشرون منه على :" لكلِّ شخص حقٌّ في التعليم. ويجب أن يُوفَّر التعليمُ مجَّانًا، على الأقل في مرحلتيه الابتدائية والأساسية. ويكون التعليمُ الابتدائيُّ إلزاميًّا. ويكون التعليمُ الفنِّي والمهني متاحًا للعموم. ويكون التعليمُ العالي مُتاحًا للجميع تبعًا لكفاءتهم " ،كما نص العهد الدولي الخاص بالحقوق الاقتصادية والإجتماعية في المادة الثالثة عشر منه الفقرة الأولى [10] على أن :" لكل فرد الحق في التربية والتعليم "، و أكدت هذه المواد على ضرورة الالتزام الفعلي للدول بالتجسيد العملي لهذا الحق من خلال التزامها بتعميم هذا الحق وإتاحته ومجانتيه بالنسبة للمراحل الأولى من التعليم ، حيث أكدت المادة السادسة والعشرون من الإعلان العالمي لحقوق الإنسان على إلزامية التعليم الابتدائي وضرورة توفيره في مرحلتي التعليم الابتدائي والمتوسط ، أما بالنسبة للتعليم العالي فقد أكدت على إتاحته تبعا لكفاءات الأفراد . وبخصوص النصوص والصكوك الإقليمية لحقوق الإنسان فلقد نص الميثاق الإفريقي لحقوق الإنسان في المادة السابعة عشر منه على حق الإنسان في التعليم وعلى ضرورة اعتماد مناهج تربوية لتعزيز وحماية التربية الأخلاقية [11]، وأكد بدوره الميثاق الأوروبي في نص المادة الأولى منه على حق التعليم من خلال منح الأولياء حق حرية الوالدين في تعليم أولادهم القيم والمعتقدات .

لم يقتصر التكريس القانوني على حق التعليم وإتاحته للفرد على حالة السلم وحسب إنما أولته الصكوك الدولية اهتماما حتى في حال النزاعات المسلحة لمخلفات وأثار الحروب على التمدرس ،وتدمير المدارس ، إذ أكدت اتفاقيات جنيف وملاحقها على ضرورة حماية الأعيان

المدنية والمدارس. إذ نصت المادة الثامنة والثلاثين من اتفاقية جنيف على : " مع مراعاة الافضليات الشخصية لكل أسير ، تشجع الدولة الحاجزة الأسرى على ممارسة الأنشطة الذهنية والتعليمية .."[12]

الفرع الثاني : حق الإنسان في التعليم في في برنامج التنمية المستدامة

لم يعد الحق في التعليم مرتبط بإقرار وتجسيد حقوق الإنسان وحسب ،بل أصبح محورا هاما من محاور التنمية المستدامة ، حيث أدرج ضمن الهدف الرابع من تلك المسطرة للتنمية دور التعليم في تحقيق التنمية . والذي يرتكز على جملة من المقومات الأساسية منها تحفيز الأفراد على العيش السليم والمستدام ، وذلك من خلال إدراج هذه القيم ضمن المناهج التربوية والتعليمية ،وفي هذا الإطار حددت منظمة الثقافة والعلوم اليونسكو جملة من الأسس الوجوب اعتمادها من طرف المتعلم وفي نظم التعليم لتحقيق جودة قطاع التعليم منها : الوصول إلى المتعلم ، قدرات المعلم، البيئة التعليمية وغيرها[13] . ولقد أكدت الجمعية العامة للأمم المتحدة إطار احتفال منظمة الأمم المتحدة باليوم الدولي للتعليم سنة2019 بموجب القرار رقم (25/73) في الجلسة العامة الرابعة والاربعون على اهمية التعليم في تحقيق التنمية المستدامة لما له من دور اساسي في بناء مجتمعات مستدامة و على دوره في تحقيق اهداف التنمية المستدامة الاخرى .

المطلب الثاني: أثار رقمنة التعليم على حق التعليم وتعميمه

إن الحديث على التعليم الرقمي في زمن الرقمنة و احد من التحديات التي لا يجب الاستهانة بها، فعلى الرغم من الشغف وتزايد الإقبال على الأدوات والوسائط الإلكترونية للأفراد إلا أن مسألة التعليم تكتنفها بعض المعوقات التي تتعارض مع الحق في التعليم لما يفرض التعليم الرقمي من ضرورة الإتقان لنظم ووسائط التعليم الرقمي (الفرع الأول) فضلا على ذلك ضرورة الإتاحة المادية لأدوات التعليم الرقمي(الفرع الثاني)

الفرع الأول : المعوقات التقنية لتعميم و إتاحة التعليم الرقمي

يصطدم التعليم الرقمي في بعض جوانبه التقنية مع قواعد أساسية يرتكز عليها حق الإنسان في التعليم وهي الحق في التعليم المجاني والحق في تعميم التعليم على حسب المراحل العمرية للفرد ، فعلى الرغم من أن الصكوك الدولية لحقوق الإنسان وفقا لما سبق ذكره تفرض على الدول ضرورة اتخاذ التدابير اللازمة لتجسيد ذلك تعترض الطبيعة التقنية

للتعليم الرقمي من جهة ، و المتطلبات المادية من جهة أخرى قدرات إتاحة وتعميم الحق في التعليم للجميع ، لأسباب عديدة ، فقد يعتقد البعض أن مجرد تخصيص وسائط وإنشاء منصات للتعليم يحقق تعليم الأفراد ، بالفعل يسهم التعليم الرقمي في تطوير وعصرنة قطاع التعليم في ظل تعزيز وتعميم وتكوين المعلمين والأساتذة ، بل وحتى الطلبة الجامعيين، والتكوين لا يقتصر على هذا المستوى وحسب إنما يقتضي ضرورة تلقين المتمدرسون مختلف التقنيات الرقمية [14] الخاصة بالولوج للمنصات الرقمية ، وسبل التعامل مع المحتوى الرقمي للدروس المنشورة عبرها فضلا عن ذلك سبل التواصل مع المؤسسات التعليمية عبر أجهزة الحاسوب ومن خلال شبكة الأنترنت .

الفرع الثاني : المتطلبات الخاصة بالإتاحة المادية لأدوات ووسائل التعليم الرقمي

على الرغم من التقدم التكنولوجي الذي يعرفه الإنسان المعاصر لاتزال دول عديدة خاصة النامية منها والإفريقية تواجه صعوبات عديدة في تمكين مختلف الأفراد في الاستفادة من حقهم في التعليم ، خاصة في مايشهده الواقع الدولي من عدم إلتحاق العديد من الأطفال في العالم بالمدارس النظامية لأسباب وظروف متباينة منها الفقر والنزاعات المسلحة فحسب الإحصائيات الأخيرة لسنة 2021 ما يزال 258 مليون طفل وشاب غير ملتحقين بالمدارس،و 617 مليون طفل ومراهق لا يستطيعون القراءة والكتابة. وحوالي ما يقرب من 265 مليون طفل ومراهق في العالم لا تتاح لهم الفرصة للدراسة أو حتى إكمالها ، وبلغت نسبة الالتحاق بالتعليم الابتدائي في البلدان النامية 91%، فضلا عن ذلك تعرف عديد الدول الإفريقية و المناطق المتضررة من النزاعات عدم التحاق الأطفال في هذه المناطق بالمدارس وهو ما يعني انتهاك الحق في التعليم ، والذي ما اعتبرته منظمة الأمم المتحدة إخلال في إتاحة فرص تعليمة شاملة ومتساوية في التعليم الجيد للجميع. في ظل هذه الإحصائيات والمعطيات يتبادر التساؤل حول كيفية الانتقال إلى التعليم الرقمي في هذه الدول في ظل غياب أو تعدر تجسيد حق الفرد في التعليم ، إن التعليم الرقمي يقتضي بالضرورة توفير وإتاحة مختلف الأدوات والوسائط الإلكترونية من أجهزة وحواسيب وشبكة أنترنت وتعميم استعمالها بين مختلف الشرائح من متمدرسين ومتعلمين ليرتقي نظام التعليم الرقمي ويتحقق حق الإنسان في التعليم في البيئة الرقمية .

الخاتمة :

يعد الانتقال إلى التعليم الرقمي تحول نوعي مهم لمواكبة التطور التكنولوجي الذي أدى بدوره إلى تطور أدوات ووسائط التعليم سمحت بتجاوز بعض العقبات المهمة التي شهدها التعليم الرقمي بخصوص تواصل الأفراد والراغبين في التعليم المتواجدين في مناطق نائية أو معزولة ، وكذلك بالنسبة لؤلائك المتواجدون في بعض الوضعيات الاجتماعية التي تمنعهم من التنقل للمؤسسات التعليمية كالمرضى ، بل حتى حل مهم لمجابهة الأزمات الصحية ، لكن ومع ذلك لا يجب إغفال الجوانب المهمة لمتطلبات التعليم الرقمي وما يقتضيه من وسائط وأدوات رقمية لا بد من إتاحتها للمتمدرسين والمعلمين وأساتذة وطلبة ، فضلا على ذلك ضرورة مد شبكات التواصل والأنترنت إلى أبعد المناطق حتى نتمكن من إتاحة وتحقيق حق الفرد في التعليم حتى في ظل الانتقال إلى التعليم الرقمي وعليه نقترح التوصيات التالية :

1 - ضرورة تحيين البرامج التعليمية بما يتوافق وطبيعة رقمنة التعليم

2 -ضرورة إجراء دورات تكوينية خاصة برقمنة قطاع التعليم للمعلمين والمؤطرين في مجال التعليم بمستوياته المختلفة

3 -ضرورة الإتاحة المادية للوسائط الإلكترونية التعليمية لتجسيد مجانية حق التعليم في المجال الرقمي.

الهوامش:

[1]) إياد عبد العزيز حسن ألطف :" أثر التعليم الرقمي باستخدام الأجهزة الذكية على التحصيل العلمي للطلاب في مقرر الوسائل التعليمية واتجاههم نحو استخدام الأجهزة الذكية في التعلم والتعليم " مجلة جامعة أم القرى للعلوم التربوية والنفسة ، المجلد 10، العدد 2، الجزء الأول ، رجب 1440 – أفريل 2019 ، ص 287.

[2]) عائشة بن السايح ، إسماعيل سيبوكر:" التعليم الرقمي وعوائق تطبيقه "، مقاليد، مج 7 ،عدد2 ، جمادى الأولى 1442هـ/ جانفي 2021، ص 70.

[3]) عائشة بن السايح ،إسماعيل سيبوكر، المرجع نفسه ، ص 70.

[4]) سليم مزهود :" أفاق التعليم الرقمي والإلكتروني في ظل جائحة كوفيد -19 - المشكلات والحلول- "، مجلة المداد ، ص 10.

[5])إياد عبد العزيز حسن ألطف ، المرجع السابق ذكره ، ص 284 .

[6]) ابراهيم عصمت مطاوع، واصف عزيز واصف ، التربية العلمية وأسس طرق التدريس ، دار النهضة العربية للطباعة والنشر، بيروت، لبنان ،1982، ص 51-52.

[7]) عائشة بن السايح ،إسماعيل سيبوكر ، المرجع السابق ذكره ، ص 82.

[8]) فلقد ألزمت الفقرة الثانية من المادة السادسة والعشرون ضرورة أن يكون يستهدف التعليم التنميةَ الكاملةَ لشخصية الإنسان وتعزيز احترام حقوق الإنسان والحريات الأساسية. وأعتبرته غاية من الغايات الأساسية لتعزيز قيم ومبادئ التسامح والصداقة بين جميع الأمم وجميع الفئات العنصرية أو الدينية.

[9]) عائشة بن السايح ،إسماعيل سيبوكر، المرجع السابق ذكره ، ص 74.

[10]) بن يطو أسامة ، مخطار ديدوش محمد :" الحق في التعليم في المواثيق الدولية والقانون الجزائري " ، مجلة بث وتربية ، المجلد 10 ، العدد 2، ديسمبر 2021 ، ص 33.

[11]) عائشة بن السايح ،إسماعيل سيبوكر ، المرجع السابق ذكره ، ص 72.

[12])اتفاقية جنيف بشأن معاملة أسرى الحرب المؤرخة في 12 آب/ أغسطس 1949، مكتبة حقوق الإنسان جامعة مانيسوتا، أنظر الموقع : hrlibrqry.umn.edu

[13]) يونس عيسى ، عماري عائشة، ميطر عائشة :" التعليم من أجل التنمية المستدامة " ، 3 (1) EL Khaldounia journal of human Social science 13(1)2021p66

[14]) بخصوص المسألة علق العالم الأمريكي لاري كوبن عند بداية انتشار المدارس السلكية أنه : " افترض صانعو السياسة أنه بمجرد أن تصبح المدارس سلكية وتوجد المعدات في مكانها سيستخدم المعلمون والطلبة تقنيات المعلومات بانتظام في الفصول الدراسية ، وبمجرد استخدام أجهزة الكمبيوتر بانتظام في المدارس ،فْن النتائج المرجوة كما كانت متباينة ستتبع بشكل طبيعي ..." ، أنظر في ذلك سليم مزهود :" تكنولوجيا التعليم عن بعد في ظل دائحة كوفيد – 19 ، الواقع والحلول ، مجلة العلوم وآفاق المعارف ،المجلد الثاني ، العدد الأول ، 2022، ص 105.

دور التكنولوجيا الرقمية في تعزيز الحق في التنمية

The role of digital technology in promoting the right to development

شايب يمينة أستاذة محاضرة ب
جامعة الجزائر3 - الجزائر
yaminachaib123@yahoo.com

ملخص :

تهدف هذه الدراسة إلى تحديد المتطلبات والآليات المرتبطة بالتكنولوجيا الرقمية التي تساهم بشكل مباشر في تعزيز الحق في التنمية على ضوء التغير الحاصل في التكنولوجيا بشكل عام وفي التكنولوجيا الرقمية بشكل خاص والتغير السريع الذي تحدثه في نوعية حياة الإنسان وفي أثرها على خصوصيته.

وقد توصلنا من خلال هذه الدراسة إلى أنه يمكن للتكنولوجيات أن تساعد في جعل عالمنا أكثر إنصافا وأكثر سلما وأكثر عدلا. ويمكن للإنجازات الرقمية أن تدعم كل هدف من أهداف التنمية المستدامة عبر توفير جملة من الآليات من بين أهمها الشمول والتمكين والتي تستجيب لمتطلبات تعزيز الحق في التنمية.

الكلمات المفتاحية : تكنولوجيا رقمية ؛ حق في التنمية ؛ شمول ؛ تمكين؛ استدامة

Abstract:

This study aims to identify the requirements and mechanisms associated with digital technology that contribute directly to the promotion of the right to development in light of the change in technology in general and in digital technology in particular, and the rapid change it causes in the quality of human life and its impact on privacy.

Through this study, we have concluded that technologies can help make a fairer, more peaceful and more just world. Digital achievements can support each of the sustainable development goals by providing a set of mechanisms, among the most important of which are inclusion and

empowerment, that respond to the requirements of promoting the right to development.

Keywords: digital technology; right to development; inclusion; Enable; sustainability

مقدمة:

إذا كان النمو الاقتصادي يعني حدوث زيادة مستمرة في متوسط الدخل الفردي الحقيقي فهذا يعني أنه يركز على التغير في الكم الذي يحصل عليه الفرد من السلع والخدمات في المتوسط دون أن يهتم بهيكل توزيع الدخل الحقيقي بين الأفراد ونوعية السلع والخدمات التي يحصلون عليها، كما أن الزيادة في متوسط الدخل لا تعني بالضرورة زيادة دخل كل أفراد المجتمع. وعلى عكس النمو الاقتصادي فإن التنمية الاقتصادية تُعنى بحدوث تغير في هيكل توزيع الدخل وتغير في هيكل الإنتاج وتغير في نوعية السلع والخدمات المقدمة للأفراد بجانب التغير في كمية السلع والخدمات التي يحصل عليها الفرد في المتوسط، وهذا لا يعني أن التنمية الاقتصادية تركز فقط على التغير الكمي بل يمتد تركيزها ليشمل التغير النوعي.

يعتبر الحق في التنمية حقا مركبا من عدد من حقوق الإنسان المدنية والسياسية والحقوق الاقتصادية والاجتماعية والثقافية المعترف بها، حيث يعمل الحق في التنمية على إعمالها وتعزيزها، وهو في ذلك يواجه جملة من التحديات أهمها استمرارية التنمية والتي ترتبط بمدى المحافظة على الموارد وكذلك التقنية الملائمة لتحقيق نمو متواصل وتغيير أساليب الإنتاج والاستهلاك المتبعة بهدف الاستغلال الأمثل للموارد النادرة.

ولقد فتح إعلان الحق في التنمية آفاقًا جديدة للإنسان حتى يتمتع بالمزيد من الكرامة والحرية والمساواة والعدالة. وطالب الإعلان أيضا بتكافؤ الفرص والتوزيع العادل للموارد الاقتصادية، بحيث يشمل الأشخاص المستضعفين والمستبعدين عن التنمية في ظل ما توفّره التكنولوجيا الرقمية من آليات لتعزيز الحق في التنمية.

طرح الإشكالية:

بناءا عليه، نطرح إشكالية هذه الدراسة على النحو التالي:

" كيف يمكن للتكنولوجيا الرقمية أن تساهم في تعزيز الحق في التنمية؟"

أهمية الدراسة:

تنبع أهمية هذه الدراسة من أهمية التغير الحاصل في التكنولوجيا بشكل عام وفي التكنولوجيا الرقمية بشكل خاص والتغير السريع الذي تحدثه في نوعية حياة الإنسان وفي أثرها على خصوصيته.

الهدف من الدراسة:

تهدف هذه الدراسة إلى تحديد المتطلبات والآليات المرتبطة بالتكنولوجيا الرقمية التي تساهم بشكل مباشر في تعزيز الحق في التنمية.

المنهج المتبع:

اعتمدنا على المنهج الوصفي التحليلي الذي نعتقد أنه يتلاءم مع طبيعة هذه الدراسة.

المحور الأو ل: التكنولوجيا الرقمية والحق في التنمية

إن الثورات التي شهدتها البشرية تضاف إليها في عالمنا المعاصر الثورة التكنولوجية؛ فثورة الحاضر هي المعلوماتية والمعرفة متمثلة في المادة الفكرية اللاّزمة للتحديث والابتكار. وتشير التكنولوجيا إلى استخدام الأدوات والآلات والمواد والتقنيات ومصادر الطاقة لجعل العمل أسهل وأكثر إنتاجية حيث جلبت التكنولوجيا الكفاءة والجودة لمختلف القطاعات، كما أصبحت علاقة المجتمع بالتكنولوجيا أحد أقوى مؤشرات التنمية.

أولا: من النمو إلى التنمية المستدامة

تتطلب عملية التنمية تفاعلا بين الموارد الطبيعية والموارد البشرية والموارد المالية لإحداث زيادة مستمرة في الدخل الوطني وتحقيق معدلات نمو مستمرة. ومع بساطة عمليات التنمية التي كانت تبحث في الرفع المستمر لمعدل النمو الاقتصادي؛ أصبحت التنمية عملية طويلة المدى تعتمد على تقدير إمكانات الحاضر والتخطيط لاستغلالها في تلبية احتياجات الأفراد الضرورية من الغذاء والتعليم والصحة وكل ما يتصل بنوعية حياة البشر ماديا واجتماعيا لأطول فترة زمنية مستقبلية، مع مراعاة الحفاظ على المحيط الحيوي للبيئة الطبيعية. وهي بذلك التنمية التي تلبي حاجات الحاضر دون المساس بقدرة الأجيال المقبلة على تلبية حاجاتهم.

تسعى التنمية المستدامة إلى تحقيق مجموعة من الأهداف التي نلخصها كمايلي[1]:

- ✓ تحقيق نوعية حياة أفضل،
- ✓ احترام البيئة الطبيعية من خلال توطيد العلاقة بين السكان والبيئة،
- ✓ تعزيز وعي السكان بالمشكلات البيئية القائمة،
- ✓ تحقيق استغلال عقلاني للموارد المحدودة والموارد غير المتجددة،
- ✓ ربط التكنولوجيا الحديثة بأهداف المجتمع من خلال توعية السكان بأهمية التقنيات المختلفة في مجال التنمية وكيفية استخدامها في تحسين نوعية حياة المجتمع،
- ✓ تغيير مستمر ومناسب في حاجات وأولويات المجتمع.

لقد أقرَّت خطة العام 2030 بأهمية التكنولوجيا لتحقيق أهداف التنمية المستدامة. ولم تتم الإشارة إلى التكنولوجيا إلا في الهدف 17 "تعزيز وسائل التنفيذ وتنشيط الشراكة العالمية من أجل التنمية المستدامة"باعتبارها **وسيلة تنفيذ رئيسية**. بيد أن من بين الـ 169 غاية، فإن 48 منها تتعلق بالتكنولوجيا سواء بشكل مباشر أو غير مباشر[2].

وتتكامل أهداف التنمية المستدامة حيث إنها تدرك أن العمل في مجال معين يؤثر على النتائج في مجالات أخرى وأن الإبداع والمعرفة والتكنولوجيا والموارد المالية من كل المجتمع أمر ضروري لتحقيق أهداف التنمية المستدامة.
نلخص أهداف التنمية المستدامة من خلال الجدول التالي[3]:

الجدول رقم (1): ملخص أهداف التنمية المستدامة

الهدف		البيان
1	**الفقر**	القضاء على الفقر بجميع أشكاله في كل مكان
2	**الجوع**	القضاء على الجوع وتوفير الأمن الغذائي والتغذية المحسَّنة

[1] شايب يمينة، "دور الاستثمار في الرأس المال البشري في تحقيق التنمية المستدامة"، رسالة دكتوراه في العلوم الاقتصادية، جامعة الجزائر3، 2015، ص 59.

[2] https://www.unodc.org/unodc/ar/commissions/SDG/commissions-2030.html موقع مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال أفريقيا، تاريخ الاطلاع 26 ماي 2022/.

[3] موقع لجنة الأمم المتحدة للقانون التجاري الدولي، تاريخ الاطلاع 30 ماي 2022، https://uncitral.un.org/ar/about/sdg

		وتعزيز الزراعة المستدامة
3	**الصحة**	ضمان تمتع الجميع بأنماط عيش صحية وبالرفاهية في جميع الأعمار
4	**التعليم**	ضمان التعليم الجيد المنصف والشامل للجميع وتعزيز فرص التعلم مدى الحياة للجميع
5	**المساواة بين الجنسين**	تحقيق المساواة بين الجنسين وتمكين كل النساء والفتيات
6	**المياه والصرف الصحي**	ضمان توافر المياه وخدمات الصرف الصحي للجميع وإدارتها إدارة مستدامة
7	**الطاقة**	ضمان حصول الجمع بتكلفة ميسورة على خدمات الطاقة الحديثة الموثوقة والمستدامة
8	**العمل اللائق والنمو الاقتصادي**	تعزيز النمو الاقتصادي المطرد والشامل للجميع المستدام والعمالة الكاملة والمنتجة وتوفير العمل اللائق للجميع
9	**الصناعة**	إقامة بنية تحتية قادرة على الصمود وتحفيز التصنيع الشامل للجميع وتشجيع الابتكار.
10	**المساواة**	الحد من انعدام المساواة داخل البلدان وفيما بينها.
11	**المدن والمجتمعات**	جعل المدن والمستوطنات البشرية شاملة للجميع وآمنة وقادرة على الصمود ومستدامة.
12	**الاستهلاك**	ضمان وجود أنماط استهلاك وإنتاج مستدامة.
13	**تغير المناخ**	اتخاذ إجراءات عاجلة للتصدي لتغير المناخ وآثاره .
14	**الحياة المائية**	حفظ المحيطات والبحار والموارد البحرية واستخدامها على نحو مستدام لتحقيق التنمية المستدامة.
15	**الحياة البرية**	حماية النظم الإيكولوجية البرية وترميمها وتعزيز استخدامها على نحو مستدام وإدارة الغابات على نحو مستدام. ومكافحة التصحر ووقف تدهور الأراضي وعكس مساره.
16	**السلام والعدالة**	التشجيع على إقامة مجامعات مسالمة لا يُهمَّش فيها أحد، وإتاحة إمكانية وصول الجميع إلى العدالة وبناء مؤسسات

		فعالة خاضعة للمساءلة وشاملة للجميع على جميع المستويات.
17	**الشراكة**	تعزيز وسائل التنفيذ وتنشيط الشراكة العالمية من أجل تحقيق التنمية المستدامة.

المصدر: من إعداد الباحثة بالاعتماد على موقع لجنة الأمم المتحدة للقانون التجاري الدولي، تاريخ الاطلاع 30 ماي 2022، https://uncitral.un.org/ar/about/sdg.

تعتبر خطة عام 2030 متجذّرة تجذّرًا لا لُبس فيه في حقوق الإنسان ومترسّخة بشكل واضح في الإعلان العالمي لحقوق الإنسان، والمعاهدات الدولية في مجال حقوق الإنسان وغيرها من الصكوك المعنية الأخرى مثل إعلان الحق في التنمية (الفقرة 10)[4]. وتسعى أهداف التنمية المستدامة "إلى إعمال حقوق الإنسان للجميع" (ديباجة خطة عام 2030) وهي قابلة للتطبيق عالميًا على جميع الأشخاص في جميع البلدان، بما فيها البلدان المتقدمة والنامية على حد سواء. والأهم من ذلك، أنّه يجب تنفيذ خطة عام 2030 بطريقة تتسق مع القانون الدولي (الفقرة 18). ما يميز أهداف التنمية المستدامة هو أنها [5]:

أ. **عالمية**: هي بمثابة إطار عالمي بكلّ ما للكلمة من معنى، وتنطبق على جميع البلدان. ويتعيّن على جميع البلدان إحراز تقدم نحو تحقيق التنمية المستدامة، وهي تواجه تحديات مشتركة وفريدة تعترض سبيل تحقيق أبعاد التنمية المستدامة الكثيرة التي تتضمنها أهداف التنمية المستدامة.

ب. **تحويلية**: تتيح خطة عام 2030، باعتبارها خطة من أجل "الناس والكوكب والازدهار والسلام والشراكة"، نقلة نوعية من نموذج التنمية التقليدي. وتوفر رؤية تحويلية من أجل تحقيق تنمية مستدامة محورها الإنسان وكوكب الأرض وقائمة على حقوق الإنسان ومراعية للمنظور الجنساني.

[4] إعلان الحق في التنمية، الأمم المتحدة، قرار الجمعية العالمة 2/55 على الخط، تاريخ الإطلاع 26 ماي 2022، https://www.un.org/en/events/righttodevelopment/pdf/rtd_booklet_ar.pdf

[5] موقع مفوضية الأمم المتحدة لحقوق الإنسان، تاريخ الإطلاع 26 ماي 2022، https://www.ohchr.org/ar/sdgs/about-2030-agenda-sustainable-development

ت. **شاملة:** تَعِدُ خطة عام 2030، إلى جانب التزامها بتحقيق سلسلة واسعة من الأهداف الاجتماعية والاقتصادية والبيئية، ببناء "مجتمعات أكثر سلامًا وعدلاً واحتضانًا للجميع، تخلو من الخوف والعنف"، وتهتمّ بشكل خاص بالحوكمة الديمقراطية وسيادة القانون والوصول إلى العدالة والأمن الشخصي (الهدف 16)، وبتهيئة بيئة دولية مؤاتية (الهدف 17 وفي الإطار ككلّ). وبالتالي، تغطي الخطة قضايا تعني كامل حقوق الإنسان، بما في ذلك الحقوق الاقتصادية والمدنية والثقافية والسياسية والاجتماعية والحق في التنمية.

ث. **جامعة:** تسعى خطة عام 2030 إلى شمل الجميع من دون أيّ استثناء، وترنو إلى بناء "عالم يسود جميع أرجائه احترام المساواة وعدم التمييز" بين البلدان وداخلها، بما في ذلك المساواة بين الجنسين، وذلك بإعادة تأكيد مسؤوليات جميع الدول عن "احترام حقوق الإنسان وحمايتها وتعزيزها، دونما تمييز من أي نوع على أساس العرق أو اللون أو الجنس أو اللغة أو الدين أو الرأي السياسي أو غيره من الآراء أو الأصل القومي والاجتماعي، أو على أساس الملكية أو الميلاد أو الإعاقة، أو على أي أساس آخر".

ثانيا: التكنولوجيا الرقمية وأهداف التنمية المستدامة

لقد كانت بدايات استخدام التكنولوجيا الرقمية في مجال الحاسبات الآلية ثم تطورت ليستفيد من مزاياها في جميع أنواع الاتصال. ويتم التعبير بموجبها عن المعلومات في شكل سلسلة من الإشارات. وتتخذ كل الصوروالرسوم والأشكال والأصوات والحروف رموزا تتكون من الرقمين الصفر(0) والواحد(1)[6].

تعددت الرؤى في تعريف التكنولوجيا الرقمية نذكر من بينها مايلي:

- ✓ **نتاج التلاحم والتكامل بين كل من تكنولوجيا الحاسبات الآلية وتكنولوجيا الاتصال.**
- ✓ **مختلف تكنولوجيا المعلومات والاتصال الحديثة التي تتشكل أساسا من عنصرين؛ الأول هو الماديات كالأجهزة والمعدات والثاني هو البرمجيات.**

---

[6] أل سيد الشيخ فاطمة و لمياء مرتاض نفوسي، " التكنولوجيا الرقمية ودورها في انتشار الصورة الرقمية"، مجلة بحوث ودراسات في الميديا الديدة، المجلد03/ العدد 02(2022)، ص ص 46-63. على الخط https://www.asjp.cerist.dz/en/downArticle/778/3/2/195806

- ✓ **الأنظمة العلمية والتكنولوجية والهندسية والإدارية المستخدمة في تناول ومعالجة المعلومات وتطبيقاتها وتفاعلها مع الانسان والأجهزة وكذلك الجوانب الاجتماعية والاقتصادية التي تتعلق بذلك**[7].

وتتميز التكنولوجيا الرقمية بجملة من الخصائص نذكر منها:

- ✓ **جعل كل الأماكن قريبة ومتجاورة**
- ✓ **سرعة الوصول إلى المعلومات المخزنة**
- ✓ **الذكاء الاصطناعي من خلال تطوير المعرفة وتقوية فرص تكوين الموارد البشرية من أجل الشمولية والتحكم في عملية الإنتاج.**

تقدمت التكنولوجيات الرقمية بسرعة تفوق أي ابتكار في تاريخنا - حيث وصلت إلى حوالي حوالي 50 في المائة من سكان العالم النامي فيما لا يتجاوز عقدين من الزمان وأحدثت تحولاً في المجتمعات من خلال تعزيز الاتصال الإلكتروني والشمول المالي وإمكانيات الوصول إلى الخدمات التجارية والعامة؛يمكن أن تمثل التكنولوجيا عاملاً كبيراً في تحقيق المساواة[8].

لقد بلغت التطورات الحاصلة في مجال تكنولوجيا المعلومات والاتصالات ذروتها بظهور الانترنت والتوسع في استعمالاتها المختلفة، ويمكن أن نلخص التسارع الكبير في استخدام الانترنت بسبب مجموعة من العوامل نذكرها على النحو التالي:

- ✓ دخول السكان في البلدان النامية عالم الانترنت واستخدام الهواتف الذكية باستخدام تكنولوجيا الجيل الثالث والرابع.
- ✓ زيادة كبيرة في تسهيلات الصوت والفيديو على شبكة الانترنت بسبب انخفاض مستويات الإلمام بالقراءة والكتابة في البلدان النامية.
- ✓ التسهيلات التي توفرها تطبيقات وسائط التواصل الاجتماعي للأفراد والمؤسسات والشركات.
- ✓ تنامي حجم التجارة الالكترونية بما فيها التسويق الالكتروني.

---

[7] فاطمة غاي، التكنولوجيا الرقمية وانعكاساتها عل أبعاد التنمية المستدامة بالجزائر للفترة الممتدة ما بين 2005، 2021م-دراسة تحليلية، مجلة قبس للدراسات الانسانية والاجتماعية، المجلد 06، العدد01، ص ص 587-610، مارس 2022، الجزائر، على الخط https://www.asjp.cerist.dz/en/downArticle/482/6/1/187068

[8] موقع الأمم المتحدة، تأثير التكنولوجيات الرقمية ، على الخط، تاريخ الإطلاع 02 جوان 2022، https://www.un.org/ar/un75/impact-digital-technologies

وفيما يلي بعض الإحصائيات المتعلقة باتجاهات تنامي استخدام التكنولوجيا[9]:

الجدول رقم 2 : الاستخدام العالمي للأنترنت

عدد المستخدمين	4،1 مليار نسمة
نسبة النفاذ	% 53،6
الفجوة بين الجنسين في استخدام الانترنت	%17
الزيادة السنوية في نسبة النفاذ	%82
متوسط الوقت الذي يمضيه مستخدموا الانترنت في الاتصال يوميا	6 ساعات و42 دقيقة
نسبة المستخدمون الذين يستخدمون البحث الصوتي شهريا	%40
نسبة المستخدمون الذين يشاهدون مقاطع الفيديو عبر الانترنت شهريا	4 مليار نسمة

المصدر: : تقرير التنمية الرقمية العربية 2019، نحو التمكين وضمان شمول الجميع، الاسكوا، الامم المتحدة،2020، على الخط التقرير -العربي-للتنمية-الرقمية-2019/https://archive.unescwa.org/ar/publications.

كما يوضح الجدول التالي أهم اتجاهات استخدام الهاتف النقال على المستوى العالمي:

الجدول رقم 3: أهم اتجاهات استخدام الهاتف النقال على المستوى العالمي

مستخدم واحد مشترك باتصال أو أكثر	**5،112 مليار نسمة**
نسبة النفاذ للمستخدم الواحد	**%67**
نسبة الاتصالات النقالة إلى مجموع السكان	**%115**
الاتصالات النقالة المرتبطة بهو اتف ذكية	**453،5 مليار نسمة**

[9] : تقرير التنمية الرقمية العربية 2019، نحو التمكين وضمان شمول الجميع، الاسكوا، الامم المتحدة،2020، على الخط التقرير -العربي-للتنمية-الرقمية-2019/https://archive.unescwa.org/ar/publications

الاتصالات النقالة المرتبطة بهواتف الميزات	**2،444 مليار نسمة**
استهلاك البيانات بواسطة الهواتف النقالة شهريا	

المصدر: : تقرير التنمية الرقمية العربية 2019، نحو التمكين وضمان شمول الجميع، الاسكوا، الامم المتحدة،2020، على الخط التقرير -العربي-للتنمية-الرقمية-https://archive.unescwa.org/ar/publications/2019

أما بالنسبة لأهم اتجاهات استخدام وسائط التواصل الاجتماعي يلخصها الجدول التالي:

الجدول رقم 4: أهم اتجاهات استخدام وسائط التواصل الاجتماعي

عدد مستخدمي وسائط التواصل الاجتماعي النشطين	**3،5 مليار نسمة**
عدد من يستخدمون وسائط التواصل الاجتماعي للعمل	**800 مليون نسمة**
متوسط عدد حسابات وسائط التواصل الاجتماعي للمستخدم الواحد	**9**
مستخدموا وسائط التواصل الاجتماعي على الأجهزة النقالة	**3،3 مليار نسمة**

المصدر: : تقرير التنمية الرقمية العربية 2019، نحو التمكين وضمان شمول الجميع، الاسكوا، الامم المتحدة،2020، على الخط التقرير -العربي-للتنمية-الرقمية-https://archive.unescwa.org/ar/publications/2019

ويوضح الجدول التالي اتجاهات استخدام شبكة الانترنت لغرض التجارة الالكترونية

الجدول رقم 5: اتجاهات الاستخدام لغرض التجارة الالكترونية

عدد مشتري السلع على الانترنت	**1،8 مليار نسمة**
معدل الزيادة السنوية للمشترين	**%3**
قيمة السلع الاستهلاكية في التجارة الالكترونية	**1،786 تريليون دولار أمريكي**
معدل الزيادة السنوية في الانفاق على التجارة الالكترونية	**%14**

المصدر: تقرير التنمية الرقمية العربية 2019، نحو التمكين وضمان شمول الجميع، الاسكوا، الامم المتحدة،2020، على الخط التقرير-العربي-للتنمية-الرقمية-https://archive.unescwa.org/ar/publications/2019.

لقد غيرت التكنولوجيا الرقمية الكثير في أوجه المعاملات اليومية للبشر حيث شهدت التكنولوجيا الرقمية أو تكنولوجيا الاتصالات طفرة كبيرة في عصرنا الحالي. كما أنها باتت تشكل تحديا إنمائيا رئيسيا قد يعيق تحقيق أهداف التنمية المستدامة مالم يتم التحكم في ضرورة تجاوز التحديات العامة التي تواجهها والتي نلخصها على النحو التالي:

- ✓ التحديات التقنية: وتتعلق بالمزيج التكنولوجي الواجب استعماله.
- ✓ التحديات الاجتماعية: وتتعلق بالتناقض الموجود بين مطالب عصر المعلومات وجمود المجتمعات باختلاف أسبابه؛ خاصة في ظل انتشار عدم الاقتناع وعدم الثقة في تطبيقات التكنولوجيا الرقمية.
- ✓ التحديات الاقتصادية: ويتعلق الأمر بمن يضمن تجنب الاحتكار في مجال المعلوماتية والاتصالات وهل ستعتبر التكنولوجيا شكلا من أشكال الرفاهية أم حتمية تنموية؟
- ✓ التحديات السياسية: وتتعلق بواجب تحديد أولويات استراتيجيات التنمية المستدامة والمتعلقة عموما بتخفيض نسبة الفقر ومحو الأمية الرقمية وإصلاح النظام التعليمي والصحة والحد من هجرة الأدمغة.

المحور الثاني: مساهمة التكنولوجيا الرقمية في تعزيز التنمية المستدامة

تحمل الثورة المعلوماتية الكثير من التحديات لعل من أشدها تأثيرا على رسم ملامح الواقع الاقتصادي الجديد تكمن في الفجوة الرقمية التي تُلقي بتداعياتها على فاعلية اندماج الدول النامية في حركية الاقتصاد العالمي؛ حيث أنّ اللاّتكافؤ في القدرات التقنية وقوى الانتاج والتفاوت في امتلاك المعرفة وأدواتها ينعكس سلبا على مستوى التنافسية وبالتالي تهميش موقع الدول على خارطة الاقتصاد الجديد وعلى مؤشرات التنمية معا. ولقد تراكمت متطلبات إحداث التغيرات الجذرية خاصة في الدول النامية ضمن مساعي إصلاح الواقع وبناء المستقبل كما تنوعت الآليات التي تعمل على تعزيز التنمية المستدامة؛

أولا: متطلبات التكنولوجيا الرقمية لتعزيز تحقيق التنمية المستدامة

لقد أصبحت التنمية عملية تتأثر إلى حد بعيد بالتكنولوجيا حيث تسهم التطبيقات التكنولوجية الحديثة بقدر كبير في مراحل تخطيط وتنفيذ وتقويم عمليات التنمية وبخاصة تقنيات المعلومات والاتصالات وتقنيات الحاسوب والانترنت التي أتاحت الاستفادة من خبرات الآخرين في مجال التنمية.

وعلى اعتبار أن أهم مطلب لعمليات التنمية في أي مجال وأي مجتمع هو العنصر البشري القادر على وضع خطط التنمية وتنفيذها ومتابعة نتائجها فإنه يستوجب الاهتمام بتنمية قدرات ذلك العنصر البشري من حيث :

- ✓ فهم لغة العلم والتكنولوجيا والقدرة على التعامل بها،
- ✓ فهم طبيعة العلم والتكنولوجيا وطبيعة العلاقة بينهما،
- ✓ الوعي بأهمية دور العلم والتكنولوجيا في تخطيط وتنفيذ ومتابعة خطط التنمية في كل المجالات.
- ✓ فهم تأثيرات العلم والتكنولوجيا على المجتمع بالسلب والإيجاب،

وإذا حققت تلك البرامج أهدافها فإنها تسهم إسهاما كبيرا في عملية التنمية؛ لا لأنها هي نوع من أنواع تنمية الموارد البشرية بل أيضا لأنها تضمن تأهيل من يمكنهم صياغة مخططات التنمية واتخاذ القرارات الصحيحة حيال تنفيذها ومتابعتها وتحقيق أقصى مخرجاتها ونواتجها[10].

يتطلب تحقيق التنمية الاقتصادية وجود قاعدة اقتصادية قوية قادرة على تحريك النشاط الاقتصادي يكون المدخل اللأساسي فيها إنتاج واستخدام التكنولوجيا المناسبة . وقد ازدادت أهمية التكنولوجيا بسبب الثورة المعلوماتية التي تضمنت تطورا واسعا في المعارف العلمية وما أفرزته من تطورات متنوعة وبالذات في مجال تكنولوجيا الاعلام والاتصال[11].

---

[10] شايب يمينة، مرجع سبق ذكره، ص 25.

[11] لحمر عباس، " البعد الاستراتيجي لتكنولوجيا المعلومات والاتصال"، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2018، ص 19.

تساعد التكنولوجيات الرقمي في جعل العالم أكثر انصافا وأكثر سلما وأكثر عدلا. ويمكن للإنجازات الرقمية أن تدعم كل هدف من أهداف التنمية المستدامة عبر توفير جملة من المتطلبات نلخصها في:

✓ **الاستثمار في رأس المال البشري وتنمية الموارد البشرية:**

ويتعلق بتعظيم الطاقات البشرية لأفراد المجتمع واستغلالها بكفاءة في كافة نواحي النشاط الاجتماعي والاقتصادي حيث أن التنمية تبدأ بتنمية البشر أولا من خلال التعليم[12]، التدريب والاستمرارية في المتابعة الذاتية؛ حيث يمكن أن تعرف التنمية البشرية على أنها: "عملية توسيع نطاق الخيارات أمام الأفراد"، وأهم هذه الخيارات هي[13]:

- حياة طويلة بدون أمراض،
- الحصول على قدر معقول من التعليم،
- أن يكون بوسع الأفراد الحصول على الموارد التي تكفل لهم مستوى معيشي كريم،
- أن يتمتع الأفراد بالحريات السياسية وحقوق الإنسان واحترام الإنسان لذاته.

إن استخدام التكنولوجيا الرقمية في تنمية الموارد البشرية أدى إلى توفير فرص تدريبية جديدة تُعرف بالتدريب الرقمي /التدريب الإلكتروني تهدف إلى نشر ثقافة المعلوماتية ورفع الكفاءة الانتاجية قصد التكيف السريع مع بيئة الأعمال التي تفرض تحديات مستمرة[14].

وتجدر الإشارة هنا إلى أن مفهوم الموارد البشرية يضع الانسان كمورد على نفس مستوى الموارد المجتمعية المادية الأخرى، وإذا كان التشبيه بين المورد الإنساني والمورد الطبيع ي صحيحا في بعض جوانبه التي تسعى إلى تحويل المورد إلى طاقة منتجة ونافعة إلا أن المورد الانساني هو صانع التحول في تلك الموارد وهو الموظف لها وهو كذلك مورد مُجدِّد ومُبدع وكذلك هو الهدف الذي من أجله تستثمر وتشغل طاقات مختلف الموارد الأخرى. وكما أن رأس المال يزيد عن طريق الاستثمار فإن الموارد البشرية تزداد عن طريق الاستثمار الانساني من خلال التغذية والصحة والتعليم بشكل خاص.

✓ **توجيه التقنية نحو تحقيق نمو مستدام:**

---

[12] شايب يمينة مرجع سبق ذكره، ص 236.

[13] بطاطا نصيرة، "التكنولوجيا الرقمية وتنمية الموارد البشرية"، مقال على الخط.ص ص 97 -103, https://www.asjp.cerist.dz/en/downArticle/321/5/2/95261

سواء في شكلها المادي أو كمعارف ومعلومات فإن التكنولوجيا تلعب دورا هاما في تحقيق التنمية، فبالنسبة للأثر الإيجابي الأكثر أهمية فيتمثل في إيجاد الحلول الناجعة للمشاكل المختلفة التي تجابه العملية الانتاجية فيما يتعلق بتخفيض التكاليف مقابل تعظيم الربح في ظل الجودة، أما بالنسبة للأثر السلبي فأن التطور التكنولوجي الهائل الذي يشهده العالم قد أدى إلى تفاقم عدد من المشكلات والقضايا الخطيرة التي باتت تهدد أمن الإنسان وغيره من الكائنات الحية وبقاءهم على كوكب الأرض.

وبناءا عليه فإن التقنية الملائمة لتحقيق نمو مستدام تعمل على تغيير أساليب الانتاج المتبعة بهدف الاستغلال الأمثل للموارد النادرة. كما يتعلق الأمر أيضا بالمزيج التكنولوجي الواجب استعماله وماهية المعايير التي تتحكم بقرار الاقتناء التكنولوجي وكيفية إقامة توازن بين ما هو متوفر من تقنيات وبين ما هو موضوع استيراد.

✓ توفير بنية تحتية للتكنولوجيا

أثبتت التكنولوجيا على مرّ السنوات الخمس الأخيرة خاصة مع انتشار وباء الكوفيد19؛ أنها العنصر الأساس لنجاح الأعمال واستمراريتها، وهو ما كان دافعا أيضا لمختلف الحكومات لتوجيه استثماراتها المالية لدعم مسيرة التحول الرقمي وتبني البرامج الالكترونية المفيدة لمختلف الأعمال والمجالات في القطاعين العام والخاص. وهو ما يدل على أهمية البنية التكنولوجية التي تدعم أعمال الحكومات والشركات الخاصة كما أنها قد سهلت ووفرت الكثير على المواطنين.

إن توفر البنية التحتية الرقمية يساهم بشكل مباشر في ازدهار مختلف القطاعات أهمها السياحة، الاتصالات، تجارة التجزئة، التكنولوجيا المالية، الرعاية الصحية والتعليم؛ وهو ما يجعل الكثير من الحكومات في مواجهة تحدي دعم الخدمات الالكترونية حتى نسبة 100% والتأكد من امتداد شبكة الانترنت ودعم البنية التحتية التكنولوجية لتستجيب لمتطلبات العملاء[15].

وبالرغم من مختلف الجهود المبذولة يظل الأشخاص الذين لم تصلهم بعد وسائل الربط الإلكتروني محرومين من منافع هذا العصر الجديد . وكثير ممن تركوا خلف الركب هم

---

[15] www.telecomreviewarabia.com/index.php/articles/reports-coverage

تطوير البنية التحتية الرقمية يحفز الابتكارات في القطاعات العامة والخاصة، مجلة تيليكوم ريفية، أفريل 2022،

من النساء أو كبار السن أو ذوي الإعاقة أو من الأقليات العرقية أو اللغوية وجماعات الشعوب الأصلية وسكان المناطق الفقيرة أو النائية. وقد أخذت وتيرة الاتصال الالكتروني في التباطؤ، بل والتراجع، في بعض الأوساط. فعدد النساء اللائي يستخدمن الإنترنت على مستوى العالم، مثلاً، يقل بنسبة 12 %عن عدد الرجال. وبينما ضاقت هذه الفجوة في معظم المناطق خلال الفترة ما بين عامي 2013 و2017 فإنها قد اتسعت في أقل البلدان نمواً من 30 %إلى 33% حسب أرقام نشرت على موقع الأمم المتحدة ضمن تقرير [16].

ثانيا: آليات التكنولوجية الرقمية لتعزيز التنمية المستدامة

يمكن للتكنولوجيات أن تساعد في جعل عالما أكثر انصافا وأكثر سلما وأكثر عدلا. ويمكن للإنجازات الرقمية أن تدعم كل هدف من أهداف التنمية المستدامة عبر توفير جملة من الآليات نلخصها في:

1. الشمول أو الاحتواء: والذي نقصد به:

- تعزيز وصول الأفراد وحصولهم والاستفادة من المختلف المنتجات لتحسين ظروفهم.
- البحث عن توفير فرص العمل الأفضل والشاملة للجميع للتغلب على الفقر والاستبعاد والتهميش وتحقيق الرخاء والرفاه للجميع.

ويقودنا مفهوم الشمول والاحتواء إلى مفهوم النمو الإحتوائي القائم على مبدأ مشاركة أطياف المجتمع المختلفة في تحقيق عملية التنمية وفي جني ثمارها أيضا بما يحقق الشعور لدى الأفراد بنتائج هذا النمو. ويأخذ في الاعتبار النمو المرتبط بمعدلات النمو المرتفعة مع البعد الاجتماعي الذي يرتبط بعدالة توزيع الفرص بين المواطنين على مستوى الأقاليم؛ حيث يعمل النمو الاحتوائي على توفير فرص العمل لأنها تعتبر الأساس في تنامي الشعور بالانتماء للمجتمع.

يعرف النمو الاحتوائي بأنه ذلك النمو الذي[17]:

- يمكّن جميع السكان من المشاركة والاستفادة من عوائده،
- يساهم في تخفيض معدّلات الفقر،

---

[16] تقرير حول تأثير التكنولوجيا الرقمية، مرجع سبق ذكره، https://www.un.org/ar/un75/impact-digital-technologies

17 صاري علي، النمو الاحتوائي من أجل عدالة اجتماعية وتعزيز مكاسب الطبقات الهشة والفقيرة مع الإشارة إلى حالة الجزائر، المجلة الجزائرية للعولمة والسياسات الاقتصادية، المجلد 12، السنة 2021، ص ص 127-148.

- يضمن الاستثمار في التدريب وتنمية المهارات
- موزعا على نطاق متسع من كافة القطاعات الاقتصادية،
- التوزيع العادل لعوائد النمو،
- يضمن التماسك الاجتماعي من خلال دعم الفئات الهشة،

ولتحقيق أهدافه وتعزيز فرص المساواة في جني ثمار عمليات التنمية يحتاج النمو الاحتوائي إلى[18]:

- تفعيل المشاركة/ توسيع مجال استخدام تكنولوجيا الاتصال والتكنولوجية الرقمية
- الحوكمة/ تعزيز الثقة بين المواطن والحكومة من خلال سياسات تعزز فرص الحصول على التعليم والرعاية الصحية والتكوين للجميع لتحقيق المزيد من فرص المساواة
- زيادة الانتاج/ تعزيز القدرات التنموية وذلك بإرساء بنية تحتية واسعة النطاق وإيجاد الامكانيات اللوجستية اللازمة،
- عدالة التوزيع/ معالجة الفوارق الجهوية
- الاهتمام بالنمو الأخضر لتحقيق التنمية المستدامة

2. التمكين:

في مجال الحديث عن التنمية نقصد بالتمكين توسيع الخيارات وحرية الفقراء والمهمشين في الحصول على أفضل نصيب من نتائج عمليات التنمية من خلال امتلاك الفرد للقوة ليصبح عنصرا مشاركا في شتى مجالات الحياة الاقتصادية والجتماعية؛ أي امتلاك القدرة على إحداث تغيير في الآخر الذي قد يكون فردا أو جماعة أو مجتمَعا بأكمله[19].

يعمل التمكين على:

- توزيع السلطة وحرية التصرف ومنح الحق في المشاركة وتحمل المسؤولية،

18 نفس المرجع، ص ص 127-148.

[19] قنوفي وسيلة، مفهوم التمكين في العملية الإنسانية، مجلة البحوث السياسية والإدارية، العدد الرابع، ص ص 304- 308، على الخط https://www.asjp.cerist.dz/en/downArticle/314/3/1/43207

- اكتساب المعرفة والمهارة والقدرة والتحكم في وسائل وتقنيات العمل،
- تعزيز قدرة الانسان على إحداث التغيير وذلك من خلال تعزيز قيم الديموقراطية والحرية
- توفير البيئة والأدوات للأفراد ليتمكنوا من الاعتماد على أنفسهم وإدارة شؤونهم الحياتية وتلبية احتياجاتهم الضرورية خاصة التمكين الاقتصادي من خلال مشاريع ربحية للأفراد.
- أن تتوفر لدى كل فرد من أفراد المجتمع إمكانية المشاركة الكاملة والحرة في اتخاذ القرار الذي يخدم المصلحة الخاصة والمصلحة العامة.

إن عملية التمكين هي عملية اجتماعية متعددة الأبعاد والصعد السياسية والاقتصادية والثقافية، وهي عملية تغييرية تستهدف خاصة حصول الشباب والمرأة على القوة من خلال إكسابهم المعلومات الخاصة ببيئتهم ومجتمعهم، وهي عملية تفاعلية في الخبرات بين الأفراد والمؤسسات، وفي الأخير هي عملية تنموية تركز على وعي الأفراد بقدراتهم وتحثهم على تطويرها ليصبحوا مؤهلين للحاق بركب التنمية.

خاتمة

لقد أصبحت قوة الأمم تقاس بمدى التقدم الذي تحرزه في مجال توظيف العلم والتكنولوجيا بهدف تحقيق الرخاء الاقتصادي والرفاهية الاجتماعية. ولقد تعالت أصوات المنادين بدور العلم والتكنولوجيا في الاستجابة لتحقيق الحاجيات الإنسانية المتطورة باستمرار. وأمام الفرص التي تتيحها تبقى الأولوية لكفاءة استخدام واستغلال الامكانيات المتاحة في ظل ما تعانيه عملية التنمية من اختلالات هيكلية لا يمكن للتكنولوجيا الرقمية تعديلها ما لم تدعم بقدرات بشرية ترفع التحدي أمام ثورة التكنولوجيا الرقمية.

لقد أصبحت التكنولوجيا من أبرز التقنيات التي تساهم في الانتقال من الممارسات التقليدية إلى الممارسات الحديثة التي تعتمد على الأجهزة والمعدات والشبكات المعلوماتية والتي تعمل على تعزيز الحق في التنمية المستدامة.

لقد غيرت الثورات التكنولوجية المتعاقبة مفهوم القوى العاملة حين استحدثت أشكال وأنماط عمل جديدة وتدفع غيرها إلى الاندثار. ففي الوقت الذي أشارت فيه بعض التقارير إلى فقدان الكثيرين لوظائفهم بسبب التشغيل الآلي فإن تقارير أخرى تؤكد على ظهور مهن ووظائف جديدة بفعل التكنولوجية الرقمية والذكاء الاصطناعي وهو ما يفرض على الحكومات تسخير هذه التكنولوجيات في استثمار فرص التنمية الاجتماعية والاقتصادية والبشرية، وهو ما يقترح مواضيع لابد أن تتضمنها السياسات العامة مرتبطة بالتكنولوجيا

الرقمية وهي الاستراتيجيات الرقمية وتكنولوجيا المعلومات والاتصالات والبنى الأساسية لتكنولوجيا المعلومات والاتصال والأمن السيبراني والفجوة الرقمية والتطبيقات الالكترونية.

النتائج :

توصلنا من خلال هذه الدراسة إلى جملة من النتائج نصوغها على النحو التالي:

- ✓ التكنولوجيات الرقمية أصبحت تستخدم لتتبع المشكلات وتشخيصها في مجالات الزراعة والصحة والبيئة، أو لأداء مهام يومية مثل التعامل مع حركة المرور أو دفع الفواتير. ويمكن استخدامها للدفاع عن حقوق الإنسان وممارستها إلا أنه يمكن استخدامها أيضاً لانتهاك تلك الحقوق.
- ✓ لقد أصبحت التكنولوجيا الرقمية من مسلّمات تحقيق التنمية بعد أن غزت كل مجالات الحياة كما أن المعلومات هي أساس أي تقدم وهي السبيل لتحقيق وتعزيز التنمية المستدامة.

التوصيات:

حاولنا من خلال هذه الدراسة صياغة جملة من التوصيات التي نذكرها على النحو التالي:

- ✓ ضرورة نشر الوعي وثقافة الاستخدام الأمثل لمختلف وسائل التكنولوجيا الحديثة لتعزيز أهداف التنمية المستدامة.
- ✓ رفع مستويات استخدام التكنولوجية الرقمية في مختلف المجالات والقطاعات والمؤسسات،
- ✓ ضرورة توسيع مجالات استخدام التكنولوجيا الرقمية خدمة لتحقيق أهداف التنمية المستدامة.

قائمة المراجع:

1. شايب يمينة، "دور الاستثمار في الرأس المال البشري في تحقيق التنمية المستدامة"، رسالة دكتوراه في العلوم الاقتصادية، جامعة الجزائر3، 2015،

2. موقع مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال أفريقيا. www.unodc.org/unodc/ar/commissions/SDG/commissions-2030.
3. موقع لجنة الأمم المتحدة للقانون التجاري الدول https:/ /uncitral.un.org/ar/about/sdg.
4. إعلان الحق في التنمية، الأمم المتحدة، قرار الجمعية العالمة 2/55 على الخط، https://www.un.org/en/events/righttodevelopment/pdf/rtd_booklet_ar.pdf
5. [1] موقع مفوضية الأمم المتحدة لحقوق الإنسان، تاريخ الإطلاع 26 ماي 2022، https://www.ohchr.org/ar/sdgs/about-2030-agenda-sustainable-development .
6. آل سيد الشيخ فاطمة و لمياء مرتاض نفوسي، " التكنولوجيا الرقمية ودورها في انتشار الصورة الرقمية"، مجلة بحوث ودراسات في الميديا الديدة، المجلد03/ العدد 02(2022)، على الخط https://www.asjp.cerist.dz/en/downArticle/778/3/2/195806
7. فاطمة غاي، التكنولوجيا الرقمية وانعكاساتها عل أبعاد التنمية المستدامة بالجزائر للفترة الممتدة ما بين 2005، 2021م-دراسة تحليلية، مجلة قبس للدراسات الانسانية والاجتماعية، المجلد 06، العدد01، مارس 2022، الجزائر، على الخط https://www.asjp.cerist.dz/en/downArticle/482/6/1/187068
8. موقع الأمم المتحدة، تأثير التكنولوجيات الرقمية ، على الخط، تاريخ الإطلاع 02 جوان 2022، https://www.un.org/ar/un75/impact-digital-technologies
9. تقرير التنمية الرقمية العربية 2019، نحو التمكين وضمان شمول الجميع، الاسكوا، الامم المتحدة،2020، على الخط التقرير-العربي-للتنمية-الرقمية-2019/ https://archive.unescwa.org/ar/publications/
10. لحمر عباس، " البعد الاستراتيجي لتكنولوجيا المعلومات والاتصال"، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2018.

11. بطاطا نصيرة، "التكنولوجيا الرقمية وتنمية الموارد البشرية"، مقال على الخط. https://www.asjp.cerist.dz/en/downArticle/321/5/2/95261
12. تطوير البنية التحتية الرقمية يحفز الابتكارات في القطاعات العامة والخاصة، مجلة تيليكوم ريفية، أفريل 2022

www.telecomreviewarabia.com/index.php/articles/reports-coverage

13. تطوير البنية التحتية الرقمية يحفز الابتكارات في القطاعات العامة والخاصة، مجلة تيليكوم ريفية، أفريل 2022،
14. صاري علي، النمو الاحتوائي من أجل عدالة اجتماعية وتعزيز مكاسب الطبقات الهشة والفقيرة مع الإشارة إلى حالة الجزائر، المجلة الجزائرية للعولمة والسياسات الاقتصادية، المجلد 12، السنة 2021، على الخط https://www.asjp.cerist.dz/en/downArticle/249/12/1/178099.
15. قنوفي وسيلة، مفهوم التمكين في العملية الإنسانية، مجلة البحوث السياسية والإدارية، العدد الرابع، ص ص 304-308، على الخط https://www.asjp.cerist.dz/en/downArticle/314/3/1/43207.

الحق في الصحة في ظل التحول الرقمي
بين الرهانات و التحديات
The right to health in light of technological development
Challenges and bets

بوغرارة مليكة – استاذة محاضرة أ
جامعة الجزائر 1
البريد الإلكتروني:m.boughrara@univ-alger.dz

ملخص :
يهدف هذا المقال إلى تبيان مفهوم الحق في الصحة الرقمية و ما حققته من انجازات في ظل التطور الرقمي و كذا رهاناتها و تحدياتها، سيما بعد أزمة كوفيد -19 التي قلبت موازين القطاع الصحي و غيرت معاييره، تجاه المنظومات الصحية المختلفة في العالم باختلاف درجة التطور التكنولوجي التي يحظى بها كل بلد.
حيث تساعد التكنولوجيات المدعومة بالذكاء الاصطناعي في إنقاذ الأرواح وتشخيص الأمراض وإطالة العمر المتوقع. لكن يظل الأشخاص الذين لم تصلهم بعد وسائل الربط الإلكتروني محرومين من منافع هذا العصر الجديد .
و على الرغم من أن الإهتمام بالصحة الرقمية برز بشكل لافت خلال جائحة كوفيد- 19 إلا أنه اهتمام قديم جديد، و تثير هذه المسألة العديد من القضايا التي تتعلق بإتاحة هذه الحقوق الأساسية للجميع.
الكلمات المفتاحية : الصحة الرقمية، جائحة كوفيد -19، انجازات ، رهانات الصحة الإلكترونية.

Abstract:
This article aims to clarify the concept of the right to digital health and its achievements in light of digital development, as well as its stakes and challenges, especially after the Covid-19 crisis, which upended the health sector balances and changed its standards, towards the different health systems in the world, according to the degree of technological development that every country has.

AI-powered technologies help save lives, diagnose diseases and extend life expectancy. However, people who have not yet reached the means of electronic connectivity remain deprived of the benefits of this new era.

Although the interest in digital health has emerged remarkably during the Covid-19 pandemic, it is an old and new interest, and this issue raises many issues related to the availability of these basic rights for all.

Keywords : Digital health, Covid-19 pandemic, achievements, e-health bets

مقدمة.

إن التقدم التكنولوجي الذي شهده العالم سيما في نهايات القرن الماضي أدى إلى التأثير على حقوق الإنسان عموما و على الحق في الصحة خصوصا ، و قد حظي حق الإنسان في الصحة بتطور كبير منذ الإعلان عنه، و لعل أبرز ما يميزه هو دخوله العالم الرقمي و إتاحته كحق أساسي للجميع.

والحق في الصحة مكرس في القانون الدولي لحقوق الإنسان، وقد تم توضيح مفهوم الحق في الصحة لأول مرة في ميثاق منظمة الصحة العالمية لعام 1946م، بأنها :

حالة كاملة من الرفاه الجسدي والعقلي والاجتماعي وليس مجرد انعدام المرض أو العجز

و هو كذلك حق اجتماعي واقتصادي أساسي نصت عليه المادة 12 من العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية لعام 1966، "تعترف الدول الأطراف في هذا العهد بحق كل إنسان في التمتع بأعلى مستوى ممكن من الصحة البدنية والعقلية."

يستند الإطار القانوني لحماية الحق في الصحة كحق من حقوق الإنسان على عدة مصادر تدعمه و تضمن تكريسه و يعتبر المصدر الأساسي في ذلك هو إنسانية الفرد و كرامته البشرية ثم ترسانة المواثيق و الإتفاقيات الدولية التي كرست هذا الحق بدرجات متفاوتة.

و في الوقت الراهن يعتبر الطب هو المجال الأكثر استخداما للرقمنة سيما في الآونة الأخيرة قبل و أثناء و بعد جائحة كوفيد-19 ، و هو ما يجب أن يؤخذ كحق طبيعي من الحقوق اللصيقة بالفرد بغض النظر عن جنسه أو عرقه أو لغته أو أصله القومي أو توجهه السياسي.

إن الصحة الرقمية اليوم لا تعد ترفا و رفاهية ، بل ضرورة ملحة و مصلحة قائمة لكل إنسان علما أن آلياتها و وسائلها و تطبيقاتها المؤسسة على الذكاء الإصطناعي و وسائطه ،تمثل المحددات الرئيسية لتطوير كافة المجتمعات و اقتصادات الدول و مختلف القطاعات الإنتاجية و الخدماتية في العالم.

كما تشكل الصحة الرقمية مستقبل الصحة المستدامة و هو مسعى حثيث للأمم المتحدة و منظمة الصحة العالمية و غيرهما من الهيئات الدولية لتسخير التكنولوجيا خدمة لتحقيق أهداف التنمية المستدامة العالمية خاصة هدف التمتع باعلى مستوى ممكن من الصحةالبدنية و رفاهية الإنسان.

و تتمثل أهمية هذه الدراسة في تبيان دور التحول الرقمي و وقعه على القطاع الصحي و مرتفقيه.

كما تتمحور مداخلتي حول الحق في الصحة في العالم الرقمي بين الرهانات و التحديات و لتناول هذا الموضوع طرحت إشكالية مفادها ما المقصود بالصحة الرقمية ؟ و ما تأثير التطور التكنولوجي على الحق في الصحة؟

و تتم الإجابة على هذه الإشكالية من خلال المحورين التاليين:

المحور الأول : مفهوم الحق في الصحة الرقمية.

المحور الثاني : تأثير التطور التكنولوجي على الحق في الصحة الرقمية.

المحور الأول : مفهوم الحق الصحة الرقمية.

إن مفهوم الحق في الصحة الرقمية يستمد أساسه من الحق في الصحة المنصوص عليه في اتفاقيات حقوق الإنسان ، وقد تم التأكيد على الحق في الصحة في معاهدات حقوق الإنسان الدولية والإقليمية، وفي الدساتير الوطنية في جميع أنحاء العالم. منها العهد الدولي الخاص بالحقوق الاقتصادية والاجتماعية والثقافية، 1966 ، اتفاقية حقوق الطفل، 1989 ، ومن الأمثلة على معاهدات حقوق الإنسان الإقليمية،الميثاق الاجتماعي الأوروبي، 1961،الميثاق الأفريقي لحقوق الإنسان والشعوب، 1981.

و قبل تعريف الحق في الصحة الرقمية لا بد من تعريف الحق في الصحة باعتباره المصطلح الأصلي الذي انبثق عنه الحق في الصحة الرقمية.

أولا: تعريف الحق في الصحة عموما.

يحتل الحق في الصحة في وقتنا الراهن مكانة رئيسية بين حقوق الإنسان الأخرى ، و هو مرتبط بها بعلاقة طردية تستدعي تفعيل جميع هذه الحقوق مجتمعة ، و يرتبط هذا الحق بالحصول على الرعاية الصحية و إنشاء المؤسسات الصحية، إلا أن الحق في الصحة يمتد إلى جملة من العناصر التي تسهم في الإستفادة من الحياة في صحة جيدة ، و هو ما أشارت إليه اللجنة المعنية بالحقوق الإقتصادية والإجتماعية والثقافية التابعة للأمم المتحدة باعتبارها المقومات الأساسية للصحة.

يقتضي حق الفرد في الصحة تكريس حماية له في كل المواثيق الدولية و الإقليمية و الوطنية التي تكفل حماية عامة أو خاصة أو معززة له سواء أكان ذلك في الجانب المتعلق بالأشخاص المخاطبين به، أو في جانب امتداد تلك الحماية لموضوع الحق في حد ذاته.[1]

وفقًا للتعريف الوارد في التعليق العام رقم 14، فإنّ الحق في الصحة هو حق شامل. وهو لا يقتصر على تقديم الرعاية الصحية المناسبة وفي حينها فحسب، بل يشمل أيضًا المقومات الأساسية للصحة، مثل:

-الحصول على مياه الشرب المأمونة والإصحاح المناسب؛

-الإمداد الكافي بالغذاء الآمن والتغذية والمسكن؛

-الظروف الصحية للعمل والبيئة؛

-الحصول على التوعية والمعلومات فيما يتصل بالصحة.

فالحق في الصحة يغطي مجموعة كبيرة من العناصر التي تساعدنا على عيش حياة صحية، أما الجوانب الأساسية الأخرى للحق في الصحة فهي:

إمكانية الوصول :يجب أن تكون المرافق والسلع والخدمات الصحية متاحة للجميع مع إمكانية الحصول عليها ماديًا بمنأىً عن أيّ تمييز.

التوافر :يجب توفير مرافق وسلع وخدمات عامة فعالة للصحة والرعاية الصحية وبكمية كافية.

المقبولية :على المرافق والسلع والخدمات أن تحترم الأخلاقيات الطبية وأن تراعي المنظور الجنساني وأن تكون ملائمة ثقافيًا.

النوعية الجيدة :يجب أن تكون المرافق والسلع والخدمات الصحية ملائمة علميًا وطبيًا وأن تكون في حالة عمل جيدة.

المشاركة :يجب أن يكون للمستفيدين من الرعاية الصحية صوتهم في ما يتعلق بصياغة وإعمال السياسات الصحية التي تؤثر عليهم.

المساءلة :يجب إخضاع المزودين والدول للمساءلة من أجل الوفاء بالتزامات حقوق الإنسان في مجال الصحة العامة. ويجب أن يحصل الناس على إمكانية طلب تعويضات فعالة عن الانتهاكات المرتكبة بحقهم مثل الحرمان من الخدمات الصحية.

الحريات :يجب أن يتمتع الناس بحرية عدم الخضوع للعلاجات الطبية بدون موافقة، مثل التجارب الطبية أو التعقيم القسري، والتعذيب وغيره من ضروب المعاملة أو العقوبة القاسية أو اللاإنسانية أو المهينة.

الاستحقاقات :يحق للناس، من بين جملة استحقاقات أخرى، بأن يتمتّعوا بأعلى مستوى من الصحة يمكن بلوغه، وبالوقاية من الأمراض ومعالجتها ومكافحتها، وبالحصول على الأدوية الأساسية، وبالصحة الإنجابية وصحة الأم والرضيع والطفل[2].

و تتميز إلتزامات الدول تجاه الحق في الصحة كما هو الحال مع حقوق الإنسان الأخرى، حيث تقع هذه الإلتزامات بصورة عامة تحت ثلاثة أنواع من الإلتزامات و هي:

- الإحترام مثل الإمتناع عن أي تدخل في التمتع بحقوق الإنسان كعدم تقييد الوصول إلى خدمات الرعاية الصحية للسجناء

- الحماية مثل منع الغير من التدخل في التمتع بحقوق الإنسان مثال: التأكد من أن العاملين في مجال الصحة يطبقون قواعد السلوك الأخلاقية

- إعمال حقوق الإنسان مثل اتخاذ الإجراءات المناسبة لإدراك وتحقيق حقوق الإنسان كاعتماد سياسة صحية وطنية أوإستراتيجية وطنية تشمل جميع السكان وأن تولي اهتماماً خاصا للفئات الضعيفة.[3]

و يجب تمييز الحق في الصحة عن بعض المفاهيم الشائعة مثل المفهوم الخاطئ الذي يلزم على الدولة أن تضمن لنا الصحة الجيدة.

يختلف الحق في الصحة عن الحق في التمتع بصحة جيدة. فالصحة تتأثر بعوامل تخرج عن سيطرة الدولة، مثل التكوين البيولوجي للفرد. وهذا هو السبب في أننا نشير إلى هذا الحق بأنه "أعلى مستوى ممكن من الصحة الجسدية والعقلية"، وليس الحق غير المشروط في التمتع بصحة جيدة.

كما أن الحق في الصحة هدف لا يمكن تحقيقه إلا على المدى الطويل .يخضع الحق في الصحة للإعمال التدريجي. لكن على الدول أن تبرهن أنّها تتّخذ خطوات عملية ومدروسة وهادفة، وبأقصى ما تسمح به مواردها المتاحة، من أجل احترام الحق في الصحة وحمايته والوفاء به.

كما أن الحالة المالية العسيرة لبلد ما تبرر تأخره في اتخاذ الإجراءات المطلوبة أو عدم اتّخاذها حتّى .لا تزال الدول مطالبة بأن تكفل فورًا التمتع بالمستويات الأساسية الدنيا للحق في الصحة. وهي تسمى الالتزامات الأساسية الدنيا، والالتزام المرتبط بها غير قابل للتقييد، وفي أصعب الظروف حتّى. ويجب أن تخصّص الميزانيات ما يكفي من الأموال من أجل ضمان وصول الجميع إلى السلع والخدمات الأساسية.

و أخيرا فإن الحق في الصحة لا يرتبط إلا بتقديم الخدمات الصحية .على الرغم من أن الحق في الصحة سيكون غير مجدٍ بدون توفير الخدمات الصحية، إلا أنه يمكن إعماله إعمالًا تامًا إذا ما تمَّ مراعاة عوامل أخرى تؤثر على صحتنا، مثل المياه الكافية والإصحاح المناسب، والسكن اللائق، والغذاء والتغذية الكافيين. كما يجب التصدي للتمييز والفقر والوصم وغير ذلك من "محددات" الصحة الاجتماعية والاقتصادية لأنه يمكن أن تحدّد :

إذا ما كان بعض الناس يتلقون الرعاية الصحية أو يُحرمون منها؛

جودة الخدمات التي يتلقاها الناس؛

إذا ما كان الناس سيختارون تفادي طلب الرعاية الصحية كليًا.

كما يرتبط الحق في الصحة البدنية والعقلية بشكل وثيق بإعمال حقوق الإنسان الأخرى ويعتمد عليه، مثل :

-الحق في الضمان الاجتماعي :يساعد النظام الشامل للحماية الاجتماعية على معالجة الأبعاد المتعددة للحرمان والمعاناة المرتبطة في أكثر الأحيان بسوء الحالة الصحية، ويكفل مستوى معيشي مناسب خلال المرض.

-الحق في الغذاء :يساعد النظام الغذائي الصحي على بناء المناعة، في حين أن التغذية السيئة أو غير المناسبة تترك آثارًا سلبية للغاية على الصحة.

-الحق في التعليم :إن الوصول إلى معلومات دقيقة وتوعية صحية يسمح لنا باتخاذ خيارات صحية بشأن كيفية تناول الغذاء وكيفية حماية أنفسنا من سوء الحالة الصحية وكيفية اختيار الرعاية والخدمات الصحية.

ويتطلب ذلك نهجًا يشمل الحكومة والمجتمع بأكملهما لوضع سياسات صحية فعالة تشمل الجميع من دون أيّ استثناء[4].

إن الحق في الصحة يرتبط ارتباطا وثيقا بالحق في الحياة ، لذلك كان لابد أن يكرس على المستوى الدولي نظرا لتداخل العوامل المؤثرة فيه ، و كذا بسبب التطورات و التغيرات البيئية و الإقتصادية و حتى المالية.[5]

ثانيا : تعريف الحق في الصحة الرقمية.

حسب منظمة الصحة العالمية و التي تبنت مصطلح الصحة الإلكترونية هي توظيف تكنولوجيا المعلومات والاتصالات و الذكاء الإصطناعي من أجهزة برامج في تقديم خدمات الرعاية الصحية . و من أبرز تطبيقات الصحة الرقمية في العالم تطبيقات الصحة المحمولة و السجلات الطبية الإلكترونية والطب عن بُعد ، في الاستعمال واسع النطاق للتكنولوجيات الرقمية للرعاية الصحية والأغراض المتعلقة بالصحة في مجموعة واسعة من البيئات، داخل وخارج بيئات الرعاية الصحية.[6]

وترى المنظمة أن مفهوم الصحة الرقمية أكثر شمولا من مفهوم الصحة عن بعد نظرا لاعتمادها على تكنولوجيا المعلومات والإتصالات بصورة أساسية، فإن الصحة الرقمية تركز على ترابط وتشابك الأنظمة الصحية المعتمدة على الأدوات الحوسبية والتطبيقات الذكية وتطبيقات تحليلات البيانات لدعم صناع السياسات ومقدمي الخدمات الصحية، والمستفيدين منها في دول العالم المختلفة في أنشطة التشخيص والعلاج والوقاية و إدارة المخاطر الصحية.[7]

كما يدور مفهوم الصحة الرقمية حول ميدان المعرفة والممارسة المرتبط بتطوير التكنولوجيات الرقمية واستخدامها من أجل تحسين الصحة. وتوسع الصحة الرقمية مفهوم الصحة الإلكترونية ليشمل مستهلكي التكنولوجيات الرقمية وطائفة أكبر من الأجهزة الذكية والمعدات الموصولة. ويشمل هذا المفهوم أيضا أوجه استخدام أخرى للتكنولوجيات الرقمية في مجال الصحة مثل إنترنت الأشياء والذكاء الإصطناعي والبيانات الضخمة والتشغيل الآلي.[8]

كما تعرف بأنها استخدام أدوات تقنيات المعلومات والاتصال في الخدمات الصحية، على سبيل المثال: استخدام الملف الالكتروني في عيادات الأطباء في مراكز الرعاية الصحية الأولية، أو المستشفيات والمراكز التخصصية[9].

كما عرفت الصحة الإلكترونية مفهوم عام يندرج تحته استخدام و تطبيق جميع أنواع تقنية المعلومات (البرمجيات والشبكات والإتصالات وغيرها) في قطاع الخدمات الصحية وفروعها، والاستفادة من هذه التقنيات في كل ما يعزز الصحة ويساعد على الوقاية من الأمراض ويدعم الأبحاث الطبية والسريرية[10].

و الجدير بالذكر أن متخصصي الصحة الالكترونية لا يبتكرون-بالضرورة– تقنيات جديدة، بل يعيدون استخدام وتوظيف الأدوات المتاحة مثل الملف الطبي الالكتروني، الأجهزة الذكية المحمولة، وحتى الانترنت لضمان استخدام هذه الأدوات من قبل المرضى، والأطباء وحتى المدراء في تطوير الرعاية الصحية[11].

وعلى الرغم من أن جائحة كورونا قد سلطت الأضواء على أهمية الصحة الرقمية وتطبيقاتها، إلا أن الإهتمام العالمي بالصحة الرقمية يعتبر اهتمام قديم متجدد.

إن نشأة مفهوم الصحة الالكترونية عند بداية ثورة الحوسبة في بداية الخمسينيات ، بدأت معها فكرة "الكمبيوتر الطبي" بالظهور في الدراسات البحثية التي حاولت أن تطرح فكرة أن يقوم الكمبيوتر بالمساعدة في تشخيص بعض الحالات بناءً على معطيات ومدخلات محددة، لكن فكرة الصحة الإلكترونية لم تتحول من مسار البحث إلى مسار التطبيق إلا في بداية الثمانينات عندما ظهرت لغات برمجة جديدة ساعدت على إنشاء برامج خاصة ببعض الخدمات في العيادات والمستشفيات مثل الجدولة والمختبرات والأشعة؛ وقد أدى هذا التطور السريع في التقنية إلى إحداث تغيير ملموس في معظم المجالات الطبية باتجاه استخدام تقنية المعلومات والإتصالات، لكن المجال الطبي بطبعه لا يتقبل التغيير بسهولة، و لعل هذه الحقيقة هي أحد العوائق التي لم تسمح بإحداث تغيير شامل في المجال الطبي مثل بقية القطاعات التي اخترقتها التقنية بشكل شبه كامل مثل الاقتصاد والطيران والإتصالات وغيرها[12].

كما برزت اهتمامات جدية وعملية من منظمة الصحة العالمية بالصحة الرقمية منذ عام 2018 ،وذلك وفق توصيات جمعية الصحة العالمية في دورتها رقم 71 في ماي 2018 بجنيف أي قبل الجائحة بسنتين، والتي ركزت على الصحة الرقمية، حيث أكدت على تقنين استخدامات التكنولوجيا الرقمية في مجال الصحة بما فيها نظم المعلومات الصحية على المستوى الوطني لتوفير خدمات صحية محورها الإنسان و ميسرة و جيدة و بتكلفة مناسبة .[13]

و قد أطلقت منظمة الصحة العالمية مشروع الإستراتيجية العالمية للصحة الرقمية 2020-2025 الغرض منه هو تعزيز النظم الصحية بفضل تطبيق تكنولوجيات الصحة الرقمية من أجل المستخدمين والمهنيين في مجال الصحة ومقدمي الرعاية الصحية بغرض تحقيق الرؤية المتعلقة بتوفير حق الصحة للجميع.

أما الطرق التي يمكن أن تساعد في الرعاية الصحية الرقمية لدينا:

-استخدام الهاتف المحمول أو جهاز آخر لتحميل سجلات الأغذية والأدوية والجرعات ومستويات سكر الدم ليراجعها ممرض يمكن التواصل معه إلكترونيًا.

-مشاهدة مقطع فيديو يوضح كيفية حساب الكربوهيدرات وتنزيل تطبيق على الهاتف المحمول للقيام بهذا الأمر.

-استخدام البرنامج ذاته لتقدير كمية الأنسولين

-استخدام الأرضية الإلكترونية لمعرفة نتائج التحاليل وتحديد المواعيد الطبية

-استلام رسالة إلكترونية أو رسالة نصية عبر الهاتف للتذكير بالحاجة إلى الحصول على لقاح أي رعاية وقائية أخرى.

و من بين أهداف الرعاية الصحة الإلكترونية أو الصحة المتنقلة، ما يلي:

-إتاحة الرعاية الصحية للأشخاص الذين يعيشون في عزله

-تقديم الخدمات بصورة أكثر سهولة أو ملاءمة للأشخاص الذين يعانون من محدودية الحركة أو الوقت أو خيارات النقل.

-إتاحة الوصول إلى المتخصصين في المجال الطبي.

-تقنية الواقع الإفتراضي المعزز التي تساعد في التدريب و التخطيط الجراحي .

ومن منظور قانوني وتنظيمي يجب أن يخضع جميع مقدمي الرعاية الصحية، ومقدمي الخدمات الصحية، والمرضى، وأي أطراف معنية أخرى مشاركة في نظام إيكولوجي للصحة الرقمية قابل للإستخدام التبادلي، لآلية فعالة وموثوق فيها للتعرف على الهوية الرقمية والتحقق منها واعتمادها تضمن الثقة في تبادل البيانات الصحية وتتسق مع الوسائل الوطنية الملائمة.[14]

وتتمثل أهمية استخدام الطب الرقمي في كونه علاوه على تشخيص الأمراض وعلاجها يساعد في تحديد أمراض جديدة أو ما إذا كانت أمراض موجودة تتفاقم، و تمكين الأطباء من التدخل في مرحلة مبكرة من المرض، ويمكن أن تساعد أدوات الصحة الرقمية في تقليص مدة المرض، أو في تخفيف الأعراض قبل أن تترسخ فعليا. كما يمكن أن تساعد الصحة الرقمية في التقليل من التكلفة الإجمالية للرعاية الصحية للشخص .

ونجد مثالا على الصحة الرقمية في الأجهزة الرقمية مثل الهاتف الذكي. فهو لا يساعد فقط في التواصل، بل لديه أيضًا عدد هائل من التطبيقات التي يمكن أن تساعد في مراقبة ضغط الدم، وتسجيل نسبة السكر في الدم، وضمان الامتثال للأدوية، وتتبع مقدار النشاط الجسدي. وهي توفر الجودة و دقة الخدمات و السرعة و المساواة بالنسبة للمرضى و تخفيف استعمال الوسائل بالنسبة للإدارت و المشافي .

كما تبرز أهمية الطب الرقمي من خلال تمكين الأطباء من التدخل في مرحلة مبكرة من المرض، ويمكن أن تساعد أدوات الصحة الرقمية في تقصير مدة المرض، أو في تخفيف الأعراض قبل أن تترسخ فعليا. كما يمكن أن تساعد الصحة الرقمية في تحسين جودة الحياة وتقليل التكلفة الإجمالية للرعاية الصحية للشخص طوال الحياة .ويتعلق الأمر بمجمله بتطبيق التحول الرقمي في قطاع الرعاية الصحية.

وضمن مسار "الرقمنة" لعل أفضل ما في الصحة الرقمية، لدينا:

-متفحّص الأعراض :هدفه الأساسي هو تقليل الزيارات غير الضرورية للأطباء وكذلك التعرف على حالات الطوارئ في وقت مبكر.

-لاستشارة عن بُعد :هي الطريقة الأسرع والأسهل لرؤية الطبيب. تتيح الاستشارة بالفيديو للأطباء ذوي المؤهلات العالية فحص الأعراض بسرعة وسهولة، وتقديم التشخيص وتوصيات العلاج والمشورة بشأن الأدوية المطلوبة.

-حجز المواعيد :يقدّر العملاء الراحة التي توفرها هذه الخدمة إذْ إنها تزيل عبء المكالمات المتعددة للحصول على موعد الطبيب المناسب[15].

و قد ساهمت أزمة انتشار فيروس كوفيد-19 في إلقاء المزيد من الضوء على أهمية الصحة الرقمية، خاصةً عندما يتعلق الأمر بتثقيف المرضى أو المستهلكين الصحيين وتشخيص إصابتهم وعلاجهم[16].

و الجدير بالذكر أن الصحة الرقمية غير مرتبطة بجائحة كوفيد-19 فالإهتمام العالمي بها ممتد منذ الإهتمام ببناء مجتمعات المعلومات و المعرفة ، و في مطلع القرن الحالي و لا تزال الأمم المتحدة من وقتها قائمة على متابعة توظيف الصحة الرقمية لتحسين صحة البشر حتى الآن .وقد سلطت الجائحة الأضواء على أهمية الصحة الرقمية، وتأخر عديد من دول العالم عن إدراك أهميتها في التشخيص و العلاج و استباق و إدارة الأوبئة ، وجودة الخدمة الصحية[17].

المحور الثاني: تأثير التطور التكنولوجي على الحق في الصحة.

لقد أدى ظهور الحواسيب الشخصية، واتصالات الإنترنت، والأجهزة المحمولة، ووسائل التواصل الاجتماعي، والذكاء الاصطناعي، والصور المجسمة، والأجهزة القابلة للارتداء، والجراحة عن بعد، إلى تطور تقنيات الصحة الرقمية وتحولها إلى منظومة متكاملة، وأضحت من الضرورة بمكان لممارسة الحق في الصحة.

أولا: إنجازات القطاع الصحي في ظل التحول الرقمي.

تعد الصحة الإلكترونية استخداما ذو مستوى عالي و آمن لتكنولوجيات المعلومات والاتصالات من أجل دعم قطاع الصحة و ملحقاته، بما في ذلك خدمات الرعاية ،والمتابعة الصحية والمنشورات ذات العلاقة والتحسيس والبحوث في المجال الصحي.

لقد حظي قطاع الصحة بتطور غير مشهود و حقق انجازات باهرة في ظل التحول الرقمي، تنطوي على العديد من الفرص و الإنجازات، إذ نجحت أنظمة الصحة الرقمية في إحداث تحول جذري في الرعاية الصحية ومكنت المرضى ومقدمي الرعاية الصحية والمديرين وواضعي السياسات بالمعلومات والأدوات التي يحتاجون إليها لإدارة وتعزيز الأنظمة الصحية وتقديم رعاية أفضل وتحسين العلاجات ومعدلات البقاء على قيد الحياة. كما مكنت من الحصول على الرعاية الصحية عالية الجودة و حسنت الوقاية ونتائج المرضى، بما في ذلك للمرضى الذين يعانون من أمراض مزمنة مثل الأمراض غير المعدية[18].

وقد **عملت** الصحة الرقمية على توفير عدة فرص و مزايا منها:

1- تحسين الصحة العامة ومؤسسات الرعاية الصحية على سبيل المثال ما يتعلق بإجراءات المستشفيات والسجلات الصحية الإلكترونية (EHR) والمعلومات الصحية. ويمكن تحسين الحصول على الرعاية الجيدة من خلال التقاسم السريع للمعلومات والبيانات بين مقدمي الرعاية والأخصائيين في مؤسسات الرعاية الصحية؛

2- دعم الأطباء: تحسين الإجراءات ،العمليات الجراحية أو المشورة، بما في ذلك الجراحة عن بُعد. ويتيح استعمال تكنولوجيات الصحة الرقمية لمجموعة من العيادات الصحية النائية أو الساتلية استعمال هذه التكنولوجيات وتطبيقها للتشخيص عن بُعد والطب عن بُعد. وعلى سبيل المثال، أجرت المستشفيات في الصين عمليات جراحية عن بُعد مكّنتها تكنولوجيا الجيل الخامس مثل عمليات الكبد وزرع عوامل التحفيز العميق للدماغ ضد مرض الشلل الرعاش.

3- الصحة الشخصية والأجهزة المخصصة (أجهزة الاستشعار والشاشات وساعات اليد والهواتف المتنقلة) لأغراض المراقبة والتغذية الراجعة. واستُعملت الهواتف المتنقلة لالتقاط صور بالموجات فوق الصوتية عن بُعد لحصوات الكلى أو الحمل، وكذلك إجراء اختبارات المسحة. كما تطورت التطبيقات الطبية بسرعة.[19]

4- تمكين عمليات التحليل والتنبؤ المحسّنة والأكثر دقة لمجموعات البيانات الصحية، بما في ذلك من خلال الذكاء الاصطناعي أو البيانات الضخمة أو عمليات المحاكاة باستعمال الواقع الافتراضي. و وفقاً لمنظمة الصحة العالمية، كان حوالي 120 بلداً قد صاغ استراتيجيات في مجالات الصحة الرقمية أو الصحة عن بُعد أو الصحة الإلكترونية بحلول منتصف عام 2018[20].

كما حقق القطاع الصحي في التحول الرقمي الآخذ بالإنتشار و بسبب الإجراءات الإحترازية التي سيطرت على دول العالم أجمع، الكثير من الإنجازات بحيث سارعت الشركات المتخصصة نحو تطوير برامج وآليات عمل تضمن حصول المريض والمستشفى على حدٍ سواء على التسهيلات اللازمة للتواصل وتشخيص الحالات وغيرها من الفوائد. فأصبحت الممارسات الطبية عن بُعد واقع ملموس بمساعدة السجلات الصحية الإلكترونية والإستشارات عبر الإنترنت وغيرها من الإبتكارات. كما استفاد المرضى من الرعاية الصحية عن بُعد بفضل رقمنة الحق في الصحة التي تتيحها المؤسسات الصحية عن طريق الخدمات الطبية عن بُعد، فيحصل المريض على إستشارات طبية فورية مع إمكانية متابعة حالته المرضية عن بعد، و هو ما يلائم أصحاب الأمراض المزمنة الذين يتعذر عليهم النتقل من بيوتهم للمراكز الصحية و المشافي .

و قد تبلورت انجازات الرقمنة الصحية في عدة مواطن أهمها:

-الرقمنة في المستشفيات.

إن تفشي جائحة كورونا جعل المستشفيات تنحو نحو الرقمنة في معاملاتها عبر تبنيها حلول الرعاية الصحية الرقمية ، لاسيما فيما يخص بيانات المرضى وسجلاتهم من خلال السجل الصحي الإلكتروني الشخصي الذي يجمع معلومات حول صحة المريض يتضمن نتائج الإختبارات والملاحظات السريرية والتشخيصات والمشكلات الصحية التي يعاني منها والأدوية التي يتناولها والإجراءات التي خضع لها وما إلى ذلك.

و تعتمد المستشفيات الذكية على مجموعة واسعة من الأجهزة الضرورية لأتمتة العمل ورقمنته بما يزيد من دقة الرعاية الصحية. وهذا النوع من الخدمات من شأنه أن يقلّل العبء على أنظمة الرعاية الصحية والأطباء ، من جهة ويزيد من إنتاجية مقدمي الرعاية الصحية من جهة أخرى.[21]

-التطبيب عن بُعد.

لقد أثبت التطبيب عن بُعد والإستشارات عن بُعد في ظل جائحة كورونا أنهما وسيلتين مفظلتين للعديد من المرضى في الحجر المنزلي والتباعد الجسدي عبر توفير عناء الذهاب إلى المستشفى والإنتظار. و قد أدركت معظم مؤسسات الرعاية الصحية والمستشفيات ضرورة المسألة، فعملت على تفعيل المواقع الإلكترونية وتحويلها إلى منصة تتيح للمريض التواصل مع الطبيب، من أي مكان وعلى مدار الساعة والحصول على الإستشارة الطبية عن بُعد والإجابة عن استفساراتهم.

-الإستشارات الطبية.

وفي الوقت الراهن و بعد اجتياز أزمة وباء كورونا أصبحت المؤسسات الصحية والمستشفيات تمتلك برامج متطورة يديرها كوادر صحية وكفاءات بشرية تعمل بمستوى عال من المهنية حيث أثبتوا جدارة ومهنية عالية لجهة التواصل مع المريض أو ذويه عبر تقنية الفيديو لتقديم الإستشارات

الطبية ونتائج التحاليل المختبرية والأشعة وإعطاء الوصفة الطبية اللازمة. فالإستشارات الطبية عن بُعد تتيح الفرصة للربط بين المريض والطبيب المختص للقيام بالمشاورات اللازمة أو كما يجب أن تسمى إستشارات دقيقة حول الحالة المرضية بحيث يستمع الطبيب إلى الحالة مع الإستعانة بالبيانات والمعلومات المقدَمة.

-الأجهزة القابلة للإرتداء.

توسع سوق الأجهزة القابلة للإرتداء والأدوات التي تحتوي على أجهزة الإستشعار لمراقبة العلامات الحيوية والظروف المختلفة لجسم الإنسان بشكل سريع، ليتم نقل المعلومات الصادرة عنها مباشرة إلى الطبيب الشخصي فيتمكن بالتالي من مراقبة الحالة عن كثب عبر جمع البيانات وتحليلها بواسطة خوارزميات الذكاء الإصطناعي من أجل تحديد الأمراض والمشاكل الصحية والنتيجة الحصول على تشخيص مبكر ونجاح العلاج والحد من المضاعفات التي يمكن ان تنتج جراء تطور الحالة.

ثانيا : التحديات التي تواجه الحق في الصحة الرقمية.

رغم التطور اللافت الذي حظي به الحق في الصحة الرقمية إلا أن القطاع يواجه عدة تحديات منها:

-نقص التخطيط عبر القطاعات هو أول التحديات، حيث بقيت التطبيقات المهمة محدودة داخل المستشفيات الكبرى في كل قطاع ولم يتم التوافق على تكوين أو استخدام الملف الطبي الإلكتروني الموحد للمواطنين و المقيمين رغم وجود بعض المحاولات لعمل ذلك إلا أن معظمها ينتهي حبراً على ورق.

من العوائق أيضا مسألة توفر الكوادر، فبرغم تميز الكوادر الحالية إلا أن العدد قليل و لايتماشى مع الحاجة الفعلية للقطاع كما أن عملية التحول الرقمي لم تكن ضمن خطة استراتيجية واضحة لجميع القطاعات بل كانت معتمدة على اجتهادات فردية أو لكل مؤسسة على حدة، و هذا بالضرورة يحد من انتشار تطبيقات الصحة الإلكترونية و مشاريعها.

كما تعد التكلفة الكبيرة لمشاريع الصحة الإلكترونية في بدايتها، عائقا من حيث أن العائد الإستثماري الفعلي لهذه المشاريع يحتاج إلى فترة طويلة ليظهر جدواه المالية[22].

و من المعلوم أن عمل المؤسسات الإستشفائية صعب و معقد، إذ تجمع المعرفة الطبية المعقدة والخبرة مع إجراءات التمريض الأساسية والمتقدمة. وغالباً ما تنشئ المستشفيات الكبيرة نظمها الإيكولوجية في جميع أنحاء منطقة ما، مع مجموعة كاملة أخرى من الوظائف والشركات المحيطة بها (مثل التصوير والوظائف المختبرية والتحليل والعلاج ودور الرعاية). وغالباً ما يترتب على إدخال

تكنولوجيات جديدة أو معقدة إجراءات متابعة كبيرة من حيث تكييف الشؤون المتعلقة بالعمالة والتدريب والتوظيف.

الخاتمة.

من خلال هذه الدراسة يمكن استخلاص عدة نتائج أهمها:

إن الصحة الرقمية في طريقها إلى إثبات ذاتها كحق من حقوق الإنسان الفردية و الجماعية و ضمان التمتع بها دون أي تمييز بسبب الجنس أو اللون أو العرق، كما أنها حق دستوري يجب ترجمته وإدراجه في هذا السياق .

إن رقمنة القطاع الصحي يضمن استدامة الحق في الصحة للجميع .

أن رقمنة الحق في الصحة اليوم أصبح حتمية تنظيمية إدارية وصحية وقانونية في العالم أجمع إذ لا مفر من رقمنة القطاع الصحي شأنه شأن جميع الميادين الأخرى .

إن الصحة الرقمية أثبتت أنها قادرة على تجاوز العقبات الزمنية و المكانية و مواجهة الأوبئة الفتاكة و الأزمات الصحية و الجوائح ، بمتابعة المرضى حيثما كانوا و مهما كانت حالتهم.

التوصيات.

على المستوى الوطني

إتاحة الوصول للخدمات الصحية بتكلفة مناسبة، بالسعي للوصول إلى المجتمعات المحلية، بما فيها الفئات المستضعفة، وتوفير خدمات الصحة الإلكترونية التي تتناسب مع احتياجاتها ،واحترام الخصوصيات والصالح العام بأخلقة هذه الخدمة الصحية.

تطوير البنى التحتية الرقمية لقطاع الصحة.

حوكمة الصحة الرقمية.

تكوين موارد بشرية متخصصة في القطاع الصحي الرقمي

ضمان متابعة تقنية ناجعة لاستراتيجية الصحة الرقمية، بالنظر في وضع وتنفيذ نظم وطنية إلكترونية لمعلومات الصحة العمومية، والقيام، عن طريق المعلومات، بتحسين القدرة على ترصد الأمراض والطوارئ الصحية العمومية وعلى الاستجابة بسرعة لمقتضياتها.

السعي لتغيير الذهنيات التقليدية حول الصحة الرقمية

على المستوى الدولي

-توثيق عرى التعاون العالمي والنهوض بنقل المعارف المتعلقة بالصحة الرقمية

-الدعم اللامشروط للصحة الرقمية على الأصعدة العالمية و الإقليمية.

لنظر في وضع خطة استراتيجية طويلة الأجل من أجل تطوير وتنفيذ خدمات الصحة الإلكترونية في مختلف مجالات قطاع الصحة، بما في ذلك الإدارة الصحية، بحيث تشمل هذه الخطة إطاراً قانونياً ملائماً وبنية أساسية مناسبة وتشجع الشراكات الدولية و الإقليمية

الهوامش:

---

[1]- كناي عبد الكريم، حماية الحق في الصحة في إطار القانون الدولي المعاصر، دكتوراه، كلية الحقوق سعيد حمدين ، جامعة الجزائر 1، ص 17

[2]-الأمم المتحدة مكتب حقوق الإنسان المفوض السامي ، الحق في الصحة الجوانب الأساسية و المفاهيم الخاطئة الشائعة، على الموقع ، https://www.ohchr.org/ar

[3]- المجلس القومي لحقوق الإنسان، الحق في الصحة ، ط1 ، جويلية 2018 ،على الموقع https://www.giz.de/en/downloads/SRIP_Right%20to%20Health%20booklet.pdf ص 4

[4]-الأمم المتحدة ، حقوق الإنسان ، مكتب المفوض السامي ، المفوضية السامية لحقوق الإنسان و الحق فس الصحة، على الموقع ،https://www.ohchr.org/

[5] - كناي عبد الكريم، مرجع سابق، ص،17

[6]- التزام بتوصيل العالم ITU، تكنولوجيا المعلومات و الإتصالات و الصحة الرقمية، على الموقع ، https://www.itu.int/ar/mediacentre/backgrounders/Pages/icts-digital-health.aspx تاريخ التصفح ، 2022/08/27 ، 11سا و 42 د.

[7]- أماني الريس ، ماجد خشبة ، الصحة الرقمية في مواجهة جائحة كورونا و غيرها ، المجلة المصرية للتنمية و التخطيط ، ص 360.

[8]- منظمة الصحة العالمية، الإستراتيجية العالمية للصحة الرقمية، 2021 ، ص 35 .

[9]- سليمان العمران ، ما هي الصحة الإلكترونية ، سلسلة تعريفية على الموقع ، https://www.ehealthsa.com/archives/1499 تاريخ التصفح 082022/12، 09سا و 30 د

[10]- نفس المرجع.

[11]-نفس المرجع.

[12]-سليمان العمران ، مرجع سابق.

[13]-أماني الريس ، ماجد خشبة ،مرجع سابق ،ص 361

[14]- منظمة الصحة العالمية ، مرجع سابق ص 31.

[15]- nextcare أهمية الصحة الرقمية على الموقع ، https://www.nextcarehealth.com/ar تاريخ التصفح 2022/07/14 ، 22سا و 00 د

[16]- موفق حوسة ، تكنولوجيا الصحة الرقمية ، كيف أسهمت التقنية في حماية البشر من كورونا، 2020/09/08على الموقع https://www.aljazeera.net/ تاريخ التصفح 2022/07/02 ، 10سا 33 د.

[17]- أماني الريس ، ماجد خشبة ، نفس المرجع.

[18]- ITU نفس المرجع السابق

[19]- تم تسجيل حوالي 325000 تطبيق من تطبيقات الصحة المتنقلة في جميع أنحاء العالم بحلول عام 2017، مما يمثل زيادة بنسبة 25 في المائة على أساس سنوي مقارنة بعام 2016. ITU نفس المرجع السابق .

[20]- نفس المرجع السابق.

[21]-بتصرف

[22]-سليمان العمران ، مرجع سابق

الحق في الخصوصية في ظل المعلوماتية

The right to privacy in the digital age

خليفي أسماء (أستاذة محاضرة ب)
جامعة 20 أوت 1955- سكيكدة - الجزائر
a.khlifi@univ-skikda.dz

بوصيدة فيصل (أستاذ محاضر ب)
جامعة 20 أوت 1955- سكيكدة - الجزائر
f.bouseida@univ-skikda.dz

ملخص:

منذ ظهور المعلوماتية بدأت تظهر سلوكات إجرامية تتم بواسطة أو ضد المعلوماتية، وقد استمرت تلك السلوكات في التطور السريع بتطور استعمالات المعلوماتية، وبعض تلك السلوكات تستهدف حقوق الإنسان المختلفة، حتى صارت تشكل تهديدا لها، ومن حقوق الإنسان التي تتعرض يوميا للانتهاك في العالم الرقمي الحق في الخصوصية، سواء تعلق الأمر بالخصوصية الرقمية نفسها كأحد عناصر الحياة الخاصة، أو العناصر الأخرى التي تتعلق بجسد الإنسان ومكانه واتصالاته وغير ذلك من مظاهر الحياة الخاصة، وهذه المداخلة تستهدف توضيح تلك الانتهاكات وبعض سبل مواجهتها التي تم اتخاذها لحد الآن.

الكلمات المفتاحية : الخصوصية ؛ المعلوماتية ؛ البيانات ؛ الحماية ؛ الإجرام السيبراني

Abstract:

Since the discovery of computers, criminal behavior carried out by or against computers has continued to develop rapidly according to the development of the uses of computers themselves, what are called informational crimes; some of these behaviors target the various human rights, and certainly the right to privacy, whether related to digital privacy itself, or other elements related to the human body, instead, communications and other aspects of privacy. This paper aims to explain these violations and the legal means that already exist to fight against them.

Keywords: privacy; informatics; data; protection; cybercriminality

مقدمـة:

يحقق العالم الرقمي ويوفر حرية المعلومات بفضل التطور الملحوظ والهائل للوسائل التقنية والإمكانيات غير المحدودة في مجال المعلوماتية وتحليلها واسترجاعها، إلا أنه مقيد بالمشروعية التي تفرضها حماية الخصوصية للأفراد وحرمة حياتهم الخاصة وموجبات حماية بياناتهم الشخصية، في ضوء التطورات التقنية التي أتاحت أن تحول البيانات التي تتعلق بالأفراد والتي تكون لوحدها وبذاتها غير ضارة إلى بيانات قد تشكل تهديدا حقيقيا لخصوصية الأفراد، وذلك بفعل ما أتاحته من إمكانية الجمع والتحليل وتحويلها إلى نوع من البيان التفصيلي عن حياة الفرد وأنشطته، لذلك كان لا بد من وجود نقطة انطلاق نحو نظام قانوني يحاكي تحديات العصر الرقمي، حيث اتجهت دول العالم إلى إنشاء قواعد البيانات لتنظيم عملها ولأغراض متعددة مثل البنوك ومراكز المعلومات الوطنية.

ورغم وجود اتفاق حول إيجابيات استخدام المعلوماتية في تلك المجالات إلا أن ذلك لم يمنع أن يستشعر الفرد مخاطر سهولة الحصول على معلوماته واتصال دائرة الاعتداء عليها، وبالتالي تهديدها للخصوصية، فكان ذلك دافعا لحركة الجهود الدولية والإقليمية والوطنية لإيجاد مبادئ وقواعد وقوانين واجب مراعاتها لحماية الحق في الخصوصية، ولإيجاد توازن بين حاجات الدول والمجتمعات إلى لجمع وتخزين معالجة البيانات الشخصية وكفالة حماية هذه البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها، خاصة وأن هذه المعلومات تتعلق بجميع جوانب حياة الفرد الشخصية (الوضع الصحي، والأنشطة الاجتماعية، والمالية، والآراء السياسية..)، لاسيما إذا كانت تحتوي على بيانات غير دقيقة أو غير صحيحة أو غير كاملة أو مبهمة.

وقد جاء التعديل الدستوري الجزائري الأخير لسنة 2020 بالنص على هذا المبدأ بشقيه المتمثلين في حماية المعطيات الشخصية، وحماية الحياة الخاصة للأفراد، وذلك بنصه أولا في المادة 47 منه على أن "حماية الأشخاص الطبيعيين عند معالجة المعطيات ذات الطابع الشخصي حق أساسي"، وثانيا بالمادة 81 التي نصت على أنه: "يمارس كل شخص جميع الحريات في إطار احترام الحقوق المعترف بها للغير في الدستور، لاسيما منها احترام الحق في الشرف، والحياة الخاصة ..."[1].

انطلاقا من ذلك فالإشكالية المطروحة هي في مدى قدرة الجهود الدولية والوطنية على توفير حماية فعالة للحق في الخصوصية في ظل المعلوماتية، وذلك عن طريق إقرار قواعد مبادئ تتفق وحجم هذه المخاطر، ومن أجل الإجابة على ذلك فالمنهج المتبع هو المنهج الوصفي التحليلي، حيث سنتعرف أولا على مظاهر انتهاك الخصوصية في البيئة المعلوماتية

أو الرقمية (المبحث الأول) ثم إلى المواجهة القانونية لانتهاك الخصوصية في العالم الرقمي (المبحث الثاني).

المبحث الأول

مظاهر انتهاك الخصوصية في ظل المعلوماتية أو العالم الرقمي

إن الحياة الخاصة للفرد أو ما يطلق عليه الخصوصية تشمل عددا كبيرا من الجوانب المتصلة بحياة الفرد، والتي تصنف بأنها جزء من حياته الخاصة، والتي هي كلها بكل أنواعها عرضة للانتهاك في العالم الرقمي، ويمكن تصنيفها إلى أربع مجموعات رئيسية، أحدها هو الخصوصية الرقمية، أو خصوصية المعلومات والبيانات الشخصية (المطلب الأول) وتشمل الأنواع الثلاثة الأخرى للخصوصية ما يتعلق بالخصوصية المكانية، والخصوصية الجسدية، والخصوصية الاتصالية[2] (المطلب الثاني).

المطلب الأول

انتهاك الخصوصية الرقمية (البيانات الشخصية)

إن الخصوصية عموما، أو الحياة الخاصة، كموضوع يصعب تعريفه، ترجع إلى فكرة السرية والألفة والحميمية، فعندما نتحدث عن الخصوصية الرقمية فهي ترجع إلى الحق في التخفي، أي في التواجد بشكل سري على شبكة الأنترنت[3]، وكذلك الحق في النسيان الرقمي، أي عدم الاحتفاظ بالبيانات الخاصة بالدخول إلى الوسائط الرقمية[4].

يقصد بالبيانات الشخصية data البيانات المخزنة في الحواسيب والمنظومات المعلوماتية المختلفة، كالهواتف المحمولة، سواء في المواقع المختلفة، أو البريد الالكتروني، أو في شكل بنوك معلومات أو قواعد بيانات، والتي تتعلق بالأشخاص، كبياناتهم الشخصية والأسرية والصحية والمالية والاجتماعية[5]، هذه البيانات يتم انتهاكها إما لأغراض الرقابة أو التسويق أو الأبحاث أو حتى مجرد الاتجار بها، فهذه البيانات تعتبر جزءا من الحياة الخاصة للأشخاص، وقد صارت هذه البيانات موضوعا لحماية قانونية خاصة في الدولة الحديثة بسبب انتشار المعلوماتية، تحت عنوان "حماية الخصوصية الرقمية"، و"حماية البيانات الشخصية"[6].

إن شبكة الأنترنت هي مصدر غني للمعلومات عن الأشخاص، وذلك عندما يقوم هؤلاء الأشخاص بتسجيل بياناتهم في مختلف المواقع من أجل الاستفادة من خدماتها، ناهيك عن معالجة

بياناتهم بطرق آلية لمعرفة عاداتهم وهواياتهم وسلوكاتهم آرائهم واتجاهاتهم إلى غير ذلك من خصوصياتهم، وهذه المعلومات يتم استخدامها لأغراض عديدة، ناهيك عن البرامج التي يمكنها أن تتجسس على الحواسيب الشخصية للأفراد، وبالتالي الاطلاع بشكل مباشر على البيانات الشخصية، وهو ما يجعل الأنترنت تهديدا مباشرا للخصوصية[7].

فقد أصبحت بيانات الأفراد تسجل في الحواسيب المتصلة بالأنترنت والهواتف المحمولة لأغراض عديدة، فقد تسجل بيانات الفرد بصفته موظفا، أو عميلا لبنك، أو مريضا، أو دافعا للضرائب، أو صاحب معاش، أو مالك سيارة، أو حتى لمجرد اتصاله بالأنترنت كمستعمل أو مشترك، وهو ما يجعل بياناته تلك عرضة لما تتعرض له المعطيات من اعتداءات[8].

وبعد انتشار التجارة الالكترونية صار الأفراد يسجلون أنفسهم وبياناتهم في مختلف المواقع التي تسمح لهم باقتناء أغراضهم، أو ما صار يطلق عليه المورد الالكتروني، حيث يقوم هذا الأخير بجمع وتخزين بيانات الزبائن والزبائن المحتملين، وهي بيانات يمكن أن يستخدمها هذا المورد لأغراض غير مشروعة منتهكا بذلك خصوصية تلك البيانات[9].

ومن أمثلة بنوك المعلومات التي تسجل فيها بيانات الأفراد، البنوك الخاصة بالبصمة الوراثية، والبصمة الجينية، ورغم أنه يبدو أن انتهاك مثل هذه البيانات صعب أو غير ذي أهمية إلا أن مظاهر التطور التي طبعت هذا العصر وصلت إلى حد ظهور عصابات إجرامية مختصة في سرقة المعلومات الجينية، مثلما حدث في بريطانيا سنة 2002، حيث قاموا بسرقة خصلة من شهر الأمير "هاري" من أجل التأكد من أنه فعلا ابن الأمير "تشارلز"، وذلك بغرض بيع معلومات هذا الاختبار للصحف، وابتزاز صاحب الشأن[10].

أما مواقع التواصل الاجتماعي فهي تعتبر مصدرا مهما من مصادر البيانات، فالأفراد يقومون بإنشاء حسابات فيها، ويضعون فيها صورهم وفيديوهاتهم، ويرسلون منها الرسائل والصور التي تتعلق بأدق تفاصيل حياتهم، ويدونون فيها أفكارهم، وقد يتسوقون منها، فهي تعد أكثر خطورة من بنوك المعلومات لأن البيانات تكون معروضة فيها بشكل ظاهر، ويؤدي هذا إلى انتهاكها بصورة أسهل[11].

يظهر انتهاك الخصوصية الرقمية أيضا من خلال قيام الدولة عبر مصالحها المختصة ولأغراض أمنية بالدخول إلى حسابات الأشخاص عبر الأنترنت، وذلك بغية كشف الجرائم

الالكترونية، أو التحقيق فيها، أو التفتيش الالكتروني، والمراقبة الالكترونية، وهذا كله يعتبر تهديدا للخصوصية الرقمية، ويحتاج إلى ضوابط لتنظيمه[12].

أما آخر تطورات انتهاك الخصوصية التي تثير مخاوف المجتمع الدولي ككل فهي التهديدات السيبرانية التي وصلت إلى حد تسميتها بالإرهاب السيبراني[13]، فهذا التهديد لا يستهدف فقط أشخاصا أو شركات صغيرة أو حسابات على مواقع الأنترنت بل يستهدف شركات عملاقة ودولا، وهي تكبد ضحاياها خسائر بمليارات الدولارات، وقد أصبح الإجرام السيبراني من أهم صور الجرائم المستحدثة المتمثلة في الجرائم المنظمة والعبارة للحدود[14].

المطلب الثاني

انتهاك الخصوصيات الأخرى

إن عناصر الحياة الخاصة التي يمكن انتهاكها في الفضاء الرقمي كثيرة، وإجمالا فالحياة الخاصة تشمل ما يلي:

- الحياة العائلية (الزواج والطلاق والحالة العاطفية والحالة الجنسية).

- ما يتصل بأحاسيس المرء ومشاعره ومعتقداته الدينية والفكرية.

- حالة الشخص الصحية (الجسمانية والنفسية والعقلية).

- أنشطة الفرد التي تتضمن مساهمته في المجتمع كنشاطه المهني وأنشطته التي يمارسها علانية.

- الحق في قضاء أوقات الفراغ.

- الحق في الدخول طي النسيان، ومن تطبيقاته الدخول طي النسيان الرقمي.

- الآراء السياسية للفرد.

- الذمة المالية للشخص[15].

لقد كان انتهاك الحياة الخاصة للآخرين في الماضي مقتصرا على الحديث عنها إما في الأماكن العامة، أو في الصحف ووسائل الإعلام المكتوبة والمرئية والمسموعة، إلا أنه بانتقال وسائل الإعلام إلى الرقمية، وما يطلق عليه الإعلام البديل المتمثل في منصات التواصل الاجتماعي، فقد أصبح

الفضاء الرقمي يعج بانتهاكات الخصوصية، سواء القذف والسب، أو نشر صور الآخرين، أو نشر الأخبار والمعلومات، أو إفشاء الأسرار، أو التشهير، أو التهديد والابتزاز، أو السخرية، إلى غير ذلك من الصور التي يقع كثير منها تحت طائلة القانون الجنائي، سواء باسم انتهاك الحق في الحياة الخاصة، أو بعناوين أخرى، كالمساس بالشرف والاعتبار، أو الجرائم الإعلامية، أو التجسس السمعي والبصري على أسرار الحياة الخاصة (التصنت وتسجيل المحادثات الشخصية والتقاط الصور)، فهناك تداخل بين هذه الأوصاف كلها، وهي تشترك كلها في تهديد خصوصية الأفراد، باعتبارها حقا من حقوق الإنسان، وحرية أساسية يضمنها الدستور والقوانين[16].

وفيما يتعلق مثلا بالحياة الجنسية للشخص كجزء من الحياة الخاصة، فالإنسان يحتفظ بحقه في سرية ما يتعلق بهذا الجانب، فقد حدث سنة 2015 أن موقع ashley madison وهو موقع مواعدة جنسية تعرض لعملية قرصنة بيانات 37 مليون مستخدم لهذا الموقع، وقد تكبد الموقع خسائر كبيرة أدت به إلى تغيير خطته واتجاهه، وهذا كمثال فقط عن الانتهاكات التي يمكن أن تطال الحياة الخاصة للأفراد، والتي تصل إلى درجة الهجوم السيبراني أحيانا، وتطال آلاف الأشخاص.

تجدر الإشارة إلى أن الخصوصية الرقمية أو البيانات الشخصية كثيرا ما تتداخل مع عناصر الحياة الخاصة، كأن تتعلق تلك البيانات بصورة الشخص أو صوته أو بصمته الوراثية أو هويته
أو حالته الصحية، ومثال ذلك ما حدث في قضية الرئيس الفرنسي فرانسوا ميتران حين قام طبيبه بتأليف كتاب عن مرضه، وبعد مصادرة الكتاب قام أحد مديري مقاهي الأنترنت بنشر الكتاب على موقع الكتروني، وبالتالي تم انتهاك خصوصية البيانات الشخصية الالكتروني التي تتعلق بالحالة الصحية للرئيس الفرنسي[17].

المبحث الثاني

المواجهة القانونية لانتهاك الخصوصية الرقمية

بالإضافة إلى المواثيق الدولية الكثيرة الصادرة في مجال حماية الخصوصية الرقمية فإن المشرع الجزائري قد تدخل بنصوص عديدة تشمل مجالات كثيرة، سواء منها ما يتعلق بالاتصالات أو بالإعلام أو الصحة أو بالعمل أو بتكنولوجيات الإعلام والاتصال وذلك بغية حماية البيانات الشخصية والحياة الخاصة في الفضاء الرقمي (المطلب الأول)، وبالإضافة إلى المواجهة التشريعية فإن القضاء كذلك له دور كبير في حماية الخصوصية الرقمية (المطلب الثاني).

المطلب الأول

المواجهة التشريعية لانتهاك حق الخصوصية في المجال الرقمي

لقد تصدى المشرع لكل صور المساس بالحق في الخصوصية داخل المجال الرقمي عن طريق مجموعة من الآليات والخطوات التشريعية المهمة تتلخص فيما يلي:

أولا: النص على مبدأ احترام الحياة الخاصة:

لقد صار شائعا استعمال التشريع لمصطلح الحياة الخاصة بعد أن كان خاليا منها، سواء في نصوص الدستور أو في القوانين المختلفة، فهو مفهوم من المفاهيم الحديثة والمتطورة بسرعة في آن واحد، وهذا ما جعل تعريفه من الناحية القانونية شبه مستحيل.

وعلى المستوى الدولي بدأ النص على احترام الحياة الخاصة مثلا في المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان التي جرى التوقيع عليها في روما في 1950/11/04، ودخلت حيز النفاذ في 1953/09/03، بعد تصديق عشر (10) دول عليها، ويعتبر قانون المعلوماتية والحريات الصادر في فرنسا عام 1978 من أول القوانين الصادرة لتنظيم عالم المعلوماتية، وبالإضافة إلى الدليل الأوروبي لسنة 1995 ودليل عام 1997 المتعلق بحماية معطيات الاتصالات نسجل أن الجمعية العامة للأمم المتحدة قد أصدرت قرارا تحت رقم 68/167 المؤرخ في 2013/12/18 خاص بالحق في الخصوصية في العصر الرقمي، وهو أول قرار يصدر في هذا الشأن على هذا المستوى[18].

ثانيا: تجريم المساس بالحياة الخاصة:

إن المساس بالحياة الخاصة كان في البداية فعلا مستوجبا للتعويض المدني باعتباره مساسا الحقوق اللصيقة بالشخصية، كما أن بعض الأفعال التي تمس الحياة الخاصة كانت مجرمة بشكل منفصل، كإفشاء الأسرار وانتهاك حرمة المسكن، وفض المراسلات، بيد أن المشرع الجنائي أصبح يتدخل لتجريم المساس بالحياة الخاصة بطريقة مباشرة، كما فعل المشرع الجزائري في المادة 303 مكرر 1 من قانون العقوبات (القانون رقم 06-23 المؤرخ في 2006/12/20 المعدل والمتمم لقانون العقوبات)[19]، وهي جرائم تتم غالبا في الفضاء الرقمي، أو باستخدام الهاتف النقال، ما يجعلها قريبة من الجرائم المعلوماتية، وإن كان من المحتمل أن تتم خارج المعلوماتية، في الصحف والمجلات مثلا، أو غيرها من وسائل النشر.

لقد تم النص على مبدأ احترام الحياة الخاصة وتجريم المساس به في العديد من النصوص القانونية، ومنها:

- القانون رقم 04-19 المتعلق بتنصيب العمال ومراقبة التشغيل، والذي نصت المادة 27 منه على تجريم فعل إفشاء المعلومات الشخصية التي تمس الحياة الخاصة لطالب التشغيل، وهذا النص يعتبر من أول النصوص التي تطرقت إلى الحياة الخاصة قبل نص قانون العقوبات الصادر في 2006، وهو نص يتماشى مع واقع التشغيل، باعتبار أن التسجيلات في طلبات العمل أصبحت في الغالب تتم الكترونيا من خلال مواقع وكالات التشغيل، وبالتالي فهذا يعرض بياناتهم الشخصية إلى خطر الإفشاء[20].

- القانون رقم 06-01 المؤرخ في 2006/06/20 المتعلق بالوقاية من الفساد ومكافحته، والذي نص في المادة 15 منه على ضرورة تمكين وسائل الإعلام والجمهور من الحصول على المعلومات المتعلقة بالفساد مع مراعاة حرمة الحياة الخاصة.

- القانون رقم 18-04 يحدد القواعد العامة المتعلقة بالبريد والمواصلات والاتصالات الالكترونية[21]، المادة 97 منه تنص على احترام شروط حماية الحياة الخاصة للمشتركين والبيانات ذات الطابع الشخصي، وتنص المادة 164 منه على تجريم انتهاك سرية المراسلات.

- القانون العضوي رقم 12-05 المؤرخ في 2012/01/12 يتعلق بالإعلام (المادة 93 منه)[22].

- القانون رقم 18-11 المؤرخ في 2018/07/02 يتعلق بالصحة (المادة 24 منه)[23].

ثالثا: حماية المعطيات ذات الطابع الشخصي:

إن المشرع الجزائري لم يكن متخلفا عن حماية المعطيات ذات الطابع الشخصي حيث نصت المادة 24 من المرسوم التشريعي رقم 94-01 المؤرخ في 1994/01/15 المتعلق بالمنظومة الإحصائية على ما يلي: "لا يحقق للمصلحة المؤتمنة أن تكشف أو تنشر المعلومات الفردية الواردة في الاستمارات التي تتضمن التسجيل الإحصائي ولها علاقة بالحياة الشخصية والعائلية، وعلى العموم الوقائع والتصرفات الخصوصية إلا طبقا للأحكام الرشيدة السارية على الأرشيف"[24].

وقد صدرت –في الجزائر- عدة نصوص قانونية متفرقة بغرض مواجهة الجريمة المعلوماتية التي تستهدف الكيانات المنطقية وأنظمة المعالجة الآلية للمعطيات، وكذلك حماية الحياة الخاصة بمختلف عناصرها داخل الفضاء الرقمي وخارجه، تتمثل أساسا في:

- القانون رقم 2000-03 يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية[25]، حيث تنص المادة 127 منه على تطبيق نص المادة 137 من قانون العقوبات (انتهاك حرمة المراسلات).

- القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات الذي أضاف قسما متكونا من ثمانية مواد (من 394 مكرر إلى 394 مكرر 7) تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"، وهو القسم المعدل بموجب القانون رقم 06-23 المؤرخ في 2006/12/20، والقانون رقم 16-02 المؤرخ في 2016/06/19، ويعتبر هذا التقنين أول نص يتطرق إلى الجرائم المعلوماتية بالتفصيل قبل أن تتطور هذه الجرائم وتتطلب تدخل المشرع بنصوص أخرى.

- القانون رقم 08-01 المؤرخ في 2008/01/23 يتمم القانون رقم 83-11 المتعلق بالتأمينات الاجتماعية[26]، تعاقب المادة 93 مكرر 2 منه على فعل الاستعمال غير المشروع للبطاقة الالكترونية للمؤمن له اجتماعيا.

- القانون رقم 09-04 المؤرخ في 2009/08/05 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

- القانون رقم 15-03 المؤرخ في 2015/02/20 المتعلق بعصرنة العدالة، والذي نص في المادة 05 منه على وجوب أن تتواجد على التراب الوطني كل المعطيات والمعلومات ذات الطابع الشخصي التي تم جمعها من طرف مؤدي خدمات التصديق الالكتروني.

- القانون رقم 16-03 المؤرخ في 2016/06/19 المتعلق باستعمال البصمة الوراثية في الإجراءات القضائية والتعرف على الأشخاص[27]، والذي نصت المادة 17 منه على تجريم استعمال العينات البيولوجية أو البصمات الوراثية لغير الأغراض المنصوص عليها في هذا القانون، وهذا النوع من التجريم يستهدف حماية الخصوصية الجينية، بالإضافة إلى المادة 18 من ذات القانون التي تجرم فعل إفشاء المعطيات المسجلة في القاعدة الوطنية للبصمات الوراثية[28].

- القانون رقم 18-07 المؤرخ في 2018/06/10 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[29].

رابعا: تجريم صور مستحدثة للإجرام السيبراني:

إن الفضاء المعلوماتي هو مجال للجرائم التقليدية (نصب، احتيال، سرقة، خيانة أمانة ...إلخ)، كما هو أيضا مجال لنوع جديد من الإجرام، هو الإجرام المعلوماتي، والذي يتميز بأنه يرتكب داخل هذا الفضاء أو باستخدامه، ومن هنا ظهرت الكثير من الجرائم التي تتصل بالحاسوب والأنظمة المعلوماتية سواء كانت متصلة بالأنترنت أم لا، ومنها القرصنة والتجسس الالكتروني وغيرها من الجرائم السيبرانية[30].

يعتبر التوجيه الأوروبي لسنة 2013 المعنون بـ "cyberattaques" بمثابة استراتيجية أوروبية لمكافحة الإجرام السيراني[31]، حيث أن ضحايا هذه الإجرام يتجاوز مليونا في اليوم الواحد عبر العالم، ولهذا -فإن هذا النوع من الإجرام يعتبر الأسرع والأسرع تطورا من بين أنواع الإجرام، ومن خلال النص المذكور الصادر عن البرلمان الأوروبي نجد أنه يستهدف كل أنواع الجرائم من هذا النوع، سواء منها المرتكبة بواسطة وسائل الكترونية (هواتف، كاميرات مراقبة ...)، أو خلال الشبكات (الأنترنت) أو النظم المعلوماتية (حواسيب، بطاقات ائتمان...)[32].

يعتبر التشهير عبر الأنترنت من أخطر الجرائم المتصلة بالخصوصية في العالم الرقمي، وما يلاحظ في هذا الشأن أنه لا توجد جريمة بهذا الوصف[33]، وإنما يقصد بهذا الاصطلاح بعض الجرائم التي تمس بشرف واعتبار الأشخاص وحياتهم الخاصة عبر الأنترنت، كالقذف والسب، ونشر الصور والأحاديث الخاصة، غير أن المشرع الجزائري وبمناسبة بعض الحوادث التي حدثت في فترة كورونا، أين قام بعض الأشخاص بالاعتداء على طواقم الصحة، قام بالنص على تجريم ذلك الاعتداء، بالإضافة إلى "تسجيل مكالمات أو حديث أو التقاط أو نشر صور أو فيديوهات أو أخبار أو معلومات على شبكة الأنترنت أو على مواقع التواصل الاجتماعي قصد المساس أو الإضرار المهنية والسلامة المعنوية للمهنيين والمستخدمين"، وهذا ما نصت عليه المادة 149 مكرر 3 الواردة تحت القسم الأول مكرر تحت عنوان: "الإهانة والتعدي على المؤسسات الصحية ومستخدميها" من الأمر رقم 20-01[34].

ونظرا للأخبار الكاذبة التي كثر تداولها في فترة تفشي وباء كورونا فقد تدخل المشرع الجزائري مرة أخرى بواسطة القانون رقم 20-06 ليجرم فعل نشر أو ترويج عمدا بأي وسيلة كانت أخبارا أو أنباء كاذبة أو مغرضة بين الجمهور يكون من شأنها المساس بالأمن العمومي والنظام العام (المادة 196 مكرر)[35]، علما أن هذه الأنباء في كثير من الأحيان تتم في الفضاء الافتراضي، وتمس الحياة الخاصة للآخرين أيضا[36].

المطلب الثاني

المواجهة الإجرائية والإدارية والقضائية للمساس بحق الخصوصية في العالم الرقمي

بمناسبة ظهور الإجرام المعلوماتي ظهرت أيضا أساليب جديدة للتحري عن هذه الجرائم، نظمها المشرع بغية أن يكون التفتيش عن هذه الجرائم مستجيبا لمطلب حماية الحياة الخاصة، وأغلب هذه الإجراءات يجب أن تستجيب لمطلب حماية حقوق الإنسان بصفة عامة، وفي الحقيقة أن هذا المطلب يخص كل الإجراءات الجزائية، ومن تلك الإجراءات نذكر ما يلي:

- تمديد الاختصاص المحلي من أجل القيام بالتفتيش (المادة 7/45 ق.إ.ج.ج).

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية (المادة 65 مكرر 6 ق.إ.ج.ج).

- تسجيل المحادثات والتقاط الصور (المادة نفسها).

- مراقبة الاتصالات الالكترونية (المادة 04 من القانون رقم 09-04).

- تفتيش المنظومات المعلوماتية (المادة 05 من القانون رقم 09-04).

- حجز المعطيات الالكترونية (المادة 06 من القانون رقم 06-04).

وبالإضافة إلى الإجراءات السابقة فقد ألزم المشرع مزدوي خدمات الاتصالات الالكترونية ببعض الالتزامات بغية الوقاية من الجرائم المعلوماتية تتعلق بالتعاون مع مصالح الأمن بخصوص التحقيق في هذه الجرائم (المواد 10، 11، 12 من القانون رقم 09-04).

وقد أنشأ المشرع هيئات جديدة متخصصة في مكافحة الجريمة المعلوماتية، تتمثل أساسا في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال (المادة 13 من القانون رقم 09-04)، والسلطة الوطنية لحماية المعطيات الشخصية (المادة 12 من القانون رقم 18-07)، وهذه الأخيرة هي سلطة ضبط إداري مستقلة في هذا المجال.، والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (تحت إشراف وزير العدل)، والمنظومة الوطنية لأمن الأنظمة المعلوماتية (تحت إشراف وزارة الدفاع).

وهناك هيئات تابعة للدرك الوطني والأمن الوطني متخصصة أيضا في هذا المجال، وتتمثل أساسا في المعهد الوطني للأدلة الجنائية وعلم الإجرام، ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني، والمصلحة المركزية لمكافحة الجريمة المعلوماتية لمديرية الأمن الوطني[37].

وعلى الصعيد القضائي صدر القانون رقم 04-14 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية لينص على توسيع الاختصاص المحلي لوكيل الجمهورية وقاضي التحقيق بخصوص الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وتم إنشاء أقطاب جزائية متخصصة[38]، طبقا للمرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 المتضمن تمديد الاختصاص المحلي لبعض المحاكم وبعض وكلاء الجمهورية وقضاة التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات[39].

خاتمـــة:

إن ما نخلص إليه من خلال هذه المداخلة أن المساس بالخصوصية في الفضاء المعلوماتي والرقمي يتمثل أساسا في المساس بالخصوصية الرقمية المتمثلة في المعلومات ذات الطابع الشخصي التي تحظى بعناية خاصة على الصعيد الدولي على أساس أنها عرضة لأشكال خطيرة من الجرائم العابرة للحدود والتي تشكل خسائر كبيرة للدول والشركات، ثم إلى حماية الحياة الخاصة للأفراد داخل الفضاء الرقمي والتي تعرف انتهاكات كبيرة خاصة في ظل مواقع التواصل الاجتماعي.

إن الحياة الخاصة بمختلف صورها ومنها الخصوصية الرقمية والخصوصيات الأخرى الجسدية والمكانية والاتصالاتية هي في واقع الأمر من حقوق الإنسان التي لازالت تثير اهتمام المجتمع الدولي بها، بالإضافة إلى القوانين الوطنية، وذلك وصولا إلى تحقيق الأمن السيبراني.

إن هذا الحق في الخصوصية يقابله حق آخر، وهو حق الحصول على فضاء رقمي وإنشاء محتوى فيه لأغراض عديدة تجارية وإعلامية وترفيهية وشخصية وسياسية وجمعوية واقتصادية، وهي حقوق حديثة، غير أن هذا الحق مرهون باحترام النظم القانونية التي تنظم العالم الرقمي، بدءا من إنشاء المواقع إلى المحتوى إلى تسجيل المنتسبين والمنضمين والزبائن، وبالأخص احترام النظام العام متمثلا في نصوص القانون العقابي الذي يتدخل لتجريم الكثير من مظاهر السلوك التي ارتبطت بالعالم الرقمي.

من التوصيات التي يمكن الخروج بها من هذه المداخلة وبغية الحد من مخاطر انتهاك الخصوصية عبر العالم الرقمي فإن المنظومة القانونية بحاجة إلى إدخال التأمين كتقنية جديدة في مجال الأمن السيبراني، وخصوصا بالنسبة للشركات، وحتى للأشخاص.

إن خطر المعلوماتية لا يمتد إلى الحياة الخاصة فحسب، بل صار يمتد إلى حياة الإنسان ذاته، عن طريق العمليات الإرهابية التي صارت نوعا من الإجرام السيبراني، ولذلك فلا مناص لمواجهة هذا الأخير من وجود تعاون دولي بهذا الخصوص، فالتحقيق في معظم هذه الجرائم يعتبر أمرًا معقدًا وصعبًا بسبب الطبيعة التقنية للإنترنت، فيتطلب ذلك وجود أحكام قانون جنائي موضوعي مناسبة، وكذلك قدرات إجرائية مناسبة، وخاصة القدرة التقنية على تحديد المهاجمين الأجانب، والحفاظ على بيانات الكمبيوتر المخزنة، وعمليات كسر التشفير، وجمع بيانات حركة المرور في الوقت الفعلي، واعتراض بيانات المحتوى، ويكون لهذه الظواهر بعد دولي، مما يتطلب تحقيقًا منسقًا في العديد من البلدان، ونتيجة لذلك فلا بد من وجود اتفاقيات دولية مناسبة وصكوك أخرى للتعاون الدولي، وهذا ما يطرح في عالم المعلوماتية بشكل عام، وكل هذا بهدف حماية حقوق الأفراد وحرياتهم، لاسيما ما يتعلق منها بحقوق الإنسان.

الهوامش:

[1] انظر: المرسوم الرئاسي رقم 20-442 مؤرخ في 2020/12/30 يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020، الجريدة الرسمية للجمهورية الجزائرية، عدد 82، مؤرخة في 2020/12/30، ص 3.

[2] هناك عدة مراجع اعتمدت هذا التقسيم الرباعي، ولا يعرف بالضبط من هو أول من استعمل هذا التقسيم، انظر: أنطونيوس أيوب بولين، الحماية القانونية للحياة الشخصية في مجال المعلوماتية، دراسة مقارنة، منشورات الحلبي الحقوقية، لبنان، 2009، ص 67.

[3] حول الخصوصية الرقمية أو المعلوماتية عموما انظر: سعيداني نعيم، الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، رسالة دكتوراه، كلية الحقوق والعلوم والسياسية، جامعة الحاج لخضر – باتنة 1، 2020، ص 80 وما يليها.

[4] انظر: موساوي عبد الحليم، الحق في الخصوصية في ظل الإعلام الرقمي، مجلة الدراسات القانونية والاقتصادية، تصدر عن: المركز الجامعي بريكة، المجلد 5، العدد 1، 2022، ص ص 1242-1278.

[5] عرفتها المادة 2/أ من الاتفاقية الأوروبية رقم 108 الصادرة عن مجلس أوروبا بأنها كل المعلومات المتعلقة بشخص طبيعي معرف أو قابل للتعرف عليه، وهو تعريف قريب جدا من التعريف الذي جاءت به المادة 2/أ من التوجيه الأوروبي رقم 95-46 الصادر بتاريخ 1995/10/24 بقولها: "المعطيات ذات الطابع الشخصي هي كل معلومة متعلقة بشخص طبيعي معرف أو قابل للتعرف عليه، يعد قابلا للتعرف عليه الشخص الذي يمكن معرفته بصفة مباشرة أو غير مباشرة لاسيما بالرجوع إلى رقم تعريف أو إلى عنصر أو عدة عناصر خاصة مميزة لهويته الطبيعية، الفيزيولوجية، النفسية، الاقتصادية، الثقافية أو الاجتماعية"، وهو التعريف الذي تبناه المشرع الجزائري بصورة تكاد تكون حرفية في المادة 1/3 من القانون رقم 18-07 المؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات

الطابع الشخصي، ج ر، عدد 34، ص 12؛ انظر: بن قارة مصطفى عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، مجلة البحوث القانونية والسياسية، تصدر عن جامعة الدكتور مولاي الطاهر سعيدة،العدد 6، 2016، ص ص 272-289.

[6] أنطونيوس أيوب بولين ، ص 11.

[7] أنطونيوس أيوب بولين ، ص 21 وما يلها.

[8] وليد السيد سليم، ضمانات الخصوصية في الأنترنت، دار الجامعة الجديدة، الإسكندرية، 2012، ص 16.

[9] رقيعي إكرام، بلال سليمة، إشكالية حماية المعطيات ذات الطابع الشخصي للمستهلك الالكتروني، المجلة القانونية للبحث الأكاديمي، تصدر عن كلية الحقوق والعلوم السياسية- جامعة بجاية، المجلد 11، العدد 02 (عدد خاص)، 2020، ص ص 691-710.

[10] رصاع فتيحة، البصمة الوراثية بين الحق في الخصوصية الجينية واعتبارات الصالح العام، مجلة الدراسات الحقوقية، المجلد 8، العدد 2، 2021، ص ص 802، 825.

[11] يحي الشريف ناصر، مزغيش عبير، الآليات المكرسة لحماية الحق في الخصوصية الرقمية في التشريع الجزائري، مجلة البحوث في العقود وقانون الأعمال، تصدر عن كلية الحقوق جامعة قسنطينة 1، المجلد 7، العدد 02، 2022، ص ص 192-213.

[12] انظر: خليف خالد، الحق في الخصوصية الرقمية في مواجهة تحديات حماية الأمن الوطني، مجلة مصداقية،تصدر عن المدرسة العليا العسكرية للإعلام والاتصال،المجلد 2، العدد 1، 2020، ص ص 174-182.

[13] لقد حل مصطلح الجرائم السيبرانية محل مصطلح الجرائم الالكترونية والجرائم المعلوماتية وهذا كتعبير عن التطور الرهيب لهذه الجرائم، ولا يوجد تعريف دقيق لها سوى أن هذا المصطلح يربط بين الإجرام وبين (الفضاءات السيبرانية cyberspac)، وهي فضاءات تسمح بتنفيذ كل أنواع الجرائم المعلوماتية، ويبقى أن هذه المقاربة غير دقيقة، وتحتاج إلى دراسة ضمن نطاق علم الإجرام لتحديدها، ويمكن رد هذه الجرائم إلى فئتين: فئة تستهدف الشبكات، وأخرى ترتكب باستخدام الشبكات، وعلى كل حال فإن الجرائم السيبرانية أخذت بعدا عالميا باعتبار أن الأنترنت نفسه هو عالم متجاوز للحدود، انظر:

Typhaine bonnet, la crise de la sanction face à la cybercriminalité : l'example du droit d'auteur, mémoire maitrise en droit, université laval, québec, canada, 2017, p1, 2.

[14] Jean-Marc Lehu, CYBERATTAQUE : LA GESTION DU RISQUE EST-ELLE ENCORE POSSIBLE ?, Analyse et enseignements du cas Sony Pictures, Direction et Gestion, « La Revue des Sciences de Gestion », 2018/3 N° 291-292 | pages 41 à 50, disponible à l'adresse : https://www.cairn.info/revue-des-sciences-de-gestion-2018-3-page-41.htm. consulté le: 16/06/2022 à 17:07.

[15] توفيق شمس الدين أشرف، الصحافة والحماية الجنائية للحياة الخاصة "دراسة مقارنة"، دار النهضة العربية، القاهرة، 2007، ص 25 وما يلها.

[16] الوردي سعيد، جرائم السب والقذف عبر وسائل التواصل الاجتماعي، دراسة فقهية وقضائية مقارنة في ضوء أحكام القانون الجنائي المغربي والقانون رقم 13.88 المتعلق بالصحافة والنشر والعمل القضائي المغربي والمقارن، دار الآفاق المغربية للنشر والتوزيع، الدار البيضاء، ط 1، 2020، ص 11 وما يلها.

[17] انظر: اللمعي ياسر محمد، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الالكتورنية دراسة تحليلية مقارنة، مجلة روح القوانين، تصدر عن كلية الحقوق، جامعة طنطا، العدد 97، 2022، ص 62.

[18] حيث أكدت الجمعية العامة على أن الحق في الخصوصية هو حق من حقوق الإنسان، وشددت على أن نفس الحقوق التي يتمتع بها الناس يتعين حمايتها أيضا على الانترنت، ودعت الدول إلى "احترام وحماية الحق في الخصوصية، وأنه إذا كانت المخاوف بشأن الأمن العام قد تبرر جمع وحماية بعض المعلومات الحساسة إلا أنه يتعين على الحكومات ضمان الامتثال التام لالتزاماتها بموجب القانون الدولي لحقوق الإنسان، انظر الرابطين التاليين:

https://news.un.org/ar/story/2013/12/193452. consulté le: 15/06/2022 à 22:51.
https://www.un.org/ar/ga/68/resolutions.shtml. consulté le: 15/06/2022 à 22:55.

[19] القانون رقم 06-23 المؤرخ في 2006/12/20 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 1966/06/08 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 84، مؤرخة في 2006/12/24، ص 11.

[20] يحي الشريف نصير، مزغيش عبير، المرجع السابق، ص 200.

[21] الجريدة الرسمية للجمهورية الجزائرية، عدد 27، مؤرخة في 2018/05/13، ص 3.

[22] القانون العضوي رقم 12-05 المؤرخ في 12 /01/ 2012 يتعلق بالإعلام، الجريدة الرسمية للجمهورية الجزائرية، عدد 2، مؤرخة في 15/01/ 2012، ص 21.

[23] الجريدة الرسمية للجمهورية الجزائرية، عدد 46، مؤرخة في 2018/07/29.

[24] الجريدة الرسمية للجمهورية الجزائرية، عدد 03، مؤرخة في 1994/01/16.

[25] الجريدة الرسمية للجمهورية الجزائرية، عدد 48.

[26] الجريدة الرسمية للجمهورية الجزائرية، عدد 4.

[27] الجريدة الرسمية للجمهورية الجزائرية،عدد 37، مؤرخة في 2016/06/22، ص 5.

[28] طاهري عبد المطلب، النحوي سليمان، الأطر القانونية المقررة لحماية الحق في الخصوصية الجينية في المواثيق الدولية وفي التشريع الجزائري والفرنسي، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، تصدر عن جامعة محمد بوضياف المسيلة، المجلد 6، العدد 2، ص ص 2102-2131.

[29] الجريدة الرسمية للجمهورية الجزائرية، عدد 34، مؤرخة في 2018/06/10.

[30] Voir : romain boos, la lutte contre la cybercriminalité au regard de l'action des états, thèse de doctorat, université de lorraine, 2016, p 24.

[31] يعتبر النموذج الأوروبي لحماية البيانات الشخصية ولموجهة التهديدات السيبرانية نموذجا عالميا في هذا المجال، انظر: شافعي آمال، شافعي أم السعد، التأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الاتحاد الأوروبي، مجلة الباحث القانوني، المجد 1، العدد 2، 2022، ص ص 108-124.

[32] Voir : pierre Berthelet, La lutte contre la cybercriminalité à l'échelle de l'Union : analyse de l'évolution juridique d'un phénomène à la confluence de plusieurs agendas institutionnels, Revue québécoise de droit international / Quebec, Journal of International Law / Revista quebequense de derecho internacional, numéro hors-série, 2018, pp 25-39, disonible à l'adresse : https://id.erudit.org/iderudit/1067257ar. consulté le 17/06/2022 à 09:37.

[33] إن مصطلح التشهير قد ورد في المادة 371 من قانون العقوبات، وهي مادة يعود تاريخها إلى القانون رقم 82-04 المؤرخ في 1982/02/13 المعدل والمتمم لقانون العقوبات، وهي تتعلق بكل من تحصل بطريق التهديد كتابة أو شفاهة أو بإفشاء أو نسبة أمور شائنة على أموال أو أوراق مالية أو على توقيع أو على المحررات المبينة في المادة 370 أو شرع في ذلك، حيث يكون بذلك قد ارتكب جريمة التهديد بالتشهير، كما سمتها المادة، وهي مادة لا تنطبق على التشهير عبر الأنترنت نظرا لعدم جواز التوسع في تفسير النص الجنائي، وهي تذكر وسائل تقليدية للجريمة المذكورة، وليس جريمة التشهير.

[34] الأمر رقم 20-01 المؤرخ في 2020/06/30 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 1966/06/08 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 44، مؤرخة في 2020/06/30، ص 4.

[35] القانون رقم 20-06 المؤرخ في 2020/04/28 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 1966/06/08 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، عدد 25، مؤرخة في 2020/04/29، ص 10.

[36] لقد عرفت فترة انتشار وباء كورونا أخطر الاعتداءات السيبرانية مستغلة الجائحة، تتعلق بالاحتيال والقرصنة والتجسس وغيرها، انظر أمثلة عنها في:

Hélène Christodoulou, La cybercriminalite à l'ère de la crise sanitaire. Les Petites Affiches, 2020, pp.11, disponible à l'adresse : https://hal.archives-ouvertes.fr/hal-03349720. consulté le 18/06/2022 à 11:02.

[37] دندن جمال الدين، الاستراتيجية الأمنية للدولة الجزائرية في مكافحة الجرائم السيبرانية، مجلة صوت القانون، تصدر عن المركز الجامعي الجيلالي بونعامة خميس مليانة، المجلد 7، العدد 2، 2020، ص ص 980-994.

[38] يعود الأساس القانوني لإنشاء الأقطاب المتخصصة إلى المادة 1/32، 2، 3 من القانون رقم 08-09 المؤرخ في 2008/02/25 المتضمن قانون الإجراءات المدنية والإدارية التي نصت على أن "المحكمة هي الجهة القضائية ذات الاختصاص العام وتتشكل من أقسام، ويمكن أيضا أن تتشكل من أقطاب متخصصة..."، ثم جاء القانون رقم 14/04 المعدل والمتمم لقانون الإجراءات الجزائية ليضع القواعد التي تسمح بتوسيع اختصاص بعض المحاكم ووكلاء االجمهورية وقضاة التحقيق في جرائم محددة، وبعدها جاء القانون رقم 04-204 المؤرخ في 2004/03/03

المتضمن تكييف العدالة مع تطور الإجرام والذي أسس 08 محاكم يمتد اختصاصها الإقليمي إلى عدة مجالس قضائية، وصدر المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05 الذي قام بتحديد وتعيين المحاكم ذات الاختصاص الإقليمي الموسع، فتقرر إسناد النظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (وجرائم أخرى) لمحاكم: الجزائر، وهران، قسنطينة، وورقلة، انظر تفصيلا حول الأقطاب الجزائية المتخصصة: طارق كور: المصالحة في جريمة الصرف، أطروحة دكتوراه، كلية الحقوق، جامعة الإخوة منتوري-قسنطينة 1، 2017، ص 103 وما يليها.

[39] الجريدة الرسمية للجمهورية الجزائرية، عدد 63، مؤرخة في 2006/10/08.

إستعمال التكنلوجيا الرقمية للتعدي على الحق في الحياة الخاصة والحق في السمعة

The use of digital technology to infringe the right to privacy and the right to reputation

الدكتورة بعلوج حسينة
كلية الحقوق_جامعة الجزائر 1_
baalohassina66@gmail.com

الدكتورة حجيمي حميدة
كلية الحقوق_جامعة الجزائر 1_
hhadiimi@ymail.com

ملخص :

إن انتشار الشائعات والمعلومات الخاطئة والرسائل الزائفة إضافة إلى الترويج إلى خطاب الكراهية عبر مواقع التواصل الاجتماعي يشجع على العنف ويمس بالإستقرار الوطني والدولي، وبدل أن تكون التكنولوجيا وسيلة لحماية الحقوق أصبحت أداة للتعدي على حقوق الإنسان ،ولعل أهمها التعدي على الحق في الحياة الخاصة والتعدي على الحق في السمعة ؛ فالمعلومات الشخصية في ظل الشبكة العالمية متوفرة ما يؤدي إلى ازدياد التهديدات لخصوصية الناس، والوصول لها بصورة غير مشروعة أكثر من ذي قبل ،إضافة إلى إزدياد جرائم السب والقذف عبر مواقع التواصل الإجتماعي، لهذا يجب إرساء قوانين دولية مشتركة تنظم مستقبل حقوق الإنسان في العصر الرقمي،كما يجب أن تواكب التشريعات الوطنية خاصة الجنائية للتطور التكنلوجي.

الكلمات المفتاحية : التكنلوجيا الرقمية،الحق في السمعة،الحق في الحياة الخاصة،التعدي،جرائم الكترونية.

Abstract:

The spread of rumors, misinformation and false messages, in addition to promoting hate speech through social media, encourages violence and harms national and international stability. in reputation; Personal information is available in light of the global network, which leads to an increase in threats to people's privacy, and illegal access to them more than before, in addition to an increase in defamation and slander crimes through social networking sites. For

this reason, joint international laws must be established that regulate the future of human rights in the digital age. It must also keep pace with national legislation, especially criminal, technological development

Keywords: digital technology, the right to reputation, the right to a private life, infringement, electronic crimes

المقدمة:

إن الإعتداء على الشرف و الاعتبار بواسطة الوسائل الالكترونية يكون أشد ضرر وأكثر ذيوعا مما يفاقم الأضراروالآلام النفسية للمضرور، فحرية التعبير عن الرأي هو حق دستوري و قانوني،إلاّ أن هذا الأخير إذا كانت ممارسته بحرية مطلقة قد يؤدي إلى نشر الفوضى، وذلك من خلال النيل من شرف الأشخاص وسمعتهم،مما حتم على المشرع سن قوانين تضع ضوابط على ممارسة الحرية الإعلامية، من خلال منع التعسف في استعمال حق النشرو تجريم القذف والسب،مع مراعاة الاحترام الواجب لهذه الحقوق و الحريات المحمية دستوريا وقانونيا.

إن الانفجار التكنولوجي والرقمي الذي عرفه حقل الإعلام والاتصال، وتغلغل هذه الوسائل الحديثة في حياة الأفراد نجم عنه وجود عالم افتراضي بدل العالم الواقعي، مما أدى لتنامي حرية الصحافة في إطار تكريسها لحق الجمهور في الإعلام، وإشباع شغف الجمهور على حساب خصوصيات الأفراد، كما أدى الاستخدام المفرط للأنترنيت من قبل الأفراد عبر مشاركة خصوصياتهم من محادثات صوتية ومصورة ولقاءات فكرية،وحتى حميمية،في ظل عدم وجود مسافات أمان كافية لحفظ السرية وحماية الخصوصية، إلى مزيد من التضييق على الحق في الخصوصية ،الأمر الذي دفع بالمشرع الجزائري للتدخل لحماية خصوصيات الأفراد عبر تقرير حماية جزائية للحق في الخصوصية في قانون العقوبات.

ولدراسة الموضوع نطرح الاشكالية الآتية :**ماهي الجرائم الماسة بالحق في السمعة والحق في الحياة الخاصة في إطارإستعمال التكنلوجيا الرقمية؟**

المبحث الأول: إستعمال التكنلوجيا الرقمية للتعدي على الحق في السمعة

لقد خولت الشريعة والقانون لكل شخص الحق في حماية شرفه واعتباره من أي اعتداء، وضمان ذلك عن طريق تجريم وتحريم تلك الأفعال التي تنقص من شرفه وتسيء إلى مكانته الاجتماعية،وفي مقدمة هذه الأفعال القذف الذي أصبح ظاهرة منتشرة تمس الإنسان في جانب حساس هو الشرف، والمشرع قصد من تجريم هذه الأفعال حماية الكيان الأدبي و المكانة الاجتماعية للشخصية الإنسانية[1](المطلب الأول).

إن جريمة السب من الجرائم الماسة بالشرف والإعتبار ،وللسب مدلول أوسع من القذف إذ يتناول كل ما يخدش الشرف والإعتبار، فحسب عبارات المادة 267 من ق ع ج يمكن أن يرد السب في ثلاثة أشكال، فيمكن أن يظهر السب في شكل تعبير مشين،كما قد يشكل السب قدحا فيكون تعبيرا في نفس الوقت جارح وعنيف وفظ، وأخيرا قد يرد السب في شكل عبارات إحتقار أي عبارات لا تحترم كرامة الشخص الذي تخاطبه وتحط من قدره علنا(المطلب الثاني).

المطلب الأول:ماهية جريمة القذف الالكتروني وأركانها

تعتبر جريمة القذف من الجرائم الماسة بشرف وإعتبار الأشخاص، فهي تحط من قدرهم ومكانتهم، ما يعني أنها تمس بالمصلحة الخاصة للأفراد،وبالرغم من التشابه بين جريمة القذف والسب والإهانة ،إلا أنه يوجد عدة إختلافات بين هذه الجرائم،لهذا سنعرف جريمة القذف الالكتوني(أولا) ونبين أركانها(ثانيا)

الفرع الأول:تعريف جريمة القذف الالكتروني

القذف اصطلاحا هو كل إسناد وإخبار لواقعة تمس شرف أواعتبارالشخص أوالجماعة التي أسندت إليها هذه الواقعة[2]،كما يقصد بالقذف قانونا،إسناد علني عمدي، أو إدعاء بواقعة محددة تستوجب عقاب أو إحتقار من أسندت إليه[3]،لقد نظم المشرع الجزائري جريمة القذف في قانون العقوبات الجزائري[4]، في المادة 296 منه التي تنص"يعدّ قذفا كل

إدعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها،أو إسنادها إليهم أو إلى تلك الهيئة،و يعاقب على نشر هذا الإدعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكرالاسم،ولكن كان من الممكن تحديدهما من عبارات الحديث أوالصياح أو التهديد أو الكتابة أو المنشورات أواللافتات أوالإعلانات موضوع الجريمة".

كما نص قانون الإعلام 12- 05على جريمة القذف في المادة 93 منه التي تنص على أنه: "يمنع انتهاك الحياة الخاصة للأشخاص وشرفهم واعتبارهم"، أمّا المادة 54 من قانون 14-04 المتعلق بالنشاط السمعي البصري فتنص أن من مهام سلطة الضبط السمعي البصري السهر على احترام الكرامة الإنسانية،حيث يعد الشرف والإعتبار أهم ما يحافظ به الإنسان على كرامته،ونظرا للطبيعة القانونية الخاصة بالجرائم المرتكبة ضد الأفراد باستخدام تكنولوجيات الاعلام والاتصال، فقد نص المشرع الجزائري على انشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ضمن المادة 13 و 14 من قانون رقم 09-04 [5] والمادة 02 من المرسوم الرئاسي رقم 15-261[6].

الفرع الثاني:أركان جريمة القذف الالكتروني

من خلال تعريف جريمة القذف نلاحظ أنها تتكون من أركان،فبالإضافة للركن اشرعي المتنمثل في نص المادة 292 من ق ع ج ،نجد أركان أخرى، وللتفصيل فيها استوجب الأمر دراستها في ثلاثة نقاط على التوالي، بحيث يتم تناول الركن المادي أولا ،ركن العلانية ثانيا، و ركن القصد الجنائي ثالثا.

أولا:الركن المادي يتجسد الركن المادي لجريمة القذف في اجتماع عدة عناصر وهي:

1: الادعاء بو اقعة معينة و إسنادها: الإدعاء هو كل سرد يحمل معنى الرواية عن الغير أو ذكر الخبر محتمل الصدق أو الكذب،أما الإسناد فهو نسبة واقعة إلى شخص على وجه الّتأكيد سواء كانت الواقعة صحيحة أوكاذبة،ويتحّقق القذف بطريقة مباشرة أوغير

مباشرة وبكلّ صور الّتعبير،ولو كان عن طريق بث الشك في أذهان الجمهور،فلا يشترط أن تكون الواقعة صحيحة أو كاذبة[7]، بل يكفي أن تكون محتملة وأن تلقي في أذهان الناس ظّنا أو احتمالا ولو مؤّقتين بصحتها، ولو كان ذلك بصفة استفهامية أو غامضة[8]،كما يستوي أن ينسب الجاني الواقعة إلى المجني عليه باعتبارها من معلوماته الخاصة أو بوصفها رواية ينقلهاعن الغير[9]،ويدل الإخبار على معنى الرواية على لسان الغير أو ذكر الخبرمحتملا الكذب والصدق،أما الإسناد فهو نسبة أمر إلى شخص معين على سبيل التأكيد بأي وسيلة من وسائل التعبير،والفرق بين الإسناد والإخبار أن الأول يكون على سبيل القطع واليقين، أما الثاني فيكون على سبيل الظن والشك.

يكون الإسناد أوالإدعاء بأي وسيلة من وسائل التعبير سواء شفاهة أو كتابة أو حتى بالإشارة ،حيث جاء في المادة 292 من ق ع ج " يعد قذفا كل إدعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به أو إسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الادعاء أو ذلك الاسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدها من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الاعلانات موضوع الجريمة" .

المقصود بإسناد الادعاء في جريمة القذف الالكتوني هو نسبة الأمر الشائن إلى المجني عليه بأية وسيلة من وسائل التعبير (صحافة مكتوبة ،السمعي البصري،لأنترنت وغيرها) ،و يستوي أن تكون عبارات القذف التي أذاعها الجاني منقولة عن الغير أو من انشائه هو، بحيث نقل الكتابة التي تتضمن جريمة و نشرها يعتبر في حكم القانون كالنشر الجديد سواء بسواء ، ولا يقبل من أحد للإفلات من المسؤولية الجزائية ، أي يتذرع بأن تلك الكتابة نقلت من صحيفة أخرى أو موقع إلكتروني[10].

2: تعيين الو اقعة:يجب أن يصب الإدعاء أو الإسناد على واقعة معينة و محددة ،وبهذا الشرط يتميز القذف عن السب لأنه إذا كان خاليا من واقعة معينة فإنه يكون سبا لا قذف،و

مثال ذلك أن يسند الفاعل إلى المجني عليه أنه سارق أو نصاب أو مرتشي،كمايعتبر قاذفا من أسند إلى شخص سرقة سيارة فلان ، ومن أسند إلى قاض أنه تلقي رشوة في قضية معينة، فتعيين الواقعة شرط جوهري حيث يعد الحد الفاصل والعلامة المميزة لجريمة القذف عن جريمة السب ، فالأخيرة تتحقق بمجرد اسناد العيب دون أن يتضمن واقعة معينة أومحددة ، أي لا يشترط فيه أن يكون الاسناد منصبا على واقعة معينة ،وإنما يتضمن خدشا للشرف والاعتبار مثل وصف الفتاة بأنها فاسقة[11]،أما القذف الموجه للهيئات فيكون باتهامها مثلا أّنها تعمل خلافا للصالح العام أو أن وضعيتها المالية غير سليمة أو أنها تلجأ إلى أساليب غير سليمة في تعاملاتها[12].

3:أن يكون من طبيعة تلك الو اقعة المساس بالشرف و الإعتبار:فالشرف لا نقصد به قيمة الإنسان في نظر الغير إنما قيمته في تصوره هو ،لذا فالفعل الماس بالشرف يعني الفعل المخالف للنزاهة،أما الاعتبار فنقصد به الصورة التي يريد أن يكون عليها الإنسان في نظر غيره،وما يمس الاعتبار هو كل ما يمس الإنسان في نظر الغير،ومسألة الشرف و الاعتبار يرجع تقديرها إلى قاضي الموضوع تبعا للظروف المحيطة بالواقعة المسندة.فالإدعاء بأن فلان يزني مع خادمته، أو كمن يقول عن فتاة بغي وأنها تسترزق من البغاء يعد قاذفا، وليس بالضرورة أن يحدث التحقير من قبل الناس كافة ، بل يكفي لقيام الجريمة أن يكون من شأن إسناد مثل هذه الوقائع تحقير المسند إليه من قبل أفراد مجتمعه الذين يخالطهم ويتعامل معهم ، كما لا يشترط للعقاب عليها أن تكون الواقعة المسندة إلى المجني عليه صادقة أو كاذبة.

4: أن تكون الو اقعة مسندة لشخص محدد أو لهيئة معينة يشترط في جريمة القذف تعيين الأشخاص سواء أكانت طبيعية أومعنوية، ولا يستوجب تحديد المجني عليه بذكر اسمه، إنما يكفي أن يكون القذف الموجه يسهل معرفة الشخص أو الهيئة محل القذف،كما يكفي أن يفهم من المقال هوية هذا الشخص الموجه أو الهيئة المعنية بالأمر[13]،و في هذا السياق ورد في قرار المحكمة العيا بأنه" ما دام المتهم أشار في المنشور الذي نشره في صحيفة

"لوماتان"إلى مدير مركب أسمدال فإنه بذلك يكون قد قصد الطرف المدني (ل،م) و هو مدير المركب إذ من الممكن تحديده من خلال الإشارة إلى صفته كمدير المركب"[14].

ثانيا:العلانية

تعتبر العلانية احدى العناصر الأساسية في جريمة القذف باعتبارها من الجرائم التي ترتكب عن طريق النشرأووسائل الاعلام المسموعة والمرئية، كما ترتكب بواسطة تكنولوجيات الاعلام والاتصال لما توفره من امكانية نشر الواقعة الماسة بشرف واعتبار الأشخاص على نطاق واسع، ولعل الشبكة العنكبوتية العالمية ومواقع التواصل الاجتماعي احدى هذه الوسائل التي توفر العلانية إذا ما تم نشر واقعة القذف عن طريقها[15].

فالعلانية تتحقق بالقول والكتابة والصور والرسوم والمنشورات والإعلانات وغيرها حسب نص المادتين 144 مكرر من ق ع ج التي تنص" يعاقب بغرامة من 100.000 دج إلى 500.000 دج، كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية ألية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أوإعلامية أخرى"،وحسب المادة 296 من ق ع ج التي تنص" يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أوالهيئة المدعى عليها به أو اسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الادعاء أو ذلك الاسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكرالاسم ولكن كان من الممكن تحديدها من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة".

مايمكن ملاحظته أن المشرع الجزائي في المواد 296 و 297 ق ع المتعلقة بالقذف والسب الموجه للأشخاص لم يضف عبارة "أو أية وسية أخرى"،خلافا للمادة 144 مكرر التي تعاقب على إهانة وسب وقذف رئيس الجمهورية بأية وسيلة كانت،سواء إلكترونية أو عادية،وهو مايجب إستدراكه ،فكثير من جرائم القذف منتشرة عبر شبكة الأنترنت،كما يتحقق القذف العلني بالنشر عن طريق استخدام الفيس بوك حيث تتحقق به العلانية،مادام المنشور

مفتوحا للعامة،وطالما يراه أي عدد من الأشخاص دون تمييز، ودون أن تربطهم صلة معينة سواء كان ذلك على صفحة شخصية أو في مجموعة مغلقة أو متاحة[16]،حيث جاء في قرار محكمة النقض المصرية "ثبوت الاتهام الثاني في حق المتهمان وهو قيامهما بقذف المجني عليه علانية على موقع التواصل الاجتماعي (الفيس بوك) عبر شبكة المعلومات الدولية (الإنترنت)، بأن أسند له أمورا لو كانت صادقة لأوجبت عقابه واحتقاره عند أهل وطنه،وقيام العديد من المشاركين بغير تمييز بالإشتراك في الصفحتين القائمين عليها المتهمان والاطلاع عليها والمشاركة بتعليقاتهم، والاطلاع على تلك التعليقات بما يحقق العلانية"[17].

ثالثا:الركن المعنوي

جريمة القذف من الجرائم العمدية إذ يتخذ ركنها المعنوي صورة القصد الجنائي العام، ويتجسد هذا القصد بإسناد واقعة القذف إلى المجني عليه مع العلم والإدراك أنها لو كانت صادقة لفرض العقاب على المجني عليه، وبالتالي تخدش كرامته و شرفه بين أهل وطنه، و متى توفر القصد الجنائي في جريمة القذف تحققت الجريمة دون اشتراط نية الإضرار، فلا عبرة لما يسبق القذف من بواعث ومايليها من أغراض ،كما لايجوز للمتهم التذرع بالاستفزاز في القذف للإفلات من العقاب ، فلا تفقد عبارات القذف طبيعتها حتى وإن كانت ردا على عبارات قاذفة.

إن قيام القصد الجنائي لتكوين جريمة القذف يستوجب زيادة على علم الجاني بتجريم فعل الاسناد أو الاخبار الذي قام به، توجه إرادته الإجرامية لإرتكابها، فالارادة التي تدخل في تكوين القصد الجنائي هي الإرادة الإجرامية تستمد صفتها من طبيعة الغرض الذي تسعى إلى تحقيقه، فالإرادة هي ذلك النشاط النفسي الذي يتوجه لتحقيق غرض عن طريق وسيلة معينة ينبغي في إطار ذلك أن تتوجه إرادة القاذف لإذاعة عبارات أو ألفاظ القذف وذيوعها بين الجمهور[18]،وينتفي القصد الجنائي إذا ثبت أن القاذف كان مكرها على توجيه عبارات القذف وإذاعتها تحت تأثيرفعل التهديد.

الفرع الثالث:عقوبة القذف الالكتروني

إن علة تجريم القذف هو مساسه بشرف المجني عليه واعتباره، ويتخذ هذا المساس صور خطيرة، لهذا فالقذف أشد جسامة من سائر جرائم الاعتداء على الشرف والاعتبار

أولا: عقوبة القذف الموجه ضد الأفراد

بالرجوع لنص المادة 298 من ق ع ج فإن عقوبة القذف الموجه للأفراد هي الحبس من شهرين إلى ستة أشهر وبغرامة من 25000 دج إلى 100000 دج أو بإحدى هاتين العقوبتين،فللقاضي السلطة التقديرية في الإختيار بين عقوبة الحبس والغرامة وذلك حسب خطورة الأفعال المجرمة، وقدر الضرر الذي أحدثته، وعدل المشرع هذه المادة من خلال الأخذ بعين الإعتبارصفح الضحية الذي كان في فترات سابقة يعتد به القضاة كظرف مخفف للعقوبة، أما الآن فيضع صفح الضحية حدا للمتابعة الجزائية.

غير أن هناك رأي يرى بأن الأمر يستدعي تشديد العقوبة في جريمة القذف المرتكبة عبر تكنولوجيات الإعلام والإتصال،كونها تؤدي إلى أضرار أوسع انتشارا من المطبوعات والصحف ووسائل الإعلام الأخرى،بحيث يتضمن تشديد العقوبة إذا كانت علانية القذف باستخدام إحدى تكنولوجيات الاعلام والاتصال كاستخدام الحاسب الألي والأنترنت[19].

ثانيا: عقوبة القذف الموجهة لشخص أوأكثر بسبب إنتمائهم إلى عرق أو مذهب أو دين معين

إذا كان قذف الأشخاص بسبب إنتمائهم إلى مجموعة عرقية أو مذهبية أو دينية يهدف إلى التحريض على الكراهية بين المواطنين والسكان، تكون العقوبة في هذه الحالة حسب ما ورد في المادة 298 فقرة 2 من قانون العقوبات الجزائري مشددة بالمقارنة مع الحالة السابقة، حيث تتراوح بين الحبس من شهر واحد إلى سنة و بغرامة من 10000 دج إلى 100000 دج أو بإحدى هاتين العقوبتين.

تكمن علة التشديد في أن هذا القذف يؤدي إلى وقوع الفتنة بين أبناء البلد الواحد مهما كانوا مختفين في العرق والدين والمذهب،مثل منطقة القبائل والشاوية في الجزائر،والأكراد في

العراق،والمسيحيين في لبنان ومصر،والحرب الطائفية في لبنان،فهذا القذف من شأنه المساس بالوحدة الوطنية واستقرار الوطن.

ثالثا:عقوبة القذف الموجهة لرئيس الجمهورية و أية هيئة نظامية أوعمومية

نص المشرع الجزائري بموجب المادة 144 مكرر من ق ع ج على عقوبة الغرامة من 100000 دج إلى 500000 دج لكل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أوسب أوقذف، سواء كان ذلك عن طريق الكتابة أوالرسم أوالتصريح،أوبأية آلية لبث الصوت أو الصورة ،أو بأية وسيلة إليكترونية أومعلوماتية أوإعلامية أخرى.

إن المشرع قد أحسن حين وسع التجريم ليشمل كل وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى ترتكب عن طريقها جرائم الإساءة إلى رئيس الجمهورية، وبالتالي يكون قد شمل كل ما قد يكشف في المستقبل من تقنيات الاعلام والاتصال[20]،كماتطبق نفس العقوبات حسب المادة 146من قانون العقوبات إذا كان القذف موجها ضد البرلمان أو إحدى غرفتيه أوضد الجهات القضائية أوضد الجيش الشعبي الوطني أوأية هيئة نظامية أوعمومية أخرى، وفي حالة العود تضاعف الغرامة في الحالتين حسب المادة 144 مكررو 146 ق ع ج.

رابعا:عقوبة القذف الموجهة ضد القضاة، الموظفين، الضباط العموميين، القادة أورجال القوة العمومية المادة 144ق ع ج

تتمثل عقوبة القذف المندرج تحت عبارة الإهانة الموجهة ضد القضاة، الموظفين، الضباط العموميين، القادة أو رجال القوة العمومية، إن كانت الأفعال غير علنية أثناء تأديتهم وظائفهم أوبمناسبة تأديتها وكان القصد منها المساس بشرفهم وإعتبارهم أو الإحترام الواجب لسلطتهم، في الحبس من شهرين إلى سنتين وبغرامة من 1000 دج إلى 500000 دج أوبإحدى هاتين العقوبتين فقط.

المطلب الثاني:ماهية جريمةالسب الالكتروني وأركانها

إن جريمة السب من الجرائم الماسة بالشرف والإعتبار ،وللسب مدلول أوسع من القذف إذ يتناول كل ما يخدش الشرف والإعتبار (الفرع الأول)،تقوم جريمة السب على أركان وهي الركن المادي ، والعلانية هي ركن أساسي في جريمة السب رغم عدم النص عليها صراحة في نص المادة 297 من قانون العقوبات الجزائري،والركن المعنوي المتمثل في القصد الجنائي(الفرع الثاني).

الفرع الأول:تعريف جريمة السب

إن السب هو كل خدش لشرف وإعتبار شخص بأي وجه من الوجوه دون أن ينطوي ذلك على إسناد واقعة معينة إليه،حيث نصت المادة 297 من قانون العقوبات أن السب يعد كل تعبير شائن بإعتباره يتضمن تحقيرا أو قدحا لا ينطوي على إسناد واقعة،موجه إلى شخص أو هيئة معينة،كما يلاحظ من هذا التعريف أن المشرع لم يذكر وسائل التعبير التي تتتم بهاجريمة السب خلافا لما سبق ذكره في تعريفه للقذف .

الفرع الثاني:أركان جريمة السب الاكتروني

بالإضافة للركن الشرعي لجريمة السب والمتمثل في نص المادة279 من ق ع ج، يشترط توافر ركنين هما، ركن مادي يتمثل في إرتكاب السلوك المعاقلب عليه قانونا، وركن معنوي يتخذ صورة القصد الإجرامي.

أولاً: الركن المادي إن الركن المادي لجريمة السب العلني،طبقا للمادة 297 من ق.ع، يتحقق بتوافر العناصر الآتية:

1: طبيعة الّتعبير المشين أو البذيء:يشترط لقيام جنحة السب إستعمال عبارات شائنة وبذيئة تخدش شرف وإعتبار الأشخاص الموجهة إليهم،بحيث تحمل الإهانة أوالإحتقارألفاظا قبيحة موجهة على الملأ لشخص معين قصد إضراره.

2:الإسناد في السب يتحقق النشاط الإجرامي المكون لجنحة السب إذا أسند الجاني إلى المجنى عليه عيباً معيناً دون أن يحدد واقعة معينة،كأن يقول له أنه مرتش أو لص،ويتحقق

النشاط بنسبة عيب غير معين إلى المجنى عليه، مثال ذلك القول عن شخص أنه عديم الخلق أو مفسد أو شريرأولا يمكن الإعتماد عليه،فالعيب المشين هو كل نقص في صفات المسند إليه أو أخلاقه أوسيرته،كمن يقول عن آخر أنه لص أو مزور أو نصاب أو سكير أو فاسق، ولا عبرة بالوسيلة أو الأسلوب التي تصاغ به عبارات السب،كذلك يقوم السب ولو دون إسناد عيب إذا كان التعبير يحمل معنى تحقير المجنى عليه كالقول عن شخص أنه حيوان.

3: تحديد الشخص المقصود بالسب يشترط في السب أن يكون موجها إلى شخص طبيعي أو معنوي بالّذات، فلا تقوم هذه الجريمة إذا كان السب موجها إلى أشخاص خياليين أوغير موجودين،ومن هذا القبيل السكران الذي يدفعه سكره إلى التفوه في الطريق العام بألفاظ السب غير قاصد بذلك شخصا معينا،وتتطلب جريمة السب كذلك تعين شخص المجنى عليه،ويجب أن يكون العيب أوالتعبيرالذي من شأنه خدش الشرف والإعتبار موجها إلى شخص معين أوأشخاص معينين، يستوي أن يكون شخصلاً طبيعياً أومعنوياً،غير أنه لا يشترط تحديد شخص المجنى عليه بالإسم،وإنما يكفي أن يكون من السهل التعرف عليه[21].

ثانيا:ركن العلانية

تشترط جنحة السب العلني العلانية، وهي نفس العلانية المقررة لجريمة القذف العلني، وبه يتميز عن السب غير العلني الذي لا يشترط العلانية ويعتبر مخالفة، وما تجدر الإشارة إليه أن المشرع الجزائري لم يشر إلى العلانية في نص المادة 297 من ق.ع، وعليه تعتبر العلانية عنصر أساسيا في جنحة السب العلني، بإحدى الطرق الممثلة كما سبق بيانه في جريمة القذف العلني مثل القول، الحديث، الصياح، الكتابة، النشر سواء في الصحف أو في الوسائل السمعية البصرية كالتلفاز، الراديو، أوعلى شبكة الانترنت، وكذا في جميع الأماكن العمومية،كالطرق والمساحات العامة،ويمكن أن تتحقق العلنية بواسطة الكتابة بموجب وثائق كالكتاب والملصقات والمناشير والرسوم والصور،كما يتم النشر بواسطة التوزيع أو إعادة التوزيع أو البيع أو العرض في الأماكن العامة.

ثالثا:الركن المعنوي

إن جريمة السب العلني من الجرائم العمدية،ومن ثم يجب أن يتوافر فيها القصد الإجرامي العام بعنصريه العلم والإرادة، إذ يتمثل القصد الإجرامي بانصراف إرادة الجاني إلى إذاعة الأمور الخادشة للشرف أوالإعتبار مع علمه بمعناها، فلابد أولاً أن يعلم الجاني بمعنى الأمور المتضمنة للسب، فعنصر العلم يكون مفترض إذا كانت عبارات السب شائنة بذاتها،ومع ذلك يجوز للمتهم أن يدحض هذا الافتراض، بإقامة الدليل على أن عبارات السب في بيئته غير شائنة وأنه كان يجهل معناها في البيئة التي أذيعت فيها[22].

الفرع الثالث:عقوبة جريمة السب الالكتروني

الملاحظ في جريمة السب وفقا لقانون العقوبات الجزائري أنها تختلف باختلاف طبيعة الشخص الذي أسند إليه السب

أولا:عقوبة السب الموجه إلى الأفراد

وهو السب الموجه إلى فرد أوعدة أفراد، وتكون العقوبة طبقا للمادة 299 من ق ع ج "بالحبس من شهر(1)إلى ثلاثة (3)أشهروبغرامة من 10.000دج إلى25.000 دج، ويضع صفح الضحية حدا للمتابعة الجزائية"،فمن خلال هذا النص تعتبر جنحة السب العلني بسيطة، إذا كان السب موجه إلى الأفراد الطبيعيين، مع الإشارة بأن صفح الضحية أو تنازلها عن الشكوى يضع حدا للمتابعة الجزائية.

ثانيا:عقوبة السب الموجه لشخص أو عدة أشخاص منتمين إلى مجموعة عرقية أو مذهبية أو إلى دين معين

حسب المادة 298 مكررمن ق ع ج يعاقب على السب الموجه إلى شخص أو أكثر بسبب انتمائهم إلى مجموعة عرقية أو مذهبية أو إلى دين معين بالحبس من خمسة (5) أيام إلى (6)أشهر وبغرامة من 5.000 دج إلى 50.000 دج أو بإحدى هاتين العقوبتين فقط.

نلاحظ أن المشرع الجزائري قد ضاعف و شدد العقوبة إذا توافر الظرف المشدد والمتمثل في توجيه السب العلني ضد شخص أو أكثر بسبب إنتمائهم إلى مجموعة عرقية أو

مذهبية أو إلى دين معين،ويمكن للقاضي أن يحكم بعقوبتي الحبس والغرامة معا أو بإحداهما فقط،وعلة التشديدأن السب هنا يؤدي إلى إثارة النزاعات والفتن،وبالتالي المساس بالأمن والنظام العموميين.

ثالثا:عقوبة السب الموجه إلى الرسول (صلى الله عليه وسلم) أو بقية الأنبياء

إن العقوبة في هذه الجريمة حسب المادة 144 مكرر2 هي الحبس من ثلاث سنوات إلى خمس سنوات وبغرامة من 50.000دج إلى 100.000دج أو بإحدى هاتين العقوبتين، وعلة تشديد العقوبة بالنسبة لجريمة سب الرسول صلى الله عليه وسلم، أوأحد الأنبياء،أنها جريمة تمس بركن من أركان الإيمان ،فالإسلام هو دين الدولة وأهم أسسها.

رابعا:عقوبة السب الموجه إلى رئيس الجمهورية

يعاقب المشرع على السب الموجه إلى رئيس الجمهورية بنفس العقوبة المقررة لقذفه، ويفهم ذلك من نص المادة 144 مكررمن ق ع ج " يعاقب بغرامة من 100.000 دج إلى 500.000 دج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن سبا سواء كان ذلك عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو صورة أو بأية وسيلة الكترونية أو معلوماتية أو إعلامية أخرى،تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيا،وفي حالة العود تضاعف الغرامة".

خامسا:عقوبة السب الموجه إلى الهيئات

إن العقوبة المقررة لجريمة السب الموجهة لرئيس الجمهورية حسب المادة 144 مكرر هي نفسها بالنسبة لجريمة السب الموجهة للهيئات، فحسب المادة146 من ق.ع ج فالعقوبة هي الغرامة من 100.000 دج إلى 500.000 دج، إذا كان السب موجه ضد البرلمان أو إحدى غرفتيه أو ضد الجهات القضائية أو ضد الجيش الوطني الشعبي أو ضد أي هيئة نظامية أخرى، وفي حالة العود تضاعف الغرامة،حيث نلاحظ أن المشرع إكتفى بعقوبة الغرامة بالنسبة للسب الموجه لرئيس الجمهورية والهيئات.

المطلب الثالث:مسؤولية مقدمي خدمات الأنترنت

يطلق على مقدمي خدمات الأنترنت تسميات كثيرة منها متعهدي الوصول أو مزودي الخدمة،وقد يكون مقدم خدمة الأنترنت شخصا طبيعيا أوشخصا معنويا مثل اتصالات الجزائر، بحيث عمله ذو طبيعة فنية ، فهو الذي يمكن مستخدمي الانترنت من الوصول إلى المواقع أوالبريد الالكتروني للأشخاص الذين يريدون مخاطبتهم في أي مكان في العالم[23].

ينص قانون رقم 16-02 على المسؤولية الجزائية بالنسبة لمقدم خدمات الأنترنت، وذلك في نص المادة 394 مكرر8 "دون الإخلال بالعقوبات الإدارية المنصوص عليها في التشريع والتنظيم الساري المفعول، يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 2.000.000 دج إلى 10.000.000 دج أو باحدى هاتين العقوبتين فقط مقدم خدمات الانترنت بمفهوم المادة 02 من القانون 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال".

لقد إستدرك المشرع الجزائري بعض العيوب التي كانت في قانون الإعلام السابق، ف نص على المسؤولية الجزائية للصحافة الإلكترونية بموجب المادة 115 من القانون العضوي 12-05، أما بالنسبة للمسؤولية الجزائية المتعلقة بخدمة الاتصال السمعي البصري عبر الانترنت فإنه أقام المسؤولية لكل من مدير خدمة الاتصال البصري أوعبر الأنترنت وصاحب الخبر، حيث يتحمل المدير مسؤول النشرية أو مدير جهاز الصحافة الإلكترونية، وكذا صاحب الكتابة أو الرسم مسؤولية كل كتابة أو رسم يتم نشرهما من طرف نشرية دورية أو صحافة إلكترونية،ويتحمل مدير خدمة الاتصال السمعي البصري أو عبر الانترنت وصاحب الخبر الذي تم بثه المسؤولية عن الخبر السمعي و/أو البصري المبث من قبل خدمة الاتصال السمعي البصري أو عبر الإنترنت.

من جهة أخرى،إن قانون الإعلام 12-05 وسع من دائرة المسؤولين فإضافة إلى كاتب المقال و مدير النشرية يعتبر مسؤولا كل من الطابع و الموزع و البائع الملصق، البات للأخبار، وهذا نظرا لخطورة الجريمة باعتبار القذف والسب بواسطة النشر يذاع على أوسع نطاق،

فلم يذكر الكاتب والمدير على سبيل الحصر إنما يجوز مسائلة كل من كان له يد في الجريمة كفاعل أصلي أو شريك[24].

المبحث الثاني: جرائم انتهاك الخصوصية في نطاق المعلوماتية

يمثل الحق في الحصول على المعلومة واحداً من أهم الحقوق الأساسية المعترف بها للفرد بمقتضى مختلف الإعلانات والاتفاقيات الدولية،والتي كرّسها التعديل الدستوري الجزائري في 2020 بموجب المادة55 فقرة 1 ،وسعى المشرع من خلال الإصلاحات القانونية الأخيرة إلى تقرير أساليب مختلفة للتمتع به في شتى المجالات المختلفة، غير أنّ تمتع الفرد بهذا الحق قد يشكل اعتداءاً على حق الغير في حرمة حياته الخاصة في بعض الحالات، لهذا سنتطرق لمفهوم جرائم انتهاك الخصوصية في نطاق المعلوماتية(المطلب الاول) ثم لصور هذه الجرائم(المطلب الثاني).

المطلب الأول: مفهوم جرائم انتهاك الخصوصية في نطاق المعلوماتية

يعرّف الحق في الحصول على المعلومات بأنّه حق قانوني يسمح لكل فرد بالحصول على المعلومات والسجلات التي تحتفظ بها الجهات التنفيذية والتشريعية والقضائية في الدولة، أوأي مؤسسة تملكها الدولة ،أوأي جهة تقوم بمهام عامة،باستثناء تلك المعلومات التي تستثنى بنص القانون،والتي لا يجوزإفشاؤها حفاظا على الأمن الوطني أو الحقوق الشخصية أو سير العدالة أو غيرها من المعلومات التي تسبب ضرراً للصالح العام أو للأفراد[25].

غيرأن تمتع الفرد بهذا الحق المكفول دستوريا يجب أن لا يمس أن تمس ممارسة هذا الحق بالحياة الخاصة للغير وبحقوقهم حيث جاء في المادة 55 من التعديل الدستوري في 2020 :" يتمتع كل مواطن بالحق في الوصول إلى المعلومات والوثائق والإحصائيات، والحصول عليها وتداولها،لا يمكن أن تمس ممارسة هذا الحق بالحياة الخاصة للغير وبحقوقهم، وبالمصالح المشروعة للمؤسسات،وبمقتضيات الأمن الوطني،يحدد القانون كيفيات ممارسة هذا الحق".

إن أول تكريس لمفهوم الحق في الخصوصية في نطاق المعلوماتية كان في مؤتمر الأمم المتحدة لحقوق الإنسان المنعقد بطهران عام 1968 أين تم تناول موضوع مخاطر التكنولوجيا على الحق في الخصوصية،أو الحق في البيانات الشخصية ،وفي الجزائر كان التشريع الجزائري يعاني من وجود فراغ في هذا المجال ،وهو ماتداركه المشرع من خلال إصدار القانون 18-07 المؤرخ في 10 جوان 2018 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[26] ،تكريسا للمادة 46 فقرة 4 من التعديل الدستوري في 2016[27] التي تنص أن "حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه ".

يمكن تعريف الحق في الخصوصية عبر الأنترنت على أنه هو ذلك الحق في الذي يحمي الحياة الخاصة للإنسان من خلال إحاطته بالسرية، ومعاقبة كل من يحاول الإعتداء عليه في ظل الأنظمة المعلوماتية أو عبر شبكات الأنترنت،فلقد بات من السهل الحصول على المعلومات المخزونة بالحاسوب المرتبط بشبكة الإنترنت، كما أنَّه يمكن تبادل المعلومات بين حاسوب وآخر، لذلك قيل أن شفافية الإنسان وخصوصيته باتت عارية أمام ما تمخض عنه العلم من إعجاز في عالم الحواسيب، فلم تعد حجة السرية التي يكفلها النظام الآلي لمعالجة البيانات حجة مقنعة، إذ أصبحت حالات اقتحام النظام الآلي مسألة واردة وليست مستحيلة.

المطلب الثاني:صورجرائم انتهاك الخصوصية في نطاق المعلوماتية

تجدر الإشارة على أن المشرع الجزائري، قد وضع النصوص التي تعاقب على الأفعال التي تشكل جرائم معلوماتية وكان ذلك سنة2001,المادة 144 مكرر،ومكرر1 ،ومكرر2، والمادة 146 من قانون العقوبات ثم أصدر نصا تشريعيا سنة 2004 يشمل سبعة مواد من المادة 394 مكرر إلى المادة 394 مكرر 7،وهذا تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"،القسم السابع مكرر من قانون العقوبات، وأخيرا القانون رقم 04-09 المؤرخ في 05 أوت2009والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال و مكافحته

الفرع الأول:أركان وعقوبة جريمة الدخول عن طريق الغش إلى النظام الآلي

تضمن قانون العقوبات الجزائري هذه الصورة من الجرائم، فبالرجوع إلى نص المادة 394 مكرر من قانون العقوبات الجزائري،يتضح لنا أن جريمة الدخول إلى نظام المعالجة الآلية للمعطيات تقوم كسائر الجرائم الأخرى على ركنين،الركن المادي والذي يشمل السلوك الإجرامي الذي يترتب عنه الدخول غير المشروع إلى النظام، والركن المعنوي المتمثل في القصد الجنائي .

أولا:الركن المادي

يتكون الركن المادي في هذه الجريمة من نشاط إجرامي، يتمثل أساسا في تحقق فعل الدخول،وحيث أن السلوك الإجرامي قد يأخذ صورة إيجابية أوسلبية،و يتطلب من الجاني مباشرة نشاط إيجابي،ولا يمكن أن تتحقق الجريمة بنشاط سلبي.

في التسلل الإلكتروني إلى البيانات،يقوم القراصنة بمحاولة الدخول إلى النظام للوصول إلى هذه المعلومات التي تكون غالباً سرية،وتجري عملية الدخول إلى النظام المعلوماتي عن طريق خرق هذه المنافذ والوصول إلى قاعدة البيانات،وتعديلها أوإضافة المعلومات المغلوطة بها، بهدف الاستفادة غير المشروعة من تلك البيانات[28]، وتجدر الإشارة كذلك إلى أن مدلول كلمة الدخول ينصرف إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي،أو السيطرة على المعلومات التي يتكون منها،كما أن فعل الدخول إلى النظام المعلوماتي لا يعتبر بحد ذاته سلوكا غير مشروع،وإنما يتخذ هذا الوصف إنطالقا من كونه قد تم دون وجه حق[29].

وهذا الدخول يكون في كثير من الأحيان لسرقة المعلومات الخاصة وتزويرها،ومثالها تلك المعلومات المتعلقة ببطاقات الائتمان وسرقة كلمة السرأو الاستيلاء عليها، و كلمة السر مثل باب المنزل، ومن يقدم على كسر هذا الباب والدخول إلى قلبه يكون قد ارتكب جريمة يعاقب عليها القانون[30]،وتخريب النظام يعني ممارسة أفعال عليه من شأنها جعله غير قابل لإستخدام أو الإستعمال،ولتحقق الظرف المشددلابد من وجود علاقة سببية بين الدخول أو

البقاء وبين النتيجة المشددة، فان حدثت هذه الأخيرة نتيجة لفعل آخر لم يتم هذا الظرف المشدد.

ثانيا:الركن المعنوي

تعد جريمة الدخول إلى نظام الآلي من الجرائم العمدية، بحيث يتخذ الركن المعنوي فيها صورة القصد الجنائي المتكون من علم وإرادة،وذلك بأن تتجه إرادة الجاني إلى فعل الدخول وأن يعلم الجاني أن ليس له الحق في الدخول إلى النظام ،وبالرجوع إلى نص المادة 394 مكرر من قانون العقوبات الجزائري، يلاحظ أن القصد الجنائي العام لا يكفي، وإنما يجب توافر قصد جنائي خاص وهو الغش، و بهذا نكون بصدد جريمة الدخول غير المشروع للنظام الآلي.

ثالثا: عقوبة جريمة الدخول عن طريق الغش إلى النظام الآلي

حسب المادة 394 مكرر من ق ع ج فعقوبة هذه الجريمة هي الحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج الى 100.000دج .

الفرع الثاني:أركان وعقوبة جريمة البقاء عن طريق الغش في النظام المعلوماتي

تناول المشرع الجزائري هذه الصورة من الجرائم في المادة 394مكررمن قانون العقوبات، والتي تنص: "...أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات ..."، وعلى ضوء هذا النص يمكن تعريف البقاء الإحتيالي في نظام المعلوماتية بأنه كل تواجد غيرعادي كالإتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي أي الدخول، والنظر فيه أي في المعطيات التي يتضمنها وغيرها من التصرفات غير المسموح بها ،والتي تشكل بدورها بقاء احتياليا،و يقصد كذلك بالبقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من

له الحق في السيطرة على هذا النظام ،وعليه لتحقق هذه الجريمة يجب تحقق الركنين المادي والمعنوي.

أولا:الركن المادي

يتحقق الركن المادي لجريمة البقاء عن طريق الغش في النظام المعلوماتي ، حيث يوجد الشخص داخل النظام عن طريق الغش ومع ذلك يقرر البقاء داخل النظام،و عدم قطع الإتصال به، وبكل بساطة هو مجرد البقاء الفعلي فيه، حيث يقاس البقاء غير المشروع بالمدة الزمنية التي يستعمل فيها الجاني النظام،وبالتالي تكتمل هذه الجريمة مع اكتمال البقاء مدة زمنية.

ثانيا:الركن المعنوي

إن جريمة البقاء غيرالمشروع داخل النظام تعد من الجرائم العمدية التي يشترط لتحقيقها توافر القصد الجنائي العام المتمثل في عنصري العلم والإرادة،حيث يجب أن يعلم الجاني أنه يقوم بالتجوال داخل نظام معلوماتي بطريقة غير مشروعة،كما يجب أن تتجه إرادته في نفس الوقت إلى البقاء فيه وعدم قطع الإتصال مع هذا النظام، وتعد جريمة البقاء في النظام الآلي لمعالجة المعطيات من الجرائم الشكلية التي لم يتطلب المشرع لتحقيقها نتيجة معينة،وهي كذلك جريمة مستمرة تتطلب تدخلا مستمرا من الجاني.

ثالثا: عقوبة جريمة البقاء عن طريق الغش في النظام المعلوماتي

تنص المادة 394 مكرر:" يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 دج الى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.....".

الفرع الثالث:أركان وعقوبة جريمة إتلاف نظام المعالجة الآلية

عالج المشرع الجزائري هذا النوع من الجرائم من خلال نص المادة 394 مكرر1 من قانون العقوبات وعليه لقيام هذه الجريمة يجب تحقق الركمن المادي والمعنوي.

أولا:الركن المادي

إن النشاط الإجرامي في هذه الجريمة يتحقق بكل وسيلة تؤدي إلي التخريب والإتلاف، يعرف البعض الإتلاف بجعه الشيء غير الصالح للإستعمال أو بإعدام صالحيته أو تعطيله،سواء بصفة كلية أو جزئية،كمايقصد أيضا بإتالف برامج الحاسوب الآلي ومعلوماته إتلاف أومحو تعليمات البرامج والبيانات ذاتها، ويطلق عليها مصطلح تدمير نظم المعلومات،وعادة لا يستهدف مرتكب هذا الإعتداء فائدة مالية لنفسه بل الهدف هوإعاقة نظام المعلومات.

وعليه يلاحظ أن المشرع الجزائري قد أطلق الوسيلة التي تقع بها الجريمة، ومهما يكن فإن الوسيلة الأكثر فاعلية والأكثر وقوعا في الجانب العملي هي إتلاف برامج الحاسب الآلي عن طريق فيروس الحاسب الآلي،وفيروس الحاسوب هوعبارة عن برنامج صغير يزرع بالأقراص والأسطوانات الخاصة بالحاسوب لأهداف تخريبية،مثل تدمير البيانات والمعلومات المخزنة داخل الحاسوب تدميراً كاملاً أو تعديلها.

ثانيا:الركن المعنوي

إن جريمة إتلاف نظام المعالجة الآلية تعد من الجرائم العمدية التي يشترط لتحقيقها توافر القصد الجنائي العام،والمتمثل في عنصري العلم والإرادة، حيث يجب أن يعلم الجاني أنه يقوم بإتلاف نظام المعالجة الآلية،كما يجب أن تتجه إرادته في نفس الوقت إلى الإتلاف.

ثالثا:عقوبة جريمة إتلاف نظام المعالجة الآلي

حسب نص المادة 394 مكرر1 من قانون العقوبات فإن عقوبة جريمة إتلاف نظام المعالجةالآلية هي الحبس من ستة(6)أشهرإلى ثلاث(3) سنوات وغرامة مالية من5000.00 دج إلى20.000.00 دج كما جرم المشرع الجزائري الاتفاق على ارتكاب إحدى الجرائم السابقة إذا

تجسد في أعمال مادية،وذلك نظرا لما يشكله الاتفاق الجنائي من خطورة،إذ تجتمع إمكانيات المتفقين بما يستوجب قطع الطريق عليهم[31]،كماجرم الشروع في تلك الجرائم نظرالخطورتها[32].

وقد شدد المشرع العقوبة إذا ارتكبت تلك الجرائم من شخص معنوي[33]، نظرا لما يأخذه ذلك من تنظيم،وكذلك تضاعف العقوبات إذا استهدفت تلك الجرائم مؤسسة الدفاع الوطني أوإحدى المؤسسات العامة،لما يشكله هذا من تهديد لأمن الوطن والمصلحة العامة[34].

إضافة فقد نص المشرع الجزائري على عقوبات تكميلية في قانون العقوبات،حيث يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم،وإغلاق المحل أو مكان الإستغلال إذا كانت الجريمة قد ارتكبت بعلم صاحبها[35].

من خلال دراسة صور الجرائم الماسة بنظام المعالجة الآلية للمعطيات في التشريع الجزائري،يلاحظ أن تدخل المشرع الجزائري في مواجهة هذا النمط من الجرائم قد جاء حديثا، و مسايرا لمختلف المراحل التي عرفتها بعض التشريعات المقارنة في هذا المجال، خاصة المشرع الفرنسي،وإن كان التدخل التشريعي ضروري وأساسي لمواجهة هذا النوع من الجرائم إلا أنه غير كاف ما لم يتم وضع إستراتيجيه وطنية لتعريف وتحديد مخاطر هذه الجرائم ، وهذا لن يكون إلا من خلال توعية الأفراد داخل المجتمع بأضرارها وأبعادها،إلى جانب تخصيص دورات تكوينية في هذا المجال لكل القائمين على مكافحة هذه الجرائم في المقررات الجامعية[36].

الخاتمة:

<u>النتائج:</u>

-على الرغم من أهمية وسائل تقنية المعلومات الحديثة، ومالها من آثار إيجابية سبق بيانها، إلا أن هنالك مخاطر عديدة تواجه الحق في السمعةو الحق الخصوصية بالنظر لإمكانية انتهاكه عبر وسائل تقنية المعلومات الحديثة، كونها تؤدي إلى أضرار أوسع انتشارا من

المطبوعات والصحف ووسائل الإعلام الأخرى، كما أن سهولة عمليات التخزين والمعالجة الالكترونية وازدياد تدفق المعلومات التي تتم عبر وسائل تقنية المعلومات الحديثة، تضعف قدرة الفرد على التحكم في تدفق المعلومات الخاصة به، إذ أصبحت المعلومات الشخصية في ظل الشبكة العالمية متوفرة ما يؤدي إلى ازدياد التهديدات لخصوصية الناس، وقد أصبح الوصول إلى المعلومات الشخصية بصورة غير مشروعة أكثر من ذي قبل، وازدادت فرص اساءة استخدامها.

-إضافة إلى ذلك فقد ازدادت عمليات مراقبة الأفراد وملاحقتهم، وعمليات التعدي على خصوصياتهم من خلال الوصول إلى سجلات البيانات المخزنة، كما أن وسائل تقنية المعلومات الحديثة ساعدت على عولمة المعلومات والاتصالات عبر الحدود دون اعتبار للجغرافية والسيادة بحيث تعطى المعلومات لجهات داخلية وخارجية بل وتعطى لجهات مجهولة وهو ما يثير إساءة استخدام البيانات خاصة في الدول التي لا توفر حماية قانونية للبيانات الشخصية أو أنها لا تستطيع توفيرها فانتشار النقل الرقمي للمعلومات والبيانات الشخصية أدى إلى ظهور جرائم ماسة بحرمة الحياة الخاصة عبر وسائل تقنية المعلومات الحديثة كالتجسس الإلكتروني

الإقتراحات:

-تخصيص باب في قانون العقوبات يتضمن جميع الجرائم المتعلقة بحماية الحق في حرمة الحياة الخاصة،بدلا من النص عليها في مادتين فقط ،وإضافة مادة في قانون العقوبات تجرم نشر الوقائع المعلومات المالية والشخصية الخاصة بالأفراد،لأهميتها ولكونها تشكل مساسا بحقهم في الخصوصية، بالإضافة إلى الأخذ بأحكام الشريعة الإسلامية خاصة في مجال حماية حرمة الحياة الخاصة.

- ضرورة القيام بتعديل مواد القذف والسب والإهانة بما يتماشى والتطور العلمي الحاصل في مجال تكنولوجيا المعلومات ونظم الاتصالات الالكترونية، كون هذه الجرائم

التقليدية باتت ترتكب بكثرة باستخدام الوسائل التقنية والتكنولوجية الحديثة لا سيما عبر شبكة الانترنت.

الهوامش:

[1] راجع: نبيل صقر، جرائم الصحافة في التشريع الجزائري ، دون طبعة، دار الهدى، الجزائر ، 2007 ، ص 88

[22] محمد عبد اللطيف عبد العال ، مفهوم الشرف و الاعتبار في جرائم القذف و السب ، دون طبعة ، دار النهضة العربية ، القاهرة ، 2002 ، ص5

[3] سالم رمضان الموسوي ، جرائم القذف و السب عبر القنوات الفضائية ، بدون طبعة ، منشورات حلبي الحقوقية ، لبنان2012 ،ص16

[4] القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 ،المعدل والمتمم لقانون العقوبات،ج ر ج ج عدد 84 صادر في 24 ديسمبر2006

[5] قانون رقم 09-04 المؤرخ في5 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ج ر عدد 47 المؤرخة في16 أوت 2009

[6] والمرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر2015 ، المحدد والمنظم لكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ج ر ، ع 53

[7] كمال بوشليق، جريمة القذف بين القانون والإعلام (دراسة تحليلية مقارنة بالإجتهاد القضائي لرجال القضاءوالإعلام على ضوء قانون العقوبات والإعلام)، دون طبعة، دار الهدى، عين مليلة، الجزائر، 2010 ، ص13

[8] أحسن بوسقيعة، المرجع السابق، ص 195

[9] تومي يحي،المرجع السابق، ص42

[10] راجع:تومي يحي،المرجع السابق، ص44

[11] نفس المرجع، ص47

[12] Javeau Jean Claud, La notion de la diffamation dans les médias, troisième édition, les édition d'organisation, paris, France, 1985, p. 65

[13] Javeau Jean Claud, op.cit, p 73

[14] أحمد بوسقيعة،المرجع السابق، ص 193

[15] تومي يحي،المرجع السابق، ص51

[16] نجاد البرعي، المرجع السابق،ص5

[17] طعن رقم 909 لسنة 2012 أورده نجاد البرعي ، المرجع السابق

[18] نبيل صقر،المرجع السابق، ص101

[19] تومي يحي ،المرجع السابق،ص66-67

[20] تومي يحي،المرجع السابق، ص69

[21] القاضي سالم الموسوي،جرائم القذف والسب عبرالقنوات الفضائية، ط1، منشورات الحلبي الحقوقية،2012 ، ص89

[22] نبيل صقر، المرجع السابق،ص133

[23] تومي يحي،المرجع السابق، ص80

[24] كمال بوشليق،المرجع السابق، ص36

[25] سمية بلغيث،المرجع السابق، ص351

[26] عبد القادر عميمر، تاثير تكنلوجيا المعلومات عى الحق في الحياة الخاصة ،حوليات جامعة الجزائر 1،المجلد 34 ،العدد 01، 2020،ص446

[27] والتي تقابلها المادة 47 من التعديل الدستوري في 2020

[28] سوزان عدنان الاستاذ ،المرجع السابق،ص445-446

[29] أحمد بن مسعود،جرائم المساس بأنظمة المعلجة الآلية للمعطيات في التشريع الجزائري ،مجلة الحقوق والعلوم الإنسانية، ،العدد2017،1 ،ص484

[30] سوزان عدنان الاستاذ ،المرجع السابق،ص445-446

[31] تنص المادة 394 مكرر 5 من القانون 04-15 المتمم لقانون العقوبات المؤرخ في 10 نوفمبر 2004،ج ر ج عدد 71 الصادرة بتاريخ10 نوفمبر 2004 : "كل من شارك في مجموعة او في إتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل او عدة أفعال مادية ،يعاقب بالعقوبات المقررة للجريمة ذاتها"

[32] المادة 394 مكرر7 من قانون 04-15

[33] المادة 394 مكرر4 من المرجع نفسه

[34] المادة 394 مكرر3 من المرجع نفسه

[35] المادة 394 مكرر6 من المرجع نفسه

[36] أحمد بن مسعود،المرجع السابق،ص 486

قائمة المصادروالمراجع:

أولا:المصادر

-القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 ،المعدل والمتمم لقانون العقوبات،ج ر ج ج عدد 84 صادر في 24 ديسمبر2006

-قانون رقم 09-04 المؤرخ في5 اوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ج ر عدد 47 المؤرخة في16 أوت 2009

-المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر2015 ، المحدد والمنظم لكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، ج ر ، ع 53

-المرسوم الرئاسي رقم 20-442 الموقع في 30 ديسمبر 2020 ،المتعلق بالتعديل الدستوري، ج ر ج ج د ش عدد82، مؤرخة في 30 ديسمبر 2020

ثانيا:المراجع

1:الكتب

-القاضي سالم الموسوي،جرائم القذف والسب عبرالقنوات الفضائية، ط1، منشورات الحلبي الحقوقية،2012 ، ص89

-سالم رمضان الموسوي جرائم القذف و السب عبر القنوات الفضائية، بدون طبعة، منشورات حلبي الحقوقية ، لبنان2012 ص16

-كمال بوشليق، جريمة القذف بين القانون والإعلام (دراسة تحليلية مقارنة بالإجتهاد القضائي لرجال القضاءوالإعلام على ضوء قانون العقوبات والإعلام)، دون طبعة، دار الهدى، عين مليلة، الجزائر، 2010 ، ص13

-محمد عبد اللطيف عبد العال، مفهوم الشرف و الاعتبار في جرائم القذف و السب ، دون طبعة ، دار النهضة العربية ، القاهرة ، 2002 ، ص5

-نبيل صقر، جرائم الصحافة في التشريع الجزائري ، دون طبعة، دار الهدى، الجزائر ، 2007 ، ص 88

2:المقالات العلمية

-أحمد بن مسعود،جرائم المساس بأنظمة المعلجة الآلية للمعطيات في التشريع الجزائري ،مجلة الحقوق والعلوم الإنسانية، ،العدد2017،1 ،ص484

-عبد القادر عميمر، تاثير تكنلوجيا المعلومات عى الحق في الحياة الخاصة ،حوليات جامعة الجزائر 1،المجلد 34 ،العدد 01، 2020،ص446

- عدنان الاستاذ، إنتهاك حرمة الحياة الخاصة عبر الأنترنت،مجلة جامعة دمشق لعلوم الإقتصادية والقانونية،المجلد 29 ،العدد2013،3، ص445

المرجع باللغة الفرنسية

[36] Javeau Jean Claud, La notion de la diffamation dans les médias, troisième édition, les édition d'organisation, paris, France, 1985, p. 65

صور الانتهاك الرقمي للحق في الحياة الخاصة

Pictures of the digital violation of the right to a private life

براجل الصالح، طالب دكتوراه

جامعة تلمسان، الجزائر

berradjel05salah@gmail.com

الملخص:

لقد عرفت البشرية في الآونة الأخيرة تطورا علميا منقطع النظير، وقد نتج عن هذا التطور اكتشاف تقنيات مختلفة عالية الدقة في عالم تكنولوجيات الإعلام والإتصال، ويقد يفضي استعمال هذه الأجهزة والتقنيات الحديثة إلى انتهاك حرمة الحياة الخاصة للإنسان، وقد يجهل هذا الأخير في كثير من الأحيان أن خصوصيته أصبحت عرضة ومكشوفة للعيان، نتيجة الجوسسة التي مورست عليه.

لذلك نجد صورا شتى للإنتهاك الرقمي للحياة الخاصة وبشتى الطرق، فقد يعتدى على خصوصية الإنسان بصفة قسرية ولا إرادية، كاستعمال تقنية النانو في الجوسسة، أو بالإجبار على المرور بالماسح الضوئي، أو بالجوسسة عن طريق زرع أجهزة سمعية وبصرية وشرائح راديوية في أماكن لا يعلم بها، وتلتقط أدق تفاصيل حياته.

وقد يعرض الإنسان حياته للكشف عن طريق ممارساته الإرادية، كاستعمال الهاتف النقال، والحاسوب والأنترنت، والبريد الإلكتروني، وتقنية تحديد المواقع الجغرافية.....

وقد يتطفل على خصوصيات الإنسان عن طريق الكشف على جسده ونفسيته، وذلك عن طريق أخذ بصمات الأصابع، أو العين، أو إجراء تحليل للبصمة الوراثية، أو وضع كبسولة رقمية للتحاليل الطبية، أو إجراء رقابة بيانية أو نانوية على نفسيته، أو باستعمال جهاز كشف الكذب.

فكل هذه الممارسات والتقنيات تعري خصوصية الإنسان وتكشفها للعيان، إن كان مستعملوها منعدمي الضمير والأخلاق.

الكلمات المفتاحية: الخصوصية، انتهاك، الرقمي، تكنولوجيات، الإنسان.

Summary

Mankind has recently experienced unparalleled scientific development, This development has resulted in the discovery of various high-precision technologies in the world of information and communication technologies And the use of these devices and modern technologies may violate the sanctity of the private life of man , And may be often unaware that his privacy has become exposed and exposed to view, as a result of spying on him.

Therefore, we find various images of the digital violation of private life in various ways. As it may infringe on the privacy of a person involuntarily and involuntarily, such as using nanotechnology in spying, Or by forcing passage of the scanner, or by spying by implanting audio-visual equipment and radio chips in places that he does not know, and picks up the most accurate details of his life.

A person may expose his life to reveal through his voluntary practices, such as using a mobile phone, computer and internet, e-mail, and geolocation technology .....

It may intrude on a person's privacy by examining his body and psyche, by taking fingerprints or an eye, by conducting a genetic fingerprint analysis, by placing a digital capsule for medical analyzes, by conducting graphic or nanological control of his psyche, or by using a lie detector.

All these practices and techniques expose the privacy of man and reveal it to the public, if its users are
unscrupulous and immoral.

keywords

Privacy, Violation, Digital, Technologies, Human.

مقدمة

إن المتأمل في قول الله تعالى: (وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ وَحَمَلْنَاهُمْ فِي الْبَرِّ وَالْبَحْرِ وَرَزَقْنَاهُم مِّنَ الطَّيِّبَاتِ وَفَضَّلْنَاهُمْ عَلَى كَثِيرٍ مِّمَّنْ خَلَقْنَا تَفْضِيلاً) (الإسراء : 70)، ليكتشف فعلا قيمة وكرامة وأفضلية الإنسان على كافة المخلوقات، وإن مما تقتضيه هذه الكرامة، ضمان ممارسة الحق في الخصوصية، والتمتع بكل حرية بحياة خاصة في كنف السرية والحفظ، وعدم التطلع إلى مالا يريد أن يبوح به الإنسان من طرف أحد.

التعريف بموضوع المداخلة

موضوع الحق في الحياة الخاصة يدخل في إطار الموضوعات العامة لمنظومة حقوق الإنسان، ويصنف ضمن الحقوق المدنية والسياسية، أو مايصطلح عليه بالحقوق الزرقاء، المرتبة في خانة الجيل الأول لحقوق الإنسان، وموضوع مداخلتي هذه؛ يتطرق إلى بعض الصور التي تعد من مظاهر الاعتداء على الحق في الحياة الخاصة عن طريق الأجهزة الرقمية والتكنولوجية الحديثة والمتطورة.

إشكالية الدراسة

لقد تضمن الإعلان العالمي لحقوق الإنسان الصادر في: 1948، والعهد الدولي الخاص بالحقوق المدنية والسياسية الصادر سنة: 1966 أهم حقوق الإنسان وحرياته الأساسية، ومنها الحق في الحياة الخاصة، إلا أننا لم نجد فيهما مايجرم بعض الممارسات التي تعد انتهاكا للخصوصية، وربما هذا يرجع إلى حداثة هذه الممارسات التي لم تكن آنذاك، ومع التقدم العلمي والتطور التكنولوجي ظهرت أجهزة وتقنيات حديثة، واستعمالها يفضي إلى التعدي على الخصوصية.

ولمعرفة هذه الممارسات الناتجة عن تلك الإستعمالات الحديثة يمكن صياغة الإشكالية الرئيسة لهذه المداخلة على هذا النحو:

ماهي أهم مظاهر الاعتداء على الحق في الحياة الخاصة، في ظل استعمال المعلوماتية وأجهزة تكنولوجيات الإعلام والإتصال الحديثة والمتطورة ؟

وتندرج تحت هذه الإشكالية الرئيسة أسئلة فرعية يمكن صياغتها على هذا النحو:

1/ ماهي أهم صور الإنتهاك الرقمي للحياة الخاصة عن طريق الممارسات اللاإرادية؟.

2/ ماهي أهم صور الإنتهاك الرقمي للحياة الخاصة عن طريق الممارسات الإرادية؟.

3/ ماهي أهم صور الإنتهاك الرقمي للحياة الخاصة عن طريق الممارسات الكشفية؟.

أهمية الموضوع

تكمن أهمية هذا الموضوع فيما يلي:

1/ معرفة أهم طرق الاعتداء على الحق في الحياة الخاصة بواسطة بعض الممارسات التي تقوم بها الدولة أثناء القيام بإجراءات حفظ الأمن والنظام العام، أو أثناء القيام ببعض الإجراءات الأمنية الإحترازية.

2/ معرفة أهم طرق الاعتداء على الحق في الحياة الخاصة بواسطة بعض الممارسات التي يقوم بها القراصنة ومحترفي استخدام تكنولوجيات الإعلام والإتصال، والمعلوماتية.

3/ معرفة أهم طرق الاعتداء على الحق في الحياة الخاصة بواسطة بعض الممارسات التي يقوم بها الإنسان المعتدى على خصوصيته، وهو يستخدم بعض تقنيات تكنولوجيات الإعلام والإتصال.

4/ معرفة أهم طرق الاعتداء على الحق في الحياة الخاصة بواسطة الممارسات الكشفية، سواء كانت تلك الممارسات متعلقة بالكشف الجسدي، أم كانت متعلقة بالكشف النفسي.

منهج الدراسة

إن طبيعة هذه الدراسة ولغرض الإجابة الوافية عن الإشكالية المطروحة في هذا البحث استوجب علي الأمر أن أتبع المنهج **الإستنباطي**، ذلك أنني قمت بالإطلاع على كيفية عمل بعض الأجهزة الحديثة والمتطورة، والتي تعمل بتقنيات مختلفة وباستخدام تكنولوجيات الإعلام والإتصال، واستنبطت منها مايعد خرقا وانتهاكا لحرمة الحياة الخاصة، أو الحق في الخصوصية.

خطة البحث

بعدما قمت بضبط إشكالية الدراسة والإطلاع على المادة العلمية المتوفرة في هذا الموضوع، ارتأيت أن أقسم هذا البحث إلى ثلاثة مباحث أساسية، وللإجابة الوافية عن تساؤل الإشكالية أحاول مناقشة ماورد تحت هذه المباحث في مطالب جزئية، إذ تندرج تحت كل مطلب نقاط أو فروع تفصيلية، وتكون المباحث الأساسية على هذا النحو:

المبحث الأول: صور الإنتهاك الرقمي للحياة الخاصة عن طريق الممارسات اللاإرادية.

المبحث الثاني: صور الإنتهاك الرقمي للحياة الخاصة عن طريق الممارسات الإرادية.

المبحث الثالث: صور الإنتهاك الرقمي للحياة الخاصة عن طريق الممارسات الكشفية.

المبحث الأول: صور الإنتهاك الرقمي للحياة الخاصة عن طريق الممارسات اللاإرادية

يقصد بالممارسات اللاإرادية هنا، تلك الأفعال والممارسات التي يقوم بها الغير ليتجسس على إنسان بشتى الطرق، دون علم المتجسس عليه وبدون إرادة هذا الأخير، وبما أن فعل التجسس خارج عن إرادة المعتدى عليه، اصطلحت على هذا العنوان بالممارسات اللاإرادية، وهي كثيرة ومتنوعة أحاول تفصيلها فيما يلي:

المطلب الأول: الجوسسة عن طريق تقنية النانو بالجهاز الرقمي للتصغير اللامتناهي

شهد العالم في الآونة الأخيرة ثورة صناعية لم يشهدها من قبل ، سميت بتكنولوجيا التصغير اللامتناهي والتي يوحي اسمها بصناعة أجهزة كانت في السابق تحمل حيزا كبيرا أصبحت بفضل هذه التكنولوجيا لاترى حتى بالعين المجردة ، و السر في ذلك يكمن في أن هذه الصناعة لا تقوم على الذرة كمقياس تقليدي ، و إنما تقوم على أساس المقياس النانوي ويستخدم النانو للتعبير عن جزء من مليار من الشيء[1]

حيث يعتبر مجال التجسس هو المجال الخصب لتقنية النانو، حتى أن البعض يخشى بأن الحياة الخاصة للأشخاص تكون مكشوفة للعيان مع هذه التقنية المخيفة، فماذا لو سقطت في أيدي العامة فلن يكون هناك خصوصية لأحد في منزله و هذا ما سيتأكد من خلال عمل تكنولوجيات النانو التي لديها القدرة على تعزيز أجهزة المراقبة بشكل كبير بفضل حجمها الصغير مثل الكاميرات والميكروفونات، وجعل اكتشافها أكثر صعوبة بكثير فقد صنعت أجهزة تجسسية بحجم الذبابة تستطع اختراق أضيق الأماكن و أكثرها سرية، كما لها القدرة على حمل أجهزة التنصت و التصوير .

حتى في جانب الخصوصية في أجهزة المعلوماتية، يمكن لهذه التكنولوجيا أن تحضر جيشًا من الجراثيم على شكل آلات متناهية في الصغر،توجه من ممرات الهواء، إلى أجهزة الكومبيوتر، وتسيطر بذلك على جميع المعطيات الشخصية الآلية ، دون أن يشعر بها أحد و تعتبر هذه من أدوات التجسس المعلوماتي عن طريق الاختراق الآلي.

ويمكن كذلك لهذه التكنولوجيا أن تصنع روبوتات تكاد تطابق الكائنات الحية ، مصممة على غرار الصراصير، تستطيع التسلق على الجدران والسلالم و حتى التضاريس الصخرية المختلفة ، .وبهذا فقد تكون في البيوت و لا يحس بها أحد.

و تعتبر حرمة الحياة الخاصة من بين المجالات التي أعدمتها هذه التقنية،التي لا مجال للكلام عنها على حق اسمه حرمة الحياة الخاصة[2].

المطلب الثاني: الجوسسة عن طريق استعمال الماسح الضوئي

قبل أن نتعرف على هذا الجهاز الرقمي، يجب أن نشير بداية إلى أنه في حد ذاته ليس بالتقنية الجديدة، ذلك أنه استعمل منذ عقود في المجال الطبي ، لكنه بقي مقتصرا عليه،.لكن أن تدخل هذه التقنية في كشف الإنسان جسديا وفي الأماكن العامة هو الشيء الجديد، الذي أثار حفيظة العالم بأسره.

حيث يعتبرالماسح الضوئي من أجهزة (السكانير)التي تعتمد على أسلوب التصوير الالكتروني بواسطة كاميرات الكترونية حيث يمر الشخص من أمامها وتقوم بتصويره رقميا لكشف ما تحت ملابسه ، بحيث تظهرالأجساد عارية تماما على لوحة كربونية الصورة، رقمية النظام ، بما فيها من التفاصيل التشريحية الدقيقة ويكشف أيضا عن الجراحات الترقيعية أو زراعة الأعضاء في الجسم، مستخدما في ذلك الأشعة السينية ذات الحساسية العالية والتي تخترق الأجسام المظلمة بصفة عامة، وتتم هذه العملية في خلال 30 ثانية، هذه المدة القصيرة تكفي لتسجل صورة جسد على نحو شفاف، كاشفة التفاصيل الدقيقة وما يمكن أن يخفيه حتى في أحشائه، وهذا مايتنافى مع الكرامة الأصلية للإنسان والتي تلازم شخصيته في كل الظروف[3].

-حيث وجهت الكثير من الإنتقادات لهذه التقنية، باعتبارها انتهاكا صارخا للحق في الخصوصية. إلا أن البعض يجيزها استنادا إلى اعتبارات الأمن و السلامة خاصة في مواجهة ظاهرة خطف وتفجير الطائرات ، وما يترتب عليه الآلاف من الضحايا ،حتى و لو كان هذا يمس الخصوصية، فالحق في الحياة يعتبر من أسمى الحقوق.

المطلب الثالث: الجوسسة عن طريق زرع الأجهزة السمعية

يدخل في نطاق الأجهزة السمعية مكبرات الصوت، وهي عبارة عن أجهزة صغيرة يمكن إخفائها في أي مكان، حيث أتاح تصغير الأجهزة الحديثة إنتاج مكبرات صوت لا يزيد حجمها على رأس عود ثقاب وما لها من قدرة على التوصيل الإذاعي الذي يصل إلى ما يتراوح بين ثلاثة

مئة قدم وما يبعد عن ربع ميل[4]، وهذه الأجهزة الجد دقيقة يمكن أن تخبأ في أي مكان أو آنية أو زاوية في المنزل دون علم صاحبه ، وتوصل بأجهزة رقمية أخرى لسماع الصوت الملتقط.

المطلب الرابع: الجوسسة عن طريق زرع الأجهزة البصرية

توجد آلات تصوير دقيقة، وصلت فعاليتها إلى درجة أصبح بالإمكان من الناحية العملية تصوير خطابات مقروءة وبصورة واضحة من بعد كيلومتر بآلة تصوير مركب بها عدسة قطرها 20 سنتمتر كما أمكن استخدام الآلات الفوتوغرافية التي لها القدرة على العمل في الظلام وفي الإمكان إخفاؤها واستخدام فنون الإضاءة بالأشعة تحت الحمراء بما يسمح بملاحظة ما يجري في الغرفة وتصويرها من غرفة مجاورة ومعها أجهزة تصوير دقيقة الحجم يسهل إخفاؤها وفي الحالة التي تكون فيها الغرفة مفتوحة فإنه يمكن ومن خلال العدسات التلسكوبية أن تلتقط الصور وهذه العدسات تستطيع أن تصور ما تحتويه المستندات والوثائق المطروحة على المكتب من مسافة نصف الميل، وتتصل هذه الكاميرات بأجهزة رقمية بدون أسلاك لقراءة الصورة أو الفيديو المصوران و الخواص المميزة لهذه الوسائل الرقمية الحديثة تنحصر في سريتها وإجرائها خلسة، بحيث يصبح سلوك الفرد مسجلا في أي وقت ودون علمه، حيث توجد الأجهزة التي تخص أماكن العمل وأخرى تتعلق بالمنازل، وبعضها بالحدائق ، كما توجد كاميرات لا تعمل إلا في الظلام وأخرى مهيأة للتصوير في الأماكن المضيئة وكل هذه الكاميرات تتوفر بخاصية التحريك عن بعد وفي كل الاتجاهات من الأعلى إلى الأسفل، ومن اليمين إلى اليسار حتى تصل إلى 360 درجة وهذا ما كان له تأثيرا بالغا على حرمة الحياة الخاصة، ويعتبر من قبيل التدخل التعسفي في الخصوصية.[5]

ذلك أن هذه الشرائط ليست مؤقتة باعتبار أن لها ذاكرة دائمة ولا يوجد ما يمنع أن يقوم عليها بعض التركيبات " المونتاج " بفضل تقنية النظام الرقمي بما يعني القدرة على تخزين بيانات تتعلق بالصوت و الصورة ومعالجتها عن طريق الحاسوب الأمر الذي ينطوي على بعض المخاطر على حرمة الحياة الخاصة، إذ يتيح النظام الرقمي إمكانية مباشرة وفورية في البحث عن الصورة وتخزينها وإعطاء معلومات مفصلة عنها.

وبالتالي يمكن لأي كان أن يراقب خصوصية الفرد الذي لا يعلم بأنه مراقب وأن صورته تبحر في أرجاء المعمورة وهو يعتقد بأنه قابع .في مكان خاص.

المطلب الخامس: الجوسسة عن طريق الشرائح اللاسلكية الراديوية"

الشرائح الراديوية هي شرائح تغرس في أي مكان وتغرس حتى تحت جلد الإنسان تعمل على تحديد الهوية وذلك باستخدام موجات راديوية، وترسل المعلومات إلى الجهاز المستقبل "RFID TAGS" [6]

و رغم الاستعمالات العديدة والفوائد الجمة لهذه التقنيات، إلا أنه لا يستطيع أحد أن ينكرها لأن باطنها يحمل خرقا لخصوصيات الأفراد، فمن كانت أحد ممتلكاته تحمل هذه الشريحة فهذا معناه أن الغير يعرف جيدا من هو، أين يعيش، و كيف يعيش، و مع من يتحدث ماذا يأكل و غيرها من البيانات التي تتيحها هذه التقنية. ويزداد كذلك التضييق من حرمة الحياة الخاصة في حالات القيام بالمعاملات التجارية من شراء وبيع وتعاملات حيث تأخذ المعلومات المتعلقة بحساب الفرد البنكي وتقيد هذه التعاملات عبر الانترنت. كما أنه بمقدور شرائح التعريف اللاسلكية المزروعة تحت الجلد أن تخزن المعلومات المتعلقة بهذا الإنسان.

تستخدم هذه التقنية في المجالات الطبية لحفظ المعلومات عن المرضى وعلاجهم. ولكن بهذا الأسلوب لا يمنع من دخول بعض المتطفلين كذلك إلى قاعدة بيانات المرضى، حيث إن هذه التقنية تسمح لأشخاص آخرين بانتهاك خصوصية مستخدمي هذه التقنية، والتي تتمتع بقدر كبير من الإحترام الذي يعتبر القاسم المشترك فيما بين مواثيق حقوق الإنسان كلها[7]، حيث يسهل استخدام هذه البيانات بطرق غير شرعية.

المبحث الثاني: صور الإنتهاك الرقمي للحياة الخاصة عن طريق الممارسات الإرادية

يقصد بالممارسات الإرادية هنا، تلك الأفعال والممارسات التي يقوم بها الإنسان بحد ذاته، باستعمال الأجهزة والمعدات التقنية الحديثة بشتى الطرق، وهو يعلم أنه عرضة للجوسسة، وأن كل أعماله مراقبة دون أن يعلم من هو المتجسس عليه و لكن تبقى هذه الإستعمالات ناتجة عن محض إرادته بدون إكراه ، وبما أن فعل التجسس يكون واردا

ومفترضا مسبقا، اصطلحت على هذا العنوان بالممارسات الإرادية، وهي كثيرة ومتنوعة أحاول تفصيلها فيما يلي:

المطلب الأول: استعمال الهواتف النقالة

تعتبر تكنولوجيا الهواتف النقالة من التكنولوجيا الرائدة في عصرنا الحالي، فالجميع يستعملها نظرا لاحتوائها على وسائط بسيطة يسهل التعامل معها.وتطورت الخدمات التي وفرتها لنا الهواتف النقالة إلى أن شملت تحميل ملفات كبيرة الحجم من المواد المسموعة والمرئية مباشرة، ثم أضيفت إليها إمكانية الدخول على الإنترنت التي فتحت بدورها آفاقا عدة لاستخدامات الهواتف النقالة، فصار بإمكان المستخدم أن يتصفح البريد الإلكتروني بسهولة وإرسال واستقبال الرسائل، واسترجاعها والبحث عنها[8]، وأن يتواصل عبر خدمة" المسنجر " وباقي الخدمات الأخرى وبصورة دائمة مع أصدقائه المتصلين بالإنترنت.

فبينما كانت الهواتف النقالة بادئ الأمر مجرد هواتف، فإنها سرعان ما انتشرت وارتقت فصارت أدوات تكنولوجية متعددة الاستخدامات عميقة التأثير في أوجه شتى من حياتنا اليومية. فلا أحد يستطيع أن ينكر مزايا الهواتف النقالة، ولا أحد كذلك يستطيع أن ينكر بأنه يخاف منها، ذلك أن هذه الأجهزة نجدها في كل مكان وعند كل واحد وقد تكون مخفية، وبهذا فقد يستعملها الجميع من أجل التجسس على الجميع والاعتداء علي الحقوق الطبيعية التي يتمتع بها البشر[9]حيث أن الكل يملك هذه الأجهزة التي تحمل في الجيب، وبإمكانه أن تصور وتسجل، وتعدل وتضيف وتنسخ وترسل. مما قد تشكل أنواعا عدة من الاعتداءات على حرمة الحياة الخاصة.

المطلب الثاني: استعمال أجهزة الحاسوب

تعتبر الحواسيب من أكثر الأجهزة الإلكترونية استعمالا في الأوجه اللامشروعة كونها تحتوي على عدة خدمات ومن بين تلك الخدمات المستعملة من طرف المعتدى عليه مايلي:

1-إدخال معطيات أو معلومات وهمية :إذ يمكن بهذه الوسيلة أن يستولى المعتدي على بيانات شخصية غالباً ما تتعلق بعناصر الذمة المالية بغية تحقيق أموال لنفسه.

2-التجسس الإلكتروني عن طريق الفيروسات و الفايروس هو مرض يصيب الحاسوب . وفيروس الحاسوب هو عبارة عن برنامج صغير يزرع عن طريق البرامج والوسائط والأقراص و الأسطوانات الخاصة بالحاسوب لأهداف تخريبية، مثل تدمير البيانات والمعلومات الشخصية المخزنة داخل الحاسوب تدميراً كاملاً أو تعديلها .وقد يزرع الفايروس بالحاسوب بقصد التطفل على الحياة الخاصة للغير، للوصول إلى معلومات شخصية عنه، واستخدام هذه المعلومات بصورة غير مشروعة .وهناك تهديد آخر للحق في احترام الحياة الخاصة، إذ يقوم الفايروس بمعالجة المعلومات الاسمية لشخص معين للحصول على معلومات أخرى جديدة، بوسائل متعددة مثل

التقريب والمقابلة بين المعلومات، وإعداد الإحصائيات، وإدماج العناصر المختلفة، وربطها ببعضها؛ وبذلك يمكن ترجمة حياة الفرد في ثوانٍ معدودة، ثم يستخدم المجرم المعلوماتي هذه المعلومات في أغراض غير مشروعة مثل فضح ماضي الفرد وابتزازه.

3- سرقة المعلومات الخاصة وتزويرها وسرقة كلمة السر أو الاستيلاء عليها.

4-التزوير المعلوماتي :عن طريق التسلل الإلكتروني إلى البيانات، إذ يقوم القراصنة بمحاولة الدخول إلى النظام للوصول إلى هذه المعلومات التي تكون غالباً سرية، وتجري عملية الدخول إلى النظام المعلوماتي عن طريق خرق هذه المنافذ والوصول إلى قاعدة البيانات، وتعديلها أو إضافة المعلومات المغلوطة بها بهدف الاستفادة غير المشروعة من تلك البيانات.[10]

المطلب الثالث: استعمال الأنترنت

تعد الانترنت الوسيلة الاتصالية الإعلامية الأكثر شيوعا اليوم، فبواستطها تتداول و تعالج و تجمع و تفكك البيانات والمعلومات بكل سهولة و سلاسة ، و لا تستغرق هذه العمليات إلا ثواني معدودة لكي تنتقل من دولة لدولة ، و من منظمة إلى منظمة و من جهة عمل إلى أخرى و من فرد إلى مؤسسة دون قيود و بكل اللغات.

فقد فاقت استعمالاتها الأجهزة التقليدية نظرا للخدمات المتنوعة و الآنية التي تقدمها، هذا ما كان له انعكاسات على موازين القوى..

وباستعمال الأنترنت ربما نجعل بياناتنا الشخصية عرضة لكل متطفل و مستفز، ويتحطم هنا معنى حرمة الحياة الخاصة الثابتة في الشرائع السماوية والأنظمة القانونية في العالم[11]

وعليه تعتبر الانترنت كوسيلة تعدي على الحياة الخاصة فقد أصبح هذا العنوان بديهة من البديهيات المسلم بها، لقناعة الكثير و حتى عموم الناس، أن الانترنت هي مرادفة لانتهاك الخصوصيات، نظرا للخصائص التي تمتاز بها، وخاصة بعد إضافة برامج متعددة للتواصل الاجتماعي غبر الأنترنت على غرار الفيسبوك والتويتر والأنستغرام....

المطلب الرابع: استعمال البريد الإلكتروني

يعتبر البريد الالكتروني - الذي أصبح في متناول الجميع– بحق الوسيلة المثلى في الاتصال سواء اقتصاديا أو زمنيا ، حيث لا يتقيد لا بالمكان ولا بالزمان وهو ما جعل بحق شعوب القارات في علبة صغيرة تتواصل بكل حرية و قد اتفق القانونيون على اعتبار العنوان الإلكتروني عبارة عن معلومة اسمية يجب المحافظة عليه خصوصا و أن العنوان الإلكتروني يشمل بلد الشخص و أحيانا اسمه الصحيح وتبقى إمكانية اعتراض الرسائل تحول دون الوثوق به، إذ من الممكن اعتراض الرسائل التي يتم تحميلها عبر الشبكة و كشف مضمونه من خلال الموزع و عبر برامج معينة قادرة على قراءة هذه الرسائل التي يجب أن تمر من خلال الموزع ليتم تحميلها إلى الطرف الآخر والمشكلة تزداد تعقيدا عندما نعلم أن هذا الأمر يجري بشكل تطفلي من قبل الموظفين أو بأمر من الإدارة لدى الموزع ، كما أنه في غالبية الدول تكون هذه الرقابة مفروضة من قبل أجهزة رسمية للتجسس بدعوى حماية الأمن والنظام العام[12].و فعل التجسس هذا لا يقتصر فقط على الحكومات وأجهزة الأمن وإنما يمتد ليشمل القائمين على الانترنت والقراصنة.

المطلب الخامس: استعمال أجهزة وبرامج تحديد المو اقع

يقصد بها أنظمة تحديد المواقع والبيانات العالمية GPS ، جي بي آس العالمي ويعمل عن طريق الأقمار الصناعية للحصول على بيانات جغرافية تحدد المواقع على الأرض بدقة بالغة، وهو يمثل برنامجًا حاسوبيًا أو تطبيقًا يؤدي مهام أكثر تعقيدًا حيث تقوم بتحليل ومعالجة البيانات الجغرافية.

وغالبا ماتستعمل هذه التقنية من طرف السائقين أو السياح حيث ترشدهم إلى الهدف، لكن هذه الاستعمالات لا تقتصر فقط على الجانب الإيجابي، بل تتعداه إلى الجانب السلبي، حيث اقتحمت من خلالها حرمة الحياة الخاصة للفرد فأعطت التفاصيل الدقيقة عنه،

فبعد أن تعود الناس بالكاميرات الأرضية تفاجئوا بكاميرات أخرى تراقب الإنسان، لكن هذه المرة من الفضاء، فأصبح متابعا في حركاته وسكناته، ولم يعد بوسع أحد بعد ذلك أن يشعر بالحق في حرمة حياته الخاصة.

هذا وقد أطلقت شركة جوجل برنامجًا جديدًا يسمح لمستخدمي أجهزة الهاتف المحمول وغيره من الأجهزة اللاسلكية الأخرى بإطلاع أهلهم وأصدقائهم على أماكن تواجدهم، وبموجب البرنامج الجديد سيصبح بوسع

المستخدمين بث موقع تواجدهم إلى أشخاص آخرين بصورة دائمة.

وباستخدام هذه التقنية التي تكبح من حرية الأفراد بالشكل الذي لا يسمح لهم التمتع بحريتهم[13] في التنقل إلى أي مكان، هذا في حد ذاته يعتبر اعتداءا على الخصوصية.

المبحث الثالث: صور الإنتهاك الرقمي للحياة الخاصة عن طريق الممارسات الكشفية

يقصد بالممارسات الكشفية هنا، بالكشف والإطلاع على ذات الإنسان، (الذات الجسدية، أو الذات النفسية) لذلك اصطلحت على هذه الممارسات بالكشفية، حيث تنقسم إلى صنفين، فربما يكشف على الإنسان عن طريق جسده، وربما يكشف عنه عن طريق نفسيته، وهو ماسأحاول التطرق إليه أدناه.

المطلب الأول: صور الإنتهاك الرقمي للحياة الخاصة عن طريق ممارسات الكشف الجسدي

الفرع الأول: أخذ بصمات الأصابع

تؤخذ بصمة الأصبع من نهايته، وهو مايسمى بالبنان، وقد ذكرت في القرآن الكريم في قوله تعالى: (أيحسبُ الإنسان ألّن نجمع عظامه بلى قاد رين على أن نسوّي بنانه "سورة القيامة، الآية3 ، وهنا إشارة في القرآن الكريم على أنه لا يوجد تطابق بصمتين لشخصين مختلفين حتى التوأم. فلقد أصبحت بصمة الإصبع من أهم الأدلة في مجال الإثبات الجنائي، مقارنة ببعض البصمات الأخرى[14].

فلقد أثبتت البحوث العلمية و الدراسات الطبية أن بصمات الأصابع تتميز عامّة بخصائص أساسية ورئيسية، إذ تتشكل لدى الإنسان قبل ولادته و تبقى إلى ما بعد الوفاة حتى تتحلّل

الجثة بكاملها. أما فيما يتعلق بالاعتداء الرقمي على خصوصية البصمات، فيتمثل في استعمال جهاز المضاهاة المعروف باسم: Automatic Fingerprint Identification System بحيث يقوم هذا الجهاز بالتعرف الآلي على البصمات ويمتاز النظام الذي يعمل به بالدقة والسرعة إذ يتم تخزين بصمات لأشخاص مشبوهين أو قاموا ببعض المخالفات المنصوص عليها في قانون العقوبات[15]، وبهذا التخزين ربما في وقت لاحق يسوء استعمال هذه البصمات ولذلك يشكل هذا العمل صورة من صور انتهاك الخصوصية، وخاصة بعدما تم العمل بنظام تخزين البصمات لإنجاز بطاقة التعريف الوطنية وجواز السفر البيوميتريين.

الفرع الثاني: أخذ بصمات العين

تم اكتشاف بصمة العين منذ سنوات قليلة من طرف الأطباء و أول من استفاد منها هي الولايات المتحدة الأمريكية و أوروبا في الاستعجالات العسكرية، وتتميز بأنها أكثر دقة من بصمات اليد لأن لكل عين خصائصها، حيث أنها لا يمكن أن تتشابه مع غيرها، ولو كانت لنفس الشخص، و يتم أخذ بصمة العين عن طريق النظر في عدسة جهاز رقمي، تم تصميمه لهذا الغرض، الذي يقوم بدوره بالتقاط صور لشبكية العين. و لقد تم تطوير تقنية التعرف على الهوية عبر قزحية العين التي تعتبر من أكثر التقنيات دقة في العالم حيث يتم تصوير المسافر بواسطة كاميرا فيديو مع التركيز على تصوير قزحية العين ثم ترمز الصورة و تحفظ، وبسبب هذا الحفظ ربما في وقت لاحق يسوء استعمال هذه البصمات ولذلك يشكل هذا العمل صورة من صور انتهاك الخصوصية،

الفرع الثالث: تحليل البصمة الوراثية

تعتبر البصمة الوراثية بيانا للخصائص و الصفات الوراثية التي تسمح بتحديد هوية الشخص و التعرف عليه من حيث خصائصه الوراثية، أي أنها تعبر عن الهوية الشخصية .وتتميز البصمة الوراثية بسهولة قراءتها و حفظها على أجهزة الكمبيوتر و في حالة الحاجة إليها يمكن الرجوع إليها. ويتم التعرف على البصمة الوراثية عن طريق التحليل الوراثي للشخص، وهي تعتبر صورة من صور الانتهاك العلمي لحرمة الحياة الخاصة، ذلك أن تحليل الشريط الوراثي بمفهومه الظاهر البسيط هو تحليل الحالة الطبية للفرد[16].

حيث أن التقدم في مجال التكنولوجيا الحيوية صاحبه تعارض مع العديد من المبادئ القانونية والتي أهمها الحق في حرمة الحياة الخاصة، و برز إلى الوجود مطلب إنساني يتمثل في وجوب حماية الحق في الخصوصية الجينية على أساس أن نتائج الفحص الجيني التي يرغب الفرد بكتمانها يجب أن تكون محل حماية، باعتبار أن هذه الفحوص تحمل معها أسرار الفرد الداخلية، هذه الأسرار التي تتعلق بصحته و حرمة جسده و من ثمة فلا يجوز إجبار الفرد بالبوح بها، حيث يصبح هو الوحيد الذي يقرر أين و متى ُتستخدم هذه البيانات، و ينتج عن هذا أنه لايجوز إجبار الفرد في الكشف عن أسراره الجينية، ومن جهة أخرى من حق الفرد أن يعرف المعلومات السرية التي هي في يد الخبراء والأطباء على سبيل الترخيص الإستثنائي للضرورة الصحية[17]،

الفرع الرابع: وضع الكبسولة الرقمية للتحاليل الطبية

عندما نتكلم عن الطب ومجالاته في هذا العصر نجد التكنولوجيات المستعملة في المجال الطبي تجعل الإنسان و كوامنه عرضة للتطفل، فالأمر لا يقتصر على الطب و العلاج، و إنما في دمج التقنيات مع بعضها البعض فالتحاليل الطبية بهذه التقنية أصبحت عبارة عن كبسولة لا ترى لكن ترصد كل شيء في جسم الإنسان عن طريق صناعة غرفة عمليات كاملة في كبسولة صغيرة، يتم وضعها داخل جسم المريض وبعدها ستدرس عبر أجهزة الكومبيوتر وتخزن هناك و تحلل إلى معطيات وأرقام في بنوك معلوماتية تستخدم عند الحاجة.

المطلب الثاني: صور الإنتهاك الرقمي للحياة الخاصة عن طريق ممارسات الكشف النفسي

الفرع الأول: المراقبة النفسية بجهاز كشف الكذب

يعتبر جهاز كشف الكذب أو ما يسمى باللغة الأجنبية Polygraph ، من الأجهزة الرقمية التي تستعمل في الأساليب العلمية الحديثة و يستعان بها في المجال الجنائي و تكمن طبيعة هذا الجهاز في معرفة أقوال و شهادات الشخص المستجوب و التحقق من صحتها أو كذبها، والكشف عن الصبغة الجنائية على بعض السلوكات التي يأتيها الفرد[18].

وللوقوف على مدى صدق أو كذب الشخص، فان الجهاز يقوم بقياس ما يطر أ عليه من تغيرات فسيولوجية للأجهزة اللاإرادية داخل جسمه كالنبض و العرق و ضغط الدم اتجاه الأسئلة الموجهة له.

الفرع الثاني: المر اقبة النفسية البيانية

الرقابة النفسية تقوم على التجسس على عقل الفرد، بواسطة جهاز مخطط كهربائية الدماغ (EEG) وهو اختبار يكشف النشاط الكهربائي في الدماغ باستخدام أقراص معدنية صغيرة (مسارات كهربائية) مثبتة على فروة الرأس. تتصل خلايا الدماغ فيما بينها عن طريق النبضات الكهربائية وتكون نشطة في جميع الأوقات حتى عند النوم. ويظهر هذا النشاط في صورة خطوط موجية في تسجيل مخطط كهربائية الدماغ، وتحفظ وتسجل على هذا الجهاز، يعد مخطط كهربائية الدماغ واحدًا من الاختبارات التشخيصية الرئيسية لمرض الصرع. ويمكن أن يؤدي دورًا أيضًا في تشخيص اضطرابات الدماغ الأخرى، وما يقوم به مخ الإنسان ، ويعتبر هذا النمط من المراقبة تعديا على الأفكار وكوامن النفس البشرية، و هذا بعني سلب الفرد حقه الأصيل في الاحتفاظ بأفكاره و أحاسيسه لنفسه، و بالتالي تؤدي إلى تعرية الفرد من الناحية النفسية و تحو ل بينه و بين استفاء حاجاته الملحة في التستر على دخائله و صد الناس عن الخوض فيها. و تعتبر الحالة النفسية الحالة الوحيدة تقريبا التي لا يختلف فيها اثنان على خصوصيتها بحيث لا يجوز لأي كان اقتحامها و بأي ذريعة كانت، لكن حاولت التقنية ومازالت تجتهد لابتكار الوسائل التي يمكن من خلالها النفاذ إلى النفس البشرية متخذة عدة ذرائع أمنية منها و اجتماعية، أو تعتبرها من الوسائل الأمنية المختلفة المستعملة لمكافحة الإجرام والإرهاب، إلا أن جانبا من هذه السياسات والإجراءات إنما جاءت على حساب حقوق الإنسان[19].

الفرع الثالث: المر اقبة النفسية النانوية

لقد وجدت تقنيات تسمح بالولوج في شخصية الإنسان، وتساعد علي قراءة نواياه العدوانية مثلا، قبل أن يقدم على أي فعل ، ويعتمد ذلك على تطوير تقنيات مسح عالي الدقة لنشاط الدماغ، يمكن من خلاله توقع تصرفات الإنسان قبل حدوثها، و قد صنعت هذه الأجهزة على أساس قراءة النوايا الإرهابية عند المشتبه بهم قبل أن يرتكبوا جرائمهم، وقد برزت هذه الأبحاث على أساس مساعدة رجال الأمن في تمييز الإرهابي المحتمل.

كما أصبح من الممكن أن يزرع في الدماغ أجهزة متناهية الصغر تقرأ أفكار الناس وتبعث بها إلى مركز المعلومات، ليتم تحليلها ودراستها ، و تستطيع هذه الأجهزة شل قدرات من يفكر، ذلك أن المواد النانوية صغيرة لدرجة أنه يمكنها اختراق أغشية الدماغ والوصول إلى خلايا المخ والتحكم فيها، أو تعطيلها.[20]

خاتمة

من خلال هذه الدراسة المتواضعة توصلت إلى عدة نتائج، ومن خلالها تبادرت في ذهني مجموعة من التوصيات أوردها فيما يلي:

أولا: النتائج

1/ تعد الجوسسة من الأعمال اللاأخلاقية التي يمارسها عديمي الضمير والأخلاق، فبعدما كانت تمارس خلسة من وراء ستار أصبحت الآن تمارس بفن وبتقنيات عالية الدقة عن طريق تقنية النانو بالجهاز الرقمي للتصغير اللامتناهي، الذي يستعمل عادة في الأعمال الأمنية والإستخباراتية، أو عن طريق الماسح الضوئى الذي يكون في يد سلطة الحكومات، ويستعمل خاصة في المطارات والسجون بداعي حفظ الأمن والنظام العام، وقد تطورت تقنية استراق السمع والبصر بشكل رهيب جدا، حيث أصبحت الجوسسة تتم بزرع أجسام غير مرئية على شكل كاميرات وميكروفونات وشرائح، ترصد الصوت والصورة بجودة عالية، لكي يطلع عليها المتجسس، إلا أن هذه الإجراءات والممارسات كلها تشكل خرقا صارخا لقواعد الآداب والأخلاق العامة، طالما أنها تكشف الإنسان وتعريه أمام القائمين على هذه التقنيات، وربما تتعداهم إلى عموم البشر.

2/ يتسبب الإنسان في كثير من الأحيان في أذى نفسه، ويكون هو الذي مهد الطريق للكشف عن خصوصياته، وذلك عن طريق استعماله لتكنولوجيات الإعلام والإتصال، كاستعمال الهاتف النقال، وأجهزة الحاسوب،وأثناه تصفحه للأنترنت، أو استعمال التطبيقات الحديثة كالفيسوبك، والمسنجر، والأنستغرام، أو أثناء استعماله للبريد الإلكتروني، أو أثناء إعتماده على تقنية تحديد المواقع الجغرافية وخاصة أثناء السفر.

3/ الحالات الاضطرارية التي يقع فيها الإنسان، تجعله عرضة للإعتداء على حرمة حياته الخاصة، ومن بين هذه الحالات الإضطرارية التي يجب للإنسان أن يذعن لها مايلي:

- أخذ بصمات الأصابع لإنجاز بطاقة التعريف الوطنية، أو جواز السفر البيوميتريين، أو لتأكيد الحضور في المؤسسة التي يشتغل فيها.
- أخذ بصمات العين أثناء السفر إلى الخارج، أو أثناء الدخول إلى المقرات الحكومية والمواقع الحساسة.
- أخذ البصمات أو إجراء تحليل البصمة الوراثية، أو إجراء رقابات نفسية في التحقيقات الجنائية.
- وضع الكبسولة الرقمية للتحاليل الطبية من أجل المتابعات العلاجية.

ثانيا: التوصيات

1/ إدراج ثقافة الفطنة والحيطة والحذر في البرامج التعليمية في كل المراحل، لكي لا يعرض الإنسان نفسه لانتهاك خصوصيته، وتعليم البرامج والتطبيقات التكنولوجية المتعلقة بحماية الحياة الخاصة لكل الفئات.

2/ وجوب العمل على توفير الإمكانيات الفنية والتقنية والبشرية من طرف الدولة للعمل في إطار الفضاء الرقمي لحماية الخصوصية.

3/ العمل على وضع إطار تشريعي وتنظيمي وإداري للحد من انتهاك حرمة الحياة الخاصة دوليا ووطنيا.

الهوامش:

الحلايقة غادة ، ماهو النانو، منشور بتاريخ: 2018/05/31، على الموقع:https://mawdoo3.com ، اطلع عليه بتاريخ: 2020/03/30، على الساعة: 13:00.

[2] بن سعيد صبرينة ، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا، أطروحة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، السنة الجامعية: 2015/2014، ص: 103.

[3] أبو العنين شريف مصطفى محمود ، حقوق الإنسان بين التفريط والتوظيف السياسي، دار الجامعة الجديدة، الإسكندرية، دط، سنة: 2017، ص: 151

[4] بن سعيد صبرينة ، المرجع السابق، ص: 107

[5] الشافعي جابر عبد الهادي سالم ، تأصيل الإعلان العالمي لحقوق الإنسان ومبادئ القانون الدولي الإنساني من منظور إسلامي، دار المطبوعات الجامعية، الإسكندرية، دط، سنة: 2017، ص: 173

[6] بن سعيد صبرينة ، المرجع السابق، ص: 113

[7] فايز محمد حسين محمد، فلسفة حقوق الإنسان ومكافحة العنف ضد المرأة، دار المطبوعات الجامعية، الإسكندرية، دط، سنة: 2016، ص: 20

[8] يسن ياسمين ، طريقة فتح رسائل البريد الإلكتروني، دت، من موقع: https://www.edarabia.com ، اطلع عليه بتاريخ: 2020/03/30، على الساعة: 16:40.

[9] عميمر نعيمة ، الوافي في حقوق الإنسان، دار الكتاب الحديث، القاهرة، ط: 1، سنة: 2009، ص: 24

[10] عدنان سوزان، انتهاك حرمة الحياة الخاصة عبر الإنترنت، مجلة جامعة دمشق ، المجلد: 29 العدد:3، سنة: 2013ص: 436

[11] الحماوي محمد جاسم ، دور المنظمات الدولية غير الحكومية في حماية حقوق الإنسان، دار الجامعة الجديدة، الإسكندرية، دط، سنة: 2013 ص:123

[12] بن سعيد صبرينة ، المرجع السابق، ص: 144

[13] الجبوري علي عبودي نعمة ، حقوق الإنسان والديمقراطية، دار الأيام، عمان، ط: 1 سنة: 2017، ص: 167

[14] احدادن سيلية، أثر الإثبات الجنائي بالوسائل التقنية الحديثة على حقوق الإنسان، مذكرة الماستر، قسم الحقوق والعلوم السياسية، جامعة بجاية، السنة الجامعية: 2017/2016، ص: 14

[15] يحياوي نورة، حماية حقوق الإنسان في القانون الدولي والقانون الإنساني، دار هومة، الجزائر، ط: 3، سنة: 2008، ص: 64

[16] احدادن سيلية، المرجع السابق، ص: 20

[17] جدو فاطمة الزهرة، الوجيز في حقوق الإنسان، دار بلقيس، الجزائر، دط، سنة:2018، ص:18

[18] عثامنية لخميسي، عولمة التجريم والعقاب، دار هومة، الجزائر، ط2، سنة: 2008، ص: 143

[19] فرحات أكرم حسام، مكافحة الإرهاب والقانون الدولي لحقوق الإنسان، دار الأيام، عمان، دط، سنة: 2017، ص: 128.

[20] بن سعيد صبرينة ، المرجع السابق، ص: 93

قائمة المصادروالمراجع

أولا: القرآن الكريم

ثانيا: الكتب القانونية

1/ أبو العنين شريف مصطفى محمود ، حقوق الإنسان بين التفريط والتوظيف السياسي، دار الجامعة الجديدة، الإسكندرية، دط، سنة: 2017.

2/ الجبوري علي عبودي نعمة ، حقوق الإنسان والديمقراطية، دار الأيام، عمان، ط: 1 سنة: 2017.

3/ جدو فاطمة الزهرة، الوجيز في حقوق الإنسان، دار بلقيس، الجزائر ، دط، سنة:2018.

4/ الحماوي محمد جاسم ، دور المنظمات الدولية غير الحكومية في حماية حقوق الإنسان، دار الجامعة الجديدة، الإسكندرية، دط، سنة: 2013.

5/ يحياوي نورة، حماية حقوق الإنسان في القانون الدولي والقانون الإنساني، دار هومة، الجزائر، ط: 3، سنة: 2008.

6/ عميمر نعيمة ، الوافي في حقوق الإنسان، دار الكتاب الحديث، القاهرة، ط: 1، سنة: 2009.

7/ عثامنية لخميسي، عولمة التجريم والعقاب، دار هومة، الجزائر، ط2، سنة: 2008.

8/ فايز محمد حسين محمد، فلسفة حقوق الإنسان ومكافحة العنف ضد المرأة، دار المطبوعات الجامعية، الإسكندرية، دط، سنة: 2016.

9/ فرحات أكرم حسام، مكافحة الإرهاب والقانون الدولي لحقوق الإنسان، دار الأيام، عمان، دط، سنة: 2017.

10/ الشافعي جابر عبد الهادي سالم ، تأصيل الإعلان العالمي لحقوق الإنسان ومبادئ القانون الدولي الإنساني من منظور إسلامي، دار المطبوعات الجامعية، الإسكندرية، دط، سنة: 2017.

ثالثا: الرسائل الجامعية

1/ بن سعيد صبرينة ، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا، أطروحة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة، السنة الجامعية: 2015/2014.

2/ احدادن سيلية، أثر الإثبات الجنائي بالوسائل التقنية الحديثة على حقوق الإنسان، مذكرة الماستر، قسم الحقوق والعلوم السياسية، جامعة بجاية، السنة الجامعية: 2017/2016.

رابعا: المجلات العلمية

*عدنان سوزان، انتهاك حرمة الحياة الخاصة عبر الإنترنت، مجلة جامعة دمشق ، المجلد: 29 العدد:3، سنة: 2013ص: 436.

خامسا: المو اقع الإلكترونية

1/ الموقع:https://mawdoo3.com

2/ الموقع: https://www.edarabia.com

الإطار القانوني الدولي لحماية الحق في الخصوصية في العصر الرقمي

د.سامية بوروبة

كلية الحقوق جامعة الجزائر 1

ملخص المداخلة:

بسبب التدخل المتزايد للرقمنة في حياة الأفراد، من الضروري تفعيل مختلف الصكوك الدولية التي تكّرس الحق في الحياة الخاصة و على رأسها الإعلان العالمي لحقوق الإنسان الذي كّرس هذا الحق. و ينبغي في هذا الصدد الإشارة كذلك إلى المبادرات الإقليمية في مجال حماية المعطيات لشخصية التي تعزّز من حماية الحق في الخصوصية، و على رأسها الاتحاد الأوروبي الذي كان من السباقين لوضع إطار قانوني يتمثل في التوجيه الصادر سنة 1995 و الذي مكّن من مواءمة تشريعا الدول الأوروبية. و تبعه صدور التنظيم العام حول حماية المعطيات الصادر سنة 2016. كما أن المقرر الخاص التابع للأمم المتحدة المعني بالحق في الخصوصية يساهم بدوره في تعزيز حماية الحق في الخصوصية.

الكلمات المفتاحية: الحق في الخصوصية– المقرر الخاص للأمم المتحدة– التعليق العام للجنة المعنية بحقوق الإنسان– الاتحاد الأوروبي–الاتحاد الإفريقي

مقدمة:

أصبح الحق في الخصوصية من المواضيع التي تشهد اهتماما مكثفا في القانون الدولي لحقوق الإنسان خصوصا مع الثورة الرقمية و تطور الوسائل التكنولوجية التي لا تعرف الحدود الزمانية و لا الإقليمية، و لا تترك للفرد إلا مساحة ضيقة من ممارسة الحرية و حماية حياته الخاصة.

و يعدّ الحق في الحياة الخاصة [1] أو في الخصوصية من المفاهيم التي يصعب الإحاطة بها بالنظر لارتباطه بالبيئة الاجتماعية و السياسية التي يوجد فيها، فنجد أن هناك اختلاف جوهري بين مفهوم الحق في الحياة الخاصة من منظور المجتمعات الغربية [2] و بين المقصود به ضمن المجتمعات العربية والإسلامية، و كذا دول شرق آسيا التي تعرف كلّها مفاهيم متباينة . فالدول الغربية تمنح تفسيرا واسعا للحق في الحياة الخاصة وهو مفهوم متطور عبر الزمان، في حين تبقي الدول العربية و الإسلامية في إطار مرتبط بالقيم الثقافية و الدينية السائدة فيها.

يُعرّف الحق في الحياة الخاصة بأنه ذلك المجال المحصّن الذي يعود للفرد وحده و لا يحق للغير التدخل فيه إلاّ باحترام ضوابط و شروط يضعها القانون، و لقد ارتبط هذا الحق في مفهومه التقليدي ارتباطا وثيقا بالمسكن، على اعتبار أن سكن الإنسان هو القلعة الحصينة التي تحمي حياته الخاصة من التطفل والانتهاك، وكان جل الدساتير تقتصر على مبدأي حرمة المسكن وسرية المراسلات كمظهرين لهذا الحق [3]، كما أن هناك توجها حديثا يضيف إلى ذلك حماية المعطيات الشخصية و التي تعد من أهم عناصر الحياة الخاصة.

---

1 ينبغي الإشارة إلى أن الصكوك الدولية التقليدية والكتابات الفقهية تشير إلى مصطلح الحق في الحياة الخاصة، في حين أن الصكوك الحديثة تستخدم مصطلح الحق في الخصوصية

2 د.محمد يوسف علوان و د.محمد خليل الموسى، القانون الدولي لحقوق الإنسان، الحقوق المحمية، الجزء الثاني، دار الثقافة للنشر والتوزيع،2008، ص 288.

3 عائشة لخشين، حماية الحق في الخصوصية في العصر الرقمي في المواثيق الدولية، مجلة جيل حقوق الإنسان، عدد 39، متوفر على الرابط: https://jilrc.com/archives/13436#:~:text=1%2D%20%D8%AD%D9%85%D8%A7%D9%8A%D8%A9%20%D8%A7%D9%84%D8%AD%D9%82%20%D9%81%D9%8A%20%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9%20%D9%81%D9%8A%20%D8%A7%D9%84%D9%85%D9%88%D8%A7%D8%AB%D9%8A%D9%82%20%D9%88%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%

و يواجه هذا الحق في الوقت الحالي تحديات تتعلق بضرورة احترامه بالنظر لتزايد استخدام الوسائل التكنولوجية و ما تبقي به من مخاطر على هذا المجال الحيوي، و يضاعف من احتمالات انتهاكه. لهذا ينبغي طرح التساؤل حول مدى توافر إطار قانوني دولي لحماية الحق في الخصوصية في ظل الثورة الرقمية؟

و سنجيب على هذه الإشكالية من خلال محورين:

يتعلق الأول بالإطار القانوني للحماية على المستوى العالمي(المبحث الأول)، و يعالج الثاني الإطار القانوني للحماية على المستوى الإقليمي (المبحث الثاني).

المبحث الأول: الإطار القانوني لحماية الحق في الخصوصية على المستوى العالمي

يعترف القانون الدولي لحقوق الإنسان بحماية للحق في الخصوصية ضمن جملة من الصكوك العالمية (المطلب الأول)، كما أنه يؤسس مجموعة من الآليات التي تتولى تلك الحماية (المطلب الثاني).

المطلب الأول: الصكوك العالمية

اهتمت الصكوك الدولية العالمية بالحق في الخصوصية، و لقد بدأت هذه الحماية بصكوك من القانون المرن ليت تكريسها فيما بعد ضمن اتفاقيات دولية تتمتع بالإلزامية. و يعد الاعلان العالمي لحقوق الانسان[1] اول هذه الصكوك حيث كرس هذا لحق في المادة 12 منه التي تنص:

D8%A7%D8%AA%20%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9%3A&text=%D8%A3%D9%85%D9%91%D8%A7%20%D8%B9%D9%86%20%D8%A7%D9%84%D8%B9%D9%87%D8%AF%20%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%20%D9%84%D9%84%D8%AD%D9%82%D9%88%D9%82,%D9%85%D8%B1%D8%A7%D8%B3%D9%84%D8%A7%D8%AA%D9%87%20%D9%88%D8%A7%D9%84%D8%AD%D9%81%D8%A7%D8%B8%20%D8%B9%D9%84%D9%89%20%D8%B3%D9%85%D8%B9%D8%AA%D9%87%20%D9%88%D8%B4%D8%B1%D9%81%D9%87.

تاريخ الإطلاع 15 سبتمبر 2022.

1 اعتمدت الجمعية العمة للأمم المتحدة نص الإعلان بتاريخ 10 ديسمبر 1948.

" **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 مثل ذلك التدخل أو تلك الحملات**".

و يظهر من نص المادة أن الإعلان العالمي اعتبر الحياة الخاصة من الحقوق المطلقة التي تتطلب احتراما صارما، و حدّدها في ثلاثة مجالات هي الأسرة، المسكن و المراسلات. و هي المجالات التقليدية التي كانت حكرا على الفرد و لا يحق لأي كان التدخل فيها.

أما العهد الدولي الخاص بالحقوق المدنية و السياسية، فلقد عالج بدوره هذه المسألة ضمن الحقوق التي كرّسها، حيث جاء في المادة 17 منه :

" .1. **لا يجوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.**
.2. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس ".

يبدو من صياغة هذه المادة أنها مستمدة من الإعلان العالمي باعتبارها تضمنت نفس العناصر التي وردت فيها، غير أنها وردت فيها إضافات بالإشارة إلى استخدام حملات **بطريقة غير قانونية** يكون هدفها المساس بشرف الشخص أو سمعته. و أضافت المادة كذلك عنصرا مهما يتمثل في التأكيد على الحماية القانونية التي يجب أن يستفيد منها كل شخص يتعرض للمساس بالحق في الخصوصية.

إذا كان العهد الدولي هو أهم صك يتعلق بتكريس الحق في الخصوصية بالنظر لطابعه الشامل و انطباقه على نطاق واسع كونه اتفاقية عالمية، إلا أن صياغة المادة جاءت واسعة تحتاج إلى تفسير، و هوما يقسّر تدخل اللجنة المعنية بحقوق الإنسان عن طريق إصدار التعليق العام رقم 16 الصادر على المادة 17 من العهد بشأن حق الفرد في احترام خصوصيته وأسرته وبيته و مراسلاته، و في حماية شرفه وسمعته .و لقد قدّت اللجنة تفسيرا عاما مفاده أنه يلزم ضمان هذا الحق في مواجهة جميع التدخلات والاعتداءات، سواء أكانت صادرة عن سلطات الدولة أم عن أشخاص طبيعيين أو قانونيين. والالتزامات

التي تفرضها هذه المادة تقتضي أن تعتمد الدولة تدابير تشريعية وغيرها من التدابير اللازمة لإعمال الحظر المفروض على تلك التدخلات والاعتداءات فضلاً عن حماية هذا الحق[1].

كما ورد في التعليق العام تعريف لبعض المصطلحات الواردة في المادة مثل عبارة غير مشروع (غير قانوني) أنه لا يمكن حدوث أي تدخل إلا في الحالات التي ينص عليها القانون. ولا يجوز أن يحدث التدخل الذي تأذن به الدول إلا على أساس القانون، الذي يجب هو نفسه أن يكون متفقاً مع أحكام العهد ومراميه وأهدافه.

وفيما يتعلق بمصطلح "الأسرة"، فإن أهداف العهد تقتضي تفسيره، لأغراض المادة 17، تفسيراً واسع النطاق بحيث يشمل جميع من تتألف منهم الأسرة بمعناها المتفق عليه في مجتمع الدولة الطرف المعنية. وينبغي أن يفهم مصطلح "بيت" على أنه يعني المكان الذي يقيم فيه الشخص أو يزاول فيه نشاطه المعتاد.

و أشار التعليق العام إلى مسألة مهمة هي الطابع النسبي لحماية الحياة الخاصة كون جميع الأشخاص يعيشون معا في المجتمع، غير أنه ينبغي ألا يكون بمقدور السلطات العامة المختصة أن تطلب من المعلومات المتعلقة بالحياة الخاصة للفرد إلا ما يكون معرفته ضرورياً حرصاً على مصالح المجتمع على النحو المفهوم بموجب العهد.

كما أن هناك نصوصا أخرى أهمها اللوائح الصادرة عن الجمعية العامة للأمم المتحدة ، ونذكر من بينها اللائحة 168/67 المؤرخة في 18 ديسمبر 2013، و اللائحة 168/69 المؤرخة في 18 ديسمبر 2014 ، و تعد من الصكوك التي تم اعتمادها بغرض أخذ التطور التكنولوجي و تأثيره على الحق في الخصوصية بعين الإعتبار إضافة إلى اللائحة 95/45 المؤرخة في 14 ديسمبر 1990 والمتعلقة بالمبادئ التوجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الالكترونية . و رغم الطابع غير الملزم لها إلا أنها تعبّر عن التوجه العام للدول بالنسبة لهذه المسألة.

1 انظر: اللجنة المعنية بحقوق الإنسان، الدورة الثانية والثلاثون (1988)، التعليق العام رقم 16: المادة 17 (الحق في حرمة الحياة الخاصة)، ص 1.

و أصدر مجلس حقوق الإنسان التابع للأمم المتحدة بدوره قرارات حول الحق في الخصوصية أهمها القراران 16/28 المؤرخ في 26 مارس 2015 و 7/34 المؤرخ في23 مارس 2017 بشأن الحق في الخصوصية في العصر الرقمي، و كذا القراران 23/ 13 المؤرخ في 1 جويلية 2016 و 38/ 7 المؤرخ في 5 جويلية 2018 بشان تعزيز و حماية حقوق الإنسان والتمتع بها على الانترنت.

و من بين الصكوك ذات الأهمية كذلك الوثيقة الختامية للاجتماع رفيع المستوى للجمعية العامة بشان الاستعراض العام لتنفيذ نتائج القمة العالمية لمجتمع المعلومات المنعقدة سنة 2003.

و يظهر من كل ما عرضنا تنوع في الصكوك التي تكرّس الحق في الخصوصية في العصر الرقمي على المستوى العالمي بين من هو ملزم و بين ما يفتقر إلى الإلزامية، و يلاحظ أن نصوص القانون المرن هي التي تنظم بصورة واسعة هذا الموضوع بسبب عمومية الأحكام الاتفاقية و افتقارها للدقة و الوضوح في أغلب الحالات، إضافة إلى العد الرقمي الذي يضع الحق في الخصوصية ضمن سياق جديد لم تنظمه النصوص الاتفاقية .

المطلب الثاني: آليات الحماية

لم تكتف مختلف الصكوك لا سيما الاتفاقية منها بتكريس الحق في الخصوصية، بل رافقت ذلك بإنشاء آليات متنوعة ذات طبيعة مختلفة، منها ما هي تعاهدية، و منها ما هي غير تعاهدية و هوما سنبينه تباعا.

فبالنسبة للآليات التعاهدية أو التعاقدية، ينبغي الإشارة إلى اللجنة المعنية بحقوق الإنسان و هي الجهاز المكلف بالرقابة على العهد الدولي للحقوق المدنية والسياسية، و هي جهاز مكون من خبراء يقومون بالرقابة إما عن طريق فحص التقارير المقدمة من قبل الدول الأطراف حول التزاماتها بموجب أحكام العهد و مدى إنفاذها لأحكامه و يشمل ذلك الحق في الخصوصية، أو عن طريق البت في الشكاوى الفردية التي تُرفع إليها من قبل الأفراد ضد الدول الأطراف التي تنتهك حقهم المكرّس في العهد.

كما تتولى للجنة المعنية بحقوق الإنسان إجراء الرقابة بطريقة غير مباشرة عن طريق اعتماد التعليقات العامة التي تتولى بها تفسير الأحكام الواردة في العهد، و هو الحال بالنسبة للتعليق العام رقم 16 المشار إليه سابقا.

أما الآليات غير التعاهدية ، فتتمثل في نظام الإجراءات الخاص لمجلس حقوق الإنسان (التي كانت في فترة سابقة تابعة للجنة حقوق الإنسان قبل أن يتم تعويضها سنة 2006 بمجلس حقوق الإنسان) و المتمثلة في الإجراءات الخاصة القطرية و الإجراءات الخاصة المواضيعية . و يتعلق الأمر هنا بكل من: –المقرر الخاص لمجلس حقوق الإنسان المعني بالحق في الخصوصية الذي تم إنشاء ولايته سنة 2015 [1]

–و المقرر الخاص لمجلس حقوق الإنسان المعني بتعزيز و حماية الحق في حرية الرأي و التعبير الذي تم إنشاء ولايته سنة 1993 [2].

و يجري المقررون الخاص رقابتهم عن طريق القيام بزيارات للدول التي تشهد انتهاكا للحق في الخصوصية، و يقومون على إثر ذلك بتحرير تقارير يتم رفعها للجمعية العامة ، كما انهم يتكفلون بحالات الانتهاكات الفردية وكذا بالانشغالات العامة عن طريق توجيه بلاغات للدول التي تعرف انتهاكات في هذا المجال، و يقوم المقررون كذلك بإعداد دراسات سنوية حول موضوع الحق في الخصوصية في العصر الرقمي.

المبحث الثاني: الحماية الإقليمية للحق في الخصوصية

إن عالمية حقوق الإنسان لا تتعارض مع خصوصيتها، و ينطبق هذا على مجال الحق في الخصوصية في العصر الرقمي، حيث تم تنظيمه على مختلف المستويات الإقليمية، و التي تشهد تفاوتا بين المنظومات الرائدة في أوروبا و الولايات المتحدة الأمريكية(المطلب الأول)، لتختلف في باقي أنحاء العالم (المطلب الثاني).

---

1 بموجب لائحة صادرة عن مجلس حقوق الإنسان. انظر:

https://spinternet.ohchr.org/ViewAllCountryMandates.aspx?Type=TM&lang=fr

2 بموجب لائحة صادرة عن لجنة حقوق الإنسان. االنظر:

https://spinternet.ohchr.org/ViewAllCountryMandates.aspx?Type=TM&lang=fr

المطلب الأول: الأنظمة الأوروبية الرائدة و المقاربة الأمريكية الخاصة

تعرف أهم الصكوك الإقليمية على مستوى القارة الأوروبية تكريسا للحق في الخصوصية، و هو حال الاتفاقية الأوروبية لحماية حقوق الإنسان في المادة 8 التي نصّت على ما يلي:

"1.**لكل إنسان حق احترام حياته الخاصة والعائلية ومسكنه ومراسلاته.**
2-لا يجوز للسلطة العامة أن تتعرض لممارسة هذا الحق إلا وفقاً للقانون وبما تمليه الضرورة في مجتمع ديمقراطي لصالح الأمن القومي وسلامة الجمهور أو الرخاء الاقتصادي للمجتمع، أو حفظ النظام ومنع الجريمة، أو حماية الصحة العامة والآداب، أو حماية حقوق الآخرين وحرياتهم."

و يُستخلص من الفقرة الأولى أن الحق في الخصوصية مكفول لكل شخص يقع ضمن ولاية أية دول طرف في هذه الاتفاقية[1]، كما ألزمت الفقرة 2 منها الدول الأطراف عند تقييدها لممارسة هذا الحق احترام الضوابط الواردة في القانون، و أن يتم ذلك في أضيق الحدود و ضمن أهداف محدّدة بدقة.

كما كرس ميثاق الحقوق الأساسية للاتحاد الأوروبي الحق في الحياة الخاصة.

و لم تخرج اتفاقية البلدان الأمريكية لحقوق الإنسان عن هذا التوجه، حيث كفلت الحق الحياة الخاصة في المادة 11 التي نصّت:

"1. **لكل إنسان الحق في أن يحترم شرفه وتصان كرامته.**
2-لا يجوز أن يتعرض أحد لتدخل اعتباطي أو تعسفي في حياته الخاصة أو في شؤون أسرته أو منزله أو مراسلاته، ولا أن يعترض لاعتداءات غير مشروعة على شرفه أو سمعته.
3-لكل إنسان الحق في أن يحميه القانون من مثل ذلك التدخل أو تلك الاعتداءات".

و يقترب هذا النص من الصياغة الواردة في الاتفاقية الأوروبية مما يوحي بتبني نفس المقاربة التي تعرف تقديس هذا الحق و فرض قيود صارمة على المساس به.

من المؤكد أن الاتحاد الأوروبي يعد أول منظمة تتولى تنظيم موضوع الحق في الخصوصية الرقمية منذ سنه 1995 بموجب التوجيه رقم CE / 46 / 1995 والذي استهدف اجراء مواءمة تشريعية على

1 انظر: عائشة لخشين، حماية الحق في الخصوصية في العصر الرقمي، مرجع سابق.

مستوى الاتحاد الاوروبي و وضع جملة من المبادئ التي تم إدماجها في قوانين مختلف الدول الاعضاء ومن أهم هذه المبادئ إنشاء سلطات(مؤسسات) للرقابة في كل منها.

و لقد استمد هذا النص مصدره من " الخطوط التوجيهية التي تحكم حماية الحق في الحياة الخاصة و المبادلات العابرة للحدود للمعطيات ذات الطابع الشخصي" [1] التي اعتمدتها منظمة التعاون والتنمية في أوروبا OCDE سنة 1980. وهي مجرد صك من القانون المرن يفتقد للإلزامية، غير أنه يكتسي أهمية معتبرة لأنه وضع القواعد الأساسية التي تهدف إلى حماية المعطيات ذات الطابع لشخصي، مما أدى إلى تأثر الاتحاد الأوروبي بما ورد فيه و الاستنباط منه[2]. و تجدر الإشارة إلى أن التوجيهات Directives الصادرة عن الاتحاد الأوروبي لا تقبل التطبيق المباشر على الرغم من إلزاميتها بل تحتاج إلى نصوص تطبيقية من قبل الدول الأطراف.

وفي إطار تعزيز الاطار القانوني للحق في الحياه الخاصة، اعتمد الاتحاد الاوروبي صكا آخر يتمثل فيه التنظيم العام حول حماية المعطيات Règlement général sur la protection des données والذي على خلاف التوجيه السالف ذكره يعتبر ذو تطبيق مباشر في قوانين الدول الاعضاء للاتحاد الاوروبي.

ولقد حدد هذا النص دخوله حيز النفاذ بمرور سنتين وحدد بتاريخ ماي 2018، بغرض منح مختلف الفواعل ذات الصلة و المتمثلة في المنظمات والمؤسسات الفرصة من أجل مواكبة أحكامه، حيث يقع عليها إجراء مطابقة مع مختلف المبادئ الواردة فيه.

ومواصلة في نفس المسار، شرع الاتحاد الاوروبي في إجراء دراسات بغية إصدار نصوص تتعلق بالخصوصية الإلكترونية وذلك بغرض مواءمة المقتضيات التقليدية المتعلقة بالحياة الخاصة عبر وسائل الاتصالات في ظل التطورات والوسائل الحديثة، عن طريق إدراج سرية المراسلات في العصر الرقمي.

[1] Lignes directrices régissant la projection de la vie privée et les flux transfrontières de données à caractère personnel.

[2] La vie privée à l'ère du numérique : Au-delà de la conformité, un enjeu de confiance, WAVESTONE, https://www.wavestone.com/app/uploads/2017/01/Vie-privee-numerique-confiance.pdf , p 18,19.

ويستنتج من كل ما سبق أن الاتحاد الاوروبي يعتمد مقاربه حمائية تقوم بها الدولة لمعطيات مواطنيها وهو أمر مختلف عما تقوم به دول أخرى في باقي مناطق العالم كما سنوضحه أدناه.

أما في الولايات المتحدة الأمريكية، فنلاحظ غياب قانون موحد على المستوى الفدرالي يعالج مسألة جمع واستخدام المعطيات ذات الطابع الشخصي، و توجد بدلا عن ذلك مجموعة مركبة من القوانين المطبقة على بعض القطاعات أو بعض الدويلات الفدرالية. و في هذا الإطار، نجد أن بعض هذه القوانين تخص أصنافا محدّدة من المعطيات ذات الطابع الشخصي مثلما هو الحال بالنسبة للمعطيات المالية أو تلك المتعلقة بالصحة. و بالموازاة لذلك، طوّرت الوكالات الفدرالية و المجمعات الصناعية جملة من الممارسات الفضلى يتم استخدامها من أجل القيام بضبط ذاتي في مجال حماية الخصوصية.

و يمكن الإشارة في هذا الصدد إلى التعديل الرابع من الدستور الأمريكي الذي يعدّ الأساس القانوني لحماية الحق في الخصوصية حيث جاء فيه:

" **لا يجوز المساس بحق الناس في أن يكونوا آمنين في شخصهم ومنازلهم ومستنداتهم ومقتنياتهم من اي تفتيش او احتجاز غير معقول، ولا يجوز إصدار مذكرة بهذا الخصوص إلا في حال وجود سبب معقول، معزز باليمين أو التوكيد، وتبين بالتحديد المكان المراد تفتيشه والاشخاص او الاشياء المراد احتجازها**"

و يمكن تعميم هذا النص ليشمل مختلف الجوانب منها حماية المعطيات ذات الطابع الشخصي.

كما ينبغي الإشارة هنا الى قوانين حماية المستهلك والتي وإن كانت لا تنظم مباشرة الحياة الخاصة، إلا أنها تتضمن أحكاما تمنع بعض الممارسات غير القانونية المشتملة على إفشاء المعطيات ذات الطابع الشخصي . غير ان المواطنين الامريكيين يحتفظون بهامش من الحرية فيما يتعلق بمشاركة معطياتهم ذات الطابع الشخصي.

نستنتج من ذلك وجود اختلاف بين المقاربة الأمريكية والمقاربة الأوروبية، ويمكن تأكيد ذلك بالإشارة الى المنظومة القانونية المتمثلة في الملجأ الآمن Safe harbor حيث كان هذا الأخير يضمن حماية تحويل المعلومات بين الاتحاد الأوروبي والولايات المتحدة الأمريكية الى غاية أكتوبر 2015 تاريخ إلغائه من

قبل محكمة العدل للاتحاد الاوروبي . ولقد استندت المحكمة لتأسيس قرارها على فكرة أن مستوى حماية المعطيات الذي تشرف عليه الولايات المتحدة الأمريكية لم يعد كافيا بالنظر للمبادئ المطبقة في الاتحاد الاوروبي، خصوصا بعد قضية المعطيات التي صرّح بها الصحفي سنودن Edward Snowden فيما يتعلق بقضية التنصت الممارسة من قبل الحكومة الأمريكية.

وعلى إثر هذا القرار، قررت الولايات المتحدة والاتحاد الاوروبي اعتماد منظومة قانونية جديدة تُعرف ب درع الخصوصية Privacy Shield بتاريخ فيفري 2016 هدفها تكريس حمايه اكثر لتحويل المعطيات ولقد دخل هذا النص حيز التنفيذ في أوت 2016.

المطلب الثاني: حماية متفاوتة في النظم الإقليمية الأخرى

تشهد باقي مناطق العالم نظما مختلفة فيما يتعلق بالحق في الخصوصية.

فتشهد القارة الآسيوية تواجد نوعين من الدول: منها من يشهد تقدما معتبرا فيما يتعلق بحماية الحياة الخاصة و هو حال كل من كوريا الجنوبية، سنغافورة، هونغ كونغ و تايوان، و منها من يعرف تأخرا في هذا المجال. و يمكن الإشارة هنا إلى الصين التي لم تعتمد نصا قانونيا يكرّس حماية المعطيات ذات الطابع الشخصي إلا مؤخرا، عن طريق نشر قانون في نوفمبر 2016 دخل حيّز النفاذ منذ جوان 2017 [1] و إذا كان هذا القانون يشتمل على عدّة مبادئ تتعلق بحماية الحياة الخاصة، إلاّ أنه يشترط أن يتم حفظ هذه المعطيات على الإقليم الصيني مما يبرز التوجه الحمائي الصارم الذي تعتمده هذه الدولة.

ويلاحظ أن موضوع حماية المعطيات ذات الطابع الشخصي لا يحظى بأي اهتمام في باقي الدول الآسيوية مما يطرح مسألة الفراغ القانوني، و كذا الانتهاكات المحتملة للحق في الحياة الخاصة التي قد تنتج عن ذلك.

أما على مستوى القارة الإفريقية، فإن هناك تأخر عن الركب مقارنة بالدول الأوربية و بعض الدول الآسيوية المتطورة، و تعد دولة الرأس الأخضر أول بلد ينظم هذه المسألة بموجب قانون صادر في 2001. كما أن بوركينا فاو تعدّ أوّل دولة إفريقية تنشئ هيئة ضابطة على المستوى الوطني. أما على المستوى الإقليمي، يمكن الإشارة إلى اتفاقية الاتحاد الإفريقي حول الأمن السيبراني و حماية المعطيات

[1] La vie privée à l'ère du numérique, op.cit., p 21.

ذات الطابع الشخصي المعتمدة بتاريخ 27 جوان 2014 و المعروفة باتفاقية مالابو، و التي اشتملت على المفاهيم المكرسة في تشريعات الدول الأوروبية. و تقوم هذه الاتفاقية على ضرورة مواءمة الدول الإفريقية و المجموعات الاقتصادية الإفريقية لتشريعاتها مع المبادئ المكرسة فيها.

و تكرّس بعض دول أمريكا اللاتينية حماية من نوع خاص للحق في الخصوصية، حيث تكرس ضمانات دستورية فيما يتعلق بحماية المعطيات ذات الطابع الشخصي كما أنشأت سلطات ضبط مستقلة تشرف على هذه الحماية، و هو حال كل من الأرجنتين و الأوروغواي و التي اعتبرتها المفوضية الأوروبية من الدول التي تضمن حماية مناسبة للمعطيات.

خاتمة

إن تدخل الدول لتنظيم تصرفات الأفراد و ضبط الحياة اليومية لا يخلو من مساس بالحياة الخاصة خصوصا مع انتشار الشبكة العنكبوتية و تزايد استعمال الوسائل التكنولوجية الحديثة التي جعلت العالم كله مرتبطا، و كشف كل ذلك عن العديد من المسائل و المعلومات التي تعدّ من صميم الحياة الخاصة للأفراد التي لا يحق لأيّ كان الاطلاع عليها. كما أن الشركات الكبرة التي تتحكم في التكنولوجيات الحديثة و تسيطر على وسائل التواصل الاجتماعي غالبا ما تقتحم مجال الحياة الخاصة باستخدام معطيات الأشخاص دون مراعاة للطابع الخاص الذي تكتسيه مما يجعل الحق في الخصوصية على المحك.

أدت كل هذه الإشكاليات إلى وضع إطار قانوني على المستوى الدولي و تم ذلك بصورة تدريجية منذ اعتماد أول صك دولي في مجال حقوق الإنسان هو الإعلان العالمي لحقوق الإنسان، و الذي شكّل اللبنة الأولى التي استلهمت منها جميع الاتفاقيات اللاحقة. غير أن النظم الإقليمية قطعت شوطا في مجال توفير الحماية اللازمة، و شدّدت على الطابع المقدس للحق في الخصوصية في سياق الثورة الرقمية التي باتت تشكل تهديدا واضحا له. و لعل أهم حماية اعتمدت على المستوى الدولي هي إنشاء آليات متعددة و مختلفة الطبيعة، قضائية و غير قضائية تسعى كل منها إلى عزل الحياة الخاصة عن الخرق الي يتم ممارسته ضدها دون وجه حق، و هذا لضمان كرامة الإنسان التي تبقى الهدف الأسمى من تحقيق حقوق الإنسان على اختلاف أصنافها. و ينبغي الإشارة في هذا السياق إلى أهمية هذه الحماية الدولية بما تشتمله من سبل انتصاف متاحة للأفراد الذين تعرضوا لمساس بحقهم في الخصوصية جراء الثورة الرقمية.

من خلال ما سبق عرضه من إطار قانوني دولي لحماية الحق في الخصوصية في العصر الرقمي، يمكن تقديم المقترحات التالية:

-ضرورة وضع حماية المعطيات الشخصية ضمن الأولويات عند قيام الدول بمواءمة تشريعاها الوطنية مع المعايير الدولية.

-ضرورة إنشاء آليات وطنية للرقابة على احترام الحق في الخصوصية تتوفر على الضمانات الدولية المتعلقة بالاستقلالية و النزاهة و الفعالية.

قائمة المراجع

باللغة العربية:

الكتب:

د.محمد يوسف علوان و د.محمد خليل الموسى، القانون الدولي لحقوق الإنسان، الحقوق المحمية، الجزء الثاني، دار الثقافة للنشر والتوزيع،2008.

المقالات:

عائشة لخشين، حماية الحق في الخصوصية في العصر الرقمي في المواثيق الدولية، مجلة جيل حقوق الإنسان، عدد 39، متوفر على الرابط:
https://jilrc.com/archives/13436#:~:text=1%2D%20%D8%AD%D9%85%D8%A7%D9%8A%D8%A9%20%D8%A7%D9%84%D8%AD%D9%82%20%D9%81%D9%8A%20%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A

%D8%A9%20%D9%81%D9%8A%20%D8%A7%D9%84%D9%85%D9%88%D8%A7%D8%AB%D9%8A%D9%82%20%D9%88%D8%A7%D9%84%D8%A7%D8%AA%D9%81%D8%A7%D9%82%D9%8A%D8%A7%D8%AA%20%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%D8%A9%3A&text=%D8%A3%D9%85%D9%91%D8%A7%20%D8%B9%D9%86%20%D8%A7%D9%84%D8%B9%D9%87%D8%AF%20%D8%A7%D9%84%D8%AF%D9%88%D9%84%D9%8A%20%D9%84%D9%84%D8%AD%D9%82%D9%88%D9%82,%D9%85%D8%B1%D8%A7%D8%B3%D9%84%D8%A7%D8%AA%D9%87%20%D9%88%D8%A7%D9%84%D8%AD%D9%81%D8%A7%D8%B8%20%D8%B9%D9%84%D9%89%20%D8%B3%D9%85%D8%B9%D8%AA%D9%87%20%D9%88%D8%B4%D8%B1%D9%81%D9%87.

الصكوك الدولية

الاعلان العالمي لحقوق الانسان

العهد الدولي الخاص بالحقوق المدنية و السياسية

اللجنة المعنية بحقوق الإنسان، الدورة الثانية والثلاثون (1988)، التعليق العام رقم 16: المادة 17 (الحق في حرمة الحياة الخاصة).

الجمعية العامة للأمم المتحدة، اللائحة 168/67 المؤرخة في 18 ديسمبر 2013 بشأن الحق في الخصوصية في العصر الرقمي.

الجمعية العامة للأمم المتحدة، اللائحة 168/69 المؤرخة في 18 ديسمبر 2014 بشأن الحق في الخصوصية في العصر الرقمي.

الجمعية العامة للأمم المتحدة، اللائحة 95/45 المؤرخة في 14 ديسمبر 1990 والمتعلقة بالمبادئ التوجيهية لتنظيم ملفات البيانات الشخصية المعدة بالحاسبة الالكترونية.

منظمة التعاون والتنمية في أوروبا، الخطوط التوجيهية التي تحكم حماية الحق في الحياة الخاصة و المبادلات العابرة للحدود للمعطيات ذات الطابع الشخصي.

الاتحاد الأوروبي، التوجيه رقم CE / 46 / 1995 .

الاتحاد الأوروبي، التنظيم العام حول حماية المعطيات.

اتفاقية الاتحاد الإفريقي حول الأمن السيبراني و حماية المعطيات ذات الطابع الشخصي المعتمدة بتاريخ 27 جوان 2014.

باللغة الأجنبية:

La vie privée à l'ère du numérique : Au-delà de la conformité, un enjeu de confiance, 2017, https://www.wavestone.com/app/uploads/2017/01/Vie-privee-numerique-confiance.pdf , consulté le 07 Juillet 2022.

الحماية القانونية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي وفقا للقانون 18-07

Légal protection of data of a personal nature in the digital space in accordance with Law 18-07

د/ بوحزمة كوثر

جامعة ابن خلدون تيارت–الجز ائر-

kawtharlakhdar93@gmail.com

ملخص:

نظرا لما تحظى به الحياة الخاصة للفرد لاسيما منها المعطيات الشخصية من قدسية وأهمية بالغة، فقد تدخل المشرع الجزائر بموجب أحكام التعديل الدستوري لسنة 2020، وقام بإصدار القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي سنة 2018 ، الذي أسهم في سد جانب من الفراغ الذي كان مسجلا في هذا المجال كافلا من خلاله إلى اعتماد اطار قانوني وتنظيمي ملائم لحماية المعطيات الشخصية، ومن خلال هذه الدراسة حاولنا إبراز آليات فعالة تضمن مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام هذا القانون، ضمانا لعدم المساس بحرمة الحياة الخاصة للأفراد، والوقوف على معرفة إلى أي مدى وفق المشرع الجزائري في تكريس الحماية القانونية للمعطيات الشخصية بموجب القانون 18-07؟

الكلمات المفتاحية: الحماية القانونية، المعطيات ذات الطابع الشخصي، القانون 18-07، المعالجة، الشخص المعني.

Abstract :

Given the sanctity and importance of the private life of the individual, especially personal data, the Algerian legislator intervened in accordance with the provisions of the constitutional amendment of 2020 and issued Law 18-07 relating to the protection of Natural persons in the field of

processing personal data in 2018, which contributed to bloc King Part of the void that was registered in this field ensured the adoption of an appropriate légal and regulatory framework for the protection of personal data. Through this study, we tried to highlights effective mechanisms that ensure compliance with the processing of personal data with the provisions of this law, in order to ensure that the sanctity of the private life of individuals is not compromised, and to know to what extent According to the Algerian legislator in devoting the légal protection of personal data under Law 18-07 ?

Keywords: Legal Protection, Personal Data, Law 18-07, Processing, Person Concerned.

مقدمة:

أسهم التطور التكنولوجي لا سيما في مجال المعلوماتية والاتصالات بشكل كبير في تسهيل الاعتداء على المعطيات الشخصية بوسائل متطورة اعتمادا على المعالجة الآلية، ولئن كان في زمن غير بعيد الاعتماد على سن تشريعات لحماية الحياة الخاصة الت يتم تكريسها بموجب مختلف المواثيق الدولية على غرار الاعلان العالمي لحقوق الإنسان الذي نص في مادته رقم 12 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 مثل ذلك التدخل أو تلك الحملات، وكذا العهد الدولي للحقوق المدنية والسياسية، المصادق على بنوده من قبل الجمعية العامة للأمم المتحدة سنة 1966، فإن التحولات المتسارعة في مجال معالجة البيانات فرضت ضرورة تكريس تشريعات متخصصة في حماية المعطيات الشخصية لا سيما المعالجة آليا[1].

كما كرس الدستور الجزائري إلى جانب حماية الحق في الخصوصية التأكيد على حماية المعطيات الشخصية بداية تزامنا مع التعديل الدستوري لسنة 2016، والمعاد تأكيده بموجب تعديل سنة 2020، بموجب أحكام المادة 47 منه، والتي نصت في فقرتها الرابعة على أن "حماية الأشخاص الطبيعيين عند معالجة المعطيات ذات الطابع الشخصي حق أساسي"

ولقد عرف المشرع الجزائري المعطيات ذات الطابع الشخصي في المادة الثالثة الفقرة الأولى للقانون رقم 07/18 كما يلي: "كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه المشار أدناه "الشخص المعني[2]" بصفة مباشرة أو غير مباشرة، لا سيما بالرجوع لرقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية."

والملاحظ أن هذا التعريف يتطابق إلى حد كبير مع التعريف الذي جاء به التوجيه الأوروبي والهيئات الدولية ومختلف التشريعات الأوربية التي سارت على نهجه[3].

ويرى البعض أن المعطيات الشخصية أنواع متعددة، منها ما يتعلق بحرمة الحياة الخاصة للانسان هذا من جهة، ومن جهة أخرى هناك بيانات متعلقة بهويته وجنسيته، وكذا الاتجاه الفكري والسياسي والاعتقاد الديني للفرد، بالإضافة إلى البيانات المتعلقة بالتعاملات المالية والمصرفية للفرد[4].

ولا يختلف الإثنان أو الآلية التشريعية بتنظيمها قانون خاص لحماية المعطيات الشخصية إنما هو للمحافظة على الحريات والحياة الخاصة للأفراد، هذه المعطيات اصبحت تتداول في العالم الافتراضي والمهددة بالمخاطر التي تهدد حياة الاشخاص خاصة، لذلك فإن معنى المعطيات بدون اقترانها بمعنى الخصوصية لا تخضع للحماية، فالخصوصية هي سبب تقرير الحماية للمعطيات[5].

وبالرغم أن هذا المسعى الذي كرسته الجزائر جاء متأخرا إلا أن هذا القانون كرس الإطار الذي يحدد نظام معالجة المعلومات ذات الطابع الشخصي والتصدي للآثار المترتبة عن التطور السريع لتكنولوجيات الاعلام على الحياة الخاصة وحريات الاشخاص عبر تحديد المبادئ الواجب احترامها أثناء جمع ومعالجة وحفظ البيانات الشخصية وقواعد استعمال هذه البيانات وكذلك حقوق الاشخاص الذين تم جمع معلوماتهم، ومن خلا ما تقدم ذكره نطرح الإشكالية التالية:

إلى أي مدى وفق المشرع الجزائري في تكريس الحماية القانونية للمعطيات الشخصية بموجب القانون 18-07؟

وقد اعتمدنا في معالجة هذا الموضوع على المنهج الوصفي التحليلي من خلال استقراء مضامين القانون رقم 18-07، وللإجابة عن الإشكالية نقترح الخطة التالية:

أولا: الأحكام المتعلقة بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

ثانيا: حقوق الشخص المعني بالمعطيات ذات الطابع الشخصي والتزامات المسؤول عن معالجتها.

ثالثا: الآثار المترتبة عن مخالفة الأحكام المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.

أولا/ الأحكام المتعلقة بالسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

نص القانون 18-07 في المادة 22 على إنشاء سلطة وطنية إدارية مستقلة لحماية المعطيات ذات الطابع الشخصي لدى رئيس الجمهورية تتمتع بالشخصية المعنوية والاستقلال المالي والإداري، تقيد ميزانيتها في ميزانية الدولة، تعد نظامها الداخلي وتصادق عليه، محدد مقرها في الجزائر العاصمة مبينا تشكيلتها واختصاصاتها، ومن هذا المنطلق سيتم التطرق وتبيان تشكيلة اللجنة الوطنية لحماية المعطيات ذات الطابع الشخصي ثم تبيان اختصاصها.

1- تشكيلة السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

حددت المادة 2" تشكية اللجنة الوطنية بثلاثة أعضاء من بينهم الرئيس يعينهم رئيس الجمهورية وثلاثة قضاة يقترحهم المجلس الأعلى للقضاة، بالإضافة لممثل عن كل غرفة بالبرلمان يعينه رئيس كل غرفة بالتشاور مع رؤساء المجموعات البرلمانية، زيادة عن ممثل عن كل قطاع من القطاعات المبينة في نفس المادة، وذلك بالاعتماد على اختصاصهم التقني و/ أو القانوني في مجال معالجة المعطيات ذات الطابع الشخصي مع إمكانية الاستعانة بأي شخص مؤهل من شأنه مساعدة السلطة في أشغالها.

وقد حددت نفس المادة عهدة الأعضاء بخمس سنوات ويتم تعيينهم بمرسوم لرئيس الجمهورية والذي يؤدون اليمين أمام مجلس قضاء الجزائر وفق الكيفيات المبينة في المادة 24 من نفس القانون.[6]

2- مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

حددت المادة 25 من القانون رقم 07/18 [7] مهام السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي على النحو التالي:

- منح تراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.
- إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.
- تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة.
- تلقي الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.
- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط القانونية المحددة في هذا الإطار.
- الأمر بتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي.
- الأمر بإغلاق معطيات أو سحبها أو إتلافها.
- تقديم أي اقتراح من شأنه تبسيط وتحسين الاطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.
- نشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني لحماية المعطيات ذات الطابع الشخصي.
- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل.
- إصدار عقوبات إدارية تتراوح بين الإندار، الإعذار، السحب المؤقت أو النهائي لوصل التصريح أو الترخيص أو الغرامة في حالة إخلال المسؤول عن المعالجة بالإجراءات المحددة قانونا.
- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.
- وضع قواعد والسلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

من خلال استقراء مختلف الصلاحيات المخولة لهذه السلطة يتجلى مدى دورها التقني الضبطي الذي يتطلب التخصص في مجال معالجة المعطيات فعليا خصوصا بعد النص عليه صراحة ضمن تشكيلة هذه السلطة، بحيث تعد آلية محورية فعالة لحماية حقوق الانسان في مجال معالجة المعطيات وسلامة مختلف الأنظمة المعلوماتية للقضاء على آثارها السلبية.

هذا كما خول المشرع هذه السلطة صلاحية القيام بجملة من الإجراءات كالقيام بالتحريات ومعاينة المحلات والأماكن التي تتم فيها معالجة المعطيات، وفي إطار ممارستها لمهامها تعلم النائب العام المختص فور المعاينة وقائع تحتمل الوصف الجزائي.

ثانيا/ حقوق الشخص المعني بالمعطيات ذات الطابع الشخصي والتزامات المسؤول عن معالجتها:

أورد المشرع الجزائري في الباب الرابع والخامس من القانون 18-07 مجموعة من الأحكام القانونية التي تبين حقوق الشخص المعني بالمعطيات ذات الطابع الشخصي والتزامات المسؤول عن معالجتها وهو ما سنحاول تبيانه :

1- **حقوق الشخص المعني بالمعطيات ذات الطابع الشخصي:**

باستقراء أحكام المواد من 32 إلى 37 من القانون رقم 18-07 السابق ذكره نجد أن المشرع الجزائري أورد خمس حقوق أساسية للشخص المعني بالمعالجة والتي سنبينها على النحو التالي:

- الحق في الإعلام: نصت عليه المادة 32 من نفس القانون، ويقصد به ضرورة اطلاع الشخص المعني بهوية المسؤول عن المعالجة وأغراضها وكل معلومة إضافية مفيدة في تلك العملية، باستثناء الحالات المذكورة في المادة 33 من نفس القانون.
- الحق في الولوج: نصت عليه المادة 34 ويعني حصوص الشخص المعني على أن معطياته كانت محل معالجة أم لا، وأغراضها وفئات المعطيات التي ينصب عليها والمرسل إليهم، إضافة لإفادته بكل معلومة حول مصدر المعطيات.

- الحق في التصحيح: نصت عليه المادة 35 ويقصد به حصول الشخص المعني مجانا من المسؤول على تصحيح وتحيين أو إغلاق ومسح المعطيات الشخصية التي تكون معالجتها غير مطابقة للقانون وذلك في أجل 10 أيام من الاخطار.
- الحق في الاعتراض: نصت عليه المادة 36 وهو اعتراض الشخص المعني لدى المسؤول عن معالجة معطياته ذات الطابع الشخصي خاصة إذا كانت مخصصة لغرض دعائي أو تجاري إذا لم ينص القانون خلاف ذلك.
- منع الاستكشاف المباشر: نثت عليه المادة 37 بمعنى منع الاستكشاف المباشر بواسطة آلية الاتصال أو جهاز الاستنساخ البعدي أو البريد الإلكتروني دون موافقة الشخص المعني[8].

2- التزامات المسؤول عن معالجة المعطيات ذات الطابع الشخصي:

نصت المواد من 38 إلى 45 من القانون 07/18 على التزامات الشخص المسؤول عن المعالجة والتي سنوضحها على النحو التالي:

- سرية وسلامة المعالجة: حيث يتعين وضع التدابير التقنية والتنظيمية الملائمة لحماية المعلومات ذات الطابع الشخصي من الإتلاف العرضي أو الغير مشروع أو الضياع العرض أو التلف أو النشر أو الولوج لغير المرخصين خصوصا عندما تستوجب المعالجة إرسال المعطيات في شبكة من الشبكات.
- معالجة المعطيات المتعلقة بالتوقيع والتصديق الالكترونيين: نصت المادة 42 أنه فيما عدا حالات الموافقة الصريحة تجمع المعطيات ذات الطابع الشخصي من قبل مؤدي خدمات التصديق الالكتروني من الاشخاص المعنيين بها مباشرة.
- معالجة المعطيات الشخصية في مجال الاتصالات الالكترونية: نصت المادة 43 أنه في حال ما أدت المعالجة في شبكات الاتصال الالكترونية إلى إتلافها أو أي مساس بها يعلم مقد الخدمات فورا السلطة الوطنية والشخص المعني إذا ادى ذلك للمساس بحياته الخاصة.
- نقل المعطيات نحو دولة أجنبية: لا يجوز لأي مسؤول نقل معطيات ذات طابع شخصي لدولة أجنبية إلا بترخيص من السلطة الوطنية وذلك حسب المادة 44، باستثناء الحالات المذكورة في المادة 45.

ثالثا/ الآثار المترتبة عن مخالفة الأحكام المتعلقة بمعالجة المعطيات ذات الطابع الشخصي:

جاء الباب الخامس القانون 07/18 السالف الذكر تبيان الأحكام الإدارية والجزائية المطبقة في حالة مخالفة الأحكام المتعلقة بمعالجة المعطيات ذات الطباع الشخصي وذلك في المواد من 46 إلى 74 لذا سيتعين تبيان الإجراءات الإدارية والقواعد الإجرائية.

1- الإجراءات الإدارية :

نص المشرع في المواد من 46 إلى 49 من القانون رقم 18-07على مجموعة من الإجراءات الإدارية التي تتخذها السلطة الوطنية في حالة التعدي على المبادئ الأساسية لمعالجة المعطيات ذات لطابع الشخصي من خلال النص في المادة 46 على عقوبة الإنذار والاعذار والسحب المؤقت لمدة لا تتجاوز سنة أو النهائي للرخصة أو التصريح، وتكون قرارات السلطة الوطنية أمام مجلس الدولة وذلك وفقا لأحكام القانون 98-01 المؤرخ في 30 ماي 1998[9] والمتعلق باختصاصات مجلس الدولة وتنظيمه وعمله المعدل والمتمم، وكذا المواد 901 من قانون الإجراءات المدنية والإدارية[10].

كما أضافت المادة 47 أن السلطة الوطنية تصدر غرامات قدرها 500 ألف دينار جزائري ضد كل مسؤول عن معالجة يرتكب أنحد المخالفات المنصوص عليها من نفس المادة.

2- القواعد الإجرائية:

نصت عليها المواد من 49 إلى 53 من القانون 18-07 السابق ذكره حيث خولت للسلطة الوطنية التحري ومعاينة المحلات والأماكن التي تتم فيها المعالجة باستثناء محلات السكن، وذلك بالولوج لمعطيات المعالجة وجميع المعلومات والوثائق اي كانت دعامتها ولا يعتد أمامها بالسر المهني.

كما نصت المادة 50 على أنه بالإضافة لأعوان وضباط الشرطة القضائية يؤهل كذلك أعوان الرقابة الذي تلجأ لهم السلطة الوطنية للقيام بالبحث ومعاينة الجرائم وتحرر محاضر ترسل مباشرة لوكيل الجمهورية.

كما نصت المادة 53 على اختصاصات الجهات القضائية الجزائرية بمتابعة الجرائم المنصوص عليها في هذا القانون التي ترتكب خارج إقليم الجمهورية ، إذا كان مرتكبها جزائري أو شخص أجنبي مقيم في الجزائر أو شخص معنوي خاضع للتشريع الجزائري.

خاتمة:

من خلال التعمق في مضامين القانون رقم 07/18 موضوع هذه الدراسة يبرز الاهتمام الخاص الذي كرسه المشرع في مجال حماية المعطيات الشخصية، الذي جاء من أجل ملئ فراغ حقيقي كان موجودا في زمن طغت تكنولوجيا المعلوماتية على كل نواحي الحياة متأخرا على الأقل بعقد من الزمن على نظيريه المشرعين المغربي والتونسي.

كما أن ضرورة التماشي والتكيف مع التطور التكنولوجي في مختلف المجالات لا سيما في جانب المعلوماتية، يقتضي خلق بيئة تشريعية متطورة تؤطر بصفة دقيقة معالجة مختلف المعطيات الشخصية داخليا وخارجيا نظرا لما تتسم به من حساسية خصوصا عند نقل أو تحويل هذه المعطيات إلى ما وراء الحدود، والتي قد تسهم بطريقة أو بأخرى في المساس بالأمن القومي، الأمر الذي يقتضي توفير مختلف الضمانات لخلق بيئة آمنة تضمن فيها حقوق الأشخاص.

ولكن بالرغم من الآليات والضمانات التي أتى بها المشرع ضمن القانون رقم 07/18 ، إلا أنها تحتاج إلى التفعيل من جهة وإزالة اللبس من جهة على بعض الإجراءات المتداخلة لا سيما وأن هذا الإطار التشريعي مستجد ومرهون بمستوى التطور التكنولوجي المعلوماتي، وعليه يمكن تقديم بعض التوصيات لضمان تفعيل مختلف آليات الحماية التي كرسها المشرع ضمن هذا القانون كما يلي:

- ضرورة تكييف وتحيين هذا القانون مع المستجدات لا سيما التكنولوجية والعلمية التي تعرف تطورا يوما بعد يوم .
- إضفاء حماية ثنائية إدارية وجزائية لردع مرتكبي المخالفات والجرائم من مسؤولي المعالجة.

- ضرورة منح الاستقلالية التامة للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي بما يتلائم والمهام العديدة الموكلة إليها بغية تمكينها من آدائها على أكمل وجه.
- ضرورة وضع حملات تحسيسية للأشخاص لتعريفهم بحقوقهم الوطنية المدرجة ضمن القانون 18-07.
- إنشاء سجل وطني إلكتروني يتضمن مختلف الطرق والآليات لاستقبال الشكاوى وكيفيات الحماية للمعطيات الشخصية عن بعد لضمان الفعالية والنجاعة.
- إنشاء جهاز أمني متخصص في متابعة ومكافحة الجرائم المرتبطة بالمعلوماتية ومختلف الأجهزة الحديثة.
- نشر الوعي الرقمي بين المستخدمين، وكيفية تفادي التعدي على معطياتهم الشخصية(عدم الاحتفاظ ببيانات شخصية أو مالية على الأجهزة، وعدم نشر معلومات شخصية، وعدم إعطاء كلمة السر...الخ).
- يجب على السلطات العمومية القيام بالتوعية والتحسيس وإشراك جميع الفاعلين الاجتماعيين والاعلاميين والحقوقيين وكل المجتمع المدني وتجنيدهم لحماية الحريات العامة والحياة الخاصة للأفراد وأسرهم ومعطياتهم الشخصية.
- ضرورة تكوين القضاة في هذا المجال الحساس والمتزايد، مع الإسراع بتزويد السلطة الوطنية بكل الليات الضرورية لا سيما القانونية منها، من أجل القيام بأعمالها على الوجه المطلوب.
- في ظل التطورات التي تشهدها تكنولوجيات الاعلام والاتصال وخطورتها على الحياة لخصوصية للأفراد يتعين إدراج مقياس خاص بحماية المعطيات ذات الطابع الشخصي ضمن المقاييس المدرسة بكلية الحقوق .

الهوامش:

[1] كحلاوي عبد الهادي، بن زيطة عبد الهادي، آليات حماية المعطيات ذات الطابع الشخصي في ظل القانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون والعلوم السياسية، المركز الجامعي بالنعامة، المجلد 7، العدد 02، 2021، ص 116.

[2] يقصد بالشخص المعني: "كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع المعالجة." أنظر المادة 3 من القانون رقم 18-07، المؤرخ في 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر.ع 11، المؤرخة في 10يونيو 2018.

[3] جبور منى أشقر ، محمود جبور، البيانات الشخصية والقوانين العربية الأمني وحقوق الأفراد، الطبعة الأولى، المركز العربي للبحوث القانونية والقضائية، بيروت، 2018، ص 90.

[4] مدحت عبد الحليم محمود، الحماية الجنائية للتجارة الإلكترونية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2001، ص77.

[5] زين العابدين صالح مروة ، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، الطبعة الاولى، مركز الدراسات العربية مصر، 2016، ص 21.

[6] خضري حمزة ، عشاش حمزة ، الحماية القانونية للمعطيات ذات الطابع الشخصي للأشخاص الطبيعيين في التشريع الجزائري، مجلة دائرة البحوث والدراسات القانونية والسياسية، المركز الجامعي تيبازة، المجلد 5، العدد 1، 2022، ص 93.

[7] القانون رقم 18- 07، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، السالف الذكر.

[8] القانون رقم 18-07، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، السالف الذكر.

[9] القانون العضوي رقم 98-01، المؤرخ في 30 مايو 1998، والمتعلق باختصاصات مجلس الدولة وتنظيمه عمله المعدل والمتمم.

[10] القانون رقم 08-09، المؤرخ في 25 فبراير 2008، والمتضمن قانون الاجراءات المدنية والادارية.

حماية الحياة الخاصة في القانون رقم 18-07 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

Protection of private life in law n° 7/18 on the protection of natural persons in the field of processing of personal data

عمروش فوزية، أستاذة محاضرة "أ"، جامعة الجزائر (1) بن يوسف بن خدة
fouzia.amrouche7@gmail.com

ملخص

تعدّ الخصوصية أو حرمة الحياة الخاصة أحد حقوق الإنسان التي تأثرت كثيرا بالتطور الرقمي أو التكنولوجي الذي غزا مختلف جوانب حياة الإنسان، بعد أن أصبحت الحواسيب أو الانترنت مستودعا تحفظ فيه الكثير بل وأهم المعلومات والبيانات الشخصية، وتشكل بنوكا للمعلومات قابلة للتداول ما يشكل خطرا ومساسا على ما كان يعتبر في وقت ما مقدسا وممنوعا الوصول إليه. بعد صدور القانون رقم 18-07 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي. والذي وضع في إطار معالجة المعطيات الخاصة جملة من القواعد والإجراءات التي تكرس كرامة الشخص وحماية حياته الخاصة، الأمر الذي يجعلنا نتساءل حول مدى كفاية الحماية المقررة للحق في الخصوصية أو الحياة الخاصة في ظل معالجة المعطيات الشخصية المنصوص عليها في قانون 18-07.

Abstract

The right to privacy or privacy is part of human rights, which has been strongly affected by the digital or technological development that has pervaded various aspects of human life. After computers or the Internet became a repository in which most personal information and data are stored and these private data became marketable information banks which present a danger and harm to what was once considered sacred and inaccessible. Following the promulgation of Act No. 18-07 on the protection of individuals with regard to the processing of personal data. In the context of the processing of private data, we have defined a number of rules and procedures that enshrine the dignity of the person and the protection of his privacy. This leads us to question whether the right to privacy or privacy is sufficiently protected by the personal data provided for by Law No. 18-07.

مقدمة

عرفت السنوات الأخيرة اهتماما كبيرا بالحياة الخاصة خصوصا في ظل التطور الرقمي والتكنولوجي وذلك نظرا لتأثيرها على كيان الفرد والمجتمع على حد السواء. حيث عرفت اهتماما تشريعا لافتا للنظر لدى مختلف الدول والمنظمات الدولية والاقليمية[1]، خاصة بعد أن احتلت الحواسيب ومختلف الوسائط الرقمية كالهواتف الذكية المتصلة بالأنترنت حياتنا بكل تفاصيلها وخصوصيتها، وتحولت إلى أكبر وسائل التواصل وتبادل المعلومات من خلال البريد الإلكتروني ومواقع الدردشة والشبكات الاجتماعية وغيرها.

يعد الحق في الخصوصية أو حرمة الحياة الخاصة واحدة من حقوق الإنسان[2]، التي تأثرت كثيرا بالتطور الرقمي أو التكنولوجي الذي غزا مختلف جوانب حياة الإنسان، ما أدى إلى جعل الحواسيب أو الانترنت مستودعا تحفظ فيه الكثير بل وأهم المعلومات والبيانات الشخصية، وتشكل بنوكا للمعلومات قابلة للتداول ما يشكل خطرا ومساسا على ما كان يعتبر في وقت ما مقدسا وممنوعا الوصول إليه، كون هذا الحق يعد من الحقوق الملازمة للشخص الطبيعي كأصل عام[3]، فهو أساس لبناء مجتمع سليم[4]. وبالرغم من كون الحق في الخصوصية أو حرمة الحياة الخاصة من الحقوق ذات المفاهيم النسبية التي تختلف من مجتمعات لأخرى، ومن ثقافات لأخرى، إلا أن التطور السابق ذكره أعطى لهذا الحق بعدا خاصاً، خاصة بانتشار ظاهرة التواصل الاجتماعي التي تم فيها فتح الحياة الخاصة على مصراعيها من خلال نشر المعلومات الشخصية والصور ومقاطع الفيديو مما يشكل خطرا كبيرا على حرمة حياة الناس الخاصة ويجعلها عرضة للانتهاك بسهولة.

ارتبط حق الخصوصية دائما بفكرة السرية فلم يكن يتصور أن يقوم الفرد بالكشف عن تفاصيل حياته للعامة من خلال نشر صور شخصية له ولعائلته أو الكشف مراسلاته الشخصية، فبعد أن كان هذا الحق مرتبطا بالجانب المادي أو العائلي[5] ، وتمحور حول حماية الجوانب غير العلنية من حياته، كالعِرض وحرمة المسكن وسرية الاتصالات الخاصة، والحفاظ على أسرار العائلة، إلا أن التطور العلمي والتكنلوجي أتاح الفرصة لجعل الحياة الخاصة للأفراد متاحة ومتداولة بسهولة خاصة في ظل تطور التعاملات الالكترونية، أين أصبحت معالجة البيانات الشخصية من متطلبات هذه التعاملات[6]، وفي ظل تطور وسائل تخزين ومعالجة هذه المعطيات[7] والاتصال والارسال الإلكتروني للملفات، وكذا برمجيات معالجة البيانات الكبرى، وإن كان لهذا التطور دورا كبير في تسهيل الحياة على المعنيين من إدارات وأشخاص[8] إلا أنها زادت من إمكانية انتهاك هذا الحق والمساس به وتعريض الأشخاص

للخطر، لذا توسع مفهوم الخصوصية وأصبح يرتبط أيضا بالبيانات أو المعطيات الشخصية المخزنة[9] وهذا ما يقتضي توفير حماية قانونية تتماشى مع هذه الخصوصية بمفهومها الجديد المرتبط ارتباطا وثيقا باستعمال التقنية، التي أدت إلى الاحتفاظ او تخزين البيانات الخاصة بالأفراد في بنوك المعلومات الحديثة، ومن ثم يمكن لأي شخص الولوج إليها والحصول على ما يريد منها، فظهر ما يمكن الاصطلاح عليه الحق في الخصوصية المعلوماتية التي تقوم على حق الفرد في أن لا تكون معلوماته الخاصة محلا للتداول أو الإعلام وحقه في منع الغير من استخدام المعلومات التي تتعلق بحياته الخاصة.

كرس المشرع حماية للحق في الحياة الخاصة في إطار معالجة البيانات ذات الطابع الشخصي في ظل التعديل الدستوري لسنة 2016 خاصة المادة 46 منه[10] إذ نصت"*لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه ويحميهما القانون، ...حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه*"[11]، ثم صدر بعده القانون رقم 18-07 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.[12]، والذي وضع في إطار معالجة المعطيات الخاصة جملة من القواعد والإجراءات التي تكرس كرامة الشخص وحماية حياته الخاصة، الأمر الذي يجعلنا نتساءل حول مدى كفاية الحماية المقررة في ظل معالجة المعطيات الشخصية المنصوص عليها في قانون 18-07 للحق في الخصوصية ؟

أصبح معالجة البيانات الشخصية وتخزينها من متطلبات العصر الرقمي، لهذا ستناول شروط معالجة المعطيات الشخصية (**أولا**)، إضافة إلى أنواع الحماية المقرر لحماية للحياة الخاصة في قانون 18-07 (**ثانيا**).

أولا: شروط معالجة المعطيات الشخصية

بمأن معالجة المعطيات الشخصية أصبحت في الوقت الراهن بفعل التطور من ضروريات الحياة، فقد حدّد قانون 18-07 للقيام بهذه العملية جملة من الشروط تستنج من أحكامه، حيث حدّد المقصود بالشخص المعني بمعالجة المعطيات (**1**)، والحقوق التي يتمتع بها (**2**) إضافة إلى تبيان المبادئ الأساسية لمعالجة المعطيات ذات الطابع الشخصي (**3**).

1- تحديد المقصود بالشخص المعني بالمعالجة

عرفت المادة 3 من قانون 18-07 الشخص المعني أنه " كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة"، فيفهم من هذا النص أن المشرع قصر الحماية على المعطيات أو البيانات التي تخص الشخص الطبيعي دون سواه ما،

يعني أن الأشخاص غير الطبيعية غير معنية بالحماية المقررة في هذا القانون[13]، ويعود سبب ذلك أي قصر الحماية على الشخص الطبيعي وحده كون الحق في الخصوصية من الحقوق اللصيقة بالشخص الطبيعي إذ أن حماية حقوق الإنسان كانت وراء الدافع لظهور هذا الحق[14]، وهناك من يرى أن الشخص الطبيعي هذا يتمتع بالحماية بعض النظر عما إذا كان مواطنا أو مجرد مقيم، ذلك أن قانون العقوبات يطبق على جميع الجرائم التي ترتكب على أرض الجمهورية[15].

لكن الملاحظ أن القانون المذكور لم يضع شروطا مميزة تتعلق بهذا الشخص الطبيعي، إلّا أنه ميّز بين الراشد وعديم الأهلية والقاصر فيما يتعلق بكيفية معالجة البيانات الخاصة بها، وما يخص الحصول على الرضا أو الموافقة لذلك. ذلك أن القاصر وعديم الأهلية يشترط لمعالجة البيانات الخاصة بهما إلى الحصول على الموافقة من ممثلهما الشرعي أو الحصول على ترخيص القاضي عند الاقتضاء حسب ما يتضح من نص المادة 8[16].

2-الحقوق المخولة للشخص المعني بالمعالجة

يتمتّع الشخص المعني في إطار معالجة المعطيات ذات الطابع الشخصي بمجموعة من الحقوق تضمن له احترام كرامته وحياته الخاصة وحرياته العامة وشرفه وسمعته حسب ما تؤكده المادة 2 من نفس القانون[17]، وتتمثل هذه الحقوق في كل من حق في الإعلام (أ)، والحق في الولوج(ب)، والحق في التصحيح(ج)، والحق في الاعتراض(د)، والحق في منع الاستكشاف المباشر(ه).

أ- الحق في الإعلام

نصت المادة32 من القانون رقم 18-07 على الحق في الإعلام وجاء فيها "ما لم يكن على علم مسبق بها، يجب على المسؤول عن المعالجة أو من يمثله إعلام مسبقا وبصفة صريحة ودون لبس، كل شخص يتم الاتصال به قصد تجميع معطياته ذات الطابع الشخصي، ..... " كهوية المسؤول عن المعالجة وعند الاقتضاء هوية ممثله، وكذلك الإعلام بكل معلومة هامة ومفيدة، كإمكانية نقل المعلومات أو حقوق المرسل إليه، وكذلك إعلام الشخص المعني، وكذا حق معرفة المعلومات الخاصة المتعلقة بهوية المسؤول عن المعالجة وكذا أغراض المعالجة، وكافة المعلومات المتعلقة بالمرسل إليه، وكذا إعلامه بإمكانية نقل هذه المعطيات لبلد أجنبي وبإمكانية تداولها في شبكات مفتوحة وأنها قد تكون عرضة للقراءة والاستعمال غير المرخص به من طرف الغير دون ضمانات السلامة، وكل ذلك حتى لا يكون ضحية لانتهاك حقه في الخصوصية دون دراية منه.

تجدر الإشارة أن المشرع لم يحدد الوسائل التي يتم بها الإعلام ولا المدة التي يتم الإعلام فيها، إلا أنه يبدو من النص المذكور أن الإعلام يشترط فيه أن يتم بطريقة دقيقة وواضحة، وسهلة الاستيعاب ودون أي لبس. إلا أنّ المادة 33 استثنت من الحق في الإعلام حالة تعذر إعلام الشخص المعني، خاصة إن تعلق الأمر بمعالجة معطيات ذات طابع شخصي لأغراض إحصائية أو تاريخية أو علمية، أو كانت المعالجة تطبيقا لنص قانوني، أو تمت لأغراض صحفية أو فنية أو أدبية.

ب الحق في الولوج

تناولت هذا الحق نص المادة 34 من قانون 18-07 ويتضح منها أن المقصود بهذا الحق، هو حق الشخص المعني بالمعالجة في النفاذ أو الوصول إلى بيانته الخاصة المخزنة آليا والاطلاع عليها، ومعرفة كل ما يتعلق من بيانات تخصه ومصادرها وطرق معالجتها، وكذا مضمونها بعد المعالجة، فهو لا يقتصر على مجرد تأكده من أنّ بياناته أو معطياته الخاصة محل معالجة، بل حقه أيضا في معرفة غايات المعالجة، ونوعية المعطيات أو البيانات التي تتم معالجتها وفئات المرسل إليهم.

يعتبر الحق في الولوج إذن ضمانة وقائية لحماية حق الخصوصية[18]، فهو يعطي للشخص المعني إمكانية مراقبة الأسس المعلوماتية والمنطقية لطريقة اتخاذ القرار في مواجهته، أي ما إن كانت المعالجة ستأثر عليه أم لا[19]، وقد منحت المادة 34 السابق ذكرها للمسؤول عن المعالجة في حالة عدم تمكنه من إعطاء التوضيحات للمعني عن المعلومات السابق ذكرها، أن يقدم طلبا للسلطة الوطنية من أجل تحديد أجل كافي للإجابة، بالإضافة إلى حق ممارسة حق الاعتراض إذا كان طلب الولوج تعسفيا خاصة في الأحوال التي يقدم فيها الشخص المعني أكثر من طلب أو طلبات متكررة.

ج- الحق في التصحيح

يحق للشخص المعني طبقا للمادة 35 من قانون 18-07، وذلك بعد اطلاعه على بياناته أن يطلب من المسؤول عن المعالجة إما تصحيح بعض هذه البيانات إذا اكتشف فيها أخطاء معينة، أو تحيينها إذا أصبحت قديمة أو حدث فيها تغيير، أو كانت تحتاج إلى إضافات معينة لتصبح موافقة للحقيقة، بل ويحق له أيضا أن يطلب مسحها أو حذفها أو إلغائها من المعالجة، أو طلب إغلاقها بجعل الوصول إليها غير ممكن، خاصة إذا لاحظ عدم قانونية المعالجة نظرا لحساسية المعطيات مثلا. ويلزم المسؤول عن المعالجة بالقيام بالتصحيحات

اللازمة مجانا لفائدة الطالب في أجل عشرة (10) أيام من إخطاره. كما أجاز المشرع استعمال حق التصحيح من قبل ورثة الشخص المعني، حسب الفقرة الأخيرة من المادة 35.

يعدّ حق التصحيح هو الآخر ضمانة أساسية لرقابة المعطيات الشخصية المعالجة التي تمت بطريقة غير مطابقة للقانون، وبالتالي حماية حق الخصوصية للمعني من خلال منع المعلومات الخاطئة أو الناقصة تجنبا لأي تأثير سلبي على سمعته أو مركزه لدى الغير الذي يتعامل معهم[20].

د- الحق في الاعتراض

يحق للشخص المعني حسب نص المادة 36 الفقرة الأولى والثانية من قانون 18-07 أن يعترض لأسباب مشروعة على معالجة معطياته ذات الطابع الشخصي أو على استعمالها لأغراض دعائية، ولا سيما التجارية منها من طرف المسؤول الحالي عن المعالجة أو المسؤول عن المعالجة اللاحقة دون موافقته. وحسب الفقرة الثالثة من نفس المادة لا يمكن للمعني أن يمارس حق الاعتراض في حالة ما إذا كانت المعالجة تستجيب لالتزام قانوني، أو إذا تم استبعاد هذا الحق بموجب إجراء صريح في المحرّر الذي يرخص بالمعالجة.

يعدّ حق اعتراض الشخص المعني على معالجة معطياته الشخصية بمثابة سلطة تخوله منع استعمال هذه المعطيات من قبل المسؤول عن المعالجة أو من قبل الغير[21]، فيمكنه الاحتفاظ بها لنفسه ويحدد ما يسمح للغير بالاطلاع عليه منها، كما يخوله رفض إعطاء أي معلومات جبرا عنه، على أن يكون ذلك مبررا بأسباب مشروعة، وأن لا يكون المعني قد تنازل عن هذا الحق مسبقا، وأن لا تكون المعالجة تستجيب لالتزام قانوني.

هـ- الحق في منع الاستكشاف المباشر

يعد الاستكشاف المباشر مشكلة حقيقة في حماية المعطيات الشخصية في المعاملات الالكترونية خاصة التجارة الالكترونية، لذا اتجهت أغلب التشريعات إلى تقرير عدم جواز إجراء أي اتصال أو أرسال بغرض هذا الاستكشاف دون رضا المشترك بخدمة الإنترنت أو البريد الإلكتروني[22]، فهو عملية إشهارية دعائية محضة يتم اللجوء إليها من خلال استغلال قواعد بيانات متوافرة في الغالب لدى متعاملي الاتصالات تتعلق بزبائنهم، وتشمل عناوينهم وأرقام هواتفهم والعنوان الالكتروني والبريد الالكتروني، قصد توجيه رسائل للمعنين ذات مضمون دعائي لتعرض عليهم سلعا أو خدمات معينة حسب كل فئة.

يهدف الاستكشاف إلى إنشاء روابط بين الشركة وعملائها، فيتم اخبارهم على الفور بالعروض التجارية المختلفة التي تقدمها علاماتها التجارية، وقد عرّفه المشرع في نص المادة 2

من قانون 18-07 على أنه" إرسال أي رسالة، مهما كانت دعامتها وطبيعتها، موجهة للترويج المباشر أو غير المباشر لسلع أو خدمات أو لسمعة شخص يبيع سلعا أو يقدم خدمات". يتم الاستكشاف باستعمال ألية اتصال أو جهاز الاستنساخ البعدي، أو بواسطة أي وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة. إلا أن الشخص المعني قد يجد نفسه ضحية إعلانات أو رسائل إشهارية غير مرغوب فيها وتترك أثرا سلبيا على نفسيته، لذا منع القانون الاستكشاف المباشر من خلال نص المادة 37 من قانون 18-07 واعتبره عملية غير مشروعة إذا تمت دون الحصول على الموافقة المسبقة للشخص المعني[23].

إضافة إلى كل هذه الحقوق التي اقرها المشرع للشخص المعني لتدعيم حقه في الخصوصية عند معالجة معطياته أو بياناته الشخص فإنّ المشرع فرض اثناء معالجة هذه المعطيات جملة من الشروط تعزيزا لذات الحماية.

3- المبادئ الأساسية لحماية المعطيات الشخصية

تناول المشرع في الباب الثاني من قانون 18-07 المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي، وهي جملة الضوابط التي يجب احترامها عند معالجة المعطيات، تتمثل في ضرورة أن تكون المعالجة مشروعة (أ)، والحصول على الموافقة المسبقة للشخص المعني (ب)، وأيضا ضرورة احترام الإجراءات المسبقة (ج).

أ- مشروعية المعالجة

جاء في نص المادة 9 من قانون 18-07 "يجب أن تكون المعطيات الشخصية: أ – معالجة بطريقة مشروعة ونزيهة، ب – مجمعة لغايات محددة، وواضحة ومشروعة وألّا تعالج لاحقا بطريقة تتنافى مع هذه الغايات....." فيقصد بذلك أن تتم معالجة هذه المعطيات بطريقة تحترم فيها المتطلبات القانونية، والتي تشترط إعلام الشخص المعني بالمعالجة، وأن لا تتم دون رضاه وأن تستند إلى مبررات كافية، وأن تكون لازمة لحماية مصالحه المشروعة، وكذا مصالح المسؤول عن المعالجة ما يقتضي مصلحة مشروعة تبررها، حيث يحكم هذا المبدأ جميع مراحل العملية من جمع وتسجيل البيانات الشخصية، وكذا تخزينها ونقلها إلى الغير.

تقتضي المشروعية الاعتماد على بيانات ومعلومات صحيحة ودقيقة ومحينه إذا اقتضى الأمر ذلك[24]، وأن تكون هذه البيانات ملائمة ومناسبة وغير مبالغ فيها بالنظر لغاية المعالجة التي من أجلها تم جمع ومعالجة المعطيات، بحيث لا تجمع إلا البيانات الشخصية التي تخدم الوصول إلى الغاية المنشودة. كما تقتضي المشروعية أن تحفظ البيانات بطريقة يسهل من خلالها التعرف على الأشخاص المعنيين خلال مدة لا تتجاوز المدة اللازمة لإنجاز

الغاية المقصودة من المعالجة[25]. بالعودة لنص المادة 11 من قانون 18-07 فإن هذه الأخيرة تمنع استخدام المعالجة الآلية لتأسيس الأحكام القضائية، أو لإنشاء قرارات ذات آثار قانونية على الشخص المعني بالمعالجة. كما يشترط أن لا تؤدي المعالجة إلى الكشف عن الأصل الإثني أو العرقي أو الآراء السياسية والمعتقدات الدينية، أو الانتماءات النقابية إلى غير ذلك[26].

ب- الموافقة المسبقة للشخص المعني بالمعالجة

اشترطت المادة 7 من قانون 18-07 ضرورة أن تتم معالجة المعطيات بالموافقة الصريحة للشخص المعني، ذلك أن رضا هذا الأخير بالمعالجة، يعد أحد أبرز الضمانات لتحقيق معالجة صحيحة ومشروعة، ويشترط في الرضا عموما أن يصدر من شخص مميز يتمتع بكامل قواه العقلية، وأن يكون رضاه خاليا من أي عيب كالغلط أو الاكراه أو التدليس أو الاستغلال، وأن يتعلق الرضا بموضوع ووقائع محددة لا يتعداها إلى غيرها، وهو ما يقتضي من المسؤول عن المعالجة الإفصاح عن المعطيات محل المعالجة.

أما إذا تعلق الأمر بشخص عديم الاهلية أو ناقصها فإن الموافقة عن المعالجة تتم وفق القواعد المنصوص عليها في القانون العام حسب نص الفقرة الثانية من المادة 7 السابق ذكرها، ويقصد بالقانون العام القواعد العامة للأهلية في القانون المدني، خاصة المادة 44 منه[27] التي تحيل لأحكام الولاية أو الوصاية أو القوامة في قانون الأسرة، وتطبيقا لهذه الأحكام فلا يمكن إبداء الموافقة الصريحة لأجل القيام بمعالجة المعطيات الشخصية بالنسبة لناقص أو عديم الأهلية إلا ممن يملك حق الولاية أو الوصاية أو التقديم، وهو ما يؤكده أيضا نص المادة 8 "لا يمكن القيام بمعالجة المعطيات المتعلقة بالأطفال إلا بعد الحصول على موافقة الممثل الشرعي لهم أو بعد الحصول على ترخيص القاضي عند الاقتضاء".

يمكن للشخص المعني الذي قدم موافقته على معالجة بياناته الشخصية أن يتراجع في أي وقت عن هذه الموافقة، وإن تعلق الأمر بقاصر أو عديم الأهلية فيمكن للقاضي في أي وقت أن يعدل عن ترخيصه، إلا أنه وعندما تكون المعالجة ضرورية فإنها لا تحتاج إلى الموافقة المسبقة للمعني سواء كان كامل الأهلية أم لا[28].

ج- احترام الإجراءات المسبقة

يشترط للقيام بمعالجة المعطيات ذات الطابع الشخصي أيضا أن تخضع لتصريح مسبق من السلطة الوطنية أو لترخيص منها[29]. وتعتبر هذه الإجراءات مهمة جدا في إطار شفافية المعالجة كما أنها أيضا تعد ضمانة لحماية المعطيات الشخصية كونها تخول للسلطة

الوطنية بممارسة الرقابة على القائمين بالمعالجة خاصة من ناحية تقيّدهم بالنصوص القانونية والتوصيات والإجراءات المطلوبة، كما يعد عدم احترام هذه الإجراءات سببا للإقرار بعد مشروعية المعالجة[30].

يعد التصريح المسبق بمثابة إخطار للسلطة الوطنية بتنفيذ وإنجاز عملية المعالجة التي تنصب على البيانات الشخصية، والغاية الأساسية من هذا الإجراء هو تمكين هذه السلطة الوطنية من رقابة العملية والتحقق من مدى احترام المسؤول عن المعالجة أو ممثله للمتطلبات القانونية في هذا المجال[31].

أما الترخيص المسبق فقد اشترطه القانون حسب نص المادة 18 في الأحوال التي يتبين للسلطة المختصة، أن المعالجة المعتزم القيام بها تتضمن أخطارا ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص، فمثل هذه المعطيات لا يكفي التصريح بها لدى السلطة المعنية، بل لابد إضافة إلى ذلك أن يحصل المسؤول عن المعالجة على ترخيص من هذه السلطة يسمح له بذلك.

حدّد المشرع الحالات المطلوب فيها الترخيص المسبق، وهي عند معالجة المعطيات الحساسة وتتمثل هذه الأخيرة في المعطيات التي تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص المعني، أو تكون متعلقة بصحته بما فيها معطياته الجينية[32]، علما أن المشرع منع كأصل معالجة هذه المعطيات، إلا أنه سمح بذلك في حالات محدّدة، وهي أسباب تتعلق بالمصلحة العامة، وأن تكون المعالجة ضرورية لممارسة المهام القانونية أو النظامية للمسؤول عن المعالجة، أو عندما تتم المعالجة بالموافقة الصريحة للمعني أو عند وجود نص قانوني يسمح بذلك أو ترخيص السلطة الوطنية. وقد ذكرت المادة 18 على سبيل المثال الحالات التي تتم فيها معالجة المعطيات الحساسة[33].

كما يشترط الترخيص أيضا عند الربط البيني للمعطيات، وهو أي شكل من أشكال المعالجة التي تتمثل في إقامة ترابط بين معطيات معالجة لغاية محددة مع معطيات أخرى يمسكها مسؤول أو مسؤولين آخرين عن المعالجة، أو يمسكها نفس المسؤول لنفس الغرض أو لأغراض أخرى[34]، كالربط البيني لملفات تابعة لشخص أو عدة أشخاص معنويين يسيرون مرفقا عموميا لأغراض مختلفة مرتبطة بالمنفعة العامة، كربط الجهات القضائية والشرطة القضائية بالقاعدة الوطنية للبصمات الوراثية، أو بالمعطيات الوطنية لصحيفة السوابق العدلية التابعة لوزارة العدل. كما يشترط الترخيص عند الربط البيني للملفات التابعة

للأشخاص الطبيعية، والذي يتم لأغراض مختلفة[35]. كما يشترط الترخيص أيضا في حالة نقل المعطيات ذات الطابع الشخصي إلى دولة أجنبية، وهو ما يتضح من نص المادة 44 من قانون 18-07[36]، وقد استثنى المشرع وفي حالات معينة نقل هذه المعطيات إلى دولة أجنبية من الحصول على الترخيص ذكرتها المادة 45 من القانون المذكور[37].

يشترط الترخيص أيضا عند معالجة المعطيات ذات الطابع الشخصي التي تهدف إلى تحقيق مصلحة عامة للبحث أو الدراسة أو التقييم في مجال الصحة، كما يمكن للسلطة الوطنية منح ترخيص واحد لنفس الطلب إذا كانت المعالجة لها نفس الأغراض وتتعلق بمعطيات مماثلة، وبنفس فئات المرسل إليهم[38].

تجدر الإشارة أن كل الإجراءات السابقة الذكر يجب أن تتم في ظل احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألاّ تمس بحقوق الأشخاص وشرفهم وسمعتهم[39].

ثانيا: الحماية الإدارية والجزائية

من أجل تعزيز حماية الحياة الخاصة في إطار معالجة المعطيات ذات الطابع الشخصي، تم إنشاء السلطة الوطنية التي تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون، وضمان عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة[40]. فيمكن لهذه السلطة في إطار ممارسة مهامها أن تتخذ في مواجهة المخالف للمقتضيات القانونية لمعالجة المعطيات ذات الطابع الشخصي جزاءات إدارية (1)، كما أقر المشرع حماية جزائية (2).

1- الحماية الإدارية

جاء في نص المادة 22 الفقرة الثانية من قانون 18-07 على أنه " تنشأ لدى رئيس الجمهورية سلطة إدارية مستقلة لحماية المعطيات ذات الطبع الشخصي، يشار إليها أدناه "السلطة الوطنية"، .... ". تتشكل السلطة الوطنية من شخصيات وطنية يختارهم رئيس الجمهورية من بين ذوي الاختصاص، ومن بينهم رئيس السلطة الوطنية، ومن قضاة يقترحهم المجلس الأعلى للقضاة وبينهم قضاة المحكمة العليا ومجلس الدولة، وعضوا من كل غرفة من البرلمان يتم اختيارهم من قبل رئيس كل غرفة بعد التشاور مع رؤساء المجموعات البرلمانية، وكذا ممثلي القطاعات ذات الصلة بنشاطها. وتكلف بالسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي لأحكام القانون[41].

تتولى السلطة الوطنية مهام متعددة لحماية المعطيات الشخصية ذكرتها المادة 24 من نفس القانون، والتي من بينها منح التراخيص أو التصاريح لأجل المعالجة السابق ذكرهما، ويمكنها أيضا أن توقع الجزاءات الإدارية على كل من قام بخرق أحكام قانون 18-07، فيمكنها أن تتخذ في مواجهة المخالف الإنذار، والإعذار، أو السحب المؤقت لمدة لا تتجاوز السنة، أو السحب النهائي لوصل التصريح أو الترخص[42]. ولقد أعطى المشرع إمكانية سحب وصل التصريح أو الترخيص إذا تبين بعد إجراء المعالجة موضوع التصريح أو الترخيص أنها تمس بالأمن الوطني أو كونها منافية للأخلاق أو الآداب العامة حسب نص المادة 48.

الملاحظ أن قانون 18-07 لم يحدد نوع الأفعال أو درجة الأخطاء التي تستوجب توقيع الجزاءات الإدارية السابق ذكرها ما، يعني أنها تخضع للسلطة التقديرية للسلطة الوطنية، وهو ما يري فيه البعض أنه قد يكون سببا للتعسف من طرف هذه السلطة رغم وجود حق الطعن المعترف به للمسؤول عن المعالجة، خاصة أنه وفي غياب نص يرجع إليه القاضي سيتعذر عليه مراقبة مدى ملاءمة العقوبة للخطأ المرتكب أم لا[43].

إلا أن أهم ما تتمتع به هذه السطلة في إطار حماية المعطيات الشخصية هي سلطة توقيع العقاب عن طريق فرض الغرامة الإدارية، وهو ما أشارت إليه المادة 46 منه، حيث يحق للسلطة الوطنية فرض الغرامة في حق المسؤول عن المعالجة في حالة رفضه دون سبب شرعي حقوق الشخص المعني، كحق الإعلام أو الولوج أو التصحيح أو الاعتراض، وفي حالة عدم القيام بالتبليغ عن هوية ممثله المقيم في الجزائر والذي يحل محله في جميع حقوقه والتزاماته، أو عدم التبليغ عن التغييرات التي حدثت في المعلومات المصرح بها أو أي حذف يطال المعالجة[44].

تتمتع السلطة الوطنية هي سلطة إدارية مستقلة، بصلاحية الضبطية القضائية في إطار مجال معالجة المعطيات ذات الطابع الشخصي، بالإضافة إلى مهام الضبط الإداري في مجال الرقابة والإشراف، وهو ما تؤكده المادة 49، إذ يمكنها أن تقوم بالتحري ومعاينة الأمكنة والمحلات التي تتم فيها المعالجة باستثناء محلات السكن. والملاحظ في هذا الإطار أن المشرع في قانون 18-07 فيما يتعلق بإجراءات الضبط القضائي الممنوحة للسلطة الوطنية في مجال معالجة المعطيات ذات الطابع الشخصي، أنه أبقى على إجراءات التفتيش المنصوص عليها في قانون الإجراءات الجزائية والمنوطة بوكيل الجمهورية نظرا لخصوصية حرمة الحياة الخاصة[45].

يمكن للسلطة الوطنية أيضا أن تقوم بالولوج إلى المعطيات المعالجة، وجميع الوثائق مهما كانت طبيعتها ودعامتها، دون إمكانية التمسك أمامها باسر المهني حسب ما تؤكده المادة 49، ويمكنها أيضا أن تستعين بأعوان الشرطة القضائية وأعوان الرقابة الأخيرين، للقيام بالبحث ومعاينة الجرائم المرتكبة في إطار معالجة المعطيات الشخصية وذلك تحت اشراف وكيل الجمهورية[46] .

2- الحماية الجزائية

سبق الذكر أن معالجة المعطيات ذات الطابع الشخصي اشترط فيها قانون 18-07 أن تتم في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة، وأن لا تمس بحقوق الأفراد وسمعتهم وشرفهم، وفي هذا الإطار يمكن للسلطة الوطنية في إطار معاينة الجرائم التي ترتكب مخالفة لأحكام القانون رقم 18-07، أن تستعين بأعوان الشرطة القضائية وأعوان الرقابة الأخيرين، للقيام بالبحث ومعاينة الجرائم المرتكبة في إطار معالجة المعطيات الشخصية، وذلك تحت إشراف وكيل الجمهورية، كما يتم معاينة هذه الجرائم بموجب محاضر يجب أن توجه فورا إلى وكيل الجمهورية حسب من المادة 52 .

تجدر الإشارة أنه سبق للمشرع وأن أصدر نصوصا تحمي أنظمة المعالجة الآلية بصفة عامة سواء تعلق بمعطيات شخصية أم لا، وذلك من خلال استحداث القسم الرابع مكرر في قانون العقوبات المعنون بـ"المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04-15[47].

وبالرجوع الى الفصل الثالث من الباب السادس من قانون رقم 18-07 المعنون الأحكام الجزائية يتضح أنه تضمن مجموعتين من الجرائم، الأولى تتعلق بالجرائم الماسة بالقواعد الموضوعية(أ)، والثانية تتعلق بالجرائم الماسة بالقواعد الإجرائية(ب).

أ- الجرائم الماسة بالقواعد الموضوعية

عاقب المشرع الأفعال التي تعد مساسا بالقواعد الموضوعية لمعالجة المعطيات الشخصية ذات الطابع الشخصي، وتتمثل في تجريم كل معالجة تتم مخالفة لأحكام المادة 2من قانون 18-07 المعالجة التي تنتهك من خلالها الكرامة الإنسانية والحياة الخاصة والحريات العامة أو تمس بالسمعة والشرف، وكذا المعالجة التي تتم مع اعتراض الشخص المعني الذي يستند لأسباب شرعية أو لأسباب تتعلق الإشهار التجاري أو دون موافقته الصريحة، أو رفض أحد حقوقه دون سبب مشروع.

كما تجرم كل معالجة تتم بناء على تصريحات كاذبة وكل إنجاز أو استعمال للمعطيات في غير الغرض المصرح به أو المرخص به، وكل عملية جمع للمعطيات تتم بطريقة تدليسية أو غير نزيهة وغير مشروعة، ويعاقب كل من يتسبب أو يسهل ولو عن اهمال الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يسلمها لغير المؤهلين لذلك. كما عاقب المشرع كل افشاء للمعلومات المحمية أو الاحتفاظ بالمعطيات بعد انتهاء المدة المحددة لذلك، أو من قام بمعالجة المعطيات ذات الطابع الشخصي والمتعلقة بالوضعية الجنائية للشخص المعني في غير الحالات المنصوص عليها قانونا، وكذا عدم إعلام السلطة الوطنية والشخص المعني بالانتهاكات التي تمس المعطيات الشخصية في مجال الاتصالات الالكترونية[48].

ب- الجرائم الماسة بالقواعد الإجرائية

تتمثل الماسة بالقواعد الإجرائية في كل من الجرائم المرتبطة بالإجراءات المسبقة، حيث عاقب المشرع كل معالجة للمعطيات الشخصية تتم بدون تصريح مسبق أو ترخيص من السلطة الوطنية، أو الاستمرار في المعالجة رغم سحب التصريح أو الترخيص، أو القيام بنقل المعطيات الشخصية إلى بلد أجنبي دون ترخيص وفي غير الحالات المحددة على سبيل الحصر[49]. وكذا الجرائم التي تتعلق بمخالفة الإجراءات المتعلقة بالتعاون مع السلطة الوطنية، كجريمة عدم اتخاذ التدابير اللازمة (التنظيمية والتقنية) لسلامة وأمن معالجة المعطيات الشخصية، وجريمة السماح لغير المؤهلين للولوج للمعطيات الشخصية، أو الولوج للسجل الوطني للمعطيات الشخصية دون أن يكون مؤهلا لذلك وجريمة عرقلة عمل السلطة الوطنية لحماية المعطيات الشخصية[50].

إن هذا التعداد للجرائم التي تمس معالجة المعطيات ذات الطابع الشخصي دليل على محاولة المشرع على عدم ترك أي مجال لانتهاك الخصوصية أو حرمة الحياة الخاصة، قصد توفير أكبر قدر من الحماية في ظل هذا التطور الرقمي[51]، ومن خلال قراءة نصوص مواد التجريم في قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، يتضح أنها شددت العقوبات فيما يخص الأفعال التي تقع انتهاكا لحرمة الخاصة من قبل المسؤول عن المعالجة بالمقارنة مع العقوبات المنصوص عليها في قانون العقوبات خاصة المواد 303 ،303 مكرر، 303 مكرر1، والمتمثلة في الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات والغرامة من 25000 إلى 500000 دج، حيث أن القانون 18-07 فيه من الجرائم ما يعاقب عليها بخمس (5) سنوات، والغرامة من 100000 دج إلى

1000000 دج، مثل ما نصت عليه المادة 54 منه، ما يفيد أن هذا القانون قد قدم حماية أفضل لحرمة الحياة الخاصة في مجال المعطيات الشخصية.

خاتمة

ختاما يمكن القول أن التطور العلمي والتكنولوجي الذي تعرفه البشرية، عن طريق استعمال المعلوماتية في مختلف الميادين أصبح يقتضي تجميع ومعالجة المعلومات المتعلقة بالأفراد للاستفادة منها في جوانب كثيرة، ما أثرا كثيرا على مضمون الحق في الحياة الخاصة أو الحق في الخصوصية وعرضه لسهولة انتهاكه بسبب الطبيعة الحساسة لهذه المعطيات التي أصبحت جزاءً لا يتجزأ من الحياة الخاصة التي هي أحد من الحقوق المحمية دستوريا، لذا فإن قانون 18-07 ورغم أنه جاء لتنظيم المعالجة الآلية وغير الآلية للمعطيات ذات الطابع الشخصي، إلا أن غالبية أحكامه تتعلق بالمعالجة الألية فقط، كونها تشكل أكبر تهديد لهذا الحق بالمقارنة مع المعالجة غير الآلية، ما يجعل حماية الحق في الخصوصية الآن أمام تحدٍّ تكنولوجي مستمر باستمرار التطور التكنولوجي.

كرس المشرع من خلال القانون 18-07 المتعلق بمعالجة المعطيات ذات الطابع مجموعة الضوابط ضمانا لحماية الحريات الأساسية للمواطن، وفي إطار احترام الحياة الخاصة، بما أقره من مبادئ أساسية لحماية المعطيات، وما فرضه من التزامات على القائم بالمعالجة بما يضمن سرية وسلامة المعطيات من جهة، ومن جهة أخرى، جعله خاضعا لرقابة سلطة إدارية مستقلة هدفها السهر على حسن تطبيق هذا القانون، بالإضافة إلى الاعتراف للمعني بالمعالجة مجموعة من الحقوق قصد تعزيز هذه الحماية.

إلا أنه نرى أن هذه الحماية وفي ظل هذا التطور المستمر لن تكون فعالة مالم تكن مرفقة باهتمام كبير بالبنية التحتية للتكنولوجيا لمواكبة التطور المستمر لمعالجة المعطيات في مختلف الميادين. إضافة الى تكثيف جهود التعاون محليا ودوليا قصد تعزيز الحماية الفعالة، إضافة الى ضرورة إرفاق قانون 18-07 بمراسيم تنفيذية لتوضيحه أكثر، خاصة لكون الكثير من مصطلحاته تقنية قصد تحديد كيفية ممارسة بعض الحقوق التي يتمتع بها الشخص المعني أو الالتزامات الملقاة على عاتق المسؤول عن المعالجة، أو ممارسة السلطة الوطنية لمهامها وصلاحياتها. إضافة إلى العمل على انسجام هذا القانون مع غيره من القوانين التي تقتضي التعامل بالمعطيات الشخصية كقانون التجارة الالكترونية وغيرها.

الهوامش:

[1]أنظر في ذلك مثلا اتفاقية بودابست بشأن جرائم الإنترنت أو اتفاقية بودابست المنعقدة في 22 نوفمبر 2001 تحت إشراف المجلس الأوروبي.

[2]نصت المادة 12 من الإعلان العالمي لحقوق الانسان على "لا يجوز تعريضُ أحد لتدخّل تعسُّفي في حياته الخاصة أو في شؤون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمسُّ شرفه وسمعته. ولكلِّ شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات". وهو نفس ما نصت عليه أيضا المادة 17 من العهد الدولي للحقوق المدنية والسياسة المصادق عليه من طرف الجمعية العامة للأمم المتحدة في 80 ديسمبر 1966 إذ نصت "لا يحوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته. من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس."

[3] Basile Ader, La protection de la vie privée en droit positif français, Légicom, n° 21, 1994 /4, p. 5. https://www.cairn.info/revuelegicom19994page5.htm.

[4]سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة، دراسة مقارنة، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، مجلد 29، العدد الثالث 2013، ص 421-455. أنظر أيضا أحمد بعجي، تطور مفهوم الحق في الخصوصية، مجلة القانون والمجتمع، المجلد الثامن، العدد الأول، 2020، ص 452.

[5]أحمد بعجي، المرجع السابق، ص 454. نعيم سعيداني، الحماية الجنائية للحق في الخصوصية في مجال المعلوماتية، رسالة دكتوراه، جامعة باتنة 1 الحاج لخضر2020-2021، ص 87.

[6]أيمن مصطفى أحمد البقلي، حماية الخصوصية المعلوماتية لمستخدمي الإنترنت في مواجهة متطلبات التجارة الإلكترونية، المجلة القانونية المجلد 9، العدد 4، 2021، ص 1001-. 1144 https://jlaw.journals.ekb.eg/article_190687.html

[7]يقصد بالمعالجة العمليات التي تنفذ على البيانات للحصول على المعلومات، أنظر في هذا المعنى مجادي نعيمة، أثر إجراءات معالجة المعطيات ذات الطابع الشخصي على الحق في حرمة الحياة الخاصة، مجلة آفاق علمية، مجلد 12، عدد 4، سنة 2020، ص 428453.

[8] Stéphane Tijardovic, La protection juridique des données personnelles, ver une nécessaire adaptation de la norme juridique aux évolutions du monde numérique, LNC, volume 4, n° 34/ 2003, p. 185-203. https://www.cairn.info/revuelescahiersdunumerique200-33page185.htm.

[9]طباش عز الدين، الحماية الجزائية للمعطيات الشخصية، في التشريع الجزائري، دراسة في ظل قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال حماية المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، العدد الثاني، 2018، ص29.

[10]قانون رقم 16-01 المؤرخ في 6 مارس 2016 يتضمن التعديل الدستوري، الجريدة الرسمية رقم 14، الصادرة 7 مارس 2016.

[11]وهو نفس النص تقريبا في ظل الدستور الحالي إذ نصت المادة 47 منه " لكل شخص الحق في حماية حياته الخاصة وشرفه.ـ لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت. لا مساس بالحقوق

المذكورة في الفقرتين الأولى والثانية إلاّ بأمر معلل من السلطة القضائية. حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي. يعاقب القانون على كل انتهاك لهذه الحقوق". الجريدة الرسمية، العدد 82، الصادرة في 20 ديسمبر 2020.

[12] المؤرخ في 10 يونيو 2018، جريدة رسمية العدد 34، الصادرة في 10 يونيو 2018.

[13] وهو ما يدل عليه أصلا عنوان هذا القانون.

[14] نعيم سعيداني، المرجع السابق، ص40.

[15] هذا ما يستفاد من نص المادة 3 من قانون 18-07 التي ذكرت الأشخاص بصفة عامة دونما تحديد لجنسيتهم، أنظر أيضا نص المادة 3 من قانون العقوبات، الأمر رقم 66-156 المؤرخ في مؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة يونيو سنة 1966، المعدل والمتمم.

[16] "لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي المتعلقة بطفل إلا بعد الحصول على موافقة ممثله الشرعي أو عند الاقتضاء، بترخيص من القاضي المختص".

[17] إذ نصت "يجب أن تتم معالجة المعطيات ذات الطابع الشخصي، مهما كان مصدرها أو شكلها، في إطار احترام الكرامة الإنسانية والحياة الخاصة والحريات العامة وألاّ تمس بحقوق الأشخاص وشرفهم وسمعتهم".

[18] نعيم سعيداني، المرجع السابق، ص 212.

[19] « Il est d'ailleurs envisageable que ces dispositions deviennent un moyen de pression juridique en cas de conflit avec l'entreprise. Il peut arriver que des salariés invoquent la non-conformité des éléments de preuve issus de fichiers non conformes à la loi sur la protection des données pour faire rejeter les arguments de l'employeur dans un conflit donné ». Yacoub Zina, De la protection des données personnelles à la lumière de la loin° 1807 : une nouvelle responsabilisation pour les entreprises p. 687.

[20] كاملة بوعكة، الحماية القانونية للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في ضوء القانون 18-07، المجلة الجزائرية لقانون الأعمال العدد الثاني ديسمبر 2020، ص 58.

[21] نعيم سعيداني، المرجع السابق، ص 223.

[22] أيمن مصطفى أحمد البقلي، المرجع السابق، ص1057 وما بعدها.

[23] استثناء أجاز المشرع الاستكشاف المباشر عن طريق البريد الالكتروني بتوافر شروط معينة، أنظر المادة 37- 2 من قانون 18-07.

[24] أيمن مصطفى أحمد البقلي، المرجع السابق، ص 1062.

[25] أنظر المادة 9 من قانون 18-07 الفقرات ج، د، وه.

[26] حيث اعبرت هذه المعطيات من المعطيات الحساسة وهو ما أكدته المادة 3 من قانون 18-07

[27] نصت المادة 44 من الأمر رقم 75-58 المؤرخ في 26 سبتمبر1975 يتضمن القانون المدني المعدل والمتمم" يخضع فاقدو الأهلية، وناقصوها، بحسب الأحوال لأحكام الولاية، أو الوصاية، أو القوامة، ضمن الشروط ووفقا للقواعد المقررة في هذا القانون".

[28] تكون المعالجة ضرورية حسب المادة 7 إذا تمت احتراما لالتزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة، أو كانت لحماسة حياة الشخص المعني، أو لتنفيذ عقد يكون الشخص المعني طرفا فيه ولتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه، أو للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه، أو لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم اطلاعه على المعطيات، أو لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني و/ أو حقوقه وحرياته الأساسية.

[29] هذا ما تؤكده المادة 12 من قانون 18-07.

[30] نعيم سعيداني، المرجع السابق، ص 277.

[31] نعيم سعيداني، المرجع نفسه، ص 228.

[32] أنظر المادة 3 من قانون 18-07.

[33] الحالات التي ذكرتها المادة 18 تتمثل في: إذا كانت المعالجة ضرورية لحماية المصالح الحيوية للشخص المعني أو لشخص آخر وفي حالة وجود الشخص المعني في حالة عجز بدني أو قانوني عن الإدلاء بموافقته، أو عند تنفيذ المعالجة، بناء على موافقة الشخص المعني، من طرف مؤسسة أو جمعية أو منظمة غير نفعية ذات طابع سياسي أو فلسفي أو ديني أو نقابي، في إطار نشاطاتها الشرعية، أو كانت تخص معطيات صرح بها الشخص المعني علنا عندما يمكن استنتاج موافقته على معالجة المعطيات من تصريحاته. كما عندما تكون المعالجة ضرورية لاعتراف بحق أو ممارسته أو الدفاع عنه أمام القضاء وأن تكون قد تمت حصريا لهذه الغاية. أو عند معالجة المعطيات الجينية، باستثناء تلك التي يقوم بها أطباء أو بيولوجيون والتي تعد ضرورية لممارسة الطب الوقائي، والقيام بتشخيصات طبية وفحوصات أو علاجات. وفي كل الأحوال، تبقى التدابير المنصوص عليها في هذا القانون لحماية هذه المعطيات، مضمونة.

[34] أنظر نص المادة 3 من قانون 18-07.

[35] نعيم سعيداني، المرجع السابق، ص 235.

[36] " لا يجوز لمسؤول عن معالجة نقل المعطيات ذات طابع شخصي إلى دولة أجنبية إلاّ بترخيص للسلطة الوطنية وفقا لأحكام هذا القانون، .....".

[37] تتمثل هذه الحالات في:1 الموافقة الصريحة للشخص المعني ، 2 إذا كان النقل ضروريا: للمحافظة على حياة هذا الشخص أو المحافظة على المصلحة العامة، أو احتراما لالتزامات تسمح بضمان إثبات أو ممارسة حق أو الدفاع عنه أمام القضاء، او تنفيذا لعقد بين المسؤول عن المعالجة والشخص المعني أو تنفيذا لإجراءات سابقة للعقد والمتخذة بناء على طلب هذا الأخير، أو لإبرام أو تنفيذ عقد مبرم أو سيبرم بين المسؤول عن المعالجة والغير، لمصلحة الشخص المعني، تنفيذا لإجراء يتعلق بتعاون قضائي دولي، للوقاية من إصابات مرضية أو تشخيصها أو معالجتها.3 إذا تم النقل تطبيقا لاتفاق ثنائي أو متعدد الأطراف تكون الجزائر طرفا فيه،4 بناء على ترخيص السلطة الوطنية، إذا كانت المعالجة تتطابق مع أحكام المادة 2 من هذا القانون.

[38] أنظر نص المادة 21 من قانون18-07.

[39] أنظر نص المادة 2 من قانون 18-07.

[40] أنظر نص المادة 22 من قانون 18-07 وما بعدها.

[41] هذا ما يتضح من نص المادة 23 و24 من قانون 18-07.

[42] أنظر نص المادة 46 من قانون 18-07.

[43] مجادي نعيمة، المرجع السابق، ص 442-453.

[44] أنظر ما جاء في المواد 4 ،14 و16 من قانون 18-07.

[45] مجادي نعيمة، المرجع نفسه، ص447.

[46] تنص المادة 50 من قانون 18-07 " إضافة إلى ضباط وأعوان الشرطة القضائية، يؤهل أعوان الرقابة الآخرون الذين تلجأ إليه السلطة الوطنية، للقيام ببحث ومعاينة الجرائم المنصوص عليها في أحكام هذا القانون، تحت إشراف وكيل الجمهورية".

[47] المؤرخ في 10 نوفمبر 2004، جريدة رسمية العدد 71 لسنة 2004.

[48] تفصيلا لهذه الجرائم، أنظر عز الدين طباش، المرجع السابق، ص 30 وما بعدها.

[49] انظر المادة 55 وما بعدها من قانون 18-07.

[50] أنظر في هذا المادة 61 وما بعدها من قانون 18-07.

[51] عز الذين طباش، المرجع السابق، ص 59.

حماية المعطيات ذات الطابع الشخصي في القانون الجزائري

Protection data of a personal nature in Algerian law

عمر شتوح، دكتوراه في القانون الدولي العام والخاص، أستاذ مؤقت في كلية الحقوق جامعة الجزائر1 والمدرسة العليا للقضاء ، الجزائر
omar-chettouh@hotmail.fr

العيداني أمال، طالبة دكتوراه تخصص قانون قضائي، كلية الحقوق جامعة الجزائر1،لجزائر
amel.laidani@outlook.fr

الملخص:

تهدف هذه الورقة البحثية موضوع المداخلة والموسومة بـ" حماية المعطيات ذات الطابع الشخصي في القانون الجزائري" إلى تحديد الإطار المفاهيمي والقانوني الذي وضعه المشرع الجزائري لحماية المعطيات ذات الطابع الشخصي، والذي جاء نتيجة لدسترة الحق في حماية المعطيات ذات الطابع الشخصي منذ التعديل الدستوري ل2016، حيث جاء القانون 18-07 كقانون خاص يعنى بحماية المعطيات ذات الطابع الشخصي من أي انتهاكات تحقيقا لمبدأ احترام كرامة الإنسان وحرمة حياته الخاصة باعتبارها من الحقوق والحريات الأساسية، فمعالجة المعطيات متوقف على الموافقة الصريحة للشخص المعني إلاّ استثناء، فهذه الأخيرة من المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي إلى جانب الإجراءات المسبقة عن المعالجة والمتمثلة في التصريح والترخيص، كما تم التطرق في هذه الورقة، إلى حقوق الشخص المعني والتزامات المسؤول عن المعالجة، كما تم الوقوف عند آليات الحماية المؤسساتية والإدارية، لننتهي بالأحكام الجزائية المقررة على مخالفة أحكام القانون.

الكلمات المفتاحية: معالجة المعطيات، معطيات ذات طابع شخصي، حماية المعطيات.

Abstract :

This research paper, the subject of the intervention, tagged with "Protection data of a personal nature in Algerian law" aims to define the conceptual and legal framework established by the Algerian legislator for the protection of personal data, which came as a result of the constitution of the right to protect personal data since the constitutional amendment of 2016, law 18-07 came as a special law concerned with the protection of personal data from any violations in order to achieve the principle of respect for human dignity and the sanctity of his private life as one of the basic rights and freedoms. In addition to the prior procedures for processing, represented in the authorization and licensing, as was discussed in this paper, the rights of the person concerned and the obligations of the person responsible for the processing, as well as the institutional and administrative protection mechanisms, to end with the penal provisions for violating the provisions of Law.

Keywords: data processing, data of a personal nature, data protection.

مقدمة:

إن الحق في الحياة الخاصة من أهم الحقوق والحريات التي عنيت بها المواثيق الدولية والتشريعات الوطنية لا سيما الدساتير منها، فضلا عن أن هذا الحق تناولته جل الكتب السماوية وفي مقدمتها الشريعة الإسلامية التي حرمت أحكامها الاعتداء أو المساس بهذا الحق، فحرمة الحياة الخاصة عنوان حرية الإنسان وصيانة كرامته، لذلك اهتمت المواثيق الدولية التي تعنى بحقوق الإنسان بهذا الحق، كما حذت التشريعات الوطنية -وفي مقدمتها الدساتير- حذو الصكوك الدولية وأولت لحرمة الحياة الخاصة ضمانات قانونية لحمايتها.

بيد أنه في العقود الأخيرة شهد العالم طفرة تكنولوجية في شتى المجالات لا سيما في تكنولوجيا الاتصالات وتقنية المعلومات وانتشار وسائل التواصل الاجتماعي والاستخدام الواسع للأجهزة الإلكترونية والرقمية كالحاسوب والهواتف النقالة...، حيث أضحى الفضاء الرقمي يعج بالمعطيات الشخصية للأفراد الأمر الذي استوجب ضرورة تدخل المشرع على الصعيدين الداخلي والدولي لحمايتها، ذلك أن الفضاء الرقمي عرف ظهور جرائم ترتكب إلكترونيا، من بينها الاستخدام غير المشروع للبيانات الشخصية والمساس بأنظمة المعالجة الآلية للمعطيات والابتزاز ...الخ وهذه الجرائم تمس بحرمة الحياة الخاصة، فقلى الصعيد الدولي نص الإعلان العالمي لحقوق الإنسان في مادته الثانية عشر على حرمة الحياة الخاصة،[1] كما تناول العهد الدولي المتعلق بالحقوق المدنية والسياسية هذا الحق في المادة 17،[2] وقد أنشأت الأمم المتحدة المفوضية السامية لحقوق الإنسان والخصوصية في العصر الرقمي،[3] وعلى الصعيد الوطني اهتم المشرع الجزائري بحماية خصوصية الحياة الخاصة وحرمتها بصفة عامة في كل الدساتير الجزائرية، كما ساير المؤسس الدستوري التطور بالنص على حماية المعطيات ذات الطابع الشخصي في دستور 2016 و2020، وفي القوانين عني القانون 18-07 بحماية المعطيات ذات الطابع الشخصي حيث تكلل ذلك بقانون خاص، كما استحدث هذا القانون السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي. كما أن قانون العقوبات واكب تطور الجرائم بنصه على المساس بأنظمة المعالجة الآلية للمعطيات.

وموضوع هذه الورقة البحثية يدور في إشكالية مؤداها: ما هي الضمانات القانونية التي كرسها المشرع الجزائري لحماية المعطيات ذات الطابع الشخصي؟

ولمعالجة هذه الإشكالية نقترح دراسة هذا الموضوع من خلال محورين، الأول نخصصه للإطار المفاهيمي للمعطيات ذات الطباع الشخصي، والثاني نخص بالدراسة الإطار القانوني لحماية المعطيات ذات الطباع الشخصي.

المحور الأول

الإطار المفاهيمي للمعطيات ذات الطابع الشخصي

إن دراسة الحماية القانونية للمعطيات ذات الطابع الشخصي تفرض أولا معرفة المقصود من المعطيات ذات الطابع الشخصي، والمصطلحات المرتبطة بها، والحق في خصوصية المعلومات والأخطار التي تواجهها في الفضاء الرقمي، وحقوق الشخص المعني[4].

أولا: مفهوم المعطيات ذات الطابع الشخصي

أ- المقصود بالمعطيات ذات الطابع الشخصي":

رغم أن المتعارف عليه أن تحديد المفاهيم ووضع تعريف للمصطلحات من مهام الفقه دون القانون، لكن المشرع الجزائري ونظرا لخصوصية القانون 18-07 المشار إليه أعلاه، وما يتضمنه من مصطلحات تقنية وفنية، خصص المادة الثالثة من القانون 18-07 لضبط المصطلحات. حيث عرف المعطيات ذات الطابع الشخصي على أنها" *كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه والمشار إليه أدناه، "الشخص 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 البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية*".[5]

كما تناولت ذات المادة المقصود بمعالجة المعطيات ذات الطابع الشخصي بنصها أنها" *كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل آخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف*"[6]

كما تناول ذات القانون المقصود بالمعالجة الآلية بأنها العمليات المنجزة كليا أو جزئيا بواسطة طرق آلية مثل تسجيل المعطيات وتطبيق عمليات منطقية و/أو حسابية على هذه المعطيات أو تغييرها أو مسحها أو استخراجها أو نشرها.[7]

وما يمكن ملاحظته من خلال التعاريف المنوه بها أعلاه أنها جاءت مستوحاة من اللائحة العامة لحماية البيانات [8]« GDPR » الصادرة عن الاتحاد الأوروبي.[9]

ب- الحق في خصوصية المعلومات ذات الطابع الشخصي والأخطار التي تهددها في الفضاء الرقمي:

01- المقصود بالحق في خصوصية المعلومات ذات الطابع الشخصي:

إن الحق في خصوصية المعلومات ذات الطابع الشخصي تعد من الحقوق الأساسية الملازمة للشخصية والتي كرستها جل الدساتير والصكوك الدولية، فالإنسان حر في حياته الخاصة، يُطلِع عليها من يشاء ومتى يشاء وكيفما يشاء.[10]

وما دام أن الإنسان في العصر الراهن لا يستطيع أن يكون بمنأى عن الفضاء الرقمي، كان لزاما تحديث المفاهيم الخاصة بحرمة الحياة الخاصة على غرار ما جاء به المؤسس الدستوري الجزائري في دستور 2016 في المادة 46 ودستور 2020 في المادة 47 بنصها على أنه" *لكل شخص الحق في حماية حياته الخاصة وشرفه.*

لكل شخص الحق في سرّيّة مراسلاته واتصالاته الخاصّة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلاّ بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

يعاقب القانون على كل انتهاك لهذه الحقوق."

ويمكن القول أن الحق في خصوصية المعلومات يهدف إلى حماية جميع المعلومات التي تتعلق بهوية الإنسان، وخصوصياته، ومراسلاته، واتصالاته، وأسراره، لا سيما الرقمية منها مضمونة ويحميها القانون، ولا يمكن المساس بها إلاّ بأمر مسبب صادر عن السلطة القضائية.[11]

كما يلاحظ أن المؤسس الدستوري الجزائري قام بدسترة الحق في حماية المعطيات ذات الطباع الشخصي، واعتبره حق أساسي يحميه القانون، لا سيما أنه تناوله في الفصل الخاص بالحقوق الأساسية والحريات العامة.

02: المخاطر المحدقة بالحق في خصوصية المعطيات ذات الطابع الشخصي:

إن الطفرة التكنولوجية التي يشهدها العالم مثلما أدت إلى سهولة الاتصال وقربت المسافات وقربت الإدارة من المواطن بظهور الإدارة الإلكترونية والحكومة الإلكترونية والاقتصاد الرقمي وبنوك المعلومات...الخ انعكس ذلك سلبا كذلك على خصوصية المعطيات ذات الطابع الشخصي، فالنقل الرقمي للبيانات أدّى إلى ظهور التجسس الإلكتروني، وبالرغم من التقدم التكنولوجي وظهور عدة برامج لحماية المعطيات إلاّ أنها تبقى قاصرة على حماية مطلقة، حيث بقيت حياة الأفراد وخصوصياتهم عبر الفضاء الرقمي مهددة بالاعتداء.[12]

كما أن اقتصاد الرقمي واعتماده على معالجة البيانات الشخصية من أجل الحصول على أكبر قدر ممكن من البيانات للوصول إلى الأفراد وإرسال الإعلانات الترويجية، نتج عنه كذلك تجارة البيانات، والاعتداء على الأشخاص بعمليات احتيال مصرفية، لذلك كان لزاما تقييد الوصول إلى الأفراد وتهديد خصوصياتهم دون إرادتهم.[13]

ثانيا: حقوق الشخص المعني بمعالجة المعطيات ذات الطابع الشخصي والتزامات المسؤول عن المعالجة

01- حقوق الشخص المعني بمعالجة المعطيات ذات الطابع الشخصي:

لقد عني الباب الرابع من القانون 18-07 بحقوق الشخص المعني بمعالجة المعطيات ذات الطابع الشخصي وتناولها في خمسة فصول نحاول تبيان بإيجاز:

أ- الحق في الإعلام:

إن المشرع الجزائري كرس للشخص صاحب المعطيات الحق في إعلامه، حيث تناوله في المادة 32 من القانون 18-07 المشار إليه أعلاه، بيد أن ذلك متوقف على عدم علمه المسبق، فاستهلت المادة " *ما لم يكن على علم مسبق بها"* ، ويجب على المسؤول عن المعالجة أو من يمثله إعلام المعني الذي يتم الاتصال به قصد تجميع معطياته ذات الطابع الشخصي، مسبقا وبصفة صريحة ودون لبس بالعناصر الآتية:

- هوية المسؤول عن المعالجة وعند الاقتضاء هوية ممثله،
- أغراض المعالجة،
- كل معلومة إضافية مفيدة، لاسيما المرسل إليه ومدى إلزامية الرد والآثار المترتبة عن ذلك وحقوقه ونقل المعطيات إلى بلد أجنبي.

إذا لم يتم جمع المعطيات ذات الطابع الشخصي لدى الشخص المعني، يجب على المسؤول عن المعالجة أو من يمثله، قبل تسجيل المعطيات أو إرسالها للغير، أن يزوده بالمعلومات المشار إليها أعلاه، ما لم يكن قد علم بها مسبقا."

وأضافت ذات المادة أنه في حالة جمع المعلومات في شبكات مفتوحة ، يجب إعلام الشخص المعني ما لم يكن على علم مسبق ، بأن المعطيات ذات الطابع الشخصي المتعلقة به يمكن أن تتداول في الشبكات دون ضمانات السلامة وأنها قد تتعرض للقراءة والاستعمال غير المرخص من طرف الغير.

والجدير بالتنويه أن المشرع الجزائري وضع استثناءات على إلزامية إعلام الشخص المعني في المادة 32 من نفس القانون، التي اعتبرت أن إلزامية الإعلام المنصوص عليها في المادة 32 غير واجبة إذا تعذر إعلام الشخص المعني، ولاسيما في حالة معالجة المعطيات ذات الطابع الشخصي لأغراض إحصائية أو تاريخية أو علمية، بيد أنه يجب على المسؤول عن المعالجة في هذه الحالة إشعار السلطة الوطنية باستحالة إعلام الشخص المعني وتسبيب ذلك.

كذلك إذا تمت المعالجة تطبيقا لنص قانوني، أو تمت المعالجة حصريا لأغراض صحفية أو فنية أو أدبية تكون معفية من إلزامية الإعلام.

ب- الحق في الولوج:

الحق في الولوج تناولته المادة 34 من القانون 18-07 ويتضمن هذا الحق أن الشخص المعني بالمعالجة يحق له التأكد من أن المعطيات الشخصية المتعلقة به كانت محل معالجة أم لا، ومعرفة أغراض المعالجة وفئات المعطيات التي تنصب عليها والمرسل إليهم، كما يتعين إفادته وفق شكل مفهوم بالمعطيات الخاصة به التي تخضع للمعالجة وبكل معلومة متاحة حول مصدر المعطيات.

وفي المقابل فإن المسؤول عن المعالجة يحق له المطالبة من السلطة الوطنية تحديد آجال الإجابة على طلبات الولوج المشروعة، كما يمكنه الاعتراض على الطلبات التعسفية، لاسيما من حيث عددها وطابعها المتكرر، بينما يقع على عاتقه إثبات الطابع التعسفي لهذا الطلب.

ج- الحق في التصحيح:

تناول القانون 18-07 الحق في التصحيح في المادة 35 منه، حيث وبموجب هذا الحق يستطيع الشخص المعني[14] الحصول مجانا من المسؤول عن المعالجة على تحيين أو تصحيح أو مسح أو إغلاق المعطيات الشخصية التي تكون معالجتها غير مطابقة لهذا القانون بسبب الطابع غير المكتمل أو غير الصحيح لتلك المعطيات على الخصوص، أو لكون معالجتها ممنوعة قانونا.

وأضافت الفقرة الثانية من ذات المادة أن المسؤول عن المعالجة يتعين عليه القيام بالتصحيحات اللازمة مجانا وفي غضون 10 أيام من إخطاره.

كما أن المشرع منح للشخص المعني في حالة رفض طلبه أو التقاعس في الرد عليه بعد انقضاء الآجال المنوه بها أعلاه الحق في رفع طلب التصحيح إلى السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، حيث تكلف هذه الأخيرة أحد أعضائها للقيام بالتحقيقات الضرورية والعمل على إجراء التصحيحات اللازمة في أقرب الآجال، وإخطار الشخص المعني بمآل طلبه.

وما يمكن الإشارة إليه من خلال استقراء المادة 35 أن الحق في التصحيح ينتقل إلى ورثة الشخص المعني.

د- الحق في الاعتراض:

يسوغ للشخص المعني أن يعترض لأسس مشروعة على معالجة معطياته ذات الطابع الشخصي، كما له الحق في الاعتراض على استعمال المعطيات المتعلقة به لأغراض دعائية، لا سيما التجارية منها، من طرف المسؤول الحالي عن المعالجة أو مسؤول عن معالجة لاحقة .

غير أن المشرع اعتبر إلى جانب ذلك أنه إذا كانت المعالجة تستجيب لالتزام قانوني، أو إذا كان تطبيق هذه الأحكام قد استبعد بموجب إجراء صريح في المحرر الذي يرخص بالمعالجة، فإنه لا يمكن تفعيل الحق في الاعتراض.[15]

هـ- الحق في منع الاستكشاف المباشر:

إن الشخص المعني يتمتع إلى جانب الحقوق السالفة الذكر، بالحق في منع استخدام بياناته الشخصية في الاستكشاف المباشر عن طريق أية آلية اتصال أو جهاز الاستنساخ البعدي أو بريد إلكتروني، أو أي وسيلة تستخدم تكنولوجيا ذات طبيعة مماثلة، باستعمال بيانات شخص طبيعي لم يعبر عن موافقته المسبقة على ذلك.

والجدير بالتنويه أنه ورغم أن المشرع أقر هذا الحق، لكن في المقابل لا يزال يلاحظ على زبائن الهاتف النقال الذين تصلهم يوميا رسائل دعائية ومسابقات وهمية بدون معرفة كيفية وصول أرقامهم إلى المرسلين ولا حتى معرفة المرسل وهويته لإمكانية المطالبة بوقف هذه الرسائل المزعجة.

02- **التزامات المسؤول عن المعالجة:**

لقد تناول القانون 18-07 في الفصل الأول من الباب الخامس، المواد من 38 إلى 41 أهم التزام يقع على عاتق المسؤول عن المعالجة ويتعلق بـ: **سرية وسلامة المعالجات الذي يمكن اختصار أهم ما جاء به في الآتي:**

- الالتزام بوضع التدابير التقنية والتنظيمية الملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف العرضي أو غير المشروع أو الضياع العرضي أو التلف أو النشر أو الولوج غير المرخصين، كما يجب أن تضمن هذه التدابير مستوى ملائما من السلامة بالنظر إلى المخاطر التي تمثلها المعالجة وطبيعة المعطيات الواجب حمايتها.
- يلزم المسؤول عن المعالجة والأشخاص الذين اطلعوا أثناء ممارسة مهامهم على معطيات ذات طابع شخصي بالسر المهني حتى بعد انتهاء مهامهم، تحت طائلة العقوبات المنصوص عليها في التشريع الساري المفعول.

هذا وبعد أن عرفنا ماذا يقصد بالبيانات ذات الطابع الشخصي والمخاطر التي تحدق بها، وبعد أن تطرقنا إلى حق الشخص المعني عند معالجة معطياته الشخصية وأهم التزامات المسؤول عن المعالجة، جدير بنا معرفة آليات حماية هذه المعطيات الإدارية والإجرائية والجزائية وذلك من خلال المحور الثاني.

المحور الثاني

الإطار القانوني لحماية المعطيات ذات الطابع الشخصي

سنحاول من خلال المحور الثاني إبراز الآليات الإجرائية والمؤسساتية والجزائية لحماية المعطيات ذات الطابع الشخصي.

أولا: المبادئ الأساسية لحماية المعطيات ذات الطابع الشخصي:

من خلال استقراء نصوص القانون 18-07 المنوه به أعلاه، نستشف من خلال التمعن في الباب الثاني منه، أن المشرع اعتبر أن الموافقة المسبقة شرط واقف على عملية معالجة المعطيات، كما حدد لهذه العملية إجراءات مسبقة يمكن إيجازها في التصريح والترخيص.

أ- شرط الحصول على المو افقة المسبقة والاستثناءات الواردة عليه:

بالرجوع إلى أحكام المادة السابعة من القانون 18-07 نجدها تنص على أنه: ""***لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلاّ بالمو افقة الصريحة للشخص المعني."***

حيث إن النص المنوه به أعلاه جاء صريحا في جعل القيام بمعالجة المعطيات يتوقف على شرط الموافقة الصريحة التي لا تثير أي لبس، حتى أن النص استهل بـ: لا يمكن القيام ....وهذا نفي قطعي، ثم نص إلاّ بالموافقة الصريحة، وإلاّ هنا ظرف لما يستقبل من الزمان تتضمن معنى الشرط، ما يفيد أن المشرع حسم بصفة قطعية في ضرورة حصول المعالج على موافقة مسبقة لصاحب المعطيات.

حتى أن المشرع ذهب أبعد من ذلك في الحماية، فقد مكن ورخص للشخص المعني التراجع عن موافقته في أي وقت.[16]

كما أحال على القواعد العامة حالة الشخص المعني العديم أو الناقص الأهلية.[17]

أمّا بخصوص معالجة المعطيات ذات الطابع الشخصي المتعلقة بطفل، فإن القيام مقترن بالحصول على موافقة ممثله الشرعي أو بترخيص من القاضي المختص، ولهذا الأخير الترخيص حتى دون موافقة ممثله الشرعي تحقيقا لمصلحة الطفل الفضلى.[18]

وبما أن لكل قاعدة استثناء، فإن موافقة الشخص المعني ترد عليها استثناءات تناولتها المادة 07 المنوه بها أعلاه في الفقرة 05 وما يليها وهي:

- لاحترام التزام قانوني يخضع له الشخص المعني أو المسؤول عن المعالجة،
- لحماية حياة الشخص المعني،
- لتنفيذ عقد يكون الشخص المعني طرفا فيه، أو لتنفيذ إجراءات سابقة للعقد اتخذت بناء على طلبه،
- للحفاظ على المصالح الحيوية للشخص المعني، إذا كان من الناحية البدنية أو القانونية غير قادر على التعبير عن رضاه،

- لتنفيذ مهمة تدخل ضمن مهام الصالح العام أو ضمن ممارسة مهام السلطة العمومية التي يتولاها المسؤول عن المعالجة أو الغير الذي يتم اطلاعه على المعطيات،
- لتحقيق مصلحة مشروعة من قبل المسؤول عن المعالجة أو المرسل إليه مع مراعاة مصلحة الشخص المعني أو حقوقه وحرياته الأساسية.

ب- <u>الإجراءات المسبقة عن المعالجة:</u>

من خلال استقراء نصوص القانون 18-07 لا سيما المواد من 12 إلى 21 نستشف إن المشرع الجزائري قيّد معالجة المعطيات ذات الطابع الشخصي بإجراءات مسبقة يتعيّن القيام بها، تتمثل في الحصول على تصريح مسبق لدى السلطة الوطنية أو لترخيص منها.[19]

01- **<u>التصريح المسبق</u>**:

رتب المشرع على المسؤول عن المعالجة التزاما بالحصول على تصريح المسبق يودع لدى السلطة الوطنية، ويمكن إرساله عن طريق البريد الإلكتروني، على أن تسلمه هذه الأخيرة فورا أو تقوم بإرساله إلكترونيا في غضون 48 ساعة.[20]

ويجب أن يتضمن التصريح المسبق ما يلي:[21]

- اسم وعنوان المسؤول عن المعالجة وعند اقتضاء اسم وعنوان ممثله،
- طبيعة المعالجة وخصائصها والغرض أو الأغراض المقصودة منها،
- وصف فئة أو فئات الأشخاص المعنيين والمعطيات أو فئات المعطيات ذات الطابع الشخص المتعلقة بهم.
- المرسل إليهم أو فئات المرسل إليهم الذين قد توصل إليهم المعطيات.
- طبيعة المعطيات المعتزم إرسالها إلى دول أجنبية.
- مدة حفظ المعطيات.
- المصلحة التي يمكن للشخص المعني عند الاقتضاء، أن يمارس لديها الحقوق المخولة له بمقتضى أحكام القانون رقم 18-07 وكذا الإجراءات المتخذة لتسهيل ممارسة هذه الحقوق.
- وصف عام يمكن من تقييم أولي لمدى ملائمة التدابير المتخذة من أجل ضمان سرية وأمن المعالجة.
- الربط البيني أو جميع أشكال التقريب الأخرى بين المعطيات، وكذا التنازل عنها للغير أو معالجتها من الباطن، تحت أي شكل من الأشكال، سواء مجانا أو بمقابل.

والجدير بالإشارة كذلك أن أي تغيير يحدث يمكنه المساس بهذه المعلومات حسب البيانات المنوه بها أعلاه، يستوجب الإخطار الفوري للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي لا سيما في حالة أي حذف يطال المعالجة.[22]

02- <u>الترخيص المسبق:</u>

إن المشرع الجزائري وإضفاء وتكريسا لحماية أكبر للمعطيات ذات الطابع الشخصي عند المعالجة، أخضع المعالجات التي يتضح عند دراسة التصريح المسبق أنها تتضمن أخطار ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص، حيث تقوم السلطة الوطنية باتخاذ قرار مسبب يبلغ إلى المسؤول عن المعالجة في غضون العشرة أيام التي تلي تاريخ إيداع التصريح.[23]

ورغم أنه يمنع معالجة المعطيات الحساسة كأصل، بيد أنه يمكن الترخيص بمعالجتها لأسباب تتعلق بالمصلحة العامة وتكون ضرورية لضمان ممارسة المهام القانونية أو النظامية للمسؤول عن المعالجة، أو عندما تتم المعالجة بناء على الموافقة الصريحة للشخص المعني، وفي حالة وجود نص قانوني يقضي بذلك أو بترخيص من السلطة الوطنية، كما نص القانون على حالات أخرى يمكن الحصول فيها على ترخيص من السلطة الوطنية.[24]

<u>ثانيا: الآليات المؤسساتية والجزائية لحماية المعطيات ذات الطابع الشخصي</u>

إن المعطيات ذات الطابع الشخصي، يتمتع صاحبها كما أسلفنا القول في المحور الأول بالحق في حمايتها، لا سيما أن هذا الحق اعتبره المؤسس الدستوري حق أساسي يحميه القانون، فكان لازما عند استحداث القانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي، التفكير في آليات جديرة بحماية هذه المعطيات، سواء من الناحية الإجرائية كما أسلفنا القول في النقطة الأولى من هذا المحور، أو من الناحية الإدارية أو الجزائية التي سنتناولها في نقطتين متتاليتين.

أ- <u>السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:</u>

لقد استحدث المشرع الجزائري في الباب الثالث من القانون 18-07 آلية تتمثل في السلطة الوطنية لحماية العطيات ذات الطابع الشخصي، حيث نصت المادة 22 من ذات القانون أنه تنشأ لدى رئيس الجمهورية، سلطة إدارية مستقلة لحماية العطيات ذات الطابع الشخصي، تتمتع بالشخصية المعنوية والاستقلال المالي والإداري.

وتتشكل السلطة الوطنية من ثلاث شخصيات من بينهم الرئيس يختارهم رئيس الجمهورية من بين ذوي الاختصاص في مجال عملها، وثلاثة قضاة يقترحهم المجلس الأعلى للقضاء من بين قضاة المحكمة العليا ومجلس الدولة، وعضو من كل غرفة من البرلمان يختاره رئيس الغرفة بعد التشاور مع رؤساء المجموعات البرلمانية، ممثل عن المجلس الوطني لحقوق الإنسان، ممثل عن وزير الدفاع

الوطني، ممثل عن وزير الشؤون الخارجية، ممثل عن الوزير المكلف بالداخلية، ممثل عن وزير العدل، ممثل عن الوزير المكلف بالبريد والمواصلات السلكية واللاسلكية والتكنولوجيا والرقمنة، ممثل عن وزير الصحة، ممثل عن وزير العمل والتشغيل والضمان الاجتماعي.

هذا ويتم اختيار أعضاء السلطة الوطنية حسب اختصاصهم القانوني أو التقني في مجال معالجة المعطيات ذات الطابع الشخصي، كما يمكن للسلطة أن تستعين بأي شخص مؤهل من شأنه مساعدتها في أشغالها، ويعين أعضاء السلطة الوطنية بموجب مرسوم رئاسي لمدى خمس سنوات قابلة للتجديد.[25]

وبموجب المرسوم الرئاسي رقم 22-187 الصادر في 18 ماي 2022، تم تعيين أعضاء السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي لعهدة مدتها خمس سنوات.[26]

وفيما يلي سنقتصر في هذه الدراسة على مهام وصور الجزاءات الإدارية للسلطة الوطنية.

01- <u>مهام السلطة الوطنية لحماية المعطيات</u>:

بالرجوع إلى القانون 18-07 فإن السلطة الوطنية تتولى مهام متعددة لحماية المعطيات ذات الطابع الشخصي، حيث تكلف السلطة بالسهر على مطابقة معالجة المعطيات لأحكام ذات القانون، وضمان عدم المساس بحقوق الأشخاص وحرياتهم العامة وحياتهم الخاصة،[27] وقد حددت المادة 25 من نفس القانون مهام السلطة الوطنية، حيث يمكن إيجازها في الآتي:[28]

- منح التراخيص وتلقي التصريحات المتعلقة بمعالجة المعطيات ذات الطابع الشخصي.
- إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم.
- تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي، أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة،
- تلقي الاحتجاجات والطعون والشكاوى بخصوص تنفيذ معالجة المعطيات ذات الطابع الشخصي وإعلام أصحابها بمآلها.
- الترخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا للشروط المنصوص عليها في هذا القانون.
- الأمر بالتغييرات اللازمة لحماية المعطيات ذات الطابع الشخصي.
- الأمر بإغلاق معطيات أو سحبها أو إتلافها.
- تقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي لمعالجة المعطيات ذات الطابع الشخصي.

- نشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني المشار إليه في المادة 28 من هذا القانون.
- تطوير علاقات التعاون مع السلطات الأجنبية المماثلة مع مراعاة المعاملة بالمثل.
- إصدار عقوبات إدارية وفقا لأحكام المادة 46 من القانون 18-07.
- وضع معايير في مجال حماية المعطيات ذات الطابع الشخصي.
- وضع قواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات ذات الطابع الشخصي.

كما أن السلطة الوطنية وفي إطار ممارسة مهامها تعلم النائب العام المختص فورا في حالة معاينتها لوقائع تحمل الوصف الجزائي، كما أن السلطة الوطنية تعد سنويا تقريرا عن نشاطها ترفعه إلى رئيس الجمهورية.

02- <u>الجزاءات الإدارية للسلطة الوطنية:</u>

تتمتع السلطة الوطنية لحماية المعطيات بصلاحية اتخاذ إجراءات إدارية في حق المسؤول عن المعالجة لا سيما في حالة خرقه لأحكام القانون 18-07، وهذا ما تناولته المواد 46، 47، و48 من نفس القانون، ويمكن حصر الجزاءات الإدارية التي تتخذها السلطة الوطنية في الآتي:

- الإنذار
- الإعذار
- السحب المؤقت لمدة لا تتجاوز سنة، أو السحب النهائي لوصل التصريح أو للترخيص.
- الغرامة،

وما تجدر الإشارة إليه في هذا المقام أن قرارات السلطة الوطنية قابلة للطعن أمام مجلس الدولة.

وتقدر الغرامة ب500.000دج يتم إصدارها ضد المسؤول عن المعالجة الذي يرفض دون سبب شرعي حقوق الإعلام والولوج أو التصحيح أو الاعتراض، أو يرفض التبليغ المنصوص عليه في المواد 04 و14 و16 من القانون 18-07.

والجدير بالذكر أن المشرع رتب على حالة العود عقوبات جزائية حسب المادة 64 من نفس القانون.

ب- <u>الحماية الجزائية للمعطيات ذات الطابع الشخصي:</u>

نظرا لحرمة الحياة الخاصة والحق في حماية الخصوصية، فإن الإجراءات والآليات الإدارية تبقى قاصرة في تكريس أكبر حماية، لذلك رتب القانون 18-07 عقوبات جزائية على العديد من الأفعال التي تشكل خرقا للقواعد التي يتعين مراعاتها عند معالجة المعطيات ذات الطابع

الشخصي، رغم أن المساس بأنظمة المعالجة الآلية للعطيات استحدث له المشرع سبع مواد في تعديل قانون العقوبات لسنة 2004 بموجب القانون 04-15 في المواد 394 مكرر إلى 394 مكرر7، إلاّ أن القانون الخاص بحماية المعطيات ذات الطابع الشخصي 18-07 مثلما حدد قواعد المعالجة وإجراءاتها جرم مخالفتها ورتب عليها جزاءات نحاول تبيانها في هذا الجزء من الدراسة، حيث يمكن تقسيمها إلى جرائم ماسة بالقواعد الموضوعية للمعالجة، وجرائم ماسة بالقواعد الإجرائية الشكلية للمعالجة.[29]

01- <u>الجرائم الماسة بالقواعد الموضوعية للمعالجة:</u>

لقد جرم المشرع الجزائري الأفعال التي تشكل خرقا للقواعد الواجب مراعاتها عند القيام بالمعالجة، لا سيما منها المعالجة غير المشروعة والاستعمال غير المشروع للمعطيات.

1-01 <u>جريمة المعالجة غير المشروعة للمعطيات ذات الطابع الشخصي:</u>

لقد رتبت المواد 57 و58 و59 و2/65 المسؤولية الجزائية على كل من ارتكب إحدى صور المعالجة غير المشروعة للمعطيات، فقد نصت المادة 57 على أنه يعاقب من سنتين إلى خمس سنوات وبغرامة من 200.000دج إلى 500.000دج كل من قام .....وفي غير الحالات المنصوص عليها في هذا القانون، بمعالجة المعطيات الحساسة.

كذلك تناولت المادة 58 من نفس القانون معاقبة كل من قام بإنجاز أو استعمال معالجة معطيات لأغراض أخرى غير تلك المصرح بها أو المرخص بها بالحبس من 06 أشهر إلى سنة، وبغرامة من 60.000دج إلى 100.000دج.

كما رتبت المادة 59 من نفس القانون عقوبة الحبس من 1 سنة إلى 3 سنوات وغرامة من 100.000دج إلى 300.000دج كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة.

كما أن الفقرة الثانية من المادة 65 من نفس القانون حملت كل من يقوم بالاحتفاظ بالمعطيات ذات الطابع الشخصي بعد المدة المنصوص عليها في التشريع الساري المفعول أو تلك الواردة في التصريح أو الترخيص، غرامة من 200.000دج إلى 500.000دج.

2-01 <u>جريمة الاستعمال غير المشروع للمعطيات:</u>

تقوم جريمة الاستعمال غير المشروع للمعطيات ذات الطابع الشخصي عندما يتسبب أو يسهل ولو عن إهمال، الاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو يوصلها إلى غير المؤهلين لذلك، المسؤول عن المعالجة وكل معالج من الباطن وكل شخص مكلف بالنظر إلى مهامه، بمعالجة معطيات ذات طابع شخصي، ويعاقب بالحبس من 01 سنة إلى 5 سنوات وبغرامة من 100.000دج إلى 500.000دج.[30]

01-3- الجرائم المرتبطة بحقوق الشخص المعني:

إن الشخص المعني بمعالجة المعطيات ذات الطابع الشخصي يتمتع بحقوق سبق الإشارة إليها في الجزء الأول من هذه الدراسة، وهذه الحقوق رتب المشرع كذلك جزاءات على كل اعتداء يطالها واعتبره فعلا مجرما، ومن بين صور هذه الجرائم ما تناولته المادة 55 من القانون 18-07 التي خصت كل من يقوم بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 07 من القانون 18-07 بعقوبة تتراوح من سنة إلى 3 سنوات وغرامة من 100.000دج غلى 300.000دج.

كما رتبت ذات المادة نفس العقوبة على من يقوم بمعالجة المعطيات ذات الطابع الشخصي رغم اعتراض الشخص المعني، لا سيما عندما تستهدف المعالجة الإشهار التجاري أو عندما يكون الاعتراض مبنيا على أسباب غير مشروعة.

02- الجرائم الماسة بالقواعد الإجرائية الشكلية للمعالجة:

مثلما رأينا في ما سبق أن معالجة المعطيات ذات الطابع الشخصي مقترنة بضرورة احترام جملة من القواعد الإجرائية المسبقة وكذا ضرورة احترام بعض الشكليات، والتي رتب المشرع على مخالفتها عقوبات جزائية.

1-02- الجرائم المتعلقة بالإجراءات المسبقة عن المعالجة:

لقد أسلفنا القول أن معالجة المعطيات يتطلب تقديم تصريح أو الحصول على ترخيص مسبق امتثالا لأحكام المادة 12 من القانون 18-07، ومخالفة هذه الأحكام يؤدي إلى قيام المسؤولية الجزائية، حيث رتبت المادة 56 من نفس القانون على مخالفة أحكام المادة 12 عقوبة بالحبس من سنتين إلى خمس سنوات وبغرامة من 200.000دج إلى 500.000دج.[31] كما رتب المشرع في ذات المادة نفس العقوبة على القيام بالتصريحات الكاذبة أو مواصلة معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح.[32]

2-02- جريمة نقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية دون ترخيص:

جرمت المادة 67 من القانون 18-07 نقل المعطيات ذات الطابع الشخصي نحو دولة أجنبية مخالفة لأحكام المادة 44 التي قيّدت هذا الإجراء بالحصول المسبق على ترخيص من السلطة الوطنية، حيث أقرت عقوبة تتراوح من سنة إلى خمس سنوات وغرامة من 500.000دج إلى مليون دينار جزائري.

3-02- الجرائم المتعلقة بإجراءات الحماية والتعاون مع السلطة:

من خلال استقراء نصوص القانون 18-07 يتضح لنا أن المشرع حث من خلال أحكامه كل مسؤول عن معالجة المعطيات ذات الطابع الشخصي بضرورة التقيّد بمجموعة من الإجراءات من أجل حماية المعطيات محل المعالجة، وفي المقابل كل إغفال أو تقصير يقيم المسؤولية الجزائية

لصاحبه، ومن بين أهم التدابير والإجراءات التي نص عليها القانون، ضرورة التعاون مع السلطة الوطنية التي يشكل الإخلال به جريمة يعاقب عليها القانون.[33]

وقد نصت المادة 61 من القانون 18-07 أنه يعاقب بالحبس من 06 أشهر إلى سنتين وبغرامة من 60.000دج إلى 200.000دج أو لإحدى هاتين العقوبتين فقط، كل من عرقلة عمل السلطة الوطنية بالاعتراض على إجراء عملية التحقيق في عين المكان أو عن طريق رفض تزويد أعضائها أو الأعوان الذين وضعوا تحت تصرفها بالمعلومات والوثائق الضرورية لتنفيذ المهمة الموكلة لهم من طرف السلطة الوطنية أو إخفاء أو إزالة الوثائق أو المعلومات المذكورة، أو عن طريق إرسال معلومات غير مطابقة لمحتوى التسجيلات وقت تقديم الطلب أو عدم تقديمها بشكل مباشر وواضح.

كما تناولت المادة 66 من نفس القانون أن نقدم الخدمات الذي يمتنع عن إعلام السلطة الوطنية والشخص المعني بكل انتهاك للمعطيات الشخصية خلافا لأحكام المادة 43، يعاقب بالحبس من سنة إلى 3 سنوات أو بغرامة من 100.000دج إلى 300.000دج.

خاتمة

يمكن القول في خاتمة هذه الورقة البحثية موضوع المداخلة، أن المشرع الجزائري كرس أقصى حماية للشخص المعني عند معالجة معطياته ذات الطابع الشخصي، بداية بالنص عليها ضمن القواعد العامة بما أنها تدخل ضمن الحياة الخاصة والحق في الخصوصية، ثم ساير العصر الذي أصبح يصطلح عليه بالعصر الرقمي، ودستر الحق في حماية المعطيات ذات الطابع الشخصي واعتبره حق أساسي يحميه القانون، وفي نفس السياق ساير القانون الدستور وبصدور القانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي، الذي كرس للشخص المعني حقوق وحمل المسؤول عن المعالجة التزامات، واستحدث السلطة الوطنية لحماية المعطيات كآلية مؤسساتية، وأحاط هذه الحماية للمعطيات ذات الطابع الشخصي بأحكام إدارية وأخرى جزائية.

وقد توصلنا من خلال هذه الورقة البحثية إلى النتائج التالية:

01- أن الحق في حماية المعطيات ذات الطابع الشخصي حق أساسي دستوري يحميه القانون.

02- أن حماية المعطيات ذات الطابع الشخصي ترتبط بالحق في حرمة الحياة الخاصة التي أصبح يتعرض لانتهاكات خاصة على مواقع التواصل الاجتماعي.

03- أن القانون 18-07 يشكل الإطار المرجعي الذي يحدد حماية المعطيات ذات الطابع الشخصي.

04- أن القانون 18-07 رغم أنه نص على المعالجة الآلية وغير الآلية إلاّ أن نصوصه جلها تتعلق بالمعالجة الآلية للمعطيات.

05- أن القانون 18-07 استحدث سلطة وطنية تعنى بالرقابة في مجال معالجة المعطيات.

06- أن الاعتداء على المعطيات الشخصية وعدم احترام الإجراءات في المعالجة يرتب عقوبات تتراوح بين الحبس والغرامة.

ومن خلال هذه الدراسة يمكن اقتراح التوصيات التالي:

01- الإسراع في إصدار النصوص التنظيمية للقانون 18-07.

02- الإسراع في تنصيب السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، لا سيما بعدما تم تعيين أعضائها.

03- إنشاء سجل إلكتروني وأرضية رقمية تستقبل فيها الشكاوى.

04- العمل على إنشاء مركز وطني للبيانات « Data Center » لتكريس حماية حقيقية للمعلومات ذات الطباع الشخصي بجعل تخزينها وطنيا وليس دوليا.

05- القيام بحملات توعوية وتكوينية للهيئات والمؤسسات ذات العلاقة بمعالجة المعطيات الشخصية، كشركات الاتصالات، والبنوك، والإدارات العمومية...

الهوامش

[1] جاء نص المادة 12 من الإعلان العالمي لحقوق الإنسان كالآتي: *" 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 مثل ذلك التدخل أو تلك الحملات."*

[2] جاء نص المادة 17 من العقد الدولي المتعلق بالحقوق المدنية والسياسية كالآتي: "لا يحوز تعريض أي شخص، على نحو تعسفي أو غير قانوني، لتدخل في خصوصياته أو شؤون أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته.
من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس."

[3] لمزيد من التفاصيل حول المفوضية السامية لحقوق الإنسان والخصوصية في العصر الرقمي، تصفح الرابط التالي:
https://www.ohchr.org/ar/privacy-in-the-digital-age

[4] عرفت المادة الثالثة من القانون 18-07 الشخص المعني بأنه "كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة".

[5] انظر المادة 3 فقرة 01 من القانون 17-08 مؤرخ في 25 رمضان عام ١٤٣٩ الموافق 10 يونيو 2018، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر عدد 34 لسنة 2018.

[6] المرجع نفسه، فقرة 03.

[7] المرجع نفسه، فقرة 05.

[8] « GDPR » : Le règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE dit règlement général sur la protection des données (RGPD, ou encore GDPR, de l'anglais *General Data Protection Regulation*), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel General Data Protection Regulation, Règlement général sur la protection des données. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

[9] للاطلاع على اللائحة العامة لحماية البيانات، ترجمة الدكتور مصطفى عبيد، انظر الرابط التالي:

https://www.mdrscenter.com/اللائحة-العامة-لحماية-البيانات-gdpr/

[10] عبد السلام طوبال ومنى غبولي، الضمانات القانونية لحماية المعطيات ذات الطابع الشخصي في التشريع الجزائري "دراسة على ضوء القانون 18-07، مجلة العلوم القانونية والاجتماعية، المجلد الخامس، العدد الثاني، جوان 2020، ص265، انظر أيضا: حميسي رضا، الضمانات القانونية لحماية البيانات الشخصية في الفضاء الرقمي، VOL 1 SUPPLEMENTARY 3 | SPECIAL EDITION-INPAC، ص 51-71.

[11] نزيهة علال، الإطار القانوني لحماية المعطيات ذات الطابع الشخصي في الفضاء الإلكتروني في ظل القانون 18-07، دائرة البحوث والدراسات القانونية والسياسية، المجلد 04، العدد 02، لسنة 2020، ص 54.

[12] المرجع نفسه، ص55.

[13] المرجع نفسه ص56.

[14] عرف القانون 18-07 الشخص المعني في الفقرة الثانية من المادة الثالثة بنصها: "الشخص المعني" كل شخص طبيعي تكون المعطيات ذات الطابع الشخصي المتعلقة به موضوع معالجة".

[15] انظر المادة 36 من القانون 18-07 المتعلق بحماية المعطيات ذات الطابع الشخصي.

[16] انظر الفقرة الثالثة من المادة 07 من القانون 18-07.

[17] المرجع نفسه، الفقرة الثانية.

[18] انظر المادة الثامنة من القانون 18-07.

[19] انظر نص المادة 12 من القانون 18-07.

[20] انظر الفقرة الأولى والثانية من المادة 13 من القانون 18-07.

[21] انظر المادة 14 من القانون 18-07.

[22] كحلاوي عبد الهادي وبن زيطة عبد الهادي، آليات حماية المعطيات ذات الطابع الشخصي، في ظل القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، مجلة القانون والعلوم السياسية، المجلد 07، العدد 02، سنة 2021، ص 118.

[23] انظر المادة 17 من القانون 18-07.

[24] تناولت المادة 18 من القانون 18-07 حالات أخرى للترخيص تناولتها الفقرة الرابعة وما يليها: "... يمنح الترخيص بمعالجة المعطيات الحساسة أيضاء في الحالات الآتية:

أ) إذا كانت المعالجة ضرورية لحماية المصالح الحيوية للشخص المعنى أو لشخص آخر وفي حالة وجود الشخص المعني في حالة عجز بدني أو قانوني عن الإدلاء بموافقته.

ب) تنفيذ المعالجة، بناء على موافقة الشخص المعني، من طرف مؤسسة أو جمعية أو منظمة غير نفعية ذات طابع سياسي أو فلسفي أو ديني أو نقابي، في إطار نشاطاتها الشرعية، شرط أن تخص المعالجة فقد أعضاء هذه المنظمة أو الأشخاص الذين تربطهم بها اتصالات منتظمة تتعلق بغايتها وإلاّ ترسل المعطيات إلى الغير دون موافقة الأشخاص المعنيين.

ج) إذا كانت المعالجة تخص معطيات صرح بها الشخص المعني علنا عندما يمكن استنتاج موافقته على معالجة المعطيات من تصريحاته
د) أن المعالجة ضرورية للاعتراف بحق أو ممارسته أو الدفاع عنه أمام القضاء وأن تكون قد تمت حصريا لهذه الغاية.
هـ) معالجة المعطيات الجينية، باستثناء تلك التي يقوم بها أطباء أو بيولوجيون والتي تعد ضرورية لممارسة الطب الوقائي ، والقيام بتشخيصات طبية وفحوصات أو علاجات.
وفي كل الأحوال، تبقى التدابير المنصوص عليها في هذا القانون لحماية هذه المعطيات، مضمونة.

[25] للتفصيل أكثر في طريقة اختيار وتنصيب أعضاء السلطة الوطنية، انظر الباب الثالث من القانون 18-07 لا سيما المواد 22 وما يليها، انظر كذلك: خالدي فتيحة، السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي كآلية لحماية الحق في الخصوصية في ظل القانون 18-07، مجلة الحقوق والعلوم الإنسانية، المجلد 13، العدد 04 لسنة 2020، ص 46-57. انظر كذلك: مشتة نسرين، بن عبيد إخلاص، الحماية القانونية للمعطيات الشخصية في ظل القانون 07/18 المتعلق بحماية المعطيات ذات الطابع الشخصي، المجلة الجزائرية للحقوق والعلوم السياسية، المجلد 06، العدد 01 لسنة 2021، ص 675-690.

[26] بموجب المادة الأولى من المرسوم الرئاسي 22-187 فإن أعضاء السلطة الوطنية هم: السيّد لطفي بوجمعة رئيسا، والسآدة: جمال الدين قاراوي، بوعلام حسان، محمد درفوف، أرزقي مسلوب، السعيد عميور، توفيق قزوط، محمد العيد بلاغ، سهيلة قمودي، بن اعمر عليوة، فريد وحيد دحمان، عبد القادر زرق الراس، مهمر بلايلية، لعرج زروقي، موهوب مسعودي، بوعلام عيساوي، أعضاء.

[27] كاملة بوعكة، الحماية القانونية للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في ضوء القانون 18-07، المجلة الجزائرية لقانون الأعمال، العدد الثاني، ديسمبر 2020، ص 60.

[28] انظر المادة 25 من القانون 18-07.

[29] انظر لمزيد من التفصيل حول الحماية الجزائية للمعطيات ذات الطابع الشخصي: طباش عز الدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري "دراسة في ظل قانون 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، العدد 02، 2018، ص 26-60.

[30] انظر نص المادة 69 من القانون 18-07.

[31] انظر المادة 56 الفقرة الأولى من القانون 18-07.

[32] المرجع نفسه الفقرة الثانية.

[33] كاملة بوعكة، المرجع السابق، ص65.

حمـاية البيـانـات الشخـصـية في الـمعـاملات الإلكتـرونية بـموجـب التشريـع الجزائري

The protection of personal data in the light of the electronic transactions in Algerian legislation

ط.د/ رحيل سمير

جامعة الجزائر1- بن يوسف بن خدة

الجزائر

Samirrahil8235@gmail.com

ملخص:

توسع إستعمال الإنترنت نتيجة التطور الهائل الذي عرفه مجال النظم المعلوماتية، فظهرت البيئة الرقمية كمجتمع إفتراضي موازي للمجتمع الحقيقي الذي نعيشه، أين أصبح الإنسان يمارس مختلف معاملاته اليومية بسرعة و سهولة. في خضم هذا التطور الذي عرفه مجال المعاملات الإلكترونية إنتشرت البيانات الشخصية، هي بمثابة المادة الأولية لعلاقات الإنسان و معاملاته في العالم الإفتراضي. مقابل ذلك أصبحت تشكل خطرا على حياته الخاصة و باقي حقوقه و ممتلكاته، لاسيما أن التعامل بالبيانات الشخصية للأفراد يتم عبر الشبكات المفتوحة التي تحيطها الكثير من المخاطر و تطالها العديد من الإعتداءات، هذه الأعمال التي عرفت طفرة نوعية بإستخدام وسائل تكنولوجية متطورة. هو الأمر الذي جعل المشرع الجزائري و على غرار باقي التشريعات يقوم بتعديل قوانينه لمواكبة التطورات الحاصلة، كما قام بإستحداث قوانين خاصة من شأنها توفير حماية أكثر للبيانات الشخصية لمتعاملي العالم الإفتراضي.

الكلمات المفتاحية: الحماية القانونية؛ البيانات الشخصية؛ البيئة الرقمية؛ المعاملات الإلكترونية

Abstract:

The use of the Internet has expanded in the heels of the tremendous development in the field of information systems. As a consequence, a digital environment has emerged in the shape of a virtual parallel to the real society where people make daily transactions quickly and easily. Nevertheless, the advances made in the field of electronic transactions had some undesired after-effects as they resulted in the spread of

personal data which is considered as the pillar of all interactions and transactions on the internet. Owing to this, people's privacy, rights and properties have become jeopardized especially considering the fact that online transactions are carried out through open networks that are subjected to multiple risks and violations that have reach an all-time high due to the use of sophisticated technology. In the wake of this and similarly to other legislations, the Algerian legislator amended its laws to keep pace with these current developments and has additionally introduced special laws in the hope of protecting the personal data of internet users more effectively.

Keywords: legal protection; personal data; digital environment; electonic transactions.

مقدمة:

لا يزال التطور التكنولوجي يلقي بظلاله على كافة مجالات حياة الإنسان كنتيجة لما شهده العالم في السنوات الأخيرة من التطور الهائل للنظم المعلوماتية، الذي بدأ بثورة المعلومات ثم تلاه تطور وسائل الإتصالات الإلكترونية، هو تزاوج أثمر عنه ميلاد عملاق الإنترنت، حيث نشأ داخل هذه الشبكة العالمية مجتمع إفتراضي موازي للمجتمع الحقيقي الذي نعيشه، أين أصبح الشخص يمارس مختلف نشاطاته اليومية بكل سرعة و سهولة من مكانه، دون عناء التنقل.

في خضم هذا التطور الذي عرفه مجال الإتصالات و النظم المعلوماتية إنتشر التعامل بالبيانات الشخصية بمختلف أنواعها، فهي بمثابة المادة الأولية لتصرفات الإنسان داخل البيئة الرقمية، كما أنها تمثل هويته التي تمكنه من إقامة علاقات و معاملات مختلفة. في مقابل ذلك تعتبر هذه البيانات خطرا بالغا على الحياة الخاصة للفرد و حرمته الشخصية، لاسيما أن التعامل بهذه البيانات يتم عبر الشبكات المفتوحة التي تحيطها الكيثر من التهديدات و المخاطر.

من هنا تتجلى أهمية دراسة هذا الموضوع، حيث بات من الضروري إيجاد الحماية اللازمة لمتعاملي العالم الإفتراضي، في الوقت الذي تعددت فيه أشكال إنتهاكات خصوصية الأشخاص و الإعتداءات على بياناتهم، هذه الأعمال الإجرامية قد عرفت طفرة نوعية بالموازاة مع تطور النظم و الوسائل التكنولوجية المستخدمة في ذلك، هو الأمر الذي يثير مسألة التوفيق بين ضرورة و فائدة إستعمال الوسائل التكنولوجية، مع تفادي أضرار المساس بالحياة الخاصة للأفراد.

فلا يخفى على أحد اليوم أن كل تطور تقني له إنعكاساته السلبية بالإضافة إلى تحقيقه للأهداف التي أنشأ لأجلها، فبالقدر الذي سهلت فيه الوسائل التكنولوجية تنظيم البيانات الشخصية و التصرف فيها؛ بالقدر الذي سهلت معه إمكانية الحصول عليها و تجميعها من طرف الغير بهدف الإستغلال غير المشروع لها، مما يثير مسألة الثقة و الأمن المعلوماتي.

هذه الإشكالات أصبحت هاجسا يؤرق المشرعين عند تنظيم مجال المعاملات الإلكترونية، كما أن تعدد المخاطر و التهديدات التي تمسها جعلت المشرع الجزائري على غرار باقي التشريعات يسعى إلى تعديل قوانينه و إستحداث أخرى، أدرج ضمنها مختلف الإجراءات و الآليات القانونية لحماية البيانات الشخصية، و وضع حد للتعدي على حقوق الأفراد في الخصوصية.

و عليه نطرح الإشكالية التالية: ما هي الحماية القانونية التي وفرها المشرع الجزائري للبيانات الشخصية الإلكترونية؟ و ما مدى فعالية النصوص المستحدثة من أجل ذلك؟

تمت الإجابة على هذه الإشكالية إعتمادا على المنهج الوصفي، كونه يساعد في التعرف على مفهوم الموضوع و إظهار مختلف الجوانب المحيطة به، كما إعتمدنا كذلك على المنهج التحليلي من أجل تحليل النصوص القانونية و المادة العلمية المتعلقة بالموضوع.

حيث تمّ تقسيم الموضوع إلى مبحثين:

تطرقنا في المبحث الأول إلى: الحماية الدستورية و الجنائية للبيانات الشخصية، من خلال التعديلات التي جاء بها المشرع الجزائري في الدستور و قانون العقوبات.

أما المبحث الثاني فخصصناه لدراسة: حماية البيانات الشخصية في بعض القوانين الخاصة في مجال المعاملات الإلكترونية، أين تطرقنا إلى حماية البيانات الشخصية المتعلقة بالتوقيع الإلكتروني في القانون رقم 15-04[1]. ثم حماية هذه البيانات من جرائم الإتصالات الإلكترونية في القانون رقم 18-04.[2]

المبحث الأول: الحماية الدستورية و الجنائية للبيانات الشخصية

تناول المشرع الجزائري حماية البيانات الشخصية بشكل ضمني في إطار القواعد العامة لحماية الحياة الخاصة بالأفراد في الدستور و قانون العقوبات، بصورة تقليدية لم تعد كافية لمواجهة التطور التكنولوجي، لاسيما مع إنتشار المعاملات الإلكترونية في شتى الميادين؛ هو الأمر الذي تطلب القيام بعدة تعديلات في المنظومة القانونية حتى لمواكبة المستجدات.

لتوضيح ذلك خصصنا (المطلب الأول)لدراسة الحماية القانونية للبيانات الشخصية في الدستور الجزائري، ثم تطرقنا في (المطلب الثاني) إلى الحماية الجنائية لهذه البيانات في قانون العقوبات الجزائري.

المطلب الأول: الحماية البيانات الشخصية في الدستور الجزائري

من خلال الدساتير المتعاقبة، أولى المشرع الجزائري أهمية بالغة لحماية المعلومات الشخصية و سريتها، أين أضفى عليها الحماية القانونية ضمن القواعد العامة لحماية الحياة الخاصة للأفراد،[3] ثم طور مفهوم هذه الحماية إلى حماية المعطيات ذات الطابع الشخصي في مجال المعالجة الآلية للبيانات عند التعديل الدستوري لسنة 2016.

هذا ما سنتطرق إليه بشيء من التفصيل في الفرعين التاليين:

الفرع الأول: حماية الحياة الخاصة في دستور1996

من جانب البيانات الشخصية لم تكن حمايتها مجسدة في صورتها الحالية، بل أوردها المشرع في دستور 1996 بشكل ضمني في إطار الحق في الحياة الخاصة، بتكريس الحقوق و الواجبات الأساسية للأفراد و ضمانها بشكل عام.[4]

حيث نصت المادة 39من دستور 1996 على أنه: " لا يجوز إنتهاك حرمة حياة المواطن الخاصة، و حرمة شرفه، ويحميها القانون.

سرية المراسلات و الإتصالات الخاصة بكل أشكالها مضمونة".

لم يكتفي المشرع بالإعتراف لخصوصية الأفراد كحق مطلق يكفله و يحميه الدستور، بل إعتبره كذلك من الواجبات التي يلتزم الأفراد بمراعاتها عند ممارستهم لحقوقهم الأخرى، و أوجب المحافظة على الحياة الخاصة للأخرين بسترها.

حيث نصت المادة 63 من دستور 1996 على أنه: " يمارس كل واحد جميع حرياته، في إطار إحترام الحقوق المعترف بها للغير في الدستور، لاسيما إحترام الحق في الشرف، و ستر الحياة الخاصة..."

من خلال قراءة هذه النصوص يتضح أن المشرع لم يتطرق إلى حماية البيانات الشخصية الإلكترونية بشكل صريح و مفصل، إلا أنه أدرجها ضمن حقوق الشخص في سرية مراسلاته و إتصالاته بشكل عام، و ذلك بإقرار الحماية القانونية لكل أشكال الإتصالات و المراسلات بما فيها الإلكترونية، و التي تحمل في مضمونها بيانات إلكترونية شخصية.

كما أن المشرع جعل من الواجب إحترامها و الحفاظ عليها من طرف الآخرين في إطار ممارسة الحقوق العامة، و ذلك بعدم التعدي على خصوصية الأخرين، فحرية الفرد في التعبير و التعامل بمعلوماته يبقى مرتبطا بواجب الحفاظ على البيانات الشخصية لغيره.

و عليه يؤكد المشرع من هذا النص حماية الحياة الخاصة للأفراد بتوجهه إلى العمل بمبدأ تقييد التمتع بجميع الحقوق و الحريات التي إعترف بها للأفراد، وذلك بواجب ممارستها في نطاق الإحترام الحتمي للحقوق الشخصية و العامة.[5]

الفرع الثاني: تكريس حق الحماية بموجب التعديل الدستوري لسنة 2020

عند تعديل الدستور الجزائري سنة 2016، حاول المشرع مواكبة التطورات التكنولوجية،[6] لاسيما في مجال المعاملات الإلكترونية، أين أعطى إهتماما أكبر للبيانات الشخصية و كرّس حق حمايتها بإضافة فقرتين لمضمون المادة(39) المذكورة أعلاه، من خلال المادة (46)، حيث جعل المعطيات ذات الطابع الشخصي حقا أساسيا و مضمون .

كما أنه من خلال التعديل الدستوري الأخير لسنة 2020[7] ،أكد على أن الحق في حماية البيانات ذات الطابع الشخصي حق أساسي لكل شخص، و أي إنتهاك لهذا الحق يعاقب عليه القانون. حيث عدلت المادة (46) سابقا بالمادة (47) التي ورد في نصها أنه: "...حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي

يعاقب القانون على كل إنتهاك لهذه الحقوق".[8]

بهذا يكون المشرع قد إستدرك النقص الذي كان يعتري نص المادة (39) سابقا، كما أنه أضفى حماية أوفر للبيانات الشخصية الإلكترونية بالنص صراحة على حماية المعطيات ذات الطابع الشخصي، مع ضمان عدم المساس بها.

وعليه يعتبر تعديل هذا النص بمثابة إرتقاء تشريعي على مستوى القواعد العامة لحماية حقوق الإنسان، وتعزيزا لحماية البيانات الشخصية خصوصا.

تجدر الإشارة إلى أن الدستور الجزائري هو الوحيد من بين الدساتير العربية الذي تطرق لحرمة المعطيات الخاصة من المعالجة الإلكترونية، بحيث إكتفت جلها بتكريس الحماية الدستورية للمراسلات بكل أشكالها فقط.[9]

المطلب الثاني: الحماية الجنائية للبيانات الشخصية

يسعى المشرع الجزائري من خلال قانون العقوبات إلى حماية الأشخاص من مختلف الإعتداءات التي تلحق بهم، سواءا تلك التي تقع على حياتهم أو أموالهم وممتلكاتهم، أو تلك الأفعال التي تمس حياتهم الخاصة و سرية معلوماتهم. و تماشيا مع تطور إستخدام النظم المعلوماتية و إنتشار أعمال الإعتداءات على البيانات الرقمية، قام المشرع الجنائي بإستحداث عدة نصوص أدرجها في قانون العقوبات، حاول من خلالها التصدي للأفعال التي تمس بأنظمة المعالجة الآلية للمعطيات، كما قام بتعديل النصوص السابقة التي تجرم الإعتداء على الحياة الخاصة للأشخاص و أسرارهم.

على أساس هذا التقسيم سنتطرق في (الفرع الأول)إلى: حماية البيانات الشخصية من جرائم الأنظمة المعلوماتية، ثم نتطرق في(الفرع الثاني) إلى: الحماية الجنائية للحياة الخاصة.

الفرع الأول: حماية البيانات من جرائم الأنظمة المعلوماتية

تنبه المشرع الجزائري للأخطار و التهديدات التي تطال البيانات الرقمية في مجال المعاملات الإلكترونية، أين تطورت أعمال التعدي على الأنظمة المعلوماتية و المعطيات التي تعالجها، فحاول المشرع مواكبتها بتعديل قانون العقوبات سنة 2004 بموجب القانون رقم 04- 15،[10] حيث أدرج من خلاله القسم السابع مكرر بعنوان: "المساس بأنظمة المعالجة الآلية للمعطيات"، تضمن هذا القسم (08) ثمانية مواد (من المادة 394 مكرر إلى المادة 394 مكرر 7 ".

عند الإطلاع على محتوى هذه النصوص يتضح أن إستراتيجية المشرع الجزائري في التصدي لظاهرة الإجرام المعلوماتي قد ركزت على جملة من قواعد قانونية موضوعية حدد من خلالها الأفعال الماسة بنظم المعالجة الآلية للمعطيات و ما يقابلها من جزاء.

بالنسبة للجرائم المستحدثة في هذا القسم فتأخذ إما وصف الإعتداء على نظم المعالجة الآلية، أو وصف الإعتداء على معطيات أنظمة المعالجة الآلية، كما يمكن لها أن تأخذ وصف الإعتداء على سير نظام المعالجة الآلية للمعطيات.[11]

أما بالنسبة للأفعال التي تمس بالبيانات الشخصية التي أدرجها المشرع في هذا القسم ضمن الجرائم المعلوماتية، نذكرها فيما يلي:

- جريمة الدخول أو البقاء في منظومة المعالجة الآلية للمعطيات عن طريق الغش (المادة 394 مكرر)، و تقوم هذه الجريمة بمجرد الدخول غير المرخص به إلى المنظومة المعلوماتية بصفة كلية أو جزئية، بغض النظر عن الغاية من ذلك، سواءا لإستهداف البرامج أو بيانات التشغيل أو بيانات شخصية... أو غيرها من البيانات. حتى لو لم يقع ضرر أو منفعة منه، طالما أن الدخول غير مشروع.[12]

و تضاعف العقوبة في حالة وقوع حذف أو تغيير في معطيات المنظومة جراء ذلك الدخول، أي أنه تشديد العقوبة إذا ترتب عن ذلك تخريب نظام تشغيل المنظومة، و المقصود بالتخريب هنا هو تعطيل نظام تشغيل الحاسوب أو أحد برامجه، عن طريق إتلاف أو محو البيانات القاعدية التي يشتغل عليها، و يطلق على هذه الأفعال مصطلح تدمير النظم المعلوماتية.[13]

- جريمة إدخال معطيات في نظام المعالجة الآلية، أو إزالة أو تعديل المعطيات التي تتضمنها المنظومة المعلوماتية(المادة 394 مكرر1).

- جريمة إستعمال الأنظمة المعلوماتية و المعطيات المتحصل عليها بغرض القيام بأفعال مجرمة(المادة 394 مكرر2)، و تقوم هذه الجريمة حسب النص من خلال تصميم أو تجميع أو توفير أو نشر أو معالجة أو إرسال أو المتاجرة في معطيات أو منظومة معلوماتية بغرض إرتكاب إحدى الجرائم المعلوماتية .

كما تجرم هذه المادة حيازة أو إفشاء أو نشر أو إستعمال المعطيات المتحصل عليها عن طريق الجرائم المنصوص عيلها في هذا القسم.

- جريمة المشاركة و الإعداد لإرتكاب جرائم معلوماتية (المادة 394 مكرر5)، فتجرم بذلك كل أعمال المساهمة و الإشتراك في إرتكاب إحدى الجرائم المعلوماتية، أو الإتفاق بغرض الإعداد للقيام بها.

أما بخصوص الجزاءات فقد رتب المشرع من خلال هذا القسم عقوبات محددة لكل جريمة ترتكب بالحبس ما بين (02) شهرين إلى (03) ثلاث سنوات، مع غرامات مالية تتراوح ما بين (50) خمسين ألف دج إلى (05) خمس ملايين دج.

و بالنسبة للشخص المعنوي فرتب له عقوبة الغرامة، تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي (المادة 493 مكرر4).

عند إستقراء نصوص هذه المواد المستحدثة يتضح أن المشرع لم يتطرق صراحة إلى الجرائم الإلكترونية التي تمس بالبيانات الشخصية، و إنما جرم كل أنواع الإعتداءات التي تستهدف الأنظمة المعلوماتية و البيانات التي تحتويها، و منه فقد جاءت صياغة هذه النصوص بمصطلحات واسعة حتى يمكن تطبيقها على كافة أشكال الأفعال التي تشملها الجريمة المعلوماتية. كما أنها لم تحدد نوعية المعطيات التي تمسها هذه الجرائم، فيما إذا كانت متصلة بمصالح شخصية أو تجارية أو فكرية... و الهدف من ذلك أن المشرع يسعى إلى تعميم الحماية القانونية للمعطيات الإلكترونية بكافة أنواعها، و التي تدخل ضمنها البيانات الشخصية، ذات القيمة المادية و المعنوية.

كما يمكن القول أن هذه النصوص القانونية الخاصة قد أوجدت حلولا للعديد من الإشكالات حول مدى تطبيق النصوص التقليدية العامة في جرائم إتلاف البيانات الإلكترونية[14] و سرقتها، نظرا للطبيعة غير المادية لهذه البيانات؛ حيث أن تطبيق النصوص التقليدية كان يصطدم بمبدأ الشرعية و صعوبة إثبات تحقق الركن المادي لأفعال الإتلاف و السرقة.

لكن بصدور هذه النصوص يكون المشرع قد وضع حدا للمشاكل التي كان يواجهها القضاء في سبيل معاقبة مرتكبي جرائم سرقة و إتلاف البيانات الرقمية الخاصة بالغير.

الفرع الثاني: الحماية الجنائية للحياة الخاصة

بعد تفشي أشكال الجرائم الحديثة لإنتهاك خصوصية الأشخاص، التي تهدد حياتهم الخاصة و سريتها عند إستعمالهم لخدمات التراسل و الإتصالات الإلكترونية، ظهر مفهوم جديد للحماية الأشخاص من مخاطر البيئة الإلكترونية؛ بات يعرف بحماية الخصوصية الرقمية،[15] أو أمن الخصوصية المعلوماتية.

و بهدف توفير حماية أكثر لهذه الخصوصية، و على غرار ما قامت به باقي التشريعات؛ عمد المشرع الجزائري إلى توسيع نطاق تجريم أفعال التعدي على الحياة الخاصة للأشخاص من خلال تعديل قانون العقوبات سنة 2006. حيث تمّم و عدل القسم الخامس المعنون ب: " الإعتداء على شرف و إعتبار الأشخاص و حياتهم الخاصة و إفشاء الأسرار"، بموجب القانون رقم 06-23.[16]

من خلا هذا التعديل توسعت الحماية القانونية للبيانات الإلكترونية للأشخاص في لإطار حماية الحق في الخصوصية، حيث تعتبر هذه البيانات جوهر و أساس الحق في الحياة الخاصة؛

نظرا لما تحتويه من معلومات سرية و خاصة، سواءاً تلك المتعلقة بممتلكات الأشخاص أو مراسلاتهم و محادثاتهم، أو حرمة عائلاتهم و صحتهم و صورهم...وغيرها

و بالرجوع لأحكام هذا القسم المعدل يمكن إستخلاص الأفعال المجرمة التي تمس بالبيانات الشخصية، من المواد (303)، (303مكرر)، (303مكرر1) و المادة (303مكرر3).

حيث جاء في نص المادة (303) أنه يعاقب كل من يفض أو يتلف رسائل أو مراسلات موجهة للغير.

نلاحظ أن المشرع تعمد عدم تحديد نوعية الرسائل، حتى يكون بإمكان هذا النص أن يستغرق كافة أنواعها، سواءا تلك التقليدية المكتوبة بخط اليد التي تحملها الأوراق، أو الرقمية التي تحتويها الدعامات الإلكترونية؛ و لم يحدد كذلك طريقة تراسلها، فينطبق الأمر على كل المراسلات الكلاسيكية التي تتم عن طريق البريد العادي، أو الإلكترونية التي تتم عبر الشبكات كالبريد الإلكتروني و مواقع التواصل الإجتماعي.

كما تجرم المادة (303مكرر) كل من تعمد المساس بالحياة الخاصة للأشخاص بأية تقنية مستخدمة لذلك، بإلتقاط أو تسجيل أو نقل مكالمات خاصة بغير إذن صاحبها، أو عن طريق إلتقاط أو تسجيل أو نقل صور لشخص في مكان خاص بدون إذنه.

إستعمل المشرع في هذا النص مصطلح "...بأية تقنية كانت" مواكبا بذلك تطور مفهوم حماية الحياة الخاصة، أين أصبحت الجرائم التي تمسها تتم بإستعمال وسائل و تقنيات تكنولوجية، فبالإضافة إلى أن المشرع تدارك هذا الوضع، يكون قد شمل كذلك التقنيات التي يمكن أن تظهر لاحقا مع التطور التكنولوجي.

و بخصوص الإستغلال غير المشروع للبيانات الخاصة بالأشخاص، فقد جاء تجريم هذه الأفعال في المادة (303مكرر1)، التي ورد في نصها أنه يعاقب كل من إحتفظ بمعلومات خاصة بالغير، كان قد تحصل عليها عن طريق الجرائم السابقة، وقام بإفشائها بأية وسيلة كانت. و يعاقب على الشروع في القيام بهذه الأفعال طبقا لهذه المادة، بنفس العقوبة المقررة للجريمة التامة.

بالإضافة للعقوبات المقررة للأشخاص الطبيعيين ، فقد جاء في المادة (303مكرر3) أنه تقوم المسؤولية الجزائية للشخص المعنوي عن الجرائم التي ترتكب لحسابه، طبقا للشروط المنصوص عليها في المادة 51مكرر، حيث يتعرض للعقوبات المنصوص عليها في المادة (18) من هذا القانون، كالغرامات المالية و الحل و الغلق و مصادرة الأجهزة و الوسائل... وغيرها من العقوبات التي تتناسب مع الطبيعة المعنوية لهذا الشخص.

يتضح مما سبق أن هذه النصوص تصلح للتطبيق على كافة الأفعال الماسة بالمعلومات المتعلقة بالحياة الخاصة، حيث جاءت صياغتها بمفهوم شامل و عام، كما أن ذكر الأفعال المجرمة ورد على سبيل المثال لا الحصر.

أما بالنسبة للجزاءات فقد رتب المشرع في هذا القسم عقوبات عن هذه الأفعال، تتراوح ما بين شهر و (03) ثلاث سنوات حبس، بالإضافة إلى غرامات مالية من (25) ألف دج إلى (300) ألف دج. تطبق هذه العقوبات بحسب كل جريمة مرتكبة و بحسب كل حالة.

المبحث الثاني: حماية البيانات الشخصية في التشريعات الخاصة

لسد الفراغ القانون الذي عرفه مجال الأمن المعلوماتي و قصور القواعد التقليدية في مواجهة التطور التقني السريع للنظم المعلوماتية، مع تطور أشكال التعدي على البيانات الشخصية في شكلها الإلكتروني، هو ما دفع المشرع الجزائري بالسعي إلى إصدار قوانين جديدة بهدف تحقيق حماية أوفر لهذا النوع من البيانات.

فبعد تعديل بعض القوانين على مستوى القواعد العامة، تبعها المشرع بإستحداث عدة قوانين خاصة في مجال المعلوماتية من شأنها تنظيم أحكام المعطيات الشخصية، كان أهما: القانون رقم 15-04 الذي يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، سنتعرض لأهم أحكامه المتعلقة بحماية البيانات الشخصية في (المطلب الأول).

و القانون رقم 18-04 الذي يحدد القواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية نتطرق له من خلاله إلى: الحماية من جرائم الإتصالات الإلكترونية في (المطلب الثاني).

المطلب الأول: حماية البيانات الشخصية في القانون رقم 15-04

بعد إعتراف المشرع الجزائري بالكتابة و التوقيع الإلكترونيين عند تعديله للقانون المدني سنة 2005،[17] تبع ذلك بجملة من النصوص القانونية التي تنظم و تحدد أحكام التعامل بها؛ فأصدر القانون رقم 15-04، الذي عرف من خلاله التوقيع الإلكتروني في المادة (02) على أنه: " بيانات في شكل إلكتروني، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق".[18]

و من منظور حماية البيانات الشخصية، يمكن تعريف هذا التوقيع على أنه مجموعة البيانات الإلكترونية الشخصية التي تحدد هوية الشخص و تمكنه من إقامة علاقات و معاملات في البيئة الرقمية، حيث ينفرد الموّقع بهذه البيانات و يتميز بها عن غيره من الأشخاص.

و لإضفاء الموثوقية على هذه البيانات و سلامة التعامل بها، جعل المشرع شهادة التصديق الإلكتروني كأساس لإنشاء هذا التوقيع و في نفس الوقت آلية للتحقق من صحته و سلامته.

حيث عرّفت المادة الثانية شهادة التصديق الإلكتروني بأنها:" وثيقة في شكل إلكتروني تثبت الصلة بين بيانات التحقق من التوقيع الإلكتروني و الموّقع".

و من هنا يتضح أن بيانات هذه الشهادة تبقى شخصية مادامت متعلقة ببيانات التوقيع و بيانات الشخص الموّقع، بالرغم من حيازتها لدى جهات التوثيق (جهات التحقق الإلكتروني).

نظرا لأهمية هذه البيانات و الدور الذي تلعبه في مجال المعاملات الإلكترونية، أحاطها المشرع الجزائري بالعناية اللازمة لمنع التعدي عليها و الإستعمال غير المشروع من الغير. لتوضيح ذلك سنتطرق في (الفرع الأول) إلى تدابير حماية بيانات التوقيع و التصديق الإلكترونيين، ثم نتعرض في (الفرع الثاني) إلى الجزاءات المقررة للأفعال الماسة بهذه البيانات.

الفرع الأول: تدابير حماية بيانات التوقيع و التصديق الإلكترونيين

تتجلى مظاهر حماية البيانات الشخصية في قانون 15-04 من خلال جملة الشروط الصارمة و الضوابط التقنية التي فرضها المشرع، و التي تخص عملية إنشاء التوقيع الإلكترونية و كذا إجراءات إصدار شهادة التصديق الإلكتروني؛ كتدابير وقائية و حماية قبلية للبيانات المتعلقة بها.

حيث جاء في المادة(08) من القانون المذكور أعلاه، أنه لا يعتد بالتوقيع الإلكتروني في مجال المعاملات الإلكترونية، إلا بالتوقيع الإلكتروني الموصوف.[19]

و هذا التوقيع حسب نص المادة(07) هو التوقيع الذي يجب أن تتوفر فيه مجموعة المتطلبات، نذكر أهمها:

أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة، أن تكون بياناته مرتبطة ببيانات الشخص الموقع وحده دون سواه، كما يجب أن يكون هذا التوقيع مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني، تجدر الإشارة إلى أن هذه الشروط قد إنفرد بها المشرع الجزائري عن غيره من التشريعات، التي لم تشر إلى شهادة التصديق الإلكتروني الموصوفة ضمن تعريف التوقيع الإلكتروني المؤمن.[20]

و من أجل موثوقية هذا التوقيع وسلامة بياناته، حدد المشرع في الفصل الثاني آليات إنشائه، بحيث يجب أن ينشأ التوقيع الإلكتروني الموصوف وفق آلية مؤمنة حسب الشروط و المتطلبات المنصوص عليها في المادة(11)، كما يجب أن ينشأ وفقاً لآلية تمكّن التحقق منه بصفة موثوقة طبقا للشروط المنصوص عليها في المادة(13).

من خلال الإطلاع على مجموعة الشروط السابق ذكرها، يتضح جليا حرص المشرع على توفير الحماية الوقائية للبيانات المتعلقة بإنشاء التوقيع الإلكتروني، في مواجهة أيّ إختراق أو تعدي عليها. كما حرص كذلك على عدم وقوع إستعماله من طرف الغير ، بالتأكيد على أنه عند إنشاء التوقيع يجب أن يكون معرّفا بشخصية الموّقع و أن يكون مميزا له عن غيره؛ وذلك لما رآه المشرع من أهمية بالغة في حماية حقوق المتعاملين مع صاحب التوقيع، بالإضافة لحماية بيانات صاحب التوقيع.

و هو ما نص عليه قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لسنة 1996، في مادته السابعة:"...إذا ما إشترط القانون وجود توقيع شخص في رسالة بيانات، يجب أن تستخدم فيها طريقة لتعيين ذلك الشخص".[21]

و لتعزيز الحماية أكثر للبيانات المستخدمة في التوقيع الإلكتروني، أكدّ المشرع في المادة(14) على أنه لا يمكن منح الإعتماد لمقدمي الخدمات الإلكترونية من طرف الهيئة الرسمية المكلفة بذلك، إلا بعد التأكد من مطابقة الآليات المستخدمة في إنشاء التوقيع مع المتطلبات و الشروط المذكورة سابقا.

أما بخصوص شهادة التصديق الإلكتروني، فالغرض منها هو توثيق البيانات الإلكترونية بتأكيد إنتسابها لمُصدِرها مع التحقق من سلامتها؛ بمعنى أن جهات التصديق الإلكتروني تلعب دور الموثق في المعاملات العادية(التقليدية).

و نظرا للدور الكبير لهذه الشهادة و أهميتها في توثيق المعاملات الإلكترونية، أقرّ المشرع مجموعة من الشروط القانونية و الضوابط التقنية لإصدارها، من طرف جهات معتمدة و مرخص لها من الدولة، تحت إشراف هيئات عليا في البلاد، في شكل سلطات، نظمها المشرع ضمن الفصل الثاني من القانون رقم 15-04 بعنوان:" سلطات التصديق الإلكتروني".

و تتمثل هذه السلطات في: السلطة الوطنية للتصديق الإلكتروني،[22] تنشأ لدى الوزير الأول،[23] و السلطة الحكومية للتصديق الإلكتروني، تنشأ لدى الوزير المكلف بالبريد و تكنولوجيا الإعلام و الإتصال.[24] كما عينت السلطة المكلفة بضبط البريد و المواصلات السلكية و اللاسلكية، كسلطة إقتصادية للتصديق الإلكتروني،[25] حيث تقوم هذه الأخيرة بدور مؤدي خدمات التصديق إلى غاية تعيين الجهة المختصة بذلك.

إلى جانب الخدمات التي تؤديها هذه السلطات في مجال الخدمات الإلكترونية و السهر على تنظيمها و تطويرها، تكلف كذلك هذه السلطات بمختلف هياكلها، بالعديد من المهام و الصلاحيات في مجال حماية البيانات الإلكترونية، نذكر أهمها في النقاط التالية:

- ترقية إستعمال التوقيع و التصديق الإلكترونيين و تطويرهما و ضمان موثوقية إستعمالهما.
- إعداد دفتر الشروط المحدد لكيفيات تأدية خدمات التصديق الإلكتروني.
- إعداد و تنفيذ تدابير الأمن المادي و سياسة الأمن المعلوماتي
- إعداد و تنفيذ تدابير الأمن التنظيمية و التقنية
- ضمان اليقظة فيما يخص أمن الأنظمة و الشبكة المعلوماتية
- منح التراخيص لمؤديي خدمات التصديق و التوقيع الإلكترونيين، مع متابعة و مراقبة نشاطهم

- حفظ البيانات المتعلقة بمنح شهادات التصديق

- الإحتفاظ بشهادات التصديق الإلكتروني المنتهية صلاحياتها[26]

كما تتجلى مظاهر حماية البيانات الإلكترونية للأشخاص في القانون رقم 15-04 من خلال الإجراءات الصارمة التي فرضها المشرع من أجل منح التخيص لمؤدي خدمات التصديق الإلكتروني، بالإضافة إلى الواجبات و المسؤولية المشددة عليه. خصص لذلك الفصل الثالث بعنوان:" النظام القانوني لتأدية خدمات التصديق الإلكتروني".

و على من يرغب القيام بنشاط مؤدي خدمات التصديق الإلكتروني أن يقدم طلب الترخيص، و أن يستوفي جملة من الشروط المذكورة في المادة(34)، نذكر أهمها:

- أن يكون خاضعا للقانون الجزائري إذا كان شخص معنوي أو الجنسية الجزائرية بالنسبة للشخص الطبيعي

- أن يتمتع بمؤهلات و خبرة ثابتة في ميدان تكنولوجيا الإعلام و الإتصال

- ألا يكون قد سبق الحكم عليه في جناية أو جنحة تتنافى مع نشاط تأدية خدمات التصديق الإلكتروني

و عند حصوله على الترخيص لمباشرة نشاطه تترتب عليه عدة إلتزامات، يهدف من خلالها المشرع تحقيق سلامة و حماية بيانات الأشخاص المتعاملين معه، منها ما جاء في المادة(42)، حيث يجب عليه الحفاظ على سرية البيانات و المعلومات المتعلقة بشهادة التصديق الإلكتروني الممنوحة.

كما نصت المادة (43) على أنه لا يمكنه جمع البيانات الشخصية إلا بعد موافقة صريحة من المعني، و لا يمكن أن يجمع إلا البيانات الشخصية الضرورية لمنح شهادة التصديق الإلكتروني، كما لا يمكنه إستعمال هذه البيانات لأغراض أخرى.

أما بخصوص المسؤولية المدنية المترتبة على مؤدي خدمة التصديق الإلكتروني فقد نصّت عليها صراحة المادة (53)، حيث أنه يكون مسؤولا عن الضرر الذي يلحق بأية هيئة أو أي شخص إعتمدوا على شهادة تصديق مسلمة من طرفه، و ذلك إذا ثبت عدم صحة المعلومات الواردة في الشهادة التي قدمها، أو في حالة منحه شهادة تصديق دون التأكد من مطابقة بيانات هوية صاحب التوقيع مع بيانات التحقق المحددة في شهادة التصديق الإلكتروني.

الفرع الثاني: العقوبات المقررة في القانون رقم 15-04

أقر المشرع نوعين من العقوبات على مخالفي أحكام هذا القانون، تضمنها الباب الرابع بعنوان :" العقوبات"، و تقسم إلى نوعين: عقوبات مالية و إدارية، و الأخرى جزائية

1- العقوبات المالية و الإدارية:

ورد في نص المادة (64) من ذات القانون أنه في حالة عدم إحترام مؤدي خدمات التصديق الإلكتروني لأحكام دفتر الشروط و سياسة التصديق الإلكتروني، تطبق عليه السلطة الإقتصادية

عقوبة مالية يتراوح مبلغها ما بين (200) ألف دج و (500) دج، كما يمكن أن تصل العقوبة إلى سحب الترخيص الممنوح له و إلغاء شهادته.

كما جاء في نص المادة (65) أنه في حالة إنتهاك مؤدي خدمات التصديق الإلكتروني لمقتضيات الدفاع الوطني و الأمن العمومي، تقوم السلطة بالسحب الفوري للترخيص منه، مع إتخاذ التدابير التحفظية اللازمة بشأن تجهيزاته.

2- العقوبات الجزائية:

لتدعيم الحماية القانونية للبيانات الشخصية، حصر المشرع في هذا القانون الأفعال المجرمة و المعاقب عليها من المادة (66) إلى المادة (75)، و أقر لها عقوبات بالحبس من (3) ثلاث أشهر إلى (3) ثلاث سنوات، مع غرامات مالية تتراوح ما بين (20) ألف دج إلى (5) خمس ملايين دج. و تتمثل هذه الجرائم في الأفعال التالية:

- حيازة أو إفشاء أو إستعمال بيانات إنشاء توقيع إلكتروني تخص الغير.
- عدم الحفاظ على سرية البيانات و المعلومات المتعلقة بالتوقيع و شهادة التصديق الإلكترونيين
- جمع البيانات الشخصية للغير دون موافقة صريحة منهم
- إستعمال بيانات التوقيع و شهادة التصديق الإلكتروني لأغراض أخرى
- الكشف عن معلومات سرية من قبل المكلف بعمليات التدقيق، كان قد علمها أثناء تأدية مهامه
- تأدية خدمات التصديق الإلكتروني دون ترخيص، أو بعد سحب الترخيص.

كما أقرت المادة (75) عقوبة الشخص المعنوي إذا ارتكبت لحسابه إحدى الجرائم المذكورة سابقا، حيث تضاعف الغرامة المالية إلى (5) خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

تجدر الإشارة إلى أن تجريم المشرع لتلك الأفعال ورد على سبيل الحصر و ليس على سبيل المثال، حيث خصص لكل فعل مادة تجرمه، و بذلك يعاب على المشرع أنه ضيق من دائرة التجريم ولم يترك المجال لهذه النصوص أن تستوعب أشكالا أخرى من أعمال الإعتداءات التي تمس بالبيانات الشخصية، لاسيما و أن هذه الأفعال تتطور بإستمرار مع كل تطور تكنولوجي.

المطلب الثاني: حماية البيانات الشخصية من جرائم الإتصالات الإلكترونية

تمّ إستحداث القانون رقم 18-04[27] لتدارك النقائص التي شابت القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال،[28] حيث توسع المشرع في توضيح المفاهيم الجديد من خلال تعاريف المصطلحات التقنية التي أوردها في المادة(10)، حتى يكون تطبيق نصوص هذا القانون أكثر دقة و تماشيا مع المستجدات الحاصلة في ميدان تكنولوجيا الإتصالات، بالإضافة لإرادة المشرع في تحقيق الأهداف المرجوة من وضع منظومة قانونية جديدة تكون أكثر ملاءمة و ضمانا لأمن و سلامة البيانات الشخصية المتبادلة عبر شبكات

الإتصالات الإلكترونية، سواءا بإتخاذ تدابير وقائية أو تقرير عقوبات لمرتكبي جرائم الإتصالات الإلكترونية.

تأسيسا على ما سبق، سنتطرق في (الفرع الأول) إلى الحماية القبلية للبيانات الشخصية في القانون 18-04، أما (الفرع الثاني) فنخصصه للعقوبات المقرر لحماية البيانات الشخصية في هذا القانون.

الفرع الأول: الحماية القبلية للبيانات الإلكترونية في قانون 18-04

من مظاهر الحماية القبلية للبيانات الشخصية التي جاء بها هذا القانون، أنه تضمّن جملة من الآليات الإدارية الوقائية و الضوابط القانونية التي ألزم المشرع إتخاذها و العمل بها عند إنشاء و إستغلال شبكات الإتصالات الإلكترونية، تحت إشراف و مراقبة سلطة ضبط البريد و الإتصالات الإلكترونية، و الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال.

أنشأت سلطة الضبط بموجب المادة (11) من هذا القانون التي ورد فيها أنه:" تنشأ سلطة ضبط... تتمتع بالشخصية المعنوية و الإستقلال المالي، تدعى بسلطة الضبط..."

من بين المهام المسندة إليها في مجال حماية البيانات الإلكترونية نذكر أهمها:

- السهر على متابعة نشاطات متعاملي البريد و الإتصالات الإلكترونية، و مراقبة مدى إحترامهم للأحكام القانونية و التنظيمية المتعلقة خصوصا بالأمن السبيراني
- السهر على حقوق المشتركين في خدمات الإتصالات الإلكترونية
- وضع إجراءات تحدد كيفية معالجة شكاوى المشتركين
- نشر كل معلومة مفيدة لحماية حقوق المشتركين، و القيام بحملات تحسيسية و توعوية لفائدتهم
- منح التراخيص لإنشاء و إستغلال شبكات الإتصالات الإلكترونية، وتراخيص الشبكات الخاصة

بإستقراء نصوص هذا القانون يتضح جليا الطابع الوقائي الذي أضفاه المشرع عليه، و الحماية القبلية التي يسعى إلى توفيرها للبيانات الشخصية، حيث أوجب أن يخضع نظام إنشاء و إستغلال شبكات الإتصالات الإلكترونية وتقديم خدمات الإتصالات الإلكترونية إلى مجموعة من القواعد و الشروط تضمنتها المادة (97)، نذكر أهمها:

- ضمان أمن و سلامة الشبكات الإلكترونية
- إحترام شروط خصوصية البيانات و المعلومات التي يتم إيصالها بواسطة شبكات الإتصالات الإلكترونية
- إحترام شروط حماية الحياة الخاصة للمشتركين و البيانات ذات الطابع الشخصي
- إلزامية إحترام الملكية الفكرية و حقوق المؤلف و الحقوق المجاورة

كما أكدت المادة(117) على أنه يجب ألا يمس إستعمال شبكات و خدمات الإتصالات الإلكترونية بكرامة و حفظ الحياة الخاصة للأخرين.

عند القراءة المتأنية لهذا النص، نلاحظ أن المشرع قد إستعمل المفهوم الواسع و الأسلوب العام في مخاطبة كل مستعملي و مستغلي الشبكات، علاوة على مقدمو خدمات الإتصالات الإلكترونية، و المقصود بذلك منع كل إستعمال غير مشروع للشبكات، سواءا كان بغرض الإستفادة من خدمات الشبكات من طرف المشتركين أو بغرض تقديم الخدمات من طرف المتعاملين.

كما نلاحظ تكرار مصطلح "الحياة الخاصة بالأخرين" في كثير من المواد، و في ذلك دلالة على تأكيد المشرع لحماية هذا الحق، كما تظهر من ذلك رغبة المشرع في أن يشمل حماية الحقوق الأخرى التي تدخل في دائرته، كالحق في سرية المراسلات، حقوق الملكية الفكرية، الحق في سرية البيانات الشخصية...و غيرها

و في إطار متابعة و مراقبة عمل المتعاملين، فقد إشترط حصولهم على رخصة تمنحها سلطة الضبط حتى يتمكنوا من ممارسة نشاطهم وفقا لدفتر شروط خاص بكل نشاط (المادة 123).

مع إلزام المتعاملين و مستخدميهم في المادة (160) بإحترام سرية المراسلات الإلكترونية، وكذا إحترام الحياة الخاصة و المعلومات الإسمية للمشتركين.

لم يكتفي المشرع بمنع المتعاملين من التعرض للبيانات الخاصة بالأشخاص، بل ألزمهم إضافة لذلك بإتخاذ التدابير التي من شأنها أن تضمن سرية المكالمات و المعلومات التي يحوزونها عن مشتركيهم، و ألا يسمحوا بالإطلاع عليها إلا بإذن مسبق من السلطة القضائية(المادة 119).

و كتدبير إحترازي جاء في المادة(118) أنه في حالة الإستعمال غير المشروع لشبكات و خدمات الإتصالات الإلكترونية، يتم إعلام المتعامل من طرف سلطة الضبط من أجل التدخل الفوري لمنع النفاذ إلى الشبكات، بغرض وقف الإعتداء.

و لتدعيم مهام و سير عمل هذه السلطة، تمّ إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، و ذلك بموجب المرسوم الرئاسي رقم 19-172،[29] هي مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الإستقلال المالي، توضع تحت سلطة وزارة الدفاع الوطني.[30] هياكلها الأساسية هي: مجلس التوجيه و المديرية العامة.

حيث يتشكل مجلس التوجيه من عدة وزراء يرأسه وزير الدفاع الوطني، ومن بين المهام الموكلة لهذا المجلس في مجال حماية البيانات الرقمية و الوقاية من جرائم الإتصالات، نذكر أهمها:

- إعداد إستراتيجية وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال
- التداول حول مسائل التطوير و التعاون مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام و الإتصال
- التقييم الدوري لحالة التهديد في مجال الجرائم الإلكترونية
- المساهمة في ضبط المعايير القانونية في مجال إختصاص الهيئة[31]

كما تساعد هذه الهيئة مديرية عامة، تتولى عدة مهام في مجال الأمن المعلوماتي، نذكر أهمها:

- تنشيط و تنسيق و مراقبة عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال
- تبادل المعلومات مع الهيئات الأجنبية بغرض تجميع كل المعطيات، بتحديد مكان مرتكبي الجرائم الإلكترونية و التعرف عليهم[32]

تضم المديرية العامة عدة مديريات، أهمها المديرية التقنية المكلفة بمهمة المراقبة الوقائية للإتصالات الإلكترونية، و في هذا الإطار حددت مهامها أساسا في:

- مساعدة السلطات القضائية و مصالح الشرطة القضائية في إطار مكافحة الجريمة المتصلة بتكنولوجيا الإعلام و الإتصال
- جمع و تسجيل و حفظ المعطيات الرقمية و تحديد مصدرها و تتبعها بغرض إستعمالها في الإجراءات القضائية.[33]

الفرع الثاني: الحماية الجزائية للبيانات في القانون رقم 18-04

بالنسبة للجزاءات المقررة لعدم إحترام أحكام القانونية في مجال الإتصالات الإلكترونية، فقد كان المشرع صريحا في تجريم أفعال الإعتداءات على المراسلات و تقرير العقوبات الخاصة بها، من خلال الباب الرابع المعنون ب:" الأحكام الجزائية".

حيث جاء في نص المادة (164) أنه يعاقب بالحبس من سنة إلى خمس سنوات، و بغرامة مالية من (500) ألف دج إلى (1) مليون دج، كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الإتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخبر بوجودها"

كما ورد في المادة (165) أنه:" يعاقب بالحبس من سنة إلى (3) ثلاث سنوات و بغرامة مالية من (1) مليون دج إلى (5) خمس ملايين دج، أو بإحدى العقوبتين كل متعامل للبريد يفتح أو يحول أو يخرب البريد، أو يساعد في إرتكاب هذه الأفعال.

و تسري نفس العقوبات على كل متعامل للإتصالات الإلكترونية يحول بأية طريقة كانت المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الإتصالات الإلكترونية، أو يأمر أو يساعد في إرتكاب هذه الأفعال".

على عكس القانون رقم 15-04 الذي تطرقنا إليه سابقا، يتضح من أحكام هذا الباب المخصص للعقوبات أن المشرع قد إستعمل المفاهيم الواسعة في تجريم أفعال الإعتداءات على المراسلات الإلكترونية، و تعمّد صياغة المصطلحات العامة حتى تستطيع هذه النصوص إستيعاب أشكال أخرى من الأفعال المجرمة قد تظهر مع التطور التكنولوجي لاحقا.

الخاتمة:

تبين من خلال هذه الدراسة أن المشرع الجزائري قد عرف تأخرا في تعديل قوانينه ولم يواكب التطورات الحاصلة في مجال المعلوماتية إلا في السنوات الأخيرة، أين عرف تحسنا ملحوظا من خلال جملة التعديلات التي قام بها، حيث إهتدى إلى تعديل القواعد العامة بدسترة حق حماية الخصوصية الرقمية للأشخاص، ثم عدل قانون العقوبات بتوسيع مفهوم حماية الخصوصية إلى الحماية من الجرائم الإلكترونية، وكذا حماية المعطيات الرقمية ذات الطابع الشخصي، تبع تلك التعديلات بإستحداث جملة من القوانين الخاصة، كانت أكثر تجاوبا مع الطبيعة الرقمية لأفعال التعدي على البينات الشخصية الإلكترونية، و منه توصلنا إلى النتائج التالية:

- إستدرك المشرع الجزائري النقص الذي كان يعتري قواعد الحماية التقليدية للأفراد، و قد واكب التطورات التكنولوجية بتكريس حق حماية المراسلات الخاصة للأشخاص.

- جاء التعديل الدستوري الأخير أكثر وضوحا في حماية البيانات الشخصية عند إدراجه لحق حماية البيانات ذات الطابع الشخصي، و هو بمثابة إرتقاء تشريعي على مستوى القواعد الدستورية في حماية حقوق الإنسان.

- واكب المشرع التطورات عند تعديله لقانون العقوبات بإدراج قسم خاص بحماية الأنظمة المعلوماتية و البيانات المتعلقة بها، ليشمل بذلك البيانات الإلكترونية الشخصية.

- طوع المشرع مفهوم حماية الحياة الخاصة من الجريمة الإلكترونية، و وسع من دائرة التجريم التي تدخل ضمنها كل الأفعال الماسة بخصوصية الأشخاص.

- أدرك المشرع الجزائري أهمية البيانات المتعلقة بالتوقيع و التصديق الإلكترونيين، فقرر جملة من التدابير الوقائية و الأحكام الجزائية لحمايتها بصدور القانون رقم 15-04، إلا أنه عند تجريم الأفعال الماسة بهذه البيانات يعاب عليه أنه حصرها و حددها في بعض الأشكال فقط، ولم يترك المجال مفتوحا أمام الأفعال الجديدة التي يمكن أن تظهرها التطورات لاحقا.

- تفطن المشرع الجزائري للنقائص التي شابت القانون رقم 09-04، و جاء بالقانون رقم 18-04 الذي كان أكثر تفصيلا و وضوحا في التصدي لجرائم الإتصالات الإلكترونية.

- يتضح من نصوص القانون 18-04 الطابع الوقائي، ورغبة المشرع توفير الحماية القبلية للبيانات الرقمية في مجال اإتصالات الإلكترونية، و يتجلى ذلك في إتخاذ آليات و تدابير إدارية و قانونية للتصدي لهذا النوع من الجرائم، خصوصا أنه عبر عنها بمفهوم الإستراتيجية الأمنية تحت رقابة سلطات عليا في الدولة.

- أحسن ما فعل المشرع في القانون رقم 18-04، عند تجريمه للأفعال الماسة بالمراسلات الإلكترونية، أنه استعمل الأسلوب العام عند صياغة المواد و توسيع نطاق الأفعال المجرمة، و بالتالي توسع مجال تطبيق النصوص على الأفعال التي يمكن أن تظهر لاحقا.

- أحسن فعلا المشرع عندما وسع من النطاق الجغرافي لمكافحة الجرائم المعلوماتية و الوقاية منها، و ذلك من خلال توسيع مهام الهيئة الوطنية إلى خارج الوطن بتبادل المعلومات مع مثيلاتها الأجنبية، نظرا لطبيعة الجريمة الإلكترونية التي لا تعترف بقواعد الحدود الجغرافية؛ لكن لتطبيق ذلك يتطلب الأمر القيام بالعديد من إتفاقيات التعاون الأمني، على المستوى الإقليمي و الدولي.

من خلال النتائج المتوصل إليها يمكن أن نقترح بعض التوصيات فيما يلي:

- ضرورة إعداد نصوص قانونية لتنظيم المراقبة الإلكترونية.
- إشتراط توفر الأمن المعلوماتي في المواقع و المنصات الرقمية، من خلال إلزام أصحابها بإتخاذ التدابير الضرورية لذلك.
- التعجيل بتفعيل العمل بالتوقيع و التصديق الإلكترونيين، من أجل وضع حد للتعامل بالهويات المزيفة، و بالتالي إمكانية تتبع آثار الإختراقات و الإستعمال غير المشروع لبيانات الغير.
- إعادة النظر في صياغة النصوص المجرمة لأفعال التعدي على بيانات التوقيع و التصديق الإلكترونيين، أو تقرير الإحالة الصريحة إلى المادة(394) و مايليها من قانون العقوبات، كونها أكثر إستجابة لمتطلبات حماية البيانات الشخصية.
- توسيع التكوين في الأمن المعلوماتي لكافة فئات المجتمع.
- ضرورة القيام بدورات تحسيسية، للتوعية من مخاطر الجرائم الإلكترونية.
- تفادي التعامل بالمعلومات الشخصية و تقديمها، في المواقع الإلكترونية إلا بعد التأكد من موثوقيتها و أنها تتوفر غلى مستوى عالي من الأمن الرقمي.

الهوامش:

[1] القانون رقم 15-04 المؤرخ في 01 فيفري 2015، المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، ج ر، ع 06، الصادر في 10 فيفري 2015.

[2] القانون رقم 18-04 المؤرخ في 10 ماي 2018، المحدد للقواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية، ج ر، ع 27، الصادر في 13 ماي 2018.

[3] كرس المشرع الجزائري الحق في الحياة الخاصة بموجب دستور 1963، الذي نص في المادة (14) على أنه: " لا يجوز الإعتداء على حرمة المسكن، و يضمن حفظ سر المراسلة لجميع المواطنين"، ثم جاء دستور 1976 ليعترف بذلك صراحة من خلال المادة (49):" لا يجوز إنتهاك حرمة حياة المواطن الخاصة و لا شرفه و القانون يصونها، سرية المراسلات و المواصلات الخاصة بكل أشكالها مضمونة".

[4] الدستور الجزائري لسنة 1996، الصادر بمقتضى المرسوم الرئاسي رقم 96-438، المؤرخ في 07 ديسمبر 1996، ج ر، ع 76، الصادر في 08 ديسمبر 1996.

[5] حزام فتيحة، الحق في الحياة الخاصة بالبيئة الرقمية (دراسة مقارنة)، مجلة الدراسات القانونية المقارنة، المجلد الثامن، العدد الأول، ص ص: 620-642، سنة 2022، ص631.

[6] القانون رقم 16-01 المؤرخ في 06 مارس 2016، المتضمن تعديل الدستوري، ج ر، ع 14، الصادر في 07 مارس 2016.

[7] المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري المصادق عليه في إستفتاء 01 نوفمبر 2020، ج ر، ع 82، الصادر في 30 ديسمبر 2020.

[8] تمّ نقل مضمون المادة (46) إلى المادة (47) بموجب التعديل الدستوري لسنة 2020.
[9] لوكال مريم، الحماية القانونية الدولية و الوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي: في ضوء قانون حماية المعطيات رقم 18-07، مجلة العلوم القانونية و السياسية، المجلد (10)، العدد (01)، ص ص: 1304-1325، أفريل 2019، ص 1313.
[10] القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المعدل و المتمم للأمر رقم 66-155 المتضمن قانون العقوبات الجزائري.
[11] عيمور راضية، الجريمة الإلكترونية و آليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية و السياسية، المجلد السادس، العدد الأول، ص ص: 87-107، سنة 2022، ص 99.
[12] خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009، ص 260.
[13] ثروت عبد الحميد، التوقيع الإلكتروني- ماهيته، مخاطره، و كيفيات مواجهتها، دار الجامعة الجديدة، مصر، 2007، ص 71.
[14] باهة فاطمة، آثار قواعد الإثبات الإلكتروني على المراكز القانونية للخصوم (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق، جامعة الجيلالي اليابس سيدي بلعباس، 2017-2018، الجزائر، ص344.
[15] أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية و الإختصاص القضائي بها (دراسة مقارنة)، دار الوفاء لدنيا الطباعة و النشر، مصر، 2016، ص 112.
[16] القانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، المعدل و المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج ر، ع 84، الصادر في 24 ديسمبر 2006.
[17] إعترف المشرع الجزائري بالكتابة و التوقيع الإلكترونيين عند تعديل القانون المدني سنة 2005، ضمن المادتين (323مكرر1) و (327)، و ذلك بموجب القانون رقم 05-10 المؤرخ في 20 جوان 2005، المعدل و المتمم للأمر رقم 75-58 المتضمن القانون المدني الجزائري، ج ر، ع 44، الصادر في 26 جوان 2005.
[18] جاء هذا التعريف في الفقرة الثانية من المادة الثانية، التي أورد المشرع ضمنها مجموعة من التعريفات، لتحديد مفهوم هذه المصطلحات الجديدة في الميدان القانوني، نظرا للطبيعة التقنية التي تميزها، كما أنه تباينت التعريفات التي تطلق عليها، سواءا من طرف المشرعين أو الفقهاء.
[19] لقد ميّز المشرع بين نوعين من التوقيع، الأول توقيع إلكتروني بسيط(عادي)، و الثاني هو التوقيع الإلكتروني الموصوف، و الفرق بينهما أن الأول يتم إنشاءه بتقنيات و إجراءات بسيطة، فهو لا يتوفر على نسبة عالية من الحماية و الأمان، أما التوقيع الإلكتروني الموصوف فهو التوقيع الذي أنشا وفقا لشهادة تصديق إلكتروني موصوفة، و وفق آلية مؤمنة و موثوقة...يحوز هذا الأخير على نسبة عالية من الأمان و المصداقية عند التعامل به.
[20] حزام فتيحة، الإثبات الإلكتروني في السائل المدنية و التجارية، أطروحة دكتوراه في العلوم القانونية، جامعة الجزائر1 بن يوسف بن خدة، سنة 2015-2016، ص32.
[21] أبو الهجاء محمد إبراهيم، عقود التجارة الإلكترونية، دار الثقافة للنشر، الأردن 2011. ص 126.
[22] تولى تنظيمها و سير عملها المرسوم التنفيذي رقم 16-134 المؤرخ في 25 أفريل 2016، المحدد لتنظيم المصالح التقنية و الإدارية للسلطة الوطنية للتصديق الإلكتروني و سيرها و مهامها، ج ر، ع 26، الصادر في 28 أفريل 2016.
[23] تولى تنظيمها المرسوم التنفيذي رقم 16-134 المؤرخ في 25 أفريل 2016، المحدد لتنظيم المصالح التقنية و الإدارية للسلطة الوطنية للتصديق الإلكتروني و سيرها و مهامها، ج ر، ع 26، الصادر في 28 أفريل 2016.
[24] نظم أحكامها المرسوم التنفيذي رقم 16-135 المؤرخ في 25 أفريل 2016، المحدد لطبيعة السلطة الحكومية للتصديق الإلكتروني و تشكيلها و تنظيمها و سيرها، ج ر، ع 26، الصادر في 28 أفريل 2016.
[25] تمّ تعيين هذه السلطة و تحديد مهامها بموجب المادتين (29) و (30) من القانون 15-04، كما أن هذه السلطة تقوم بدور مؤدي خدمات التصديق الإلكتروني و كذا منح الإعتمادات لمقدمي خدمات التوقيع و التصديق الإلكترونيين، خلال مرحلة إنتقالية حددت بخمس سنوات إلى حين صدور النصوص التنظيمية التي تحدد الجهات المعنية بذلك، و هذا طبقا للمادتين (78) و (79) من نفس القانون، لكن من الناحية العملية لم يتم تعيين أي جهة تقوم بذلك، و هو الأمر الذي جعل معظم النصوص المنظمة للتوقيع الإلكتروني دون تفعيل.
[26] للمزيد من التفصيل و الإطلاع على مزيد من المهام، راجع مواد المرسومين التنفيذيين المذكورين أعلاه.

[27] القانون رقم 18-04 المؤرخ في 10 ماي 2018، المحدد للقواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية، ج ر، ع 27، الصادر في 13 ماي 2018.

[28] القانون رقم 09-04 المؤرخ في 05 أوت 2018، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، ج ر، ع 47، الصادر في 16 أوت 2018.

[29] المرسوم الرئاسي رقم 19-172 المؤرخ في 06 يونيو 2019، المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها و تنظيمها و كيفيات سيرها، ج ر، ع 37، الصادر في 09 يونيو 2019.

[30] المادة (02) من نفس المرسوم، تجدر الإشارة إلى أن هذه الهيئة كانت تحت سلطة وزير العدل في ظل المرسوم الرئاسي رقم 15-261، قبل إلغاء أحكامه بموجب المادة 24 من المرسوم الرئاسي رقم 19-172.
لمزيد من التفصيل إطلع على: المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، ج ر، ع 53، الصادر في 08 أكتوبر 2015.

[31] المادة (06) من المرسوم الرئاسي رقم 19-172.

[32] المادة (09) من نفس المرسوم.

[33] المادتين (11) و (12) من نفس المرسوم.

قائمة المراجع:

أ) الكتب:

1) أمير فرج يوسف، الإثبات الجنائي للجريمة الإلكترونية و الإختصاص القضائي بها (دراسة مقارنة)، دار الوفاء لدنيا الطباعة و النشر، مصر، 2016.

2) أبو الهجاء محمد إبراهيم، عقود التجارة الإلكترونية، دار الثقافة للنشر، الأردن،2011.

3) ثروت عبد الحميد، التوقيع الإلكتروني- ماهيته، مخاطره، و كيفيات مواجهتها، دار الجامعة الجديدة، مصر، 2007.

4) خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، مصر، 2009.

ب) الأطروحات:

1) حزام فتيحة، الإثبات الإلكتروني في السائل المدنية و التجارية، أطروحة دكتوراه في العلوم القانونية، جامعة الجزائر1 بن يوسف بن خدة، سنة 2015-2016.

2)باهة فاطمة، آثار قواعد الإثبات الإلكتروني على المراكز القانونية للخصوم (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، كلية الحقوق، جامعة الجيلالي اليابس سيدي بلعباس، 2017-2018.

ج) المقالات:

1) عيمور راضية، الجريمة الإلكترونية و آليات مكافحتها في التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية و السياسية، المجلد السادس، العدد الأول، ص ص: 87-107، سنة 2022.

2) لوكال مريم، الحماية القانونية الدولية و الوطنية للمعطيات ذات الطابع الشخصي في الفضاء الرقمي: في ضوء قانون حماية المعطيات رقم 18-07، مجلة العلوم القانونية و السياسية، المجلد (10)، العدد (01)، ص ص: 1304-1325، أفريل 2019.

3) حزام فتيحة، الحق في الحياة الخاصة بالبيئة الرقمية (دراسة مقارنة)، مجلة الدراسات القانونية المقارنة، المجلد الثامن، العدد الأول، ص ص: 620-642، سنة 2022.

د) القوانين:

1) الدستور الجزائري لسنة 1996، الصادر بمقتضى المرسوم الرئاسي رقم 96-438، المؤرخ في 07 ديسمبر 1996، ج ر، ع 76، الصادر في 08 ديسمبر 1996.

2) القانون رقم 16-01 المؤرخ في 06 مارس 2016، المتضمن تعديل الدستوري، ج ر، ع 14، الصادر في 07 مارس 2016.

3) المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، المتعلق بإصدار التعديل الدستوري المصادق عليه في إستفتاء 01 نوفمبر 2020، ج ر، ع 82، الصادر في 30 ديسمبر 2020.

4) القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المعدل و المتمم للأمر رقم 66-155 المتضمن قانون العقوبات الجزائري.

5) القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المعدل و المتمم للأمر رقم 66-155 المتضمن قانون العقوبات الجزائري.

6) القانون رقم 09-04 المؤرخ في 05 أوت 2018، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، ج ر، ع 47، الصادر في 16 أوت 2018.

7) القانون رقم 15-04 المؤرخ في 01 فيفري 2015، المحدد للقواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، ج ر، ع 06، الصادر في 10 فيفري 2015.

8) القانون رقم 18-04 المؤرخ في 10 ماي 2018، المحدد للقواعد العامة المتعلقة بالبريد و الإتصالات الإلكترونية، ج ر، ع 27، الصادر في 13 ماي 2018.

9) القانون رقم 06-23، المؤرخ في 20 ديسمبر 2006، المعدل و المتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج ر، ع 84، الصادر في 24 ديسمبر 2006.

10) القانون رقم 05-10 المؤرخ في 20 جوان 2005، المعدل و المتمم للأمر رقم 75-58 المتضمن القانون المدني الجزائري، ج ر، ع 44، الصادر في 26 جوان 2005.

ه) المراسيم:

1) المرسوم التنفيذي رقم 16-134 المؤرخ في 25 أفريل 2016، المحدد لتنظينم المصالح التقنية و الإدارية للسلطة الوطنية للتصديق الإلكتروني و سيرها و مهامها، ج ر، ع 26، الصادر في 28 أفريل 2016.

2) المرسوم التنفيذي رقم 16-135 المؤرخ في 25 أفريل 2016، المحدد لطبيعة السلطة الحكومية للتصديق الإلكتروني و تشكيلها و تنظيمها و سيرها، ج ر، ع 26، الصادر في 28 أفريل 2016.

3) المرسوم الرئاسي رقم 19-172 المؤرخ في 06 يونيو 2019، المحدد لتشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها و تنظيمها و كيفيات سيرها، ج ر، ع 37، الصادر في 09 يونيو 2019.

4) المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015، المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، ج ر، ع 53، الصادر في 08 أكتوبر 2015.

حدود حماية الحق في الخصوصية في الفضاء الرقمي في ضوء التشريع الجزائري

The limits of protecting the right to privacy in the digital age in the light of Algerian legislation

د/ ميرة وليد

كلية الحقوق والعلوم السياسية جامعة المسيلة - الجزائر

walidmira@gmail.com

ملخص :

أدى الانتشار الواسع إلى الوسائل الإلكترونية التي تسمح بتسجيل المكالمات والتقاط الصور والفيديوهات ونشرها عبر الأنترنت أو تداولها في كثير من الحالات إلى المساس بالحياة الخاصة للأفراد، لذلك سعت مختلف الدول سن مختلف النصوص التشريعية لحماية حق الفرد في الخصوصية ، من خلال تكريسه دستوريا وسن النصوص القانونية التي تجرم العديد من صور المساس بالحياة الخاصة للفرد ، عن طريق تجريم التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه، وتجريم التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه، كما جرم كذلك الاحتفاظ أو وضع في متناول الجمهور أو الغير التسجيلات أو الصور ، كما جرم الدخول عن طريق الغش إلى منظومة المعالجة الآلية للمعطيات أو يحاول الدخول إليها .

الكلمات المفتاحية : الحق في الخصوصية ، الفضاء الرقمي ،حماية قانونية

Abstract:

The wide spread of electronic means that allow recording calls, taking pictures and videos and publishing them via the Internet or circulating them in many cases has led to compromising the private lives of individuals. Therefore, various countries have sought to enact various legislative texts to protect the individual's right to privacy, by constitutionally enshrining it and enacting legal texts that many ways of compromising the private life of an individual are criminalized by criminalizing capturing, recording or transmitting private or confidential calls or conversations without the permission or consent of the person concerned, and criminalizing taking or transmitting a picture of a person in a private place without his permission or consent, as well as Keeping or making available to the public or third parties recordings or images, as well as the offense of fraudulently entering or attempting to access the automated data processing system

Keywords: The right to privacy, digital space, legal protection

مقدمة

أدى التقدم التكنولوجي إلى خلق حالة من الاضطراب وعدم التوافق بين حماية الحق في الخصوصية وتجميع البيانات المكثف الذي يقوم عليه الاقتصاد الرقمي ، مما يتعين معه البحث في كيفيات حماية هذا الحق بما لا يتعارض مع التمتع بما من توفر من مزايا لمستخدميه في الفضاء الرقمي ، وقد كان موضوع مداخلتنا حول حدود حماية الحق في الخصوصية في الفضاء الرقمي في ضوء التشريع الجزائري،

من خلال ما سبق يمكن أن نطرح الإشكالية التالية ، ماهي القيود التي وضعها المشرع الجزائري على مستخدمي التكنولوجيا لأجل حماية الحق في الخصوصية .

سنتناول موضوع حدود حماية الحق في الخصوصية في الفضاء الرقمي في ضوء التشريع الجزائري من خلال العناصر التالية:

1- مظاهر الحماية القانونية للحق في الخصوصية.

2 - مظاهر قصور النصوص الحالية على حماية حق الفرد في الخصوصية .

خاتمة تتضمن بعض الاقتراحات والتوصيات لضمان حماية كافية لحماية حق الفرد في الخصوصية .

1- مظاهر الحماية القانونية للحق في الخصوصية :

حماية الحق في الخصوصية تم تكريسه دستوريا من خلال المادة 39 والمادة 47 من الدستور ، حيث نصت المادة 1/39 من دستور الجمهورية الجزائرية على ما يلي :**" تضمن الدولة عدم انتهاك حرمة الإنسان" ، كما نصت المادة 47 من الدستور على ما يلي: " لكل شخص الحق في حماية حياته الخاصة وشرفه.**

لكل شخص الحق في سرّية مراسلاته و اتصالاته الخاصة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلاّ بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

يعاقب القانون على كل انتهاك لهذه الحقوق".

أما بالنسبة للقوانين العادية فقد تم وضع مجموعة من النصوص القانونية التي تجرم العديد من صور المساس بالحياة الخاصة للفرد ، عن طريق تجريم التقاط أو تسجيل أو

نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه، وتجريم التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه، كما جرم كذلك الاحتفاظ أو وضع في متناول الجمهور أو الغير التسجيلات أو الصور ، كما جرم الدخول عن طريق الغش إلى منظومة المعالجة الآلية للمعطيات أو يحاول الدخول إليها، هذه الجرائم وردت ضمن المواد 303 مكرر والمادة 303 مكرر 1 والمواد المادة 394 مكرر إلى غاية المادة 394 مكرر7.

وفيما يلي نشير إلى صور الحماية القانونية للحق في الخصوصية المنصوص عنها في قانون العقوبات على النحو التالي :

أ - تجريم تسجيل المكالمات الخاصة دون إذن صاحبها:

ب- تجريم تصوير شخص في م كان خاص دون إذنه:

ج – تجريم الاحتفاظ أو وضع في متناول الجمهور أو الغير التسجيلات أو الصور التي تمت بغير إذن صاحبها :

د -تجريم المساس بأنظمة المعالجة الآلية للمعطيات :

أ - تسجيل المكالمات الخاصة دون إذن صاحبها:

نصت المادة 303 مكرر من قانون العقوبات على ما يلي: **" 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".

جريمة انتهاك الحق في حرمة الاتصالات الهاتفية لها ثلاثة صور تتمثل في التقاط أو تسجيل ،أو نقل مكالمات، أو أحاديث خاصة، ويقصد بالتسجيل حفظ الحديث المسجل بغرض الاستماع إليه بعد التسجيل ،أما نقل الحديث . فهو استراق السمع بواسطة جهاز

لإرساله من مكان إلى مكان آخر باستخدام جهاز ،أما الالتقاط فهو التصنت والدي يقصد به الاستماع سرا بأية وسيلة إلى حديث بين شخصين أو أكثر.[1]

يلاحظ أنه يشترط لقيام جريمة تسجيل المكالمات أن يتصف الحديث بطابع الخصوصية أو السرية فالعبرة بطبيعة الحديث سواء تم في مكان عام أو خاص ،[2] حيث أن المشرع عبر عن هذا الشرط في نص المادة 303 مكرر بالعبارة التالية "**... أحاديث خاصة أو سرية...**"

يلاحظ كذلك أن هذه الجريمة عمدية، وقد عبر المشرع على هذا الشرع بالعبارة التالية " **...كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص...**" ، ومن ثم لابد من أن يكون هناك قصد جنائي بأن تتجه إرادة الجاني إلى قيام بفعل التسجيل ، فلا تقع الجريمة إذا حصل التسجيل على سبيل الخطأ كأن تلامس يد الشخص زر التسجيل دون أن يدرك ذلك .

يلاحظ كذلك أن القانون نص صراحة على تجريم الشروع في التسجيل،[3] فالجريمة تقع بمجرد أن يشرع الجاني في نشاطه الإجرامي حتى ولم تتحقق النتيجة، حتى ولم يحصل التسجيل طالما أن الجاني شرع في الأفعال المؤدية إلى التسجيل لكن التسجيل لم يتم بسبب خارج عن إرادته ،[4] فالشروع في الجريمة هي "كل محاولة أو بدء في تنفيذ فعل أو أفعال لابس فيها بغرض ارتكاب جناية أو جنحة تؤدي أو يؤدي مباشرة إلى ارتكاب الجريمة إذا لم توقف أو يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يكن بلوغ المقصود بسبب ظرف مادي يجهله مرتكبها "[5]

حيث أن الجريمة تتم بتسجيل مكالمات أو أحاديث خاصة ، والشروع في هذه الجريمة يقع بمجرد أن يضع الشخص جهاز ا مخصص لتسجيل مكالمات أو أحاديث خاصة ويضغط على زر التسجيل فإن هذا النشاط معاقب عليه قانونا حتى ولو لم يتم التسجيل فعليا بسبب عطل في الجهاز أو نفاذ بطاريته أو اكتشاف وجود الجهاز ، الشروع في الجريمة يشترط فيها أن يقوم الجاني بفعل يؤدي إلى ارتكاب الجريمة غير أن النتيجة لا تتحقق بسبب ظروف مستقلة عن إرادة الجاني .

فالجريمة تقع بجرد أن يقوم الجاني بالتسجيل، حتى ولو قام بحذف التسجيل مباشرة ولم يقم بالاحتفاظ به في جهازه فإن الجريمة تقع ، وان الحذف اللاحق للتسجيل لا ينفي قيام الجريمة ، وإن كان حذف التسجيل في الغالب لن يترك اثر في جهاز الجاني ، غير أنه لا يمحو الجريمة إلا اذا صفح الضحية حيث أن صفح الضحية يضع حدا للمتابعة الجزائية .

فمجرد قيام الجاني بالتسجيل تقوم الجريمة و لا يشترط أن يحتفظ بالتسجيل ، فالاحتفاظ بالتسجيلات والصور هي جريمة مستقلة منصوص عنها في المادة 303 مكرر 1 من قانون العقوبات وسنشير إليها في موضعها .

يلاحظ أن المشرع نص على أن صفح الضحية يضح حدا للمتابعة في جريمة تسجيل مكالمات وأحاديث خاصة .

كما يلاحظ أن المشرع لم يشترط تقديم شكوى من الضحية لتحريك الدعوى العمومية ، فيمكن للنيابة العامة أن تقوم بتحريك الدعوى تلقائيا اذا بلغها ذلك .

يلاحظ أن المشرع الجزائري لم يبين مدى إباحة التسجيل من عدمه إذا كان الغرض منه إثبات جرائم تقع حالا أو جرائم وقعت ،كأن يقوم الشخص بتسجل إقرار أو معلومات هامة عن جريمة أو يقوم بتسجيل تهديد بالقتل من طرف شخص آخر .

رغم أن القانون لم يتطرق لهذه لمسالة التسجيل لإثبات أفعال إجرامية لاستغلالها طرف الضبطية القضائية أو القضاء لحمل الفاعل على الاعتراف ،أو تسهيل الوصول إلى الفاعلين ، فإني أرى أن تسجيل مكالمات لأجل إثبات وقائق إجرامية لا يندرج ضمن الأفعال المنصوص عنها في المواد 303مكرر والمادة 303 مكرر واحد ، حيث أن المشرع استعمل عبارة "... **كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص...**" أي أن الغرض من التسجيل هو المساس بالحياة الخاصة للأشخاص.

يلاحظ كذلك أن إثبات هذه الجرائم يطرح إشكالات في إثباتها خصوصا اذا انكر المشبه فيه أو المتهم قيامه بأي نشاط فإن تفتيشه فيه اعتداء على خصوصيته بتفتيش هاتفه وتفتيش مختلف ملفاته الصوتية في أجهزته التي تحتوي على خصوصياته .

بالنسبة للعقوبة المقررة لهذه الجريمة ، فقد نص المشرع على الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج.[6]

ب- تصوير شخص في م كان خاص دون إذنه:

نصت المادة 303 مكرر من قانون العقوبات على ما يلي :" **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- .....

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"

حتى تقوم هذه الجريمة لابد أن يتوافر مجموعة من العناصر ، فلابد أن يكون هناك التقاط أو تسجيل أو نقل صورة شخص بأية وسيلة كانت من غير إذن و رضا المجني عليه وأن يتم أن يتم الاعتداء في مكان خاص .[7]

لا يهم الوسيلة المستعملة للتصوير سواء كان هاتفا أو آلة تصوير أو كاميرا أو كاميرا في حاسوب ، ولا يهم نوع الصورة سواء كانت صور ثابتة أو فيديو بصوت وصورة أو دون صوت ، المهم أن يتم التصوير بوسيلة تقنية .

وان يتم التصوير في مكان خاص حساب العبارة الوردة ضمن المادة 303 مكرر /3 من قانون العقوبات "... بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص..." ، ويقصد بالمكان الخاص "ذلك المكان المغلق الذي لا تستطيع أن تنفذ إليه عيون الناس من الخارج ولا يمكن الولوج إليه إلاّ بعد أخذ الإذن" ،[8] أما الأماكن يستعملها عامة الناس للمرور والتجوال كالطرق والشوارع والممرات والساحات العمومية والحدائق والغابات والشواطئ والجبال، حتى ولو كانت داخل سيارة خاصة في الطريق العمومي، أو كانت متوقفة في مكان عمومي فلا تعد أماكن خاصة،[9] بل تعد أماكن عامة ، ومن ثم فإن تصوير شخص في مكان عام لا يعاقب عليه القانون ولا يندرج ضمن أحكام المادة 303 مكرر من قانون العقوبات حتى ولو تم من غير رضا الشخص ، بل حتى ولو تم رغم اعتراضه ، فالقانون جرم التصوير فقط إذا كان في مكان خاص دون الأماكن العامة ، يلاحظ أن المشرع استورد هذا النص من القانون الفرنسي حيث أن طبيعة المجتمع الفرنسي تختلف عن طبيعة المجتمعات العربية ، حيث تصوير فتاة في الدول الأوروبية في الأماكن العامة وفقا لثقافتهم لا يعد مساسا بخصوصية الشخص لخلافا للمجتمعات العربية التي لازالت محافظة حيث أن الأعراف والتقاليد لا تبيح تصوير شخص من غير رضاه حتى ولو كان في مكان عام .

اشترط المشرع لمعاقبة مرتكب جريمة التقاط، أو تسجيل، أو نقل صورة لشخص، في مكان خاص أن يتم الفعل باستعمال أداة، أو آلة تصوير، أو تسجيل، تحقق ذلك الغرض دون العين المجردة، "ومن ثمة فإن الجريمة لا تتحقق إذا اطلع شخص من خلال ثقب الباب

أو نافذة مفتوحة على آخر، حتى ولو كان هذا الأخير في وضع مخجل، ولا يغير من هذا الحكم في شيء أن يروي هذا الشخص إلى الناس ما شاهده.[10]

يشترط أن ينصب الالتقاط، أو التسجيل، أو النقل على صورة شخص، استعمل المشرع في المادة 303 مكرر عبارة "**التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص**.. " للدلالة على اشتراط أن يكون من ينصب عليه فعل الالتقاط أو التسجيل أو النقل هو صورة شخص فقط، فالتقاط صورة للحيوان أو الجماد غير مشمولة بالحماية، فالقانون لا يحمي سوى الإنسان، أما الأشياء الأخرى مهما كانت أهميتها أو الضرر الناجم عن تصويرها فلا تدخل في نطاق هذه الحماية،[11] الجزائية المنصوص عنها في المادة 303 مكرر من قانون العقوبات .

يلاحظ أن القانون نص صراحة على تجريم الشروع في التصوير مثلما عليه الحال في الشروع في التسجيل المشار إليه سابقا ، فيعاقب على الشروع في التصوير بنفس العقوبة المقررة للجريمة التامة بمجرد أن يشرع الجاني في نشاطه الإجرامي حتى ولم تتحقق النتيجة، كأن يحمل شخص هاتفا أو آلة تصوير يوجهها لشخص بغرض تصويره، غير أن التصوير لا يتم بسبب تغطية المجني عليه لوجهه أو اختبائه وراء شيء ما أو يقوم شخص آخر بانتزاع الهاتف من يد الجاني أو لي يده لمنعه من التصوير.

فجريمة تصوير تشخص في مكان خاص تقع بجرد أن يقوم الجاني بالتصوير ، حتى ولو قام بحذف التصوير ولم يقم بالاحتفاظ به في جهازه ، فإن الجريمة تقع ، وأن الحذف اللاحق للتصوير لا ينفي قيام الجريمة ، و لا يمحو الجريمة إلا اذا صفح الضحية ،إذ أن صفح الضحية يضع حدا للمتابعة الجزائية .

فمجرد قيام الجاني بالتصوير تقوم الجريمة و لا يشترط أن يحتفظ بالتصوير ، فالاحتفاظ بالصور هي جريمة مستقلة منصوص عنها في المادة 303 مكرر 1 من قانون العقوبات .

يلاحظ أن المشرع نص على أن صفح الضحية يضح حدا للمتابعة في فجريمة تصوير تشخص في مكان خاص.

كما يلاحظ أن المشرع لم يشترط تقديم شكوى من الضحية لتحريك الدعوى العمومية ، فيمكن للنيابة العامة أن تقوم بتحريك الدعوى تلقائيا اذا بلغها ذلك .

يلاحظ أن المشرع الجزائري لم يبين مدى إباحة التصوير من عدمه إذا كان الغرض منه إثبات جرائم تقع حالا أو جرائم وقعت .

مثلما سبقت الإشارة في مسألة عن تسجيلات المكالمات والاحاديث الخاصة ،رغم أن القانون لم يتطرق لمسالة التصوير لإثبات أفعال إجرامية لاستغلالها من طرف الضبطية القضائية أو القضاء لحمل الفاعل على الاعتراف ،أو تسهيل الوصول إلى الفاعلين ، فإني أرى أن التصوير لأجل إثبات وقائق إجرامية لا يندرج ضمن الأفعال المنصوص عنها في المواد 303مكرر والمادة 303 مكرر واحد ، حيث أن المشرع استعمل عبارة "... كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص..." أي أن الغرض من التصوير وفقا للمادة 303 مكرر من قانون العقوبات هو المساس بالحياة الخاصة للأشخاص.

بالنسبة للعقوبة المقررة لهذه الجريمة ، فقد نص المشرع على الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج.[12]

ج – تجريم الاحتفاظ أو وضع في متناول الجمهور أو الغير التسجيلات أو الصور التي تمت بغير إذن صاحبها:

نصت المادة 303 مكرر 1 من قانون العقوبات على ما يلي : **"يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أو سمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون.**

عندما ترتكب الجنحة المنصوص عليها في الفقرة السابقة عن طريق الصحافة، تطبق الأحكام الخاصة المنصوص عليها في القوانين ذات العلاقة، لتحديد الأشخاص المسؤولين.

يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة.

ويضع صفح الضحية حدا للمتابعة الجزائية".

سبق أن تطرقنا إلى جريمة تسجيل محادثات ومكالمات خاصة من غير إن أصحابها وكذا إلى جريمة تصوير شخص في مكان خاص من غير إذن ورضا صاحبها ، وزاد المشرع جريمة أخرى وهي جريمة الاحتفاظ أو وضع في متناول الجمهور أو الغير التسجيلات أو الصور التي تمت بواسط الأفعال السالفة الذكر أي بواسطة الأفعال المنصوص عنها في المادة 303 مكرر ، حيث يلاحظ أن جريمة الاحتفاظ بالتسجيلات والصور التي تمت بواسط الأفعال المنصوص عنها في المادة 303 مكرر هي جريمة تبعية ، فإذا انعدمت الجريمة الأولى انعدمت معها جريمة الاحتفاظ بالتسجيلات والصور .

فجنحة الاحتفاظ الأحاديث أو الصور الملتقطة تتطلب أن تكون تلك التسجيلات والصور تم الحصول عليها بمساعدة أحد الفعلين الواردين في المادة 303 مكرر من قانون العقوبات ، أي أن جريمة المادة 303 مكرر 1 لا تقوم سوى بقيام جريمة المادة 303 مكرر. وبعبارة أخرى لا تقوم جنحة الاحتفاظ متى لم يتحقق الشرط المسبق والمتمثل في قيام جنحة التسجيل والتصوير قبلها.[13]

فالمشرع لم يكتف بتجريم الاعتداء على حرمة الحياة الخاصة للأفراد من خلال المعاقبة على التقاط أو تسجيل أو نقل كل من المكالمات الهاتفية و الأحاديث الخاصة أو السرية و كذا الصورة في مكان خاص. بل راح يتعقب هذه التسجيلات والصور في يد الجاني أو غيره و يسد الباب أمامه بتجريم أي استعمال لهذه التسجيلات أو الصور من خلال نص المادة 303 مكرر1 من قانون العقوبات المشار أعلاه ،[14] يتجسد السلوك الإجرامي لهذه الجريمة في أحد الصور التالية : الاحتفاظ بالتسجيل، أو الصور، أو الوثائق، السماح بالوضع في متناول الجمهور، أو الغير.[15]

بالنسبة للعقوبة المقررة لهذه الجريمة ، فقد نص 303 مكرر1 من قانون العقوبات على معاقبة الفاعل بالعقوبات المنصوص عنها في المادة 303 مكرر [16]، وبالرجوع إلى نص المادة 303 مكرر نجدها تنص على عقوبة الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50.000 دج إلى 300.000 دج.[17]

د -تجريم المساس بأنظمة المعالجة الآلية للمعطيات :

نص المشرع الجزائري في قانون العقوبات على مجموعة من الجرائم والتي تعاقب على المساس بأنظمة المعالجة الآلية للمعطيات في المواد 394 مكرر إلى غاية المادة 394 مكرر 7 ،

وتشمل جريمة الدخول غير المشروع في جزء من منظومة للمعالجة الآلية للمعطيات ، وجريمة الاعتداء على المعطيات .

د-1 جريمة الدخول غير المشروع في جزء من منظومة للمعالجة الآلية للمعطيات:

نصت المادة 394 مكرر من قانون العقوبات على ما يلي :" **يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.**

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة".

تعد جريمة الدخول أو البقاء غير المشروع في نظام المعالجة الآلية أو كما تسمى أيضا بجريمة | الاختراق الإلكتروني أكثر الجرائم انتشارا وخطورة وكذا أهمية؛ لأنها تعبر عن المرحلة التمهيدية لبقية | الجرائم الأخرى التي تستهدف المعطيات الموجودة في هذا النظام.[18]

يتمثل الركن المادي في هذه الجريمة في الدخول غير المشروع لأنظمة المعلومات المعالجة آليا والعائدة للغير بدون وجه حق، ويتم الدخول باستخدام طرق متعددة منها كلمة السر أو البطاقات الممغنطة الخاصة أو حيازة جهاز معين يتيح هذا الولوج ، إذ يلج الفاعل في نظام الاتصال دون أن يكون له حق الولوج عن طريق الحصول على كلمة السر بطريقة غير مشروعة أو تجريب الأرقام أو الاستعانة بأجهزة إليكترو مغناطيسية أو صوتية أو ميكانيكية.[19]

يلاحظ من خلال نص المادة 394 مكرر أن المشرع يعاقب على المحاولة الدخول بنفس العقوبة المقررة للدخول ، كأن يجرب أرقام سر عدة مرات للتجريب أو غيرها من الطرق بهدف الدخول ، حيث استعمل المشرع عبارة "**... أو حاول ذلك** "

أما بالنسبة للعقوبة المقررة للدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات، فهي الحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى100.000 دج، تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.[20]

د-2 جريمة الاعتداء على المعطيات:

نصت المادة 394 مكرر 1 من قانون العقوبات على ما يلي : **" يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".**

تقوم جريمة الاعتداء على المعطيات بارتكاب الجاني لأحد الأفعال الثلاثة ، الإدخال أو الإزالة أو التعديل.

يقصد بفعل الإدخال إضافة معطيات جديدة على الدعامة الخاصة بها سواء كانت خالية أو كان يوجد عليها معطيات من قبل، وقد يتم الفعل بإدخال معطيات وهمية إلى النظام المعلوماتي أو بإدخال معطيات صحيحة ولكن من شأنها التشويش على المعطيات الموجودة قبلا في النظام، ويقصد بالإزالة محو جزء من المعطيات المسجلة على الدعامة والموجودة داخل النظام أو تحطيم تلك الدعامة، أما التعديل فيقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى ويتحقق التعديل مثل الإزالة عن طريق البرامج الضارة أهمها الفيروسات والقنابل الزمنية والمنطقية.[21]

بالنسبة للعقوبة المقررة لجريمة الاعتداء على المعطيات بالإزالة أو الإدخال أو التعديل فهي الحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000دج إلى 2.000.000 دج.[22]

د -3 جريمة التعامل غير المشروع في المعطيات :

نصت المادة 394 مكرر 2 من قانون العقوبات على ما يلي : **" يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:**

1- تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات محزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

و هذه الجريمة تأخذ شكلين : جريمة التعامل غير المشروع في معطيات صالحة لارتكاب جرائم المساس بأنظمة المعالجة الآلية ، كما تأخذ شكل جريمة التعامل غير المشروع في معطيات متحصل عليها من جرائم ماسة بأنظمة المعالجة الألية

- **جريمة التعامل غير المشروع في معطيات صالحة لارتكاب جرائم المساس بأنظمة المعالجة الآلية:**

يقوم الركن المادي لهذه الجريمة على توافر واحد أو أكثر من الأفعال التالية ، والمتمثلة في التصميم والبحث والتجميع والتوفير والنشر و الإتجار

يقصد بالتصميم إعداد برامج وتقنيات صالحة لارتكاب الجريمة ، ومثاله تصميم البرامج الخبيثة كبرامج الفيروسات والقنابل المنطقية والزمنية أو برامج الاختراق والتجسس المعلوماتي، ويقصد بالبحث البحث عن المعطيات التي يمكن أن ترتكب بها الجريمة أو يشير إلى البحث في كيفية تصميم برامج لارتكاب الجريمة. [23]

و يقصد بالتجميع القيام بجمع قدر كبير عن المعلومات التي تشكل خطرا كبيرا والتي من الممكن أن ترتكب بها إحدى جرائم الاعتداء على نظم المعالجة الآلية، ويقصد بالتوفير عرض المعلومات وإتاحتها وجعلها في متناول الغير، ومن قبيل ذلك كلمة المرور وشفرة الدخول أو أية بيانات مشابهة تسمح بالولوج لكل أو جزء من نظام المعالجة، ويشمل كذلك الكشف أو الإفشاء العلني للثغرات الأمنية في النظام، ويقصد بالنشر إعلام وإذاعة المعطيات وتمكين الغير من الاطلاع عليها، ويقصد بالإتجار أي تصرف من شأنه توفير عاد أو منفعة مادية نظير تقديم المعطيات للغير كالإنتاج والبيع والاستيراد والتصدير. [24]

- **جريمة التعامل غير المشروع في معطيات متحصل عليها من جرائم ماسة بأنظمة المعالجة الآلية:**

يقوم النشاط الإجرامي لهذه الجريمة عن طريق القيام بأحد الأفعال التالية ، حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم الماسة بأنظمة المعالجة الألية للمعطيات .

بالنسبة للعقوبة المقررة لجريمة التعامل غير المشروع في المعطيات هي الحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000 دج، [25] سواء أخذت الجريمة شكل التعامل غير المشروع في معطيات صالحة لارتكاب جرائم المساس بأنظمة

المعالجة الآلية ، أو أخذت شكل التعامل غير المشروع في معطيات متحصل عليها من جرائم ماسة بأنظمة المعالجة الألية،

2 -مظاهر قصور النصوص الحالية على حماية حق الفرد في الخصوصية:

رغم سن المشرع الجزائري لمجموعة من النصوص القانون التي تحمي خصوصية الفرد في الفضاء الرقمي ، غير أن هناك جوانب من خصوصية الفرد تحتاج إلى حماية قانونية بما يتماشى مع ثقافة وتقاليد المجتمع الجزائري كمجتمع عربي ، يمكن رد عدم كفاية النصوص الحالية في حماية خصوصية الفرد لمجموعة من الأسباب :

السبب الأول : قيام المشرع الجزائري باستيراد تلك النصوص من فرمسا أو غيرها من الدول الأوروبية دون مراعاة لطبيعة وأعراف المجتمع الجزائري كمجتمع عربي مسلم ، حيث يلاحظ أن المشرع جرم تصوير شخص دون رضاه في مكان خاص دون أن يجرم أو يمنع التصوير في مكان عام ، ومن ثم لابد تجريم تصوير الشخص دون إذنه ورضاه حتى ولو كان التصوير في مكان عام ولا يبقى التجريم منحصرا في التصوير في الأماكن الخاصة ، حيث أن المادة 303 مكرر من قانون العقوبات حصرت تجريم التصوير في الأماكن الخاصة فقط دون الأماكن العامة ، وهذه المادة منقولة حرفيا من قانون الفرنسي ، ونظرا لخصوصية المجتمعات العربية ، فإن تصوير امرأة أو فتاة من غير إذنها حتى ولوكان في مكان عام ، فيه مساسا بحياتها وخصوصيتها ، بخلاف المجتمعات الأوروبية التي تختلف في ثقافتها واعرفها عن المجتمعات العربية ، لذا نقترح تجريم تصوير الشخص دون إذنه ورضاه حتى ولو كان التصوير في مكان عام .

السبب الثاني : عدم مواكبة النصوص القانونية للثورة التكنولوجيا الحاصلة سيما مع انتشار الهواتف الذكية ووسائل التوصل الاجتماعي ، حيث أن النص الذي يجرم تسجيل المكالمات والاحاديث الخاصة ادرج في قانون العقوبات سنة 2006 ومنذ ذلك الوقت لم يطرأ عليه أي إضافة أو تعديل ، وقتها لم يكن هناك انتشار للهواتف الذكية ووسائل التواصل الاجتماعي مثل ما عليه الحال اليوم ، لذلك لا نجد أي تجريم لتصوير ونشر المحادثات الإلكترونية سواء كانت المحادثات عبر البريد الإلكتروني أو عن طريق مختلف وسائل التواصل الاجتماعي ، فالمشرع استعمل كلمة "التقط" ، وعبارة التقط غير دقيقة في مجال

التجريم فهي لا تفيد هل التقط محادثات مسموعة أو رسائل مكتوبة عن طريق ما يسمى صورة شاشة (screen capture) ، فالنصوص الجنائية لا بد أن تكون عباراتها صريحة لا تحتمل أي شك في تحديد مدلولها ، لذا نقترح تعديل المواد 303 مكرر والمادة 303 مكرر 1 بإدراج تصوير المحادثات المكتوبة التي تتم بالطرق الإلكترونية ضمن أحكام المواد 303 مكرر والمادة 303 مكرر 1.

ومن مواطن القصور في حماية الحق في الخصوصية بسبب عدم مواكبة النصوص القانونية للتطورات التكنولوجيا ، نلاحظ عدم وجود نصوص قانونية صريحة تجرم فتح حساب أو صفحة أو موقع باسم شخص ما دون إذنه أو طلبه ، باستثناء بعض النصوص العامة القديمة التي تعاقب على انتحال الصفة ، لذا نقترح على المشرع الجزائري سن نصوص قانونية صريحة تجرم فتح حساب أو صفحة أو موقع باسم شخص ما دون إذنه أو طلبه وتشدد العقوبة إذا قام المعني بنشر منشورات باسم الضحية .

خاتمة:

من خلال درستنا لموضوع حدود حماية الحق في الخصوصية في الفضاء الرقمي في ضوء التشريع الجزائري توصلنا إلى مجموعة من النتائج والتوصيات نشير إليها على النحو التالي :

حماية للحق في الخصوصية في الفضاء الرقمي تم سن مجموعة من النصوص القانونية التي تجرم بعض صور المساس بالحياة الخاصة للفرد في الفضاء الرقمي ، عن طريق تجريم التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية، بغير إذن صاحبها أو رضاه، وتجريم التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه، كما جرم كذلك الاحتفاظ أو وضع في متناول الجمهور أو الغير التسجيلات أو الصور ، كما جرم الدخول عن طريق الغش إلى منظومة المعالجة الآلية للمعطيات أو يحاول الدخول إليها.

يلاحظ عدم مواكبة النصوص القانونية للثورة التكنولوجية الحاصلة سيما مع انتشار الهواتف الذكية ووسائل التوصل الاجتماعي ، حيث أن النص الذي يجرم تسجيل المكالمات والاحاديث الخاصة ادرج في قانون العقوبات سنة 2006 ومنذ ذلك الوقت لم يطرأ عليه أي إضافة أو تعديل ، وقتها لم يكن هناك انتشار للهواتف الذكية ووسائل التواصل الاجتماعي

مثل ما عليه الحال اليوم ، لذا نقترح تعديل المواد 303 مكرر والمادة 303 مكرر 1 بإدراج تصوير المحادثات المكتوبة التي تتم بالطرق الإلكترونية ضمن أحكام المواد 303 مكرر والمادة 303 مكرر 1.

يلاحظ أن المشرع الجزائري لم يبين مدى إباحة التسجيل من عدمه إذا كان الغرض منه إثبات جرائم تقع حالا أو جرائم وقعت ،كأن يقوم الشخص بتسجيل معلومات هامة عن جريمة أو يقوم بتسجيل تهديد بالقتل من طرف شخص آخر. فإني أرى أنه يتعين إدراج تسجيل مكالمات وأحاديث لأجل إثبات وقائق إجرامية ضمن أسباب الإباحة .

يلاحظ أن المشرع يجرم التصوير الذي يكون بغير رضا الشخص إذا كان في مكان خاص فقط ، دون تجريم تصوير الشخص في مكان عامة ، لذا نقترح ضرورة تجريم تصوير الشخص اذا تم دون إذنه ورضاه حتى ولو كان التصوير في مكان عام ولا يبقى التجريم منحصرا في التصوير في الأماكن الخاصة ، حيث أن المادة 303 مكرر من قانون العقوبات حصرت تجريم التصوير في الأماكن الخاصة فقط دون الأماكن العامة ، وهذه المادة منقولة حرفيا عن قانون العقوبات الفرنسي ، ونظرا لخصوصية المجتمعات العربية ، فإن تصوير امرأة أو فتاة من غير إذنها حتى ولوكان في مكان عام ، فيه مساس بحياتها وخصوصيتها .

نقترح النص صراحة على تجريم تصوير ونشر المحادثات الإلكترونية سواء كانت المحادثات عبر رسائل هاتفية أو البريد الإلكتروني أو عن طريق مختلف وسائل التواصل الاجتماعي.

كما نقترح لنص صراحة بنصوص مستقلة تجريم فتح حساب أو صفحة أو موقع باسم شخص ما دون إذنه أو طلبه ، وتشدد العقوبة إذا قام المعني بنشر منشورات باسم الضحية .

الهوامش:

[1] زواوي شنة ،الحماية القانونية للحق في حرمة المحادثات الهاتفية ، دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية جامعة بسكرة ، عدد 19 جوان 2018 ، ص 660.

[2] زواوي شنة ،مرجع سابق ، ص 660.

[3] المادة 303 مكرر /4 من قانون العقوبات " يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذه المادة بالعقوبات ذاتها المقررة للجريمة التامة".

[4] المادة 30 من قانون العقوبات :"كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها".

[5] أوهايبية عبد الله ، شرح قانون العقوبات - القسم العام- المؤسسة الوطنية للفنون المطبعية ، وحدة الرغاية ، الجزائر ، طبعة 2011 ص 252 .

[6] المادة 303 مكرر من قانون العقوبات " 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."

[7] سارة مهناوي الحماية الجنائية للحق في حرمة الحياة الخاصة في التشريع الجزائري، مجلة العلوم القانونية و الاجتماعية ،جامعة الجلفة ،المجلد الخامس ، العدد الثاني ، جوان 2020،ص 192 .

[8] سارة مهناوي مرجع سابق ،ص 192 .

[9] سارة مهناوي مرجع سابق ،ص 192 .

[10] سمية بلغيث ، الحماية الجنائية للحق في حرمة الحياة الخاصة، أطروحة دكتوراه ، كلية الحقوق ،جامعة أم البواقي ، السنة الجامعية 2020 – 2021،ص 79.

[11] سمية بلغيث ، مرجع سابق ص79.

[12] المادة 303 مكرر من قانون العقوبات " 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- .....

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"

[13] نويري عبد العزيز ، الحماية الجزائية للحياة الخاصة ، أطروحة دكتوراه كلية الحقوق والعلوم السياسية ،جامعة باتنة ، السنة الجامعية 2010 – 2011 ،ص144

[14] سمية بلغيث ، مصدر سابق ، ص86 .

[15] سمية بلغيث ، مصدر سابق ، ص87 .

[16] المادة 303 مكرر 1 من قانون العقوبات : " يعاقب بالعقوبات المنصوص عليها في المادة السابقة كل من احتفظ أو وضع أوسمح بأن توضع في متناول الجمهور أو الغير، أو استخدم بأية وسيلة كانت، التسجيلات أو الصور أو الوثائق المتحصل عليها بواسطة أحد الأفعال المنصوص عليها في المادة 303 مكرر من هذا القانون.

[17] المادة 303 مكرر من قانون العقوبات " 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"

[18] نادية سلامي ، آليات مكافحة التجسس الإلكتروني، أطروحة دكتوراه كلية الحقوق ،جامعة تبسة ،السنة الجامعية 2018-2019 ص 208 .

[19] سهيل محمد العزام، الوجيز في جرائم الأنترنت ،الطبعة الأولى ،دائرة المكتبة الوطنية، الأردن، 2009 ، ص 115-116

[20] نصت المادة 394 مكرر من قانون العقوبات على ما يلي :" يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة".

[21] نادية سلامي ، مرجع سابق، 115- 116 .

[22] نصت المادة 394 مكرر 1 من قانون العقوبات على ما يلي : " يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات وبغرامة من 500.000دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

[23] نادية سلامي ، مرجع سابق، 218

[24] نادية سلامي ، مرجع سابق، 219

[25] المادة 394 مكرر 2 :" يعاقب بالحبس من شهرين (2) إلى ثلاث (3) سنوات وبغرامة من 1.000.000دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي:

- 1تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات محزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

-2 حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

نطاق الحماية القانونية للحق في الخصوصية الرقمية
في ظل الاتفاقيات الدولية و في التشريع الجزائري

الاستاذة كباب مباركة /استاذة محاضرة ا
كلية الحقوق سعيد حمدين - جامعة الجزائر -1-
البريد الالكتروني : yelles1@outlook.fr

الملخص :

في ظل تطور التكنولوجيا الحديثة زاد من مخاطرها على الحق في الحياة الخاصة وأضحى الفرد مقيدا في تعاملاته ، من خلال رصد البيانات الشخصية وتخزينها ومعالجتها بواسطة مختلف الوسائط المعلوماتية، كتقنيات المراقبة والتجسس والقرصنة والمساس بالمعطيات الخاصة بالأفراد ، و هي جميعها تمثل تهديدا مباشرا على حياتهم الخاصة و حرياتهم الفردية .

و هذا ما أدى الى تكريس الحماية على هذا الحق ، سواء على المستوى الدولي أو على المستوى الداخلي ، حيث أخذت مختلف التشريعات الداخلية على عاتقها وضع قواعد لحماية ومكافحة جرائم تقنية المعلومات بشكل عام و محاربة الانتهاكات الماسة بحق الخصوصية في المجال المعلوماتي بشكل خاص .

و المشرع الجزائري كغيره عمل على الاعتراف بهذا الحق كمبدأ دستوري بشكل عام وحمايته في مختلف القوانين الداخلية بشكل خاص .

الكلمات المفتاحية : الحق في الخصوصية ، المواثيق الدولية ، الحياة الخاصة ، الحرية الفردية .التجسس .

Summary :

In light of the development of modern technology, it has increased its risks to the right to private life, and the individual has become restricted in his dealings by monitoring, storing and processing personal data by various information media, such as surveillance techniques, espionage, piracy and compromising the data of individuals, all of which represent a direct threat to their private lives and individual freedoms. .

This is what led to the protection of this right, whether at the international level or at the internal level, as the various internal legislations have taken upon themselves the establishment of rules for the protection and combating of information technology crimes in general and the fight against the dire violations of the right to privacy in the information field in particular.

And the Algerian legislator, like others, worked to recognize this right as a constitutional principle in general and to protect it in various internal laws in particular.

Keywords: the right to privacy, international conventions, private life, individual freedom. Espionage.

المقدمة

يعد الحق في الخصوصية أحد الحقوق الملازمة لحياة الفرد ، وتعتبر من أهم الحقوق المتصلة بشخصيته، لما لها من أثر كبير في حفظ الكرامة الإنسانية كما يصنف الحق في الخصوصية ضمن أهم الحقوق لاتصاله بكيان الفرد وتستهدف حماية الحق في الخصوصية صون كرامة الإنسان واحترام أدميته، لكن التقدم التكنولوجي أصبح يشكل انتهاك على الخصوصية وهذا عبر وسائل الإعلام الجديد بمختلف وسائله. وعلى هذا الأساس أوجبت المنظومة الأممية على الدول الأطراف احترام الحق في الخصوصية والالتزام بحمايته من التدخل التعسفي وغير المشروع.

وسنحاول في هذه الورقة البحثية الاجابة عن الاشكالية التالية: ما مدى ملائمة النصوص الدولية واستجابتها لحماية الخصوصية في العصر الرقمي؟ و هل وفق المشرع الجزائري في تحقيق هذه الحماية من خلال مختلف النصوص التشريعية الصادرة في هذا الشأن .

وسوف يتبع هذا البحث المنهج الوصفي التحليلي لما عليه الحال بشأن الحق في الخصوصية، حيث سوف يتم إدراج مجموعة من النصوص الدولية و الوطنية وتحليلها.

المحور الأول : حماية الحق في الخصوصية في المواثيق والاتفاقيات الدولية

سوف نتطرق في هذا المحور إلى نطاق حماية الحق في الخصوصية في مختلف المواثيق و الاتفاقيات الدولية و لكن قبل الولوج في هذا النطاق لا بد من التطرق الى مفهوم هذا الحق .

أولا : مفهوم الحق في الخصوصية

كثيرة هي المصطلحات التي تدل على المعنى الواحد، فنجد فئة تتكلم عن الحق في الخصوصية وفئة أخرى تتكلم عن الحياة الخاصة، وهناك من يتكلم عن الحياة الحميمية، والبعض الآخر عن الوحدة والعزلة [1] ، ولهذا كان من الضروري أن ينصب هذا المفهوم على لفظ واحد متفق عليه ، يلم الأفكار المشتتة في قالب واحد، ذلك أن توحيد المفاهيم في المجال الواحد يسهل عملية التحليل والتركيب ومن ثمة إيجاد صيغ موحدة تكون على أساسها التعريفات[2]

ولقد وجدنا أغلب الدراسات تناولت الموضوع تحت عنوان الحق في احترام الحياة الخاصة، أو الحق في حرمة الحياة الخاصة، وهو المصطلح الأول والتقليدي الذي ظهر به الحق والذي ارتبط بالفهم والتصور الذي كان سائدا وهو أن سكن الإنسان هو القلعة الحصينة التي تحمي حياته الخاصة من التطفل والانتهاك.

وكانت جل الدساتير تقتصر على مبدأي حرمة المسكن وسرية المراسلات، كمظهرين لهذا الحق، مما جعل مصطلح الحياة الخاصة يربط الذهن بأنها تلك الحياة التي يمارسها الأفراد في الأماكن الخاصة.

كما أن القانون الفرنسي هو الذي كان له السبق في الاعتراف بهذا الحقن فلقد اعتمد على مصطلح الحق في الحياة الخاصة مستندا في ذلك على معيار المكان، أي أن الحياة الخاصة هي تلك الأحداث التي تدور خلف الجدران، وهو ما يؤكد أن مصطلح الحق في الحياة الخاصة مرتبط بالمكان أكثر من الشخص [3].

لكن التطور التي طرأ على العالم من خلال جمع وتخزين وتبادل ونقل البيانات الشخصية، أي يمكننا أن نقول أصبح عالم رقمي، وهو ما غير المفهوم من الحياة الخاصة إلى الخصوصية، وهذه الأخيرة ترتبط بالشخص أكثر من المكا ن [4] ، وبهذا نجد القانون يهدف إلى حماية الأشخاص، فالخصوصية هي التي تسبغ الحماية على المكان سواء كان عاما أو خاصا، فالمهم هي الحالة التي يكون عليها الشخص لكي يتمتع بالحماية القانونية، وهو ما ذهب إليه المشرع الجزائري حيث بين أن الخصوصية مرتبطة بالوقائع والتصرفات من خلال المادة (24) من المرسوم التشريعي المتعلق بالمنظومة الاحصائية [5] " لا يحق للمصلحة المؤتمنة أن تكشف أو تنشر المعلومات ... ولها علاقة بالحياة الشخصية والعائلية وعلى العموم الوقائع والتصرفات الخصوصية."...

وهناك كثير من الدول يربطون مفهوم الخصوصية بمفهوم حماية البيانات، وهو ما يضع الخصوصية ضمن اطار الحق في حماية البيانات الخاصة، وفي خارج نطاق هذا المفهوم فإن الخصوصية ظهرت كوسيلة لتحديد الخطوط الفاصلة بين حق الفرد المطلق وبين حق المجتمع بالتعرض لشؤونه .

وفي أنظمة قانونية أخرى كانت الخصوصية هي الحرية في مواجهة كل اعتداء أو انتهاك [6] ، وكان هذا التباين السبب وراء نشوء العديد من التعريفات التي كانت إما تتوسع في تحديد فكرة الخصوصية إلى درجة اقتران الفكرة بالحرية عموما، وإما تتعمد إلى التضييق من نطاق الخصوصية لتكون لدى البعض بمعنى الخصوصية المادية التي لا تعني أكثر من حق العزلة، وإما تمتد الخصوصية المعنوية لتشمل السرية، أو نجدها تمتد لكل مظهر من مظاهر التدخل فتكون الحق العام في السيطرة على المعلومات الشخصية، الحق في العزلة والسرية في أن يترك الشخص وحيد ا.

وهناك العديد من التعريفات ، حيث أن فكرة الخصوصية فكرة مرنة تحكمها معايير وعادات وتقاليد المجتمع الذي تنتمي إليه، فكل فرد يرغب في الاحتفاظ بجزء من حياته وأفكاره، الخاصة لنفسه بعيدا عن حب استطلاع الآخرين، وهذه الأشياء تتطور وتتغير باستمرار من مجتمع لآخر.

و بالتالي فأن الفرق بين الحق في الحياة الخاصة وبين الحق في الخصوصية هو أن المصطلح الأول يمثل غالبا الجانب المادي كحرمة المسكن وحرمة المراسلات، أما مصطلح الخصوصية يمثل غالبا المظاهر المعنوية كالمحادثات الشخصية والمكالمات الهاتفية.

ثانيا: الحماية الدولية للحق في الخصوصية

حظيت حقوق الإنسان بالاهتمام اللازم من طرف الدول، وذلك تطبيقا لإرادة شعوب العالم التي سعت بإلحاح للمطالبة بها، وقد تبلور هذا الاهتمام بصدور الإعلان العالمي لحقوق الإنسان عن الأمم المتحدة والذي جاء بجملة من الحقوق من بينها الحق في الخصوصية، واهتمت به جميع المنظمات الدولية عالمية أم إقليمية فعقدت بشأنه الاتفاقيات وكذا المؤتمرات الدولية [7]..

1- في المواثيق والاتفاقيات الدولية

إن مجمل المواثيق والاتفاقيات الدولية المتعلقة بحقوق الإنسان تعبر عن التزام الدول باحترامها لخصوصية الأفراد، هذا الالتزام يثبت من خلال مراجعة النصوص الداخلية للدول وتعديلها حسب نصوص المواثيق والاتفاقيات الدولية والتي تكون الدولة طرفا فيها، ولقد أصبح الآن معروفا بأن بعض أحكام المواثيق والاتفاقيات قد ارتقت

وأصبحت قواعد عرفية، ما يعني التزام الدول بها حتى ولو كانت غير موقعة عليها ، ومن أبرز هذه المواثيق الإعلان العالمي لحقوق الإنسان والذي نص على:" لا يجوز أن يتعرض أحد للتدخل التعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو بحملات على شرفه وسمعته ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات .

أمّا عن العهد الدولي للحقوق المدنية والسياسية فقد نص على ضرورة عدم التدخل بشكل تعسفي أو غير قانوني في خصوصيات الشخص وأسرته وحرمة مسكنه وسرية مراسلاته والحفاظ على سمعته وشرفه .

ولقد جاء النص عليه أيضا في الاتفاقية الأوروبية لحقوق الإنسان حيث اهتمت هذه الاتفاقية بالحفاظ على الحقوق والحريات العامة والشخصية للمواطنين الأوروبيين، وكذا بتحريم المساس بحرمة الحياة الخاصة مع تقرير حق الأفراد في الخصوصية من خلال احترام حياته الخاصة والعائلية ومسكنه ومراسلاته، وجاء النص فيها أيضا على عدم التدخل في ممارسة هذا الحق من خلال السلطة العامة إلا ما كان ينص عليه القانون .

وبالرجوع إلى المادة (18) في فقرتها الأولى، يلاحظ أنها تضمنت احترام كل من الحياة الخاصة والعائلية والمسكن والمراسلات لكل فرد يوجد على إقليم أي من الدول الأطراف في الاتفاقية الأوروبية لحقوق الإنسان، بمعنى أنها سوت بين مواطني الدولة التي يتم فيها خرق هذه الحقوق ومواطني الدول الأخرى الأطراف في الاتفاقية، وحتى بين مواطني الدول غير الأعضاء فيها، طالما هم مقيمون في إحدى الدول الأطراف . أما الفقرة الثانية من المادة (18) فإنها ترفض أي تدخل للسلطة العامة في كيفية ممارسة هذا الحق من طرف صاحبه كما لا تجيز للسلطة ذاتها تقييد ممارسته، إلا إذا كانت النصوص التشريعية للدول المعنية تجيز لها ذلك، وبما لا يتعدى القدر الضروري لتحقيق الأغراض التي من أجلها سمح بالتدخل .

كما أن الاتفاقية الأمريكية لحقوق الإنسان هي الأخرى جاء النص فيها على حماية الحق في الخصوصية من خلال احترام الفرد لشرفه وعدم الاعتداء غير المشروع عليه وصون كرامته ، كما لا يجوز التدخل بشكل تعسفي في حياته الخاصة أو شؤون أسرته أو منزله أو مراسلاته، وإن كان هناك تدخل أو اعتداء فالقانون يحميه

ويلاحظ أن الاتفاقية الأمريكية نصت كنظيرتها الأوروبية على حماية حقوق المواطن الأمريكي بطريقة مباشرة، إضافة إلى أنها ميزت مثلها أيضا بين الحياة الخاصة والحق في الشرف والاعتبار، ودعمت ضمان تنفيذ هذه الحقوق بصفة إلزامية عن طريق الجهازين الرسميين لهذا الغرض.

2- من خلال المؤتمرات

عقدت العديد من المؤتمرات منها ما هو دولي ومنها ما هو اقليمي كلها دعت إلى المحافظة على الخصوصية، وهذا خاصة بعد الانتهاكات التي أصبح يتعرض لها بصفة متزايدة وخطيرة، بسبب التطورات العلمية والتكنولوجية منها:

أ -(مؤتمر طهران :1968

أنعقد في الفترة ما بين 22 أبريل و13 ماي 1968، يعد هذا المؤتمر الأول على الصعيد الدولي لبحث قضايا حقوق الإنسان من كافة جوانبها، حيث عني ببحث الصعوبات المتعلقة بأعمال هيئة الأمم المتحدة الهادفة إلى تدعيم احترام حقوق الأنسان والحريات الأساسية. وصدر عن المؤتمر عدّة قرارات بهذا الشأن، يهم في هذا المقام القرار 11 الذي يهدف إلى حماية حق الإنسان في حياته الخاصة.

ب مؤتمر مونريال 1968

انعقد من 14 إلى 18 أكتوبر 1968، تم فيه البحث ودراسة الآثار السلبية التي يعكسها التقدم التكنولوجي على خصوصية الأفراد.

ج -المؤتمر الدولي لخبراء اليونسكو :1970

اجتمع خبراء اليونسكو في مدينة باريس في الفترة الممتدة بين 19 إلى 23 جانفي 1970، وهذا قصد دراسة موضوع الحياة الخاصة للفرد، حيث أن هذا الموضوع قد تفرعت عنه مشكلات أدت إلى تعارض مصلحة الفرد وحقه في حرمة حياته الخاصة مع حق المجتمع والمصلحة العامة مما استلزم بحث هذه المسائل بجدية لإحداث توازن بينهما.

والملاحظ على هذه الاتفاقيات والمؤتمرات بالرغم من حمايتها للحياة الخاصة بصورتها التقليدية إلا أنها لم تعالج مسألة حماية الحياة الخاصة في ظل نشوء وتطور التكنولوجيا المعلوماتية فكلها نصوص تحمي الحياة الخاصة بشكلها التقليدي لا بشكلها المستحدث.

فعمليات الكشف الهائلة المتعلقة بنطاق عمل أنظمة المراقبة التابعة للدول أثار مناقشة دولية بخصوص الحق في الخصوصية مقابل الأمن الوطني، ومع التسليم بأن التطورات التكنولوجية الهائلة زادت قدرة الدول والجهات التجارية الفاعلة على المراقبة وفك الشيفرات وجمع مقادير ضخمة من البيانات، وهو ما قد يفضي إلى التدخل بشكل خطير في حق الناس في الخصوصية، فقد ركزت الدول في نقاشاتها على المسألة الحاسمة المتعلقة بكيفية تحقيق

توازن ملائم بين الشواغل الأمنية الوطنية المشروعة والحريات الفردية وكنتيجة لذلك ظهرت عديد من التوجهات الدولية بهذا الخصوص، أهمها قرار الجمعية العامة للأمم المتحدة رقم (68/167) الخاص بالحق في الخصوصية في العصر الرقمي.

ولقد جاء في هذا القرار بشأن الحق في الخصوصية في العصر الرقمي، القلق الشديد بشأن القدرة المتنامية للمؤسسات الحكومية على الوصول إلى خصوصيات الأفراد من خلال المراقبة عبر الوسائل التكنولوجية سواء كان الأشخاص المراقبين داخل الدولة أو خارجها. في هذا الصدد جاء القرار باتجاهين فيما يتعلق بهذه المسألة.

فالاتجاه الأول يتضمن التأكيد على حق الأفراد في الخصوصية في ظل هذا التقدم التكنولوجي المستوى ذاته الذي أقرته الاتفاقيات والأحكام الدولية بشأن الحق في الخصوصية، وعلى وجه التحديد أشار القرار في الفقرة الثانية من ديباجته إلى ما أقرته المادة (12) من الإعلان العالمي لحقوق الإنسان والمادة (17) من العهد الدولي للحقوق المدنية والسياسية بشأن الحق في الخصوصية وواجب التقيد بهما دوليا، كما اعتبر القرار أن الحماية القانونية للحق في الخصوصية كما جاءت به هذه المواد يعد أساسا للحق في التعبير عن الرأي وحمل الأفكار دون تدخل، وأكد القرار في فقرته التنفيذية الثالثة أن" ذات الحقوق التي تثبت للأفراد في خارج نطاق الانترنيت يجب أن تكون محمية على الانترنيت بما فيها الحق في الخصوصية."

كما أن هذا التقرير أكد على ارتباط الحق في التجمع السلمي بالحق في الخصوصية من خلال المراقبة الالكترونية وجمع البيانات الشخصية ، اما الاتجاه الثاني الذي جاء به القرار، فقد كان في إطار عدم إجماع الدول على موقف واحد بشأن ما يعد تدخلا تعسفيا في خصوصيات الأفراد، والذي كان نتيجة صدور هذا القرار دون تصويت. ولقد طلب القرار من المفوض السامي لحقوق الإنسان إعداد تقرير حول حماية الحق في الخصوصية وتعزيزه في ضوء التطور التكنولوجي، على أن يسلم هذا التقرير إلى مجلس حقوق الإنسان والجمعية العامة للأمم المتحدة .

المحور الثاني : نطاق حماية الحق في الخصوصية في ظل التشريع الجزائري

أخذت مختلف التشريعات الداخلية للدول على عاتقها تأسيس قواعد حماية لمكافحة جرائم تقنية المعلومات بشكل عام ، و محاربة الانتهاكات الماسة بحق الخصوصية في المجال المعلوماتي بشكل خاص .

كغيره من التشريعات عمل المشرع الجزائري على الاعتراف بحق الخصوصية بشكل عام كمبدأ دستوري من خلال بنص صريح ." لا يجوز انتهاك حرمة المواطن الخاصة و حرمة شرفه و يحميها القانون ، سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة ".

و قبل التطرق الى هذه الحماية لا باس ان نقدم بعض المبررات في هذا الشأن .

مبررات الحماية للحق في الخصوصية الرقمية في التشريع الجزائري

ان التطور التكنلوجي الحديث و في ظل ازدياد المخاطر على الحق في الحياة الخاصة ، اصبح الفرد مقيدا في تعاملاته من خلال رصد البيانات الشخصية و تخزينها ، بواسطة مختلف الوسائط المعلوماتية و المساس بالمعطيات الخاصة بالأفراد ، و من أهم هذه المبررات يمكن ذكر ما يلي :

- اتساع شبكة الانترنت : لقد أثبت الواقع ان اهم التقنيات التي تتحكم في مجموع التعاملات الالكترونية تعتمد على شبكة الانترنت ، فتدفق المعلومات و الاتصالات عبر الحدود دون أي اعتبار لحدود جغرافية ، يعمل الافراد على تبادل المعطيات الخاصة بهم لجهات مختلفة داخلية و خارجية ، و هو مايثير مخاطر اساءة استخدام هذه البيانات خاصة في الدول التي لا تتوفر فيها الحماية القانونية للبيانات الشخصية .

- فقدان آليات السيطرة في قنوات التعامل الالكتروني : ان اقرار قانون فعال يكرس من وجود استراتيجية ملائمة لحماية حق الافراد بعيدا عن العالم الرقمي قد يكون نوعا من السهولة بحيث يمكن للدولة وضع رقابة على الاعتداءات المختلفة ، الا ان الواقع يصدم في الصعوبة في التحكم في مركزية أسماء النطاقات و عناوين المواقع و غيرها ، و هو ما يوسع من دائرة اختراق حق الأفراد و يصعب من الحماية ضد أي انتهاكات لخصوصيتهم و هذا لفقدان المركزية و آليات التي تعمل على السيطرة على هذه الخروقات .

نطاق الحماية للحق في الخصوصية الرقمية في التشريع الجزائري

يعتبر المشرع الجزائري المحادثات الشخصية وصورة الشخص مظهرين أساسين للحق في الخصوصية، وذلك حماية لما يدور من حديث وما يتخذه الشخص من أوضاع اعتمادا على أنه لا يطلع عليه أحد، ولقد حدد المشرع أشكال الاعتداء على الأحاديث الشخصية والسرية من خلال المادة 303 مكرر الفقرة الأولى من قانون العقوبات الجزائري حيث أنه يعتبر أن التقاط أو تسجيل مكالمات أو أحاديث خاصة أو سرية أو صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه جنحة يعاقب عليها بالحبس .

و عليه فلقد كرس المشرع الجزائري مبدأ الحماية الجنائية بموجب قانون العقوبات الذي نص على أنه : يعاقب بالحبس من 06 أشهر الى 3 سنوات كل من تعمد المساس بحرمة الحياة الخاصة باي تقنية كانت ذلك :

- التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أ سرية بغير اذن صاحبها أو رضاه .
- التقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير اذن صاحبها او رضاه و يعتبر هذا النص قد حمل في طياته الحماية المرنة التي تمتد الى أي طبيعة لحق الخصوصية أو الحديث و هذا باستخدام عبارة أي تقنية كانت "

و من هذا المنطلق نجد أن المشرع لم يتجه الى اصدار قانون ينص على الحماية للخصوصية في المجال الالكتروني ، الا أنه اكتفى بمواكبة محاربة جريمة المساس بالحق في الخصوصية في العالم الرقمي بموجب القانون رقم 15-04 المتضمن تعديل قانون العقوبات في القسم المعنون المساس بأنظمة المعالجة الآلية للمعطيات ، و من خلال نص المادة 39 السالفة الذكر : يعاقب بالحبس من 03 أشهر الى سنة أو بغرامة من 50 ألف الى 100 ألف كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك .

بالإضافة الى تجريم عمليات تجميع أو توفير أو نشر او الاتجار في معطيات مخزنة أو افشاء أو استعمالها لأي غرض كل المعطيات المتحصل عليها من الجرائم المنصوص عليها في هذا القسم ..

لقد وفر المشرع الجزائري الحماية الجنائية لحق الخصوصية الرقمية بموجب القانون 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال [8] في المادة الرابعة منه ، و هذا بضمن عدم المساس بالحياة الخاصة للأفراد في حالة قيام السلطات المختصة بالقيام بعمليات المراقبة لكل الاتصالات الالكترونية بهدف الوقاية من الافعال الموصوفة بجرائم الارهاب و التخريب او الجرائم الماسة بأمن الدولة .

ويتبن لنا أن المشرع الجزائري قد اتخذ معيار خصوصية المحادثات ضابطا لا تتحقق دونه جريمة الاعتداء على الحق في الخصوصية، فالعبرة ليست بحماية المكان وإنما بطبيعة الواقعة أو المحادثة، فحماية القانون تمتد لتشمل المكالمات وكل حديث خاص أو سري ولو كان قد أجري في مكان عام .

الخاتمة:

و في الختام يمكننا القول أن قواعد القانون الدولي و كذا القوانين الوطنية قد وفرت الحماية للخصوصية الا أنها لم تتعاط مع اشكالية التطور التكنولوجي.

كما نستخلص ان الحماية الدولية لحقوق الانسان ذات أهمية كبيرة نظرا للدور الذي تقوم به مختلف المواثيق و المؤتمرات الدولية في ترسيخ تلك الحقوق و دعمها على المستوى الاقليمي في ظل النظام القانوني للدول .

الا أن الاستغلال السيء لتقنية المعلومات باستخدام البيانات الخاصة للافرا د من خلال الصور و البصمة الرقمية تؤدي الى انشاء حسابات وهمية تضر بالأشخاص أو تمس بالأمن الوطني .

و هذا ما يؤدي بنا الى تقديم بعض التوصيات في هذا الشأن و تتمثل في :

- وضع قوانين خاصة و عقوبات صارمة تجرم الابتزاز و الاحتيال الالكتروني و التجسس الالكتروني.
- اعادة التكييف القانوني لهذه الجرائم في القانون الجزائري من جنحة لجناية .

قائمة المراجع

الكتب

-أحمد أبو الوفا، الوسيط في القانون الدولي العام، دار النهضة العربية، (القاهرة: 1998.(

-أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة: الطبعة 2، مصر ، 1962.

-حسين عمر، المنظمات الدولية، ، الطبعة الأولى ، دار الفكر العربي، القاهرة: ، 1993.

-عبد الفتاح بيومي حجازي، النظام القانوني للتجارة الالكترونية، المجلد الأول، دار الفكر الجامعي، الاسكندرية: 2002.

-عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشورات الحلبي الحقوقية، بيروت، 2003.

-نسرين عبد الحميد بنيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الاسكندرية، 2008.

-نعيم مغبغب، مخاطر المعلومات والانترنيت، منشورات زين الحقوقية، بيروت، 1998 .

- المقالات:

-بن بادة عبد الحليم وبوحادة محمد سعد، جريمة التجسس الإلكتروني نمط جديد من التهديدات السيبرانية الماسة بأمن دول المنطقة –دراسة سياسية قانونية-، ملتقى دولي أول أمن المعلومات في الفضاء الإلكتروني (الرهان والتحديات في شمال افريقيا)، المنعقد يومي 17و18 فيفري 2020، كلية الحقوق والعلوم السياسية، جامعة غرداية.

-حسن السوداني، تكنولوجيا الإعلام الجديد وانتهاك حق الخصوصية، مجلة دفاتر السياسة والقانون، العدد 11، جوان 2014.

-زينب محمد جميل الضناوي، الحماية القانونية للخصوصية على الانترنيت في ظل الجهود الدولية والداخلية، مؤتمر دولي: الخصوصية في مجتمع المعلوماتية، لبنان، 19 و2019/07/20.

- **الرسائل الجامعية**:

-بشاتن صيفية، الحماية القانونية للحياة الخاصة (دراسة مقارنة)، رسالة دكتوراه، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، 2012.

-بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا، أطروحة دكتوراه، تخصص قانون دستوري، جامعة الحاج لخضر، باتنة، 2014-2015 .

- **التقارير:**

-مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، الدورة 27، 30 جوان 2014،

-مفوضية الأمم المتحدة، التقرير السنوي لمفوضية الأمم المتحدة، 19 ديسمبر 2011.

-مجلس حقوق الإنسان، تقرير المقرر الخاص المعني بتعزيز وحماية حقوق الإنسان والحريات الأساسية في سياق مكافحة الإرهاب، الدورة 13، 28 ديسمبر 2009، ص17.

- **الاتفاقيات الدولية:**

-الاتفاقية الأمريكية الصادرة سنة 1969

-العهد الدولي للحقوق المدنية والسياسية الصادر في 16 ديسمبر 1966.

-الاتفاقية الأوروبية لحقوق الإنسان الصادرة في 1950.

-الإعلان العالمي لحقوق الإنسان الصادر 10 ديسمبر 1948.

القوانين :

-المرسوم التشريعي رقم 94-01، المتعلق بالمنظومة الاحصائية. المؤرخ في 15 جانفي 1994، ج العدد 03، المؤرخة في 16 جانفي 1994.

-القانون رقم 09-06 المؤرخ في 2009/08/05 ، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، ج ر العدد 47.

الهوامش

[1]وهو ما قال به الفقيه " مارتن"، ينظر: عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، منشورات الحلبي الحقوقية، بيروت، 2003، ص244.

[2]بن سعيد صبرينة، حماية الحق في حرمة الحياة الخاصة في عهد التكنولوجيا، أطروحة دكتوراه، تخصص قانون دستوري، جامعة الحاج لخضر، باتنة، 2014-2015، ص10.

[3] بن حيدة محمد، الحق في الخصوصية في التشريع الجزائري (دراسة مقارنة)، رسالة ماجستير، تخصص حقوق وحريات، الجامعة الافريقية العقيد أحمد دراية، ادرار، 2009-2010، ص23

[4] حسام الدين كامل الأهواني، الحق في احترام الحياة الخاصة والحق في السمعة، د.د، القاهرة، ط3، ص118.

[5] المرسوم التشريعي رقم 94-01، المؤرخ في 15 جانفي 1994، المتعلق بالمنظومة الاحصائية، ج العدد 03، المؤرخة في 16 جانفي 1994،

[6] أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، ط2، 1992، ص11.

[7] هدى حامد قشقوش، جرائم الحاسب الالكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص10 وما بعدها.

[8] القانون رقم 09-06 المؤرخ في 2009/08/05 ، المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام و الاتصال و مكافحتها ، ج ر العدد 47.

خصوصية الجريمة الالكترونية و آليات مكافحتها في التشريع الجزائري
" الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها نمـوذجا "

Privacy of cybercrime and mechanisms to combat it in Algerian legislation "The National Authority for the Prevention and Control of Crimes Related to Information and Communication Technologies is developing and modelling "

لقب وإسم : د/ سماتي حكيمة أستاذة محاضرة قسم أ

مؤسسة الانتماء – كلية الحقوق ، جامعة الجزائر 1

البريد الإلكتروني: ***douchakima.univ@gmail.com***

البريد الإلكتروني المهني : ***h.smati@univ-alger.dz***

ملخص :

تعد الجرائم الإلكترونية أو كما يسميها المشرع الجزائري **بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال**" من أخطر الجرائم التي شهدها العالم اليوم ، وهي تشكل الوجه السلبي لانتشار استعمال تكنولوجيا و الانتقال من العالم الواقعي إلى العالم الرقمي الذي يرتكز على اقتحام التكنولوجيا في جميع مجالات الحياة، وفي سبيل التصدي لهذه الجريمة التي أصبحت تشكل تهديدا ليس فقط للأفراد، بل حتى الدول و المؤسسات الوطنية كونها تمس بالأمن الوطني ، عملت الدولة الجزائرية على غرار العديد الدول وفي إطار سياسات وطنية و دولية واسعة إلى تبني إستراتيجية شاملة لمواجهة الجرائم الالكترونية ومكافحتها.

وعلى هذا الأساس تهدف هذه المداخلة إلى إبراز خصوصية الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال"، و موقف الفقه و التشريع الجزائري ، في طبيعتها ومضمونها و نطاقها، و أنواعها ووسائلها و في خصوصية و تميز مرتكبيها، هذا من جهة ، ومن جهة أخرى، تبيان الإستراتيجية الجزائرية لمواجهة هذا النوع من الجرائم المستحدثة سواء على المستوى القانوني أو المؤسساتي أو القضائي ، مع دراسة نموذجية لأهم الآليات المستحدثة في هذا المجال ألا وهي" **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها**" كجهة رقابية الخاصة بهذا النوع من الجرائم ، **وعليه ستعتمد هذه** الدراسة على دراسة أهم الأحكام التي جاء بها القانون

04/09 المؤرخ في 5 أوت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال،و كذا المرسوم الرئاسي 172/19 مؤرخ في 2019/06/06 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تنظيمها و سيرها.

الكلمات المفتاحية : الجريمة الالكترونية، التكنولوجيا ، **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال،**

ABSTRACT

Cybercrime is one of the most serious in today's world. technology ", which constitutes the negative face of the widespread use of information and communication technology and the transition from the real world to the digital world where technology is broken into in all spheres of life, In order to address this crime, which has become a threat not only to individuals Even States and institutions that are prejudicial to national security, The Algerian State, like many States, has worked within the framework of broad national and international policies to adopt a comprehensive strategy to counter and combat cybercrime.

*It is on this basis that this intervention aims to highlight the privacy of cybercrime or "**Crimes relating to information technologies on communication**", attitude of Algerian jurisprudence and legislation, In their nature, content, scope, types, means and in the privacy and distinction of the perpetrators, On the one hand, and on the other hand, the Algerian strategy for combating this type of crime is established at the legal, institutional or judicial levels. with a model study of the most important mechanisms developed in this area: "National Authority for the Prevention and Control of Crimes Related to Information and Communication Technologies" As a supervisory body for this type of crime, the study will study the most important provisions of Law 09/04, and the same Presidential Decree 19/172 dated 06/06/2019 establishes the composition of the National Authority for the Prevention, Control, Organization and Conduct of Crimes Related to Information and Communication Technologies.*

مقدمة :

تعد الجرائم الالكترونية نتاجاً للممارسة السيئة لثورة التكنولوجيا المعلوماتية، وهذا ما أكسبها خصوصية تميزها عن الجرائم التقليدية ، كما تعتبر من بين الجرائم التي تباينت تسمياتها عبر المراحل الزمنية لتطورها التي ارتبطت بتقنية المعلومات، فقد اصطلح على تسميتها بداية " بإساءة استخدام الكمبيوتر" ، ثم " احتيال الكمبيوتر" ، " فالجريمة المعلوماتية " و " الجرائم السيبرانيـة " و " جرائم الانترنت" و غيرها ، فإن المشرع الجزائري اعتمد تسمية **" الجرائم المتصلة بتكنولوجيات الإعلام على و الاتصال"** في محاولة منه لمد نطاق التجريم على أقصى الحدود الممكنة و من أجل لفت الانتباه إلى أن السلوك الإجرامي يتجاوز المساس أو التلاعب بالمعطيات الآليـة إلى استعمال الوسائل التكنولوجيا لارتكاب حتى الجريمة بصورتها التقليدية.

و بغية ضمان الحق الدستوري[1] الذي أكده التعديل الدستوري لعام 2020 في المادة 47 و الذي يتضمن أنه **لكل شخص الحق في سرية مراسلاته و اتصالاته الخاصة في أي شكل كانت ... حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق شخصي .. يعاقب القانون على كل انتهاك لهذه الحقوق "** و في إطار مكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال وفي سبيل التصدي لهذه الجريمة التي أصبحت تشكل تهديدا ليس فقط للأفراد، بل حتى الدول و المؤسسات كونها تمس بالأمن الوطني ، عملت الدولة الجزائرية على غرار العديد الدول وفي إطار سياسات وطنية و دولية واسعة إلى تبني إستراتيجية شاملة لمواجهة الجرائم الالكترونية ومكافحتها.

وعلى هذا الأساس تهدف هذه المداخلة إلى إبراز خصوصية الجرائم الالكترونية أو " الجرائم المتصلة بتكنولوجيات الإعلام على و الاتصال"، و موقف الفقه و التشريع الجزائري ،و كذا إبراز الإستراتيجية الجزائرية لمواجهة هذا النوع من الجرائم المستحدثة سواء على المستوى القانوني أو المؤسساتي أو القضائي ، مع دراسة نموذجية لأهم الآليات المستحدثة في هذا المجال ألا وهي**" الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها"** كجهة رقابية الخاصة بهذا النوع من الجرائم ، كما ستعمد الدراسة على دراسة أهم الأحكام التي جاء بها القانون 04/09 ، و كذا المرسوم الرئاسي 172/19 مؤرخ في 2019/06/06 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تنظيمها و سيرها.

و عليه، يمكن طرح الإشكاليــة التالية: **فيما تتمثل خصوصية الجريمة الالكترونية، وما هي الإستراتيجية التي تبنها الدولية الجزائرية لمواجهة الجرائم الالكترونية في ظل التشريعات الوطنية و الدولية ؟**

و للإجابة على الإشكالية المطروحة تم تقسيم دراسة هذه الورقة البحثية إلى ثلاثة محاور:

المحـور الأول: خصوصية الجريمة الالكترونية

(الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال)

المحور الثاني: الإستراتيجية الجزائرية لمواجهة الجرائم الالكترونيـة في التشريع الجزائري

المحـور الثالث: " الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها كآليـة لمواجهة الجرائم الالكترونية

المحور الأول: خصوصية الجريمة الالكترونية في التشريع الجزائري
(الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال)

أولا: مفهوم الجريمة الالكترونيـة

اختلفت و تعدد تعاريف الجريمة الالكترونية ، و ذلك حسب الزاوية التي تعالجها أو التي ينظر إليها من خلالها ، فهناك التعاريف القانونية و أخرى تعرفها حسب أنماطها أو مواضعيها أو حسب مرتكبيها (سواء كانوا أفراد أو منظمات أو حكومات)، و سنعرض أهم التعريفات للجريمة الالكترونية ، و التي غطت مختلف الزاويا و التصورات لهذا المفهوم :

فهناك من عرفها بأنها " **كل نشاط إيجابي او سلبي من شأنه الاتصال دون وجه حق بالكيان المعنوي للحاسب الآلي او بنظام المعلومات العالمية و الإبقاء عليه عند تحققه ، أو التأثير عليه بتعطيله أو إضعاف قدرته على أداء وظائفه بالنسخ أو التعديل أو التعديل بالاضافةأو الحذف الكلي أو الجزئي أو بالمناقلة للخصائص الأساسية للبرامج ، أو مجرد النسخ أو الوصول إلى البرامج أو المعلومات المخزنة أو الوصول إليها أثناء نقلها أو إرسالها أو الاتصال بها من غير وجه حق بأي وسيلة كانت**".[2]

وقد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تينته " منظمة التعاون الاقتصادي و التنمية" للجريمة المعلوماتية في اجتماع باريس عام 1983 من أنها " **كل سلوك غير مشروع ، او غير أخلاقي ، أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها** ".

أما بالنسبة للمشرع الجزائري ، نلاحظ انه قد أغفل تنظيم مجال الجريمة الالكترونية ، إلا أنه في سنة 2004 تدراك المشرع ذلك الفراغ من خلال سن قواعد قانونية لمواجهة هذه الجريمة ، وذلك

تجلى في القانون رقم 15/04 المتضمن تعديل قانون العقوبات التي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الآلية للمعطيات، ثم تلاه القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتهما، فقد حدد القانون 04/ 15 من المادة 394 مكرر إلى المادة 394 مكرر 2 مفهوم المساس بأنظمة المعالجة الآلية للمعطيات ، حيث حددها في المادة 394 مكرر الآتي: "

- **الدخول و البقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.**
- **حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.**

أما المادة 394 مكرر 1 فقد أشارت إلى مايلي:

. إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها ، و بالنسبة للمادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات من الآتي :

- **تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طرق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم،**
- **حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم " .** [3]

أما القانون 09/ 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتهما، فقد عرف الجريمة الالكترونية او كما يسميها المشرع الجزائري ب **(الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال)** في المادة 02 بنصها " **يقصد في مفهوم هذا القانون بما يأتي : الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال : جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية**

- **منظومة معلوماتية : أي نظام منفصل او مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.**
- **معطيات معلوماتية : أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية ، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها ".** [4]

ثانيا: السمات الخاصة بالجرائم الالكترونية مقارنة بالجرائم التقليدية

تعد الجرائم الالكترونية أو جرائم المتصلة بتكنولوجيات الإعلام و الاتصال جرائم مستحدثة، وذلك في مقابل الجرائم التقليدية، ومن أبرز خصائص الجرائم الالكترونية ، يمكن ذكر ما يلي:

1/ الجريمة الالكترونية من الجرائم العابرة للحدود :

تعد هذه الخاصية من أهم الخصائص التي تميز هذه الجريمة هي تخطيها الحدود الجغرافية و اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها **" الجرائم العابرة للحدود"** ، لأن أماكن متعددة في مختلف الدول قد تتأثر بجريمة تكنولوجيا المعلومات الواحدة في آن واحد ، و بالنظر إلى سهولة ارتكابها عبر تقنية الانترنت.

وتثير هذه خاصية عالمية الحدود للجريمة الالكترونية عدة آثار أهمها القانون الواجب التطبيق عليها ، و القضاء المختص بها ، فهل هو قانون الدولة التي وقع فيها النشاط الإجرامي ، أم الدولة التي يقيم فيها الجاني أو الدولة التي تضررت مصالحها نجة هذا التلاعب [5]، و قد قام المشرع الجزائري بموجب القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها بسن قواعد خاصة بالتعاون و المساعدة القضائية و الدولية المتبادلة في الفصل السادس منه عن طريق المواد 16،17، 18 من ذات القانون ، كما أكدت المادة 15 من القانون 04/09 على أنه" زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني ، عندما يكون مرتكبها أجنبياً و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

2/ الجريمة الالكترونية سهلة الارتكاب : تقوم خصوصية الجريمة الالكترونية على سهولة ارتكابها بصورة فردية، إذ لا تحتاج أحينا الاستعانة بأشخاص آخرين لارتكابها، بعكس الجريمة التقليدية، فالجرم قادر على تنفيذ مخططه الإجرامي وهو جالس أما الكمبيوتر في منزله أو مكتبه أو مقهى الانترنت ضد الضحية الموجود في دولة أخرى و دوت الحاجة إلى بذل جهد عضلي لممارسة جريمته ، كما هو الشأن في الجريمة التقليدية التي تحتاج إلى التخطيط و الاستعانة بمعدات لتنفيذ الفعل الإجرامي.[6]

3/ **أن الجريمة الالكترونية من الجرائم الناعمة :** أن أول يلفت النظر في هذا النوع من الجرائم هو نعومتها و بعدها عن العنف فلا تتطلب لارتكابها الشدة و لا استعمال الأدوات الخطرة كالأسلحة و

لا تحتاج إلى مدعمات و كسر الأبواب أو تسلق الجدران، فنقل بيانات ممنوعة أو التلاعب بالأرصدة البنكية مثلا لا يحتاج إلا إلى لمسات أزرار، كما أنها تمتاز بسرعة تنفيذها ، كما أنها تمتاز أيضا بإمكانية ارتكابها عن بعد فلا تتطلب وجود الفاعل في مكان الجريمة بل يمكنه تنفيذها في مكان بعيد عن مسرح الجريمة ، [7]فالمجرم المعلوماتي القائم على الحاسوب في ألمانيا يمكنه تحويل مبلغاً من المال على أحد فروع المصاريف في سويسرا مثلا.

3/ **صعوبة إثبات الجريمة الالكترونية:** في حال اكتشاف الجريمة الالكترونية ، فإن إثباتها أمر تحيطه الكثير من الصعاب، فالجريمة الالكترونية تتم في محيط غير تقليدي حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب و الانترنت مما يجعل الأمور تزداد صعوبة و تعقيدا لدى سلطات البحث و التحري و التحقيق ، حيث تكون البيانات و المعلومات عبارة عن نبضات الكترونية غير مرئية تنساب عبر النظام المعلوماتي، مما يجعل أمر محو الدليل و طمسه آلياً من قبل المجرم في غاية البساطة و السهولة.[8]

4/ **أن الجريمة الالكترونية يتطلب ارتكابها وجود جهاز الكتروني:** يعد الجهاز الالكتروني هو أداة الجريمة ووسيلة تنفيذها، أو هو موضوع الجريمة كإتلاف أو سرقة البيانات و المعلومات، كما تتطلب هذه الجريمة دراية كافية و خبرة فائقة بالكمبيوتر و الانترنت في بعض الجرائم، وقد أثبت الواقع العلمي أن الجرائم الالكترونية قد ترتكب من خلال الهواتف المحمولة خاصة بعد ظهور أجهزة الهاتف الذكية و التي هي في الحقيقة عبارة عن أجهزة كمبيوتر صغيرة ، و التي يتم من خلالها الاتصال بشبكة الإنترنت ، و يسهل تخزين و نقل المعلومات من خلالها.[9]

و دون ان نغفل في سرد الخصائص و السمات التي تتميز بها الجريمة الالكترونية عن غيرها من الجرائم عن الفاعل أو مرتكب هذه الجريمة الذي أصبح بعرف" **بالمجرم المعلوماتي** " ، لتميزه أيضا عن المجرم التقليدي في أسلوبه المنفرد في تنفيذه للجريمة و سرعته و مهارته، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية ، و يمكن أن يكون المجرم الواحد مزيجًا من أكثر من طائفة.[10]

المحور الثاني: الإستراتيجية الجزائرية لمواجهة الجرائم الالكترونية في التشريع الجزائري

عملت الجزائر انطلاقاً من واقع التفشي السريع و الخطير للجرائم الالكترونية أو ما يعرف **"بجرائم تكنولوجيات الإعلام و الاتصال "** في المجتمع و في إطار سياسات وطنية و دولية واسعة

على بذل كافة الآليات القانونية لمكافحة الجريمة الالكترونية ، و ذلك من خلال استحداث أجهزة وحدات قانونية تم تكليفها بصورة خاصة و مباشرة بمتابعة و رصد هذه الجرائم ، كما حرص المشروع تعزيز الجانب القانوني بعقوبات صارمة تفوق بكثير المقررة في إطار الجرائم التقليدية و ذلك لإقرار بمدى خطورة هذه الجرائم و حرصا على ضمان أكبر قدر من الوقاية منها و مكافحتها ، وقد مست هذه الإستراتيجية العديد من المستويات نوضحها في ما يلي:

أولا : مواجهة الجريمة الالكترونية على المستوى القانوني:

من أجل مواجهة الجريمة الالكترونية، عمد المشرع الجزائري إلى إعادة النظر في العديد من التشريعات الوطنية الموجودة ، كما استحدث قوانين خاصة من اجل ضمان الحماية الجنائية للمعاملات الالكترونية و ما سنوضحه من خلال العناصر التالية :

1/ مواجهة الجريمة الالكترونية في إطار القوانين العامة

1/ في إطار قانون العقوبات : كخطوة أولى لمواجهة ما يعرف **"بجرائم تكنولوجيات الإعلام و الاتصال** "، أجرت الحكومة الجزائرية بعض التعديلات على قانون العقوبات بموجب القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل و المتمم للأمر رقم 156/66 المؤرخ في 08 يونيو 1966 ، و المتضمن قانون العقوبات، حيث استحدث عقوبات تتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات، وهو مانصت عليه المواد 394 مكررو 394مكرر 1ز 394 مكرر 2، 394 مكرر 3 ، و 394 مكرر 4 ، 394 مكرر 5، 394 مكرر 6، 395 مكرر 7 ، من القسم السابع مكرر ، و تراوحت هذه العقوبات مابين الحبس من شهرين إلى ثلاثة سنوات مع دفع غرامة مالية من 50000,00 دج إلى 5000000,00 دج ، و ذلك حسب حجم و درجة خطورة الجريمة الالكترونية المرتكبة.

وفي عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون 23/06 المؤرخ في 20 ديسمبر 2006 ، حيث مس هذا التعديل القسم السابع مكرر و الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، و قد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص الوارد في هذا القسم من القانون 04/ 15 و ربما يرجع سبب التعديل إلى زيادة الوعي بخطورة هذا النوع المستحدث من الاجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى و شيوع ارتكابه من قبل الجميع بمختلف الأعمار و مستويات التعليم نتيجة انتشار الانترنت كوسيلة لنقل المعلومات .[11]

2/ **في إطار قانون الإجراءات الجزائية :** نظرا لخصوصية الجريمة الالكترونية فإن المشرع الجزائري خصص لها مجموعة من الإجراءات ذات طبيعة مميزة ، تنفرد بها هذه الجرائم مقارنة بالجرائم التقليدية ، و هي التي جاءت مفصلة في تعديل قانون الإجراءات الجزائية لسنة 2006 بموجب القانون 06 ، تتعلق ب

- تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية طبقا للمادة 37 من قانون الإجراءات الجزائية
- خصوصية التفتيش المنصب على المنظومة المعلوماتية على ذلك التفتيش المتعارف عليه.
- تمديد آجال التوقيف للنظر لمقترف هذه الجرائم طبقا للمادة 51 من هذا القانون .
- النص على إجراءات خاصة للتحري و التحقيق و لاسيما استحداث أسلوب " اعتراض المراسلات و التقاط الصور و تسجيل " ، طبقا للمواد من 65 مكرر 05 إلى 65 مكرر 10 من القانون 22/06 السالف الذكر.
- إضافة أسلوب " التسرب" في المواد من 65 مكرر 11 إلى 65 مكرر من القانون كإحدى الأساليب التي يمارسها ضباط الشرطة القضائية و أعوانهم عند ضرورة التحري أو التحقيق في مجموعة من الجرائم ، و فيما يتعلق بشأن إجراء المحاكمة و المتابعة فهي نفس الإجراءات المطبقة على الجرائم العادية.[12]
-

2/ **/ مواجهة الجريمة الالكترونية في إطار القوانين الخاصة**

سعياً منه لمواجهة الجريمة الالكترونية و الإحاطة بها بشكل يحد منها فعليا ، عمد المشرع الجزائري إلى وضع نصوص خاصة تساهم في تفادي وقوع الجريمة الالكترونية و الكشف عنها من خلال :

أ/ القانون رقم 09/ 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ويعد قانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، أول قانون في الجزائر قانون إجرائي بامتياز يهدف حسب المادة الأولى منه إلى وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، كما اهتم بكيفية تبادل المعلومات

الرقمية و تجري فيها كل أنواع المعاملات و الخدمات الالكترونية، و يحتوي القانون على 19 مادة موزعة على 6 فصول .

ب/ القانون 05/03 المتعلق بحقوق المؤلف و الحقوق المجاورة

ج/ المرسوم الرئاسي رقم 172/19 المعدل بالالغاء أحكام المرسوم الرئاسي رقم 261/15 الذي جاء ليحدد تشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، و الذي سيكون محل دراسة خاصة في إطار المحور الثالث من هذه الدراسة

ثانيا : مكافحة الجرائم الالكترونية على المستوى المؤسساتي

في سبيل مكافحة الجريمة الالكترونية عملت وزارة الداخلية و الجماعات المحلية إلى أنشاء وحدات تابعة لسلك الأمن الوطني ، و التي تم على مستواها استحداث مصلحة نيابة مديرية الشرطة العلمية و التقنية ، هذه الأخيرة التي تم تقسيمها إلى المخبر المركزي للشرطة و العلمية و الذي تم تحديد مقره بالجزائر العاصمة إلى جانب أربعة مخابر جهوية مقرها كل من قسنطينة ، وهران، وبشار و تمنراست ، وتم على مستوى هذه المخابر انشاء دائرة علمية و دائرة تقنية تم تكليفها بالقيام بمهام التحري و التحقيق وتحليل الأدلة الجنائية المتحصل عليها من ارتكاب الجرائم الالكترونية .

كما لعب الدرك الوطني دورا مهما في مجال مكافحة الجريمة الالكترونية ، حيث تم استحداث على المستوى المركزي مدرية الأمن العمومي و الاستغلال و المصلحة المركزية للتحريات الجنائية ، و تم في هذا الإطار استحداث هيئة وطنية جد هامة في هذا المجال ألا وهي " **المعهد الوطني للأدلة الجنائية و علم الإجرام**" ، و الذي نص المشرع أنه " **يحدث معهد وطني للأدلة الجنائية و علم الإجرام للدرك الوطني**".

ثالثا: مكافحة الجرائم الالكترونية بتفعيل الجهاز القضائي بقطب متخصص في جرائم تكنولوجيات الإعلام و الاتصال (استحداث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال)

إن إنشاء قطب جزائي متخصص في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال يندرج ضمن إستراتيجية شاملة للدولة إزاء هذا النوع من الجرائم ، إذ يمثل هذا القطب خطوة إضافية في مسار

التصدي للجرائم الالكترونية ، حيث ان الأقطاب الجزائية عموماً عبارة عن " **جهات قضائية متخصصة للنظر في بعض الجرائم** التي حددها القانون و ليس بجهات قضائية خاصة تنشط بإجراءات قانونية مستقلة تخرج عن نطاق النظام القضائي الساري المفعول" ، و تاسيساً على ذلك يظهر القطب الجزائي كوسيلة لضمان فعالية الممارسة القضائية بخصوص الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، و يمكن اعتباره خطوة لارساء نظام التخصص القضائي في الجزائر. حيث منح له صلاحية الفصل بشكل حصري في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و كذا الجرائم المرتبطة بها ، و ذلك من خلال نص المادة 211 مكرر 24 من قانون الإجراءات الجزائية.

1/ الاختصاص النوعي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، منح المشرع الجزائري للقطب الجزائي الوطني المتخصص صلاحية الفصل بشكل حصري في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و كذا الجرائم المرتبطة بها ، و ذلك من خلال نص المادة 211 مكرر 24 ، و التي جاء فيها " مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و قاضي التحقيق و رئيس ذات القطب ، حصرياً بالمتابعة و التحقيق و الحكم في الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال أدناه ، وكذا الجرائم المرتبطة بها:

- الجرائم التي تمس امن الدولة أو بالدفاع 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 العموين ذات الطابع المنظم أو العابر للحدود الوطنية\جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالادارات و المؤسسات العمومية
- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين.
- جرائم التمييز و خطاب الكراهية.

2/ الاختصاص المحلي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال

نصت المادة 211 مكرر 23 من القانون 21/ 11 المتضمن قانون الإجراءات الجزائية على أنه" **يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، و كذا قاضي التحقيق و رئيس ذات القطب صلاحياتهم في كامل التراب الوطني "**

غير أن هذا الاختصاص الموسع الى كامل التراب الوطني فصل فيه المشرع بشئ من الدقة ، وذلك كالأتي:

- اختصاص حصري للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ، و ذلك بموجب المادة 211 مكر 26 ، حيث خول المشرع القطب الجزائي اختصاصاً حصريا فيما يخص الجرائم التي حددتها المادتين 211 مكرر 24 و 211 مكرر 25، في كافة أمحاء التراب الوطني دون سواه ، و ذلك بالنظر إلى خصوصية تلك الجرائم التي وجدت من لأجلها و بموجب تشكيلة قضاة متخصصة في هذا النوع من الجرائم التي تتسم بالخطورة و التعقيد و التي تمتد خارج حدود الدولة الجزائرية.
- اختصاص مشترك للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ، و هذا حسب المادة 211 مكرر 27 بمناسبة قيام الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، و التي تمد الاختصاص المحلي بها و فق نص الكادة 37 /2 لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى .
- **اختصاص وجوبي للقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال** وفقا لنص المادة 211 مكرر 28 من القانون 11/21 ، حيث يقوم الاختصاص المحلي وجوبا للقطب الجزائي الوطني لمكافحو الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال إذا ما تزامن مع اختصاص القطب الجزائي الوطني الاقتصادي و المالي.[13]

المحور الثالث : " الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها كآلية لمواجهة الجرائم الالكترونية

أولا : إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها

تعتبر الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال من أهم الجهات القانونية المكلفة بمكافحة الجريمة الإلكترونية و الوقاية منها ، و التي تم استحداثها لهذا الغرض بموجب المادة 13 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، و التي نصت على أنه" **تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته**"، ويعتبر هذا التشريع نقلة نوعية في النصوص الإجرائية الجزائية بالنظر إلى نوعية الإجراءات التي نص عليها كمراقبة الاتصالات السلكية و اللاسلكية و المراسلات الالكترونية و الاتصالات الهاتفية، و كذا مراقبة كل المعطيات الشخصية على الانترنت، وهو ما قد يتخذ أحيانا بقصد أو دون قصد كطريق للمساس بحرمة حياة الأشخاص و أمن اتصالاتهم و بياناتهم الشخصية ، وبالتالي إنشاء هذه الهيئة ضمان للحق الدستوري انه لكل مواطن الحق في حرمة حياته و مراسلاته من المساس بها بداعي مكافحة الجرائم.

وبقصد تفعيل نص المادة 13 من القانون 04/09 صدر في البداية المرسوم الرئاسي15/ 261 المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، غير أنه في 2019 صدر المرسوم الرئاسي 172/19 المعدل بالإلغاء للأحكام المرسوم الرئاسي 261/15 و ذلك نتيجة لظروف السياسية و الأمنية التي عرفتها البلاد في تلك الفترة مما افضى لظهور مخاطر فعلية على الأمن العمومي ، فجاء هذا المرسوم ليغير من الطبيعة القانونية لهذه الهيئة و تم منحها صلاحيات واسعة وهامة في هذا المجال ، كما تم تحديد تشكيلتها و تنظيمها و مختلف المهام الموكلة لها في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، ووضح كيفيات سيرها ومختلف الأحكام المالية و القانونية المتعلقة بها

1/ الطبيعة القانونية للهيئة الوطنية للوقاية من جرائم تكنولوجيات الاعلام و الاتصال

كيف المرسوم الرئاسي 261/15 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها في المادة 2 على أنها سلطة إدارية مستقلة ، حيث نصت المادة على أنه" **" الهيئة سلطة إدارية مستقلة تتمتع بالشخصية القانونية و الاستقلال المالي وتوضع لدى**

الوزير المكلف بالعدل" ، و تم تحديد مقرها بالجزائر العاصمة. و طبقا للمادة 4 من المرسوم الرئاسي 261/15 تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون 04/09 ، تحت رقابة السلطة القضائية طبقا لإحكام التشريع الساري المفعول لاسيما منها قانون الإجراءات الجزائية و القانون 09\/04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها [14].

أما المرسوم الرئاسي رقم 172/19 المعدل بالإلغاء أحكام المرسوم الرئاسي 261/15 فقد تراجع المشرع عن تكييف الهيئة بالسلطة الإدارية المستقلة الى مؤسسة عمومية ذات طابع اداري وحول تبعيتها من وزير العدل على وزارة الدفاع الوطني ، حيث نصت المادة الثانية على " **انها الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية و الاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني"** ، و ذلك مرده في الغالب تزايد خطورة هذه الجرائم في الآونة الأخيرة على امن الدولة الجزائرية و استقرارها ، و إرادة السلطة التنفيذية للتحكم فيها.[15]

2/ تشكيلة الهيئة الوطنية للوقاية من جرائم تكنولوجيات الاعلام و الاتصال و تنظيمها

طبقا للمادة 4 من المرسوم الرئاسي 172/19 تنظم الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها في مجلس توجيه ومدرية عامة ، و الملاحظ أن المرسوم الجديد قد لجأ إلى التقليص من الهياكل المكونة للهيئة على خلاف سابقه فقد كانت تضم لجنة مديرة ، مديرية عامة، مديرية للوقاية و اليقضة الالكترونية، مدرية للتنسيق التقني، مركز للعمليات التقنية، ملحقات جهوية [16]

2.1 مجلس التوجيه : حددت المادة 5 من المرسوم الرئاسي 172/19 تشكيلة مجلس التوجيه و التي يرأسها وزير الدفاع الوطني ممثله ، وهو يتشكل من ممثلي الوزرات الآتية :

. وزارة الدفاع الوطني
. الوزارة المكلفة بالداخلية
. وزارة العدل
. الوزراة المكطلفة بالمواصلات السلكية و اللاسلكية

تتولى المدرية العامة أمانة المجلس ، ويجتمع مجلس التوجيه في دورة عادية مرتين في السنة، بناء على استدعاء من رئيسه. و يمكنه أن يجتمع في دورة غير عادية كلما كان ذلك ضروريا بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو المدير العام للهيئة .

أما **مهام مجلس التوجيه** فقد حددتها المادة 06 من المرسوم 172/19 ، حيث يكلف مجلس التوجيه على وجه الخصوص بما يأتي:

- ✓ التداول حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها .
- ✓ التداول حول مسائل التطوير و التعاون مع المؤسسات و الهيئات الوطنية المعنية بجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.
- ✓ القيام دورياً بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال للتمكن من تحديد مضامن عمليات المراقبة الواجب القيام بها و الهداف المنشودة بدقة.
- ✓ اقتراح كل نشاط يتصل بالبحث و تقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.
- ✓ الموافقة على برنامج عمل الهيئة
- ✓ إعداد نظامه الداخلي و المصادقة عليه أثناء أول اجتماع له.
- ✓ دراسة التقرير السنوي لنشاطات الهيئة و المصادقة عليه
- ✓ إبداء رأيه في كل مسألة تتصل بمجال اختصاص الهيئة.
- ✓ المساهمة في ضبط المعايير القانونية في مجال اختصاصه
- ✓ دراسة مشروع ميزانية الهيئة و الموافقة عليه.[17]

2.2 المدرية العامة : نصت المادة 9 من المرسوم الرئاسي 172/19 على أنه يدير المديرية العامة مدير عام ، و تتولى على وجه الخصوص الصلاحيات الآتية:

- السهر على حسن سير الهيئة
- إعداد مشروع ميزانية الهيئة
- إعداد و ننتنفيذ برنامج عمل الهيئة
- تنشيط و تنسيق و متابعة و مراقبة أنشطة هياكل الهيئة

- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها

- تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجمع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و التعرف عليهم .

- تحضير اجتماعات مجلس التوجيه و إعداد التقرير السنوي لنشاطات الهيئة .

وطبقا للمادة 10 من المرسوم الرئاسي 172/19 ، تضم المدرية العامة

- مدرية تقنية ، مدرية للإدارة و الوسائل ، - مصالح

3/ **مهام الهيئة الوطنية للوقاية من جرائم تكنولوجيات الاعلام و الاتصال**:

تمارس الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام و الاتصال طبقا للقانون 09/04 و المرسوم الرئاسي 172/19 العديد من الصلاحيات، طبقا للمادة 14 من القانون المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ، تتمثل مهام الهيئة في:

- ✓ **تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته.**
- ✓ **مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات و انجاز الخبرات القضائية.**
- ✓ **تبادل المعلومات مع نظرتها في الخارج قصد جمع كل المطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و تجديد مكان تواجدهم.**

وطبقا المرسوم 172/19 يمكن تصنيف صلاحيات الهيئة إلى صلاحيات استشارية و رقابية و إدارية و مالية

1.3 **الصلاحيات الاستشارية :**

في إطار المرسوم 172/19 أبقى المشرع على نفس الاختصاص الاستشاري للهيئة من خلال منح مجلس التوجيه على مستواها :

- ✓ **التداول حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها .**
- ✓ **التداول حول مسائل التطوير و التعاون مع المؤسسات و الهيئات الوطنية المعنية بجرائم المتصلة بتكنولوجيات الإعلام و الاتصال.**
- ✓ **القيام دورياً بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال للتمكن من تحديد مضامن عمليات المراقبة الواجب القيام بها و الهداف المنشودة بدقة.**
- ✓ **اقتراح كل نشاط يتصل بالبحث و تقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها.**

3. **2 الصلاحيات الرقابية :** بناءا على أحام القانون رقم 09/04 و المرسوم الرئاسي 172/19 تمارس الهيئة صلاحيات رقابية و المتملة في : مراقبة الاتصالات الالكترونية و إجراءات التفتيش و الحجز داخل المنظومة المعلوماتية

.أ/ **مراقبة الاتصالات الالكترونية** : عرف القانون 09/ 04 الاتصالات الالكترونية في المادة 2 فقرة (و) على أنها " **أي تراسل أو ارسال أو استقبال علامات أو اشاررات أو كتابات أو صور أو أصوات او معلومات مختلفة بواسطة أي وسيلة الكترونية** "، وقد اشترط المشرع شروط للممارسة إجراء مراقبة الاتصالات الالكترونية وهو صدور إذ مكتوب من السلطة القضائية المختصة **وعندما يتعلق الأمر بالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة ، يختص النائب العام لدى مجلس قضاء الجزائر بمنح الضباط الشرطة الفضائية المنتمين** للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها غذنا لمدة 6 اشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة و الأغراض الموجهة لها ، وهذا من خلال المدرية التقنية للمدرية العامة للهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها ، وهذا طبقا لنص المادة 11 من المرسوم الرئاسي 172/19 ، حيث نصت على أنه: " **تكلف المدرية التقنية بمهمة المراقبة الوقائية للاتصالات الالكترونية في إطار الوقاية من الجرائم الموصوفة بالأفعال الإرهابية و التخريبية و الاعتداء على أمن الدولة** "، كما

أنها بموجب المادة 13 من المرسوم تمارس المهام المرتبطة بالشرطة القضائية كون أعضاء هذه المدرية من المستخدمين الخاضعين لقانون القضاء العسكري ، كما نصت على ذلك المادة 19 من ذات المرسوم و الذين يخضعون في أداء مهامهم للقانون 14/18 المعدل لقانون القضاء العسكري خاصة المادة 26 منه التي حددت مفهوم المستخدمين الخاضعين لقانون القضاء العسكري و الذين يمارسون مهامه وفق أحكام المواد 43 ، 45 ، كما ان المدرية التقنية تمارس أعمال الضبط القضائي وفق أحكام المادة 15 و 15 مكرر من قانون الإجراءات الجزائية .[18]

و قد حددت المادة الربعة من نفس القانون الحالات التي تسمح بمر اقبة الالكترونية و المتمثلة في :

- **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 يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.**
- **لمقتضيات التحريات و التحقيقات القضائية ، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المر اقبة الالكترونية.**
- **في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة .**

. **ب/ إجراء التفتيش و الحجز :** كرست المادة 5 من القانون 04/09 إجراء تفتيش المنظومات المعلوماتية ، حيث نصت على أنه " **يجوز للسلطات القضائية المختصة و كذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية و في الحالات المنصوص عليها في المادة 4 أعلاه، الدخول. بغرض تفتيش ، ولو عن بعد إلى :**
أ/ منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها
ب/ منظومة تخزين معلوماتية ...."
ج / حجز المعطيات المعلوماتية (المواد من 6 إلى 8 من القانون 04/09) تنتهي عملية التفتيش بحجز المعطيات المعلوماتية، و يتخذ هذا الحجز إحدى الصورتين : حجز عادي : يتم فيه حجز كامل المنظومة المعلوماتية المحتوية على المعطيات الضرورية المتعلقة بالجريمة أو جزء منها ، و يتم تحويل الدلائل من آثار معنوية غير ملموسة إلى دلائل مادية ملموسة يمكن التعامل معها عن طريق نسخها. و إما عجز عن طريق منع الوصول إلى المعطيات ، وهذا بغية جعل الدليل في مأمن من

الإتلاف أو التخريب أو تغيير المعالم و ذلك لمنع الدخول إليه من قبل أي شخص حتى تتخذ التدابير الممكنة للولوج للنظام للحصول على الدليل.[19]

ثانياً: دور الهيئة الوطنية للوقاية من جرائم تكنولوجيات الإعلام و الاتصال في مجال المساعدة القضائية الدولية و التعاون الدولي

أضحى التعاون الدولي في مواجهة الجرائم الالكترونية أو كما يسميها المشرع الجزائري " بالجرائم المتصلة بتكنولوجيات الإعلام و الاتصال" ضرورة ملحة لا رجعة فيها ، كون ام الدولة لا تستطيع بمفردها مواجهة الجرائم الالكترونية خاصة مع التطور المذهل في تكنولوجيات الإعلام و الاتصال على أساس أنها جرائم عابرة للحدود الوطنية و تمس أضرارها سيادة العديد من الدول بحيث تتطلب عملا منسقا بين مختلف الدول من خلال اتخاذ تدابير فعالة للحد منها و القضاء عليها و معاقبة مرتكبيها [20]، و تمارس الهيئة الوطنية للوقائية من جرائم المتصلة بتكنولوجيات الإعلام و الاتصال دورا مهما في مجال المساعدة القضائية و التعاون الدوليين و هو ما أكدته القانون 09/ 04 و المرسوم الرئاسي 172/19 السالف الذكر.

وقد نص المشرع الجزائري على مبدأ المساعدة القضائية الدولية المتبادلة لجمع الأدلة الخاصة بالجريمة الالكترونية في المادة 16 من القانون 04/90 ، و التي نصت على أنه " في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون و كشف مرتكبيها ، يمكن للسلطات القضائية الدولية لجمع الأدلة الخاصة في الشكل الالكتروني.
يمكن في حالة الاستعجال ، ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل ، قبول طلبات المساعدة القضائية المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال السريعة بما في ذلك أجهزة الفاكس أو البريد الالكتروني ، و ذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها" .

لكن المشرع وضع مجموعة من القيود على طلبات المساعدة القضائية الدولية ، نصت عليها المادة 18 من القانون 04/19 و هي :

- **يرفض تنفيذ طلبات المساعدة إذا كان من شأنه المساس بالسيادة الوطنية أو النظام العام.**
- **يمكن ان تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عم استعمالها في غير ماهو موضح في الطلب .[21]**

و تأخذ صور المساعدة القضائية و التعاون الدوليين صورتين هما تبادل المعلومات و طلب إجراءات تحفظية، وذلك بشروط محدد قانونا.

1/ تبـادل المعلومات : تعد آلية تبادل المعلومات من الآليات الأكثر شيوعا في مختلف الاتفاقيات الدولية و الثنائية ، ذكر منها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود إذ ألزمت الأطراف الموقعة عليها على وضع آليات تسيير تبادل المعلومات المتعلقة بكافة جوانب النشاط الإجرامي ،[22] و قد نص المشرع الجزائري في إطار القانون 94/09 المتعلق بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال في المادة 17 منه التي نصت **" تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة و الاتفاقيات الثنائية و مبدأ المعاملة بالمثل" .**

2/ **طلبات اتخاذ الإجراءات التحفظية** : تتميز هذه الإجراءات بانها ذات طابع جزائي مانتقال للمعاينة للدليل ، أو حجز دليل أو تفتيش منظومة معلوماتية ، و يتم طلب اتخاذ هذه الإجراءات كحجز دليل ، أو نظام الانابات الدولية .

الخاتمــة:

وفي ختام هذه الورقة البحثية التي حاولنا من خلالها تسليط الضوء على الجريمة الالكترونية والتجربة الجزائرية لمواجهتها في ظل التشريعات الوطنية والدولية، انطلاقا من إشكالية رئيسية تتمحور حول الإطار القانوني الذي نظمته التشريعات الوطنية و الدولية في سبيل الوقاية من الجرائم الالكترونية ، وخلصنا على أن التوجه الالكتروني الذي يشهده العالم و انتقال الأفراد من العالم الواقعي إلى العالم الافتراضي خلق نوع جديد من الجريمة المسماة " الجريمة السيبرانية الالكترونية"

وقد خلصنا من خلال هذه الورقة البحثية إلى مجموعة من النتائج أهمها:

1/إدراكا منه لخطورة الجريمة الالكترونية عمل المشرع الجزائري على الحرص على تجريم الجرائم الالكترونية و العمل على الحماية منها بإجراءات قانونية صارمة كانت بدايتها مع تعديل قانون العقوبات بموجب القانون 15/04 و الذي تم من خلاله استحداث قسم خاص بهذه الجرائم بموجب المواد من 394 مكرر إلى 394 مكرر 7 ، الأمر الذي عززه صدور القانون 04/09 الذي تم تخصيصه للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و

مكافحتها و الذي حملته مواده إجراءات هامة في هذا المجال عززها المشرع بالنص على استحداث هيئة وطنية متخصصة في الوقاية من هذه الجرائم و مكافحتها بموجب المادة 13 منه.

2/ أن الانتشار الوسع للجرائم الالكترونية مع الاستعمال الواسع لتكنولوجيات الإعلام و الاتصال دفع المشرع إلى التدخل سنة 2021 لإنشاء قطب جزائي ذو اختصاص وطني يعني بمكافحة جرائم تكنولوجيات الاعلام و الاتصال ، و ذلك من خلال تعديله لقانون الإجراءات الجزائية بموجب القانون 11/21 المتضمن قانون الإجراءات الجزائية و الذي يعد نقلة نوعية في مجال القضاء الجزائري .

انطلاقا من جملة هذه النتائج، حاولنا وضع بعض التوصيات التي من شأنها المساهمة في خدمة الموضوع وتغطية بعض نقاط العجز و القصور التي تم تسجيلها من خلال الدراسة، والمتمثلة في :

1/ ضرورة توحيد الجهود الدولية من طرف المختصين و الخبراء و كذا المنظمات الدولية في هذا المجال لوضع تعريف موحد للجريمة الالكترونية باعتبارها العقبة الأساسية لتحقيق التعاون الدولي لمكافحة هذه الجريمة .

2/ ضرورة نشر الوعي الرقمي بين المستخدمين و كيفية تفادي التعدي على بياناتهم الشخصية و تعريفهم بحجم الخطورة التي ترصدهم في حالة عم اتخاذ الاحتياطات الوقائية.

3/ ضمان تخصص القضاة في المسائل ذات العلاقة بالجرائم المتصلة بتكنولوجيات الإعلام ، حيث يعد ارهان الأول لمتابعة هذه الجرائم و الكشف السريع عن وجودها.

4/ تشجيع الجامعات و كليات الحقوق على وجه الخصوص على تنظيم العديد من الندوات و المؤتمرات التي تعالج تطور الإجرام المعلوماتي و كيفية محاكمة الجرائم الالكترونية و الحد من آثارها

الهوامش:

[1] كفل الدستور الجزائري لسنة 1996 و المعدل لسنة 2020 ، حماية الحقوق الأساسية و الحريات الفردية و على أن تضمن الدولة عم انتهاك حرمة الإنسان ، و قد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أورها قانون العقوبات و الإجراءات

الجزائية و قوانين خاصة تحظر المساس بهذه الحقوق ، ومن أهم المبادئ الدستورية العامة نجد نص المادة 35" **تضمن الدولة الحقوق الأساسية و الحريات**" ، المادة 47 " **لكل شخص الحق في حماية حياته الخاصة و شرفه....**"

[2]لمزيد من التفاصيل بخصوص تعريف الجريمة الالكترونية راجع :

مزيزد سليم، **الجرائم المعلوماتية و اقعها في الجزائر و آليات مكافحتها**"، المجلة الجزائرية للإقتصاد و المالية، العدد الأول، أفريل2014، ص ص94 -107

محمد الصغير مسكية ، **مفهوم الجرائم المستحدثة وطبيعتها القانونية- الجرائم الالكترونية**- مجلة الدراسات القانونية و السياسية ، المجلد 08، العدد 01 جانفي 2022 ص ص 132 – 146.

حبيباتي بثينة ، **الطبيعة الخاصة للجريمة المعلوماتية** ، مجلة دراسات و أبحاث ، المجلة العربية للأبحاث و الدراسات في العلوم الإنسانية و الاجتماعية، المجلد 13 ، العدد 03، جويلية 2020، ص 15

[3]القانون رقم 04/ 15 المؤرخ في في 10 نوفمبر 2004 يعدل و يتمم الأمر 66 / 156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات ، الجريدة الرسمية ، العدد 71 لسنة 2004.

[4]القانون رقم 04/09 المؤرخ في 5 أوت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، الجريدة الرسمية ، العدد 47 لسنة 2009.

[5]صهيب ياسر محمد شاهين، بشرى محمد حسن أبو ترابي ، **الجريمة الالكترونية و بعدها القانــوني(دراسة مقارنة بين التشريع الجزائري و الفلسطيني)** ، مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الأول 2021 ص ص 150 – 169

لمزيد من التفاصيل راجع القانون 04/ 14 المؤرخ في 11/10/ 2014 المعدل و المتمم للأمر رقم 66/ 155 المتضمن قانون الإجراءات الجزائية ،الجريدة الرسمية ، رقم 71 الصادرة بتاريخ 10 نوفمبر 2010 ، ص 4- 8

[6]بدر خلاف ، **التنظيم القانوني للجريمة المعلوماتية في الجزائر**/ مجلة العلوم القانونية و الاجتماعية، جامعة عباس لغرور، الجزائر ، المجلد السادس، العدد الثاني، السنة جوان 2021 ، ص 335

[7]بن شهرة شول، مراد مشوش، **السمات الخاصة للجريمة المعلوماتية**، مجلة المستقبل للدراسات القانونية و السياسية، مجلة تصدر عن معهد الحقوق و العلوم السيسية ، المركز الجامعي آفلو ، المجلد 04، العدد 01، جوان 2020.، ص 03

[8]حبيباتي بثينة ، **الطبيعة الخاصة للجريمة المعلوماتية** ، مجلة دراسات و أبحاث ، المجلة العربية للأبحاث و الدراسات في العلوم الإنسانية و الاجتماعية، المجلد 13 ، العدد 03، جويلية 2020، ص 610

[9]بن شهرة شول، مراد مشوش،**المرجع السابق** ، ص 07

[10]لمزيد من التفاصيل بخصوص أصناف المجرم المعلوماتي راجع بن شهرة شول، مراد مشوش، نفس المرجع ، ص ص 15 -16

[11]إسعداني إسلام، طارق طراد، **التجربة الجزائرية لمواجهة الجريمة الالكترونية في ظل البيئة التفاعلية الجديدة(عرض تشريعي)** ، مجلة الحقوق و العلوم السياسية، العدد 12 جوان 2019، ص ص 245 ، 275.

[12] بدر خلاف ، **المرجع السابق**، ص 341

[13] لمزيد من التفاصيل بخصوص هذا الموضوع راجع بن عميور أمينة ، بوحلايس إلهام، **القطب الجزائي الوطنب=ي لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال** ، مجلة البحوث في العقود و قانون الأعمال، الجلد 07، العدد 01، السنة 2022، ص ص 67 – 83

[14] المرسوم الرئاسي 15/ 261 المؤرخ في 008 2015/10 يحدد كيفية تشكيل و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها ، ج ر عدد 35 مؤرخة في 08 / 2015/10 .

[15] المرسوم الرئاسي 172/19 مؤرخ في 2019/06/06 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تنظيمها و سيرها ، ر ج ، عدد 37 مؤرخة في 09/06/ 2019.

[16] لمزيد من التفاصيل بخصوص هذا الموضوع راجع
خرشي الهام ، **النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها**، مجلة الأبحاث القانونية و السياسية، المجلد 04، العدد01، السنة 2022، ص ص 76.59

[17] راجع المادة 6 من المرسوم الرئاسي 172/19 مؤرخ في 2019/06/06 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تنظيمها و سيرها ، ر ج ، عدد 37 مؤرخة في 09/06/ 2019.

[18] حكيمة بوكحيل، سامية بن عديد ، **الهيئة الوطنية للوقاية من جرائم الاعلام و تكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية** ، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد، 01، السنة 2021، ص ص 1542. 1560.

[19] حابت أمال **دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال**، المجلة الدولية للبحوث القانونية و السياسية ، المجلد 05، العدد03، السنة 2021، ص 473

[20] بن حاج الطاهر محمد، شكرين ديلمي ، **سبل الحماية الدولية من الجريمة الالكترونية** ، مجلة الناقد للدراسات السياسية، المجلد 06/ العدد 01 2022 ، ص ص 710 – 720

[21] القانون رقم 04/09 المؤرخ في 5 أوت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، الجريدة الرسمية ، العدد 47 لسنة 2009.

[22] حكيمة بوكحيل، سامية بن عديد ، **الهيئة الوطنية للوقاية من جرائم الاعلام و تكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية** ، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد، 01، السنة 2021، ص ص 1542. 1560.

قائمة المصادر و المراجع:

قائمة المصادر:

القانون 04/ 14 المؤرخ في 11/10/ 2014 المعدل و المتمم للأمر رقم 66/ 155 المتضمن قانون الإجراءات الجزائية ،الجريدة الرسمية ، رقم 71 الصادرة بتاريخ 10 نوفمبر 2010 ، ص 4- 8

القانون رقم 04/ 15 المؤرخ في في 10 نوفمبر 2004 يعدل و يتمم الأمر 66 / 156 المؤرخ في 08 يونيو 1966 المتضمن قانون العقوبات ، الجريدة الرسمية ، العدد 71 لسنة 2004.

القانون رقم 04/09 المؤرخ في 5 أوت 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال، الجريدة الرسمية ، العدد 47 لسنة 2009.

القانون رقم 21/ 11 المؤرخ في 25 أوت ، يتمم الأمر رقم 155/66 المؤرخ في 08 يونيو 1966 و **المتضمن قانون الإجراءات الجزائية** ، ج ر عدد 65 الصادرة بتاريخ 26 أوت 2021 ص ص7-9

المرسوم الرئاسي 15/ 261 المؤرخ في 008 2015/10 يحدد كيفية تشكيل و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها ، ج ر عدد 35 مؤرخة في 08 / 2015/10 .

المرسوم الرئاسي 172/19 مؤرخ في 2019/06/06 يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها و تنظيمها و سيرها ، ر ج ، عدد 37 مؤرخة في 2019 /06/09.

المرسوم التنفيذي رقم 06/ 348 المؤرخ في 2006/10/05 يتضمن تمديد الاختصاص المحلي ببعض المحاكم ووكلاء الجمهورية و قضاة التحقيق ح ر رقم 63 ، المعدل بموجب المرسوم التنفيذي رقم 16 /267 المؤرخ في 17 / 10 / 2016 ، جريدة الرسمية رقم 62.

المرسوم التنفيذي 257/98 المؤرخ في 25 أوت 1998 ، الذي يحدد شروط و كيفيات وضع استغلال خدمة الانترنت ج ر عدد 47. السنة 1998.

المقالات العلميــة :

إسعداني إسلام، طارق طراد، **التجربة الجزائرية لمواجهة الجريمة الالكترونية في ظل البيئة التفاعلية الجديدة(عرض تشريعي)** ، مجلة الحقوق و العلوم السياسية، العدد 12 جوان 2019، ص ص 245 ، 275.

بهلول سمية ، **الإطار القانوني للوقاية من الجرائم السيبرانية ضد الأطفال و مكافحتها** ، مجلة العلوم القانونية و الاجتماعية، المجلد السادس، العدد الرابع، السنة ديسمبر 2021.، ص 331-346

بن شهرة شول، مراد مشوش، **السمات الخاصة للجريمة المعلوماتية**، مجلة المستقبل للدراسات القانونية و السياسية، مجلة تصدر عن معهد الحقوق و العلوم السيسية ، المركز الجامعي آفلو ، المجلد 04، العدد 01، جوان 2020.، ص ص 1- 21

بدر خلاف ، **التنظيم القانوني للجريمة المعلوماتية في الجزائر/** مجلة العلوم القانونية و الاجتماعية، جامعة عباس لغرور، الجزائر ، المجلد السادس، العدد الثاني، السنة جوان 2021

بن حاج الطاهر محمد، شكرين ديلمي ، **سبل الحماية الدولية من الجريمة الالكترونية** ، مجلة الناقد للدراسات السياسية، المجلد 06/ العدد 01 2022 ، ص ص 710 – 720

بن عميور أمينة ، بوحلايس إلهام، **القطب الجزائي الوطنب=ي لمكافحة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال** ، مجلة البحوث في العقود و قانون الأعمال، الجلد 07، العدد 01، السنة 2022، ص ص 67 – 83

حكيم سياب، **السمات المميزة للجرائم المعلوماتية عن الجرائم التقليدية**، مجلة دراسات و أبحاث ، جامعة زيان عاشور، الجلفة المجلد الأول ، العدد الأول، ص ص 212 .240.

حاجة عبد العالي، قلات سمية، **المكافحة الإجرائية للجرائم الالكترونية " دراسة حالة الجزائر"** ، مجلة المفكر، كلية الحقوق و العلوم السياسية، جامعة محمد خيضر بسكرة، العدد 16، ديسمبر 2017، ص ص 227- 243

حبيباتي بثينة ، **الطبيعة الخاصة للجريمة المعلوماتية** ، مجلة دراسات و أبحاث ، المجلة العربية للأبحاث و الدراسات في العلوم الإنسانية و الاجتماعية، المجلد 13 ، العدد 03، جويلية 2020.

خرشي الهام ، **النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها**، مجلة الأبحاث القانونية و السياسية، المجلد 04، العدد01، السنة 2022، ص ص 76.59

حكيمة بوكحيل، سامية بن عديد ، **الهيئة الوطنية للوقاية من جرائم الاعلام و تكنولوجيا الاتصال ودورها في تفتيش نظم المعلوماتية** ، مجلة الدراسات القانونية المقارنة، المجلد 07، العدد، 01، السنة 2021، ص ص 1542 .1560.

حابت أمال **دور الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال و مكافحتها في مواجهة الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال**، المجلة الدولية للبحوث القانونية و السياسية ، المجلد 05، العدد03، السنة 2021.

صهيب ياسر محمد شاهين، بشرى محمد حسن أبو ترابي ، **الجريمة الالكترونية و بعدها القانــوني(دراسة مقارنة بين التشريع الجزائري و الفلسطيني)** ، مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الأول 2021 ص ص 150 – 169

مزيزد سليم، **الجرائم المعلوماتية واقعها في الجزائر و آليات مكافحتها"**، المجلة الجزائرية للإقتصاد و المالية، العدد الأول، أفريل2014، ص ص94 -107

محمد الصغير مسكية ، **مفهوم الجرائم المستحدثة وطبيعتها القانونية- الجرائم الالكترونية-** مجلة الدراسات القانونية و السياسية ، المجلد 08، العدد 01 جانفي 2022 ص ص 132 – 146.

انتهاكات حقوق الإنسان بفعل الجرائم الإلكترونية

Human rights violations caused by cybercrime

لقب واسم المؤلف: ضامن الجيلالي / **الرتبة العلمية:** أستاذ جامعي مؤقت
مؤسسة الانتماء: جامعة التكوين المتواصل لولاية تيارت / **الدولة:** الجزائر
البريد الإلكتروني: dhamene.djilali@gmail.com

ملخص:

هـدفت الدراسـة إلى إبـراز انتهاكـات حقـوق الإنسـان بفعـل الجـرائم الإلكترونيـة المستحدثة.

وبناء على هذه الدراسة التحليلية، توصلنا إلى أن البحث عن مثل هذه الانتهاكات أصبح يشكل مطلبا حضاريا، نظرا للتحديات التي يعيشها الإنسان الرقمي اليوم، والذي أضحى يعيش في عالم معلوماتي يتسم حسب نظرنا بقلة الإيجابيات وكثرة السلبيات.

الكلمات المفتاحية: الجريمة الإلكترونية، حقوق الإنسان، الانتهاكات، الجرائم، التكنولوجيات الرقمية.

Abstract:

The study aimed to highlight human rights violations caused by emerging cyber crimes.

Based on this analytical study, we concluded that the search for such violations has become a civilized requirement, given the challenges experienced by the digital person today, who has come to live in an informational world characterized by few positives and many negatives according to our view.

Keywords: cybercrime, Human rights, violations, crimes, digital technologies.

مقدمة:

تعد حقوق الإنسان من الموضوعات الجوهرية التي حظيت باهتمام واسع النطاق من طرف المفكرين والفلاسفة، خاصة بعد التطورات السياسية والاقتصادية والاجتماعية والثقافية والعلمية المعاصرة.

ولقد ارتبط هذا الموضوع ارتباطا وثيقا بالتقدم السريع للتكنولوجيات الرقمية بمختلف وسائلها، من حيث الانتهاكات الصريحة لهذه الحقوق بفعل التفشي الواسع للجرائم المستحدثة التي صاحبت الثورة الرقمية، والتي أصبحت سلاحا ذو حدين، فعلى الرغم من إيجابياتها الفعالة فإنها لا تخلو من سلبيات تسبب أضرارا جسيمة وانتهاكات خطيرة لحقوق الإنسان.

إن الطرح القانوني لموضوع انتهاكات حقوق الإنسان بفعل الجرائم الالكترونية يتعدى الإشكاليات التقليدية التي تناولت الأسلوب الكلاسيكي للعملية الاجرامية الذي كان يفتقر الى المعلومات والمنهجيات العلمية الدقيقة مقارنة بالأسلوب الالكتروني المعاصر، والذي أصبح اليوم هاجسا يطرح بشكل قوي على مستوى البحث العلمي المتخصص، نظرا للتحديات الحاصلة في العالم التي تهدد بشكل مباشر وجود الإنسان الرقمي في جل الميادين بما فيها ممارسات حياته اليومية.

ومن هذا المنطلق حاولنا في هذه الدراسة ابراز اهم انتهاكات حقوق الانسان بفعل الجرائم الدولية، انطلاقا من الإجابة عن الإشكالية الرئيسية للبحث التي تتمحور حول: **ماهي انتهاكات حقوق الإنسان في ظل انتشار الجريمة الالكترونية؟**

سيتم الإجابة عن هذه الاشكالية وغيرها من التساؤلات الفرعية وفق الخطة المنهجية المتبعة كالآتي:

المبحث الأول: الجريمة الإلكترونية في نطاق التكنولوجيات الرقمية المعاصرة

المطلب الأول: مفهوم الجريمة الإلكترونية

المطلب الثاني: دوافع ارتكاب الجريمة الإلكترونية

المبحث الثاني: انتهاكات حقوق الإنسان في ظل انتشار الجريمة الإلكترونية

المطلب الأول: مفهوم حقوق الإنسان

المطلب الثاني: انتهاكات حقوق الإنسان في عصر الفتوحات الإلكترونية

المبحث الأول: الجريمة الإلكترونية في نطاق التكنولوجيات الرقمية المعاصرة

عرفت الجريمة كظاهرة اجتماعية ونفسية تطورا ملحوظا تناسب مع تلك الثورة العلمية والرقمية التي شهدها العالم في العصر الحديث، فبعدما كانت الجريمة تعتمد على أساليب يدوية تقليدية، أصبحت اليوم تخضع لتكنولوجيات عالية راقية المستوى، يتفق المجتمع العلمي الحديث على تسميتها بالجريمة الإلكترونية وفي مسميات أخرى نجدها تسمى بالجريمة المعلوماتية، سنناقش هذا المبحث من خلال مفهوم الجريمة الإلكترونية (المطلب الأول)، ثم دوافع ارتكاب الجريمة الإلكترونية (المطلب الثاني).

المطلب الأول: مفهوم الجريمة الإلكترونية

نتيجة لحداثة الجرائم الإلكترونية وارتباطها بالتكنولوجيات المتطورة سنحاول من خلال هذا المطلب التعرض إلى التعاريف المختلفة للجريمة الإلكترونية، وكذا خصائصها وسماتها الخاصة بها، وذلك من خلال الفرعين المواليين.

الفرع الأول: تعريف الجريمة الإلكترونية

لم يتفق الفقه على وضع تعريف جامع للجرائم الإلكترونية، نظرا لغياب تعريف قانوني لهذا النوع من الجرائم في أغلب التشريعات، بالإضافة إلى غياب مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة الإلكترونية أو المعلوماتية[1].

وقد أدت الحداثة التي تتميز بها الجرائم الإلكترونية، واختلاف النظم القانونية والثقافية بين الدول إلى عدم الاتفاق إلى مصطلح موحد للدلالة عليها، وعدم الاتفاق، هذا انجر عليه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية وذلك خشية حصرها في مجال ضيق[2].

وفي ظل هذا الفراغ القانوني بذلت محاولات فقهية متعددة لإيجاد تعريف للجرائم الإلكترونية وانقسمت بدورها إلى اتجاهين رئيسين، وهذا بالنظر إلى الزاوية التي ينظر من خلالها لهذا النوع من الجرائم، الاتجاه الأول مضيق لمفهوم الجرائم الإلكترونية، أما الاتجاه

الثاني فقد حاول التوسع في مفهوم الجريمة الإلكترونية، وسنحاول التعرض لهذه التعاريف من خلال البندين المواليين:

أولا: الاتجاه المضيق من تعريف الجريمة الإلكترونية

من أهم التعريفات التي وضعها أنصار هذا الاتجاه على أنها: «كل فعل غير مشروع يكون العلم بتكنولوجيات الحاسبات الآلية بقدر كبير لازم لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى»[3].

من خلال هذا التعريف يتبين لنا أنه لا يكفي فقط أن تتوافر معرفة تكنولوجيات الحاسبات الآلية بدرجة كبيرة من أجل ارتكاب الجريمة المعلوماتية، ولكن أيضا من أجل ملاحقتها ومتابعتها، وقد انتقد هذا التعريف لكونه يحصر الجريمة المعلوماتية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية في ارتكابها[4].

وهناك من يعرفها على أنها: «نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي، أو تلك التي يتم تحويلها عن طريقه»، وما يعاب على هذا التعريف أن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التجريم، ومثالها الاحتيال المعلوماتي[5].

ويرى الأستاذ (باركار) أن الجريمة الإلكترونية هي: «كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل»[6].

ثانيا: الاتجاه الموسع من تعريف الجريمة الإلكترونية

على عكس الاتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة خشية حصرها في مجال ضيق، فمنهم من عرفها بأنها: «كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب»[7].

ودائما حسب أنصار هذا الاتجاه يرى البعض أن الجريمة الإلكترونية هي: «كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية، يهدف إلى الاعتداء على الأموال المادية أو المعنوية»[8].

كما ترى الدكتورة (نائلة عادل محمد فريد) أن الجريمة الإلكترونية هي: «كل نشاط إجرامي يؤدي فيه نظام الحاسب الآلي دورا لإتمامه، على أن يكون هذا الدور على قدر من الأهمية»[9].

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فيتطلب تعريف المفردات المتعلقة بأركان الحاسوب الآلي، وهي: «الحاسب الآلي، برنامج الحاسب الآلي، البيانات، الممتلكات، الدخول، الخدمات، الخدمة الحيوية»[10].

وبناء على هذا تبنى الجريمة الإلكترونية على ثلاثة شروط أساسية من حيث أنها تتطلب استخدامات الحاسب الآلي كوسيلة ضرورية في تحقيق هذا الفعل كشرط أول، كما تتطلب إلمام جيد بتقنيات الشبكة الحاسوبية كشرط ثاني، من أجل القدرة على الوصول إلى المعلومات الخاصة كشرط ثالث لها، ومن هنا اصطلح المشرع الجزائري على تسمية الجرائم الإلكترونية بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب أحكام المادة 02 من القانون رقم (09-04) على أنها: «جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات الإلكترونية»[11].

وحسب المشرع الجزائري فإنه قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الاتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية[12].

الفرع الثاني: خصائص الجريمة الإلكترونية

تختلف الجريمة الإلكترونية عن الجريمة التقليدية، فالأولى هي نتاج التطور العلمي والتكنولوجي، والثانية ترتكب في الواقع المادي الملموس، وبهذا الشكل نجد للجريمة الإلكترونية مجموعة من الخصائص، أو السمات تجعلها منفردة عن غيرها من الجرائم، سواء من حيث الجريمة ذاتها، أو من حيث مرتكب الجريمة، وهذا ما يتم بيانه من خلال البندين التاليين:

أولا: بعض السمات المتعلقة بالجريمة الإلكترونية ذاتها

نظرا للطبيعة المميزة للجريمة الإلكترونية باعتبارها تمس المعلومات، هذا ما جعلها تتميز عن نظيرتها التقليدية بمجموعة من الخصائص والسمات تتلخص فيما يلي:

- تتميز بالعالمية، فهذه الجريمة لا يحدها مكان والعالم الافتراضي لا ترسمه حدود معينة، وربما هذا يؤكد افتراضية أن "هذه الجرائم هي صورة صادقة من صور العولمة"[13]. وهذه الخاصية ساعدتها على قابلية التوسع الناتج عن "سهولة تكرار الجرائم على نطاق واسع بسبب توحيد البرامج وإمكانية الوصول إلى ملايين أجهزة الكمبيوتر بدون أي قيود لوجستقنية"[14]. مما ساهم في عملية اختراق الحسابات الشخصية، والبيانات الحكومية، والشركات الاقتصادية، والبنكية وغيرها من المشاريع الحيوية التي تبنى عليها اقتصاديات وسياسات البلدان.

- ارتباط الجريمة الإلكترونية بالحاسوب الإلكتروني، وذلك بالمساهمة في تطوير أدواتها وأساليبها، فهي مرتبطة في الأساس بالتقدم التقني المعلوماتي، فكلما ظهرت تقنية جديدة ظهرت معها جرائم جديدة[15].

- صعوبة كشف الجريمة الإلكترونية والوصول إلى مرتكبيها، وهذا يعني أن المجهولية والقرب الزائف يشعر الجناة بالأمان الشديد ويمكنهم بسهولة إخفاء الهوية الحقيقة على الإنترنيت[16].

- عدم ارتباطها فيزيولوجيا بين الجاني والمجني عليه إذ يكفي فقط ضغط بعض الأزرار لأذيته، وهدر كرامته، واستفزازه بأبشع الصور، كما تزيد صعوبة كشفها إذا تعلق الأمر بمسألة البصمة من حيث أنها جريمة تقع في بيئة إلكترونية يتم فيها نقل المعلومات وتداول البصمات الإلكترونية غير المرئية ولا توجد مستندات ورقية[17].

- صعوبة الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على الدليل المتوفر[18].

- الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بالمجني عليه، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والأنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها، لتغطية عملية التلاعب وتحويل المكاسب[19].

ثانيا: بعض السمات المتعلقة بالمجرم الإلكتروني

مرتكبو الجرائم الإلكترونية لهم العديد من الصفات والمميزات لغرض ارتكاب الجرائم الإلكترونية نذكر منها على سبيل المثال ما يلي:

- يتميز المجرم الإلكتروني بالثقافة والعلم التكنولوجي (المعرفة والمهارة والذكاء)، فالمجرم في هذا النوع من الجرائم ليس عاديا، فهو يرتكب جريمة متخصصة خاصة إذا ما تمثلت هذه الجريمة بسرقة معلومات مشفرة ما يستتبع معه خبرة تقنية عالية في هذا المجال، يمكن للمجرم الإلكتروني أن يكون له تصورا كاملا لجريمته، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التي يستهدفها وذلك قبل تنفيذه جريمته، حتى لا يفاجأ بأمور غير متوقعة من شأنها إفشال مخططات أو الكشف عنها[20].

- المجرم الإلكتروني يبرر ارتكاب جريمته، إذ يوجد شعور لديه بأن ما يقوم به لا يدخل في عِداد الجرائم، أو بمعنى آخر لا يمكن لهذا الفعل أن يتصف بعدم الأخلاقية وخاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في اللاأخلاقية، وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم[21].

- المجرم الإلكتروني يتصف بالخوف من كشف جريمته، مما يترتب عنها فقد مركزه الوظيفي في كثير من الأحيان.

- يتميز المجرم الإلكتروني بخاصية التكيف الاجتماعي حيث يحيى وسط المجتمع، ويمارس عمله في المجال المعلوماتي أو غيره من المجالات، لكن كثر من جرائمه الإلكترونية ترتكب بدافع الكبرياء (موظف طرد من عمله)، أو بدافع النصب أو الحسد أو اللهو وإظهاره قدراته[22].

- يساهم وجود المجرم الإلكتروني في جماعة إجرامية إلى سرعة اكتسابه للمهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة، ويمكن تقسيم المجرم الإلكتروني إلى عدة طوائف مختلفة منها (المخترقون أو المتطفلون – مجرمو الحاسب الآلي المحترفون – الحاقدون – صغار السن – مجرمون ذوي دوافع سياسية).

المطلب الثاني: دو افع ارتكاب الجريمة الإلكترونية

إذا كان الدافع هو ذلك العامل المحرك للإرادة والذي يوجه السلوك الإجرامي كالمحبة أو الشفقة والبغضاء والانتقام، فهو إذن قوة نفسية تدفع الإرادة إلى ارتكاب الجريمة ابتغاء تحقيق غاية معينة فهو يختلف من جريمة إلى أخرى، وبالنسبة للجريمة الإلكترونية فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الاعتداء المختلفة المنطوية تحت هذا المفهوم[23]، وأهم هذه الدوافع سيتم بيانها من خلال الفرعين الآتيين.

الفرع الأول: الدو افع الشخصية لارتكاب الجريمة الإلكترونية

يمكن تصنيف هذه الدوافع إلى دوافع مادية وأخرى ذهنية، وذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب الجريمة الإلكترونية، أو تأثير العنصر الذهني المعنوي على المجرم الإلكتروني ودفعه لارتكاب جريمته، هذا ما سيتم بيانه من خلال البندين المواليين.

أولا: الدو افع المادية

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الإلكتروني إلى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الآلية لها من خلال اكتشافه لفجواتها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه، أو لحساب شركائه، أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة. كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب، وقد أشارت في هذا الإطار مجلة "sécurité informatique" وهي مجلة متخصصة في الأمن المعلوماتي، أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، و23% من أجل سرقة معلومات، و19% أفعال إتلاف، و15% الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية. وفي حقيقة الأمر أن في حال نجاح المجرم الإلكتروني في ارتكاب جريمته فإن ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الإلكترونية، حيث تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة للأنظمة المعلوماتية، وأن 64% لحقت بهم خسائر مادية جراء هذه الاعتداءات[24].

ثانيا: الدو افع الذهنية لارتكاب الجريمة الإلكترونية

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات. وقد تكون هذه الدوافع مجرد شغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه، وعلى صعيد آخر قد يكون إقدام المجرم الإلكتروني على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي وإثبات المقدرة[25].

الفرع الثاني: الدو افع الموضوعية لارتكاب الجريمة الإلكترونية

عندما يتأثر المجرم الإلكتروني ببعض المواقف قد تكون دافعة له على اقتراف الإجرام الإلكتروني ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن إبراز أهم الدوافع من خلال البندين المواليين.

أولا: دافع الانتقام وإلحاق الضرر بمستخدمه

يتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته[26]، ويعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المجرم الإلكتروني الرغبة في الانتقام من رب عمله أو مستخدمه.

ثانيا: دافع التعاون والتواطؤ

يتكرر هذا النوع كثيرا في الجرائم الإلكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم[27].

المبحث الثاني: انتهاكات حقوق الإنسان في ظل انتشار الجريمة الإلكترونية

إذا كانت حقوق الإنسان من الموضوعات الجوهرية التي اهتمت بها الفلسفة اليونانية القديمة والفلسفات الحديثة المعاصرة، فإنها باتت من المسائل التي ترتبط بالتطور التكنولوجي الحديث ارتباطا من حيث الانتهاكات الصريحة لهذه الحقوق بفعل الانتشار الواسع للجرائم المستحدثة التي صاحبت الثورة الرقمية، والذي تعتبر الجريمة الإلكترونية أهم مظاهرها حاليا، من حيث أنه تتميز بخصائص تم ذكرها سابقا تسهل على مرتكبيها القيام بها من مسافات بعيدة وبتكنولوجيا عالية تتجاوز كل أدوات الإجرام الكلاسيكي، هدفها انتهاك حقوق الإنسان في مختلف المجالات، ومن هنا سنحاول إثراء هذا المبحث من خلال التعرض لمفهوم حقوق الإنسان (المطلب الأول)، ثم التعرض لانتهاكات حقوق الإنسان في عصر الفتوحات الإلكترونية (المطلب الثاني).

المطلب الأول: مفهوم حقوق الإنسان

تعتبر حقوق الإنسان من المفاهيم التي عرفت تطورا تاريخيا، حيث ارتبط ظهورها بظهور الإنسان في حد ذاته، وبظهور أطروحات المفكرين والفلاسفة وتعاليم الأديان والعقائد منذ العصور القديمة، ومن أجل توضيح مفهوم حقوق الإنسان سنقوم بتعريفها وإظهار أهم خصائصها من خلال الفرعين المواليين.

الفرع الأول: تعريف حقوق الإنسان

حاول العديد من الباحثين إعطاء تعريف لحقوق الإنسان كل حسب اختصاصه، فمثلا عرفها (كاسان رينيه): «حقوق الإنسان هو علم يتفرع من العلوم الاجتماعية، وموضوع دراسة الروابط بين الناس تبعا للكرامة الإنسانية، محددا الحقوق والإمكانيات التي تكون ضرورية لتفتح شخصية كل كائن بشري»[28]، كما عرفتها الأستاذة (سعاد محمد صباح) بأنها: «حقوق الإنسان هي تلك المطالب التي يتعين الوفاء بها لجميع الأفراد دون أي تمييز بينهم، سواء بسبب النوع أو الجنس أو اللون أو العقيدة أو الأصل أو لأي سبب آخر، ويجب أن يكفل للأفراد جميعا التمتع بهذه الحقوق والمطالب بحكم كونهم بشرا وباعتبار أن وجودهم بهذه الصفة لا يتحقق إلا بذلك»[29].

وفي بعض التعاريف الأخرى تعني حقوق الإنسان: «الرخص والصلاحيات والحريات التي ينبغي أن يتمتع بها الإنسان أينما كان وتؤدي إلى اشباع حاجاته الخاصة وتسهم دون شك في

إفادة وتطوير المجتمع الذي يحيا فيه»[30]، وهناك من يربطها بالدولية ويرى بأنها: «مجموع الحقوق الفردية والجماعية المعترف بها من قبل الدول ذات السيادة ومكرسة في تشريعاتها المحلية وفي المعايير الدولية لحقوق الإنسان»[31].

وعموما فإن مصطلح حقوق الإنسان يشير إلى مجموعة الحقوق الطبيعية والاجتماعية والاقتصادية والثقافية التي من الضروري أن يتمتع بها الإنسان والتي تكتمل من خلالها فطرته ويحقق إنسانيته ويرتقي بها عن مصاف الكائنات الأخرى[32].

الفرع الثاني: خصائص حقوق الإنسان

تتميز حقوق الإنسان ببعض السمات مما أدى إلى علو شأنها وقيمتها ومكانتها، وتتمثل هذه الخصائص فيما يلي:

- تتميز حقوق الإنسان بالعالمية، فهي من المواضيع ذات الطابع العالمي وتظل محل اهتمام كل دول العالم، وهذه الميزة تعتبر ضمانا ضروريا للحاضر والأمان بالنسبة للمستقبل، وما لم يقبل مبدأ العالمية يكون من المستحيل التقدم للأمام بالنسبة لعملية الحماية الدولية[33].

- تتميز حقوق الإنسان بالشمولية، فهي لا تقتصر على فئة معينة دون أخرى، وبالتالي تستند في الأساس على مبدأ المساواة بين البشر جميعهم[34].

- تتميز حقوق الإنسان بالضرورة، من حيث أنها تعبر عن إنسانية الإنسان وتحافظ على حياته وتسمح له بالعيش بكرامة واستقلالية، في جو يسوده الأمن والاستقرار والمساواة وحرية التعبير وحرية ممارسة الطقوس وغيرها من الحقوق المعنوية الأساسية[35].

المطلب الثاني: انتهاكات حقوق الإنسان في عصر الفتوحات الإلكترونية

ليس من الغريب أن نطلق عصر الفتوحات الإلكترونية على العصر الحالي، نظراً إلى غزو الحاسوب لحياتنا بجوانبها كلّها، فعملية خزن المعلومات أدت إلى ظهور بنوك المعلومات التي حظيت بحماية قانونية في كثير من التشريعات، وظهر ما يسمى بالإجرام المعلوماتي الذي أخذ ينتشر بشكل أكثر حدة مع انتشار الإنترنت، فقد ولدت هذه التكنولوجيات مشكلات اجتماعية وإنسانية لا تقل خطورة عن الآفات التي عرفتها البشرية في تاريخها[36]. ولمعرفة انتهاكات حقوق الإنسان في عصر الفتوحات الإلكترونية نتطرق لجرائم انتهاك حقوق

الإنسان في نطاق التكنولوجيات المعاصرة ثم نتطرق لأبرز صور التعدي الإلكتروني على حقوق الإنسان في الفرعين المواليين.

الفرع الأول: جرائم انتهاك حقوق الإنسان في نطاق التكنولوجيا الرقمية المعاصرة

أصبح البحث في انتهاكات حقوق الإنسان بفعل الجرائم الإلكترونية مطلبا حضاريا، وهذا نظرا للتحديات التي يعيشها الإنسان الرقمي في عصرنا الحالي، وقد تعددت جرائم انتهاكات حقوق الإنسان في النطاق الإلكتروني، وبات من السهل تقسيم الجرائم الإلكترونية المنتهكة لحقوق الإنسان على النحو التالي:

أولا: الجرائم الإلكترونية الواقعة على الأشخاص الطبيعية

تنقسم هذه الجرائم إلى جرائم واقعة على حرمة الحياة الخاصة للإنسان، وجرائم واقعة على حقوق الملكية الفكرية والأدبية.

1- الجرائم الإلكترونية الواقعة على حرمة الحياة الخاصة للإنسان

يعد حق حماية الحياة الخاصة من أهم الحقوق، وذلك لما له من ارتباط وثيق بحرية الفرد الخصوصية، وقد جاء تجريم هذا النوع من الأفعال كحماية من التهديد الحقيقي الذي تشكله تكنولوجيا المعلومات لحق الأفراد في احترام حياتهم الخاصة، خاصة مع انتشار ما يسمى ببنوك المعلومات بمختلف أنواعها (الأمنية، المالية، السياسية، الطبية، العسكرية ... إلخ)[37].

وفي هذا النوع من الجرائم الإلكترونية بات من السهل الحصول على المعلومات المخزونة بالحاسوب المرتبط بشبكة الإنترنت، كما أنَّه يمكن تبادل المعلومات بين حاسوب وآخر، لذلك قيل: إن شفافية الإنسان وخصوصيته باتت عارية أمام ما تمخض عنه العلم من إعجاز في عالم الحواسيب. فلم تعد حجة السرية التي يكفلها النظام الآلي لمعالجة البيانات حجة مقنعة، إذ أصبحت حالات اقتحام النظام الآلي مسألة واردة وليست مستحيلة[38].

وإذا أضفنا إلى ذلك احتمال الخطأ في عمل الآلة، وصعوبة تصحيح المعلومة، فضلاً عن إمكان تحويرها أصلاً لتضاعف الخطر الذي يهدد حياة الإنسان الخاصة بسبب النظام الآلي لمعالجة المعلومات، فالبيانات الشخصية المتصلة بالحياة الخاصة للفرد أو عائلته غالباً ما يقدمها الشخص بنفسه، أو قد تتوصل الهيئات إليها بوسيلة أو بأخرى، وتهديد المساس

بالحياة قد يثور إذا أفشيت هذه المعلومات دون رضاء منه، أو نشرت بإحدى طرائق العلانية دون موافقته، سواء أكانت هذه المعلومات على شكل خبر أو تعليق أو صورة؟ وتكون متصلة بأسرار حياته الخاصة أو العائلية ولو كانت صحيحة[39].

وتظهر صور التعدي الإلكتروني على حرمة الحياة الخاصة للإنسان أو حرياته العامة بصور متعددة نذكر منها:

- اختراق الحسابات الشخصية للأشخاص وبياناتهم الخاصة، وهذه الصورة تعد من أهم مظاهر الجريمة الإلكترونية التي تمس بحقوق الإنسان، بحيث يلجأ فيها المجرم الإلكتروني إلى الدخول غير القانوني لهذه الحسابات وبطرق احترافية يجمع فيها بين المهارة العالية في استخدام الكمبيوتر وفهم عميق لأسرار الشبكة العنكبوتية، بهدف انتهاك السرية[40].

وهذا النوع من الجرائم يدخل في نطاق التصعيد الاحتيالي الذي أصبح يعرف انتشارا واسعا بين الدول فقد لاحظ (روديون ناساكين) في دراسته للاستخدام غير القانوني للمعلومات الشخصية في روسيا أن النمو السريع للتصيد للاحتيال منذ عام 2000، حيث نجح المخادعون في خداع العملاء للكشف عن كلمات المرور وأرقام التعريف الشخصية، وبالتالي تمكين الوصول إلى الحسابات المصرفية وبطاقات الائتمان[41].

- التجسس الإلكتروني على حياة الإنسان الخاصة، وهو مرض يصيب الحاسوب (مخاطر الفيروسات) يؤدي إلى تدمير البيانات والمعلومات المخزنة داخل الحاسوب تدميرا كاملا أو تعديلها[42].

- تزوير المعلومات وسرقتها، ويتم ذلك عبر التسلل الإلكتروني إلى البيانات بواسطة قراصنة إلكترونيين محاولين بذلك الدخول إلى النظام للوصول إلى هذه المعلومات التي ما تكون غالبا سرية[43].

2- الجرائم الإلكترونية الواقعة على حقوق الملكية الفكرية والأدبية

يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفكرية والأدبية، ومثال ذلك استخدام النظام المعلوماتي في السطو على بنوك المعلومات التي تتضمنها برامج نظام معلوماتي آخر دون إذن صاحبها، فهذا الفعل يعتبر اعتداء على حق معنوي، إضافة إلى كونه

اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع. وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الأمر رقم (03-05) الصادر في 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم (03-07) الصادر في 2003 المتعلق ببراءات الاختراع[44].

الفرع الثاني: جرائم إلكترونية أخرى واقعة على حقوق الإنسان

يمكن أن يكون النظام المعلوماتي وسيلة فعالة للاعتداء على حقوق الإنسان الأخرى، ومن بينها تضييق نطاق حقوق حرية التعبير، بالإضافة إلى انتهاكات حقوق الأطفال على مستوى النطاق الإلكتروني، وهو ما نبحثه في البندين المواليين.

أولا: الجرائم الإلكترونية الواقعة على حق حرية التعبير

يعني الحق في حرية التعبير ذلك الكلام المتعلق بمحتوى الإنترنيت، فبسبب التوظيف السلبي لمواقع النت تحول هذا المحتوى إلى شكل من أشكال التحريض الإلكتروني، وهو ما يعرف بجريمة الترويج لخطاب الكراهية، وغالبا ما يكون هذا عن طريق نشر العداوة بين الدول والطوائف والأشخاص والسكان، عن طريق إرسال رسائل وهمية تحمل في طياتها كل أنواع الشتم والتمييز العنصري والتفرقة والإشاعات، بهدف تفعيل كل آليات الحرب، وهذا الأمر يتسبب في أعمال عنف تعسفية ضدهم، عن طريق الإهانة أو التحقير بطريقة خبيثة أو تشويه سمعة أجزاء من السكان بطريقة يمكن تعكير صفو السلم العام[45].

وما يلاحظ أن خطاب الكراهية يتعارض تماما مع حرية التعبير، فالأول يهدف للتفرقة والهدم وينتهك الحقوق الأساسية للإنسان[46]، في حين أن حرية التعبير تهدف على مساعدة كل فرد على تحقيق الذات واكتشاف الحقيقة وتقويتها، وإقامة توازن مقبول بين الاستقرار والتغيرات في المجتمع، ويسمح للجميع بخلق معتقداته الخاصة ونقلها للآخرين بحرية[47].

وفي هذا السياق حدد مقرر الأمم المتحدة الخاص بحماية حق التعبير أربعة أشكال من التعبير يجب أن يحظرها القانون الدولي وهي: استغلال الأطفال في المواد الإباحية، التحريض المباشرة والعام لارتكاب إبادة جماعية، الترويج للكراهية القومية أو العنصرية أو الدينية التي تشكل تحريضا على التمييز العدائي أو العنف والتحريض[48].

وحسب المفوضية الأوروبية لحماية حقوق الإنسان فإن هذه الحرية بما فيها على الانترنت تختفي فيها حالات انتهاك الحقوق، عند استخدامها لغرض تدمير الحقوق والحريات[49].

لكن الحاصل أنه بالرغم من هذه المجهودات الدولية في سعيها لفرض القيود على حرية التعبير، إلا أن الأمر الواقع يوحي بصعوبة تقييد الحريات على مساحة الانترنت، فهي منطقة متاحة أكثر من الإعلام التلفزيوني والصحافة بشتى أنواعها، بسبب احترافية الجناة في هذا المجال، وربما تمظهر فشل هذا المسعى في انتشار جريمة الإرهاب الإلكتروني في العالم بدرجة رهيبة وخطيرة[50].

ثانيا: الجرائم الإلكترونية الواقعة في حق الأطفال

نتيجة الاستخدام السيء لمواقع التواصل الاجتماعي والإنترنيت أصبح من السهل جدا الوصول إلى المواد الإباحية والصور الفاحشة لنشرها واستغلالها عن طريق الأطفال والقصر بغرض تحقيق الجناة مآربهم، ومحاولة الاعتداء عليهم جنسيا، وإذايتهم نفسيا وجسديا، ويكون هذا الأمر بداية بإقامة علاقة صداقة ومحبة سواء بالرسائل النصية أو التواصل الصوتي، مع اتباع أساليب الإطراء وتقديم الهدايا[51].

وفي دراسة أجريت سنة 2009 على 155 من الجناة كانوا يقدمون شروطا لاستخدام الأطفال في المواد الإباحية عبر الإنترنيت فاكتشفوا أنه على الرغم من أنه 26% من هؤلاء الرجال لديهم سجلات جنائية رسمية تتعلق بالجنس وجرائم ضد القاصرين الأطفال، إلا أن 85% من هؤلاء الرجال اعترفوا بارتكابهم جهة اتصال واحدة على الأقل ضد قاصر أثناء العلاج[52].

كما يستغل جناة المواقع الإلكترونية عملية اختطاف الأطفال، فحسب بعض الإحصائيات في أمريكا عام 2011 شملت عمليات الاختطاف 9% من الأطفال الضحايا بسبب الدور الذي لعبته التكنولوجيات في الاتصال المسبق بين الجاني والضحية التي أدت إلى الاختطاف، أو استخدام الجاني للأجهزة الإلكترونية مثل الهواتف المحمولة أو أجهزة الكمبيوتر وفي بعض الحالات يستغل الوالدين هذه الوسائل في استغلال أطفالهم مثلما أثبتت البحوث أن الأم استخدمت الإنترنيت لبيع ابنتها لممارسة الجنس لرجل كانت لديه طفل أسير[53].

الخاتمة:

في آخر المطاف، فإننا حاولنا معالجة موضوع انتهاكات حقوق الإنسان بفعل الجرائم الإلكترونية من خلال مبحثين أساسيين حيث تعرضنا في الأول إلى الجريمة الإلكترونية في نطاق التكنولوجيات الرقمية المعاصرة. أما في المبحث الثاني فقد تعرضنا لانتهاكات حقوق الإنسان في ظل انتشار الجريمة الإلكترونية، وخلصنا إلى بعض النتائج والمقترحات للإجابة عن التساؤل المثار ضمن مشكلة البحث.

أولا: النتائج

1- إن عدم إجماع الفقهاء على تعريف موحد للجريمة الإلكترونية يعود أساسا إلى الاختلاف حول تحديد نطاق هذه الجريمة، خصوصا أن البعض وسع كثيرا من نطاقها واعتبر أن كل فعل غير مشروع يكون للحاسب الآلي دورا فيه جريمة إلكترونية.

2- وجدنا أن حقوق الإنسان من المفاهيم التي عرفت تطورا تاريخيا حتى وصلت إلى ما هي عليه اليوم بفعل الرؤى الجديدة بفلسفات مرتبطة ارتباطا وثيقا بتاريخ الفلسفة وتعاليم الأديان والعقائد منذ العصور القديمة في تنظيرها لها، ولا زالت تطرح العديد من الإشكالات في وقتنا الراهن بسبب التغييرات الحاصلة التي يعيشها المجتمع المعلوماتي في العصر الحديث.

3- وجدنا أن هذه الجريمة مع تميزها عن الجرائم التقليدية، وتعدد أنماطها واحتراف مرتكبيها، سواء كانت جرائم واقعة على النظام المعلوماتي أو باستخدامه، فان لها جوانب سلبية خطيرة تهدد حقوق الإنسان، وبهذا الشكل رصدنا أن هناك طبيعة مميزة بين حقوق الإنسان والجرائم الإلكترونية، فكلما أكدت القوانين على احترام حقوق الإنسان والحريات العامة أسهمت الجرائم الإلكترونية في انتهاك حقوق الإنسان بشكل أكبر.

4- الجرائم الإلكترونية أسهمت وتسببت في أذية الإنسان وانتهاك حقوقه على جميع النواحي والأصعدة، الأخلاقية والسياسية والاقتصادية والاجتماعية، بالرغم من احتشام المساعي الدولية لوضع الشروط اللازمة للتحكم في هذه الجرائم إلا أنها تبقى الشغل الشاغل لها من حيث تحديث القوانين الخاصة بالجريمة حتى يتسنى مواجهتها بشكل فعال.

5- وجدنا أن الجرائم الإلكترونية من الجرائم المستحدثة تشكل تداعياتها خطرا كبيرا على الفرد والمجتمع برمته، وتشكل أزمة حقيقية تقف أمام تطور الدول والحضارات، وتطرح العديد من الإشكالات تتعلق بمصير حقوق الإنسان في ظل التطور اللامحدود الذي يعرفه العلم والبحث العلمي.

ثانيا: التوصيات

1- ضرورة مجابهة الجريمة الإلكترونية، انطلاقا من الأسرة باعتبارها النواة الأولى للمجتمع، وذلك بالاهتمام بتنشئة الطفل على القيم الصحيحة باستعمال الأسلوب التربوي الناجع الذي ينعكس إيجابا على تطور حركة المجتمع ورقيه، مما يساهم في تعزيز حقوق الإنسان وحمايتها من انتهاكات الجرائم الإلكترونية.

2- ضرورة نشر الوعي لدى المواطنين والهيئات والشركات الذين قد تتعرض أنظمتهم الإلكترونية والمعلوماتية للانتهاك، وذلك بضرورة التبليغ والكشف عن مثل هذه الجرائم، لأن التستر والكتمان يؤثر سلبا في السياسة التي يمكن أن تضعها الدولة لمكافحتها.

3- ضرورة تفعيل التعاون الدولي لمواجهة الجرائم المعلوماتية والحد منها وذلك من خلال تعزيز النصوص القانونية من طرف المنظمات الدولية، والدخول في اتفاقيات ومعاهدات جديدة تنص على تبادل الخبرات والمعلومات، بغرض الدفاع عن حقوق الإنسان وحمايتها بشكل جدي وفعال بعيدا عن المصالح الشخصية والأبعاد السياسية التي تفرق بين الدول.

4- ضرورة إعادة النظر في المناهج المتبعة في الجامعات الجزائرية، وذلك بتدريس مقاييس لها علاقة بالتقنيات الجديدة، وتفعيل التظاهرات العلمية والنشاطات الثقافية والاجتماعية، الهادفة إلى صناعة الوعي الذاتي والمجتمعي من أجل اكتساب آليات مواجهة تداعيات الجريمة الإلكترونية، بما يضمن حماية حقوق الإنسان والحريات العامة.

5- الاستفادة من التجارب الدولية في مجال الدفاع عن حقوق الإنسان ضد الجرائم الإلكترونية، وذلك بكسب المهارات اللازمة من أجل مواكبة التقدم والازدهار الحاصل في كثير من دول العالم.

الهوامش:

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، طبعة 1، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 46.

[2] عسال رضا، عماد عبد الرزاق ، الجريمة الإلكترونية والمجرم الإلكتروني، مقاربة مفاهيمية، مجلة بيليوفيليا لدراسان المكتبات والمعلومات، العدد 5، مارس، 2020، ص 153.

[3] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة، 2012/2011، ص 13.

[4] سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية، جامعة أبو بكر بلقايد، تلمسان، 2010، ص 12.

[5] سوير سفيان، مرجع سابق، ص 13، نقلا عن هشام فريد رستم، جريمة الحاسب كصور من صور الجرائم الاقتصادية المستحدثة، بحث مقدم لمؤتمر الأمم المتحدة، التاسع لمنع الجريمة ومعاملة المجرمين، مجلة الأمن العام، العدد 151، سنة 1995، ص 31

[6] محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنيت، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، 2004، ط 1، ص 8 – 9.

[7] سوير سفيان، مرجع سابق، ص 14.

[8] حمزة بن عقون، مرجع سابق، ص 14

[9] نائلة عادل محمد فريد، جرائم الحاسب الاقتصادية (دراسة نظرية وتطبيقية)، القاهرة، 2004، ص 25.

[10] معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة الفكر، العدد 17، جوان، 2018، ص 406.

[11] القانون رقم 09-04 الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 47.

[12] سوير سفيان، مرجع سابق، ص 14 إلى 16.

[13] محمود صالح العادلي، الجرائم المعلوماتية، ماهيتها وصورها، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية. مسقط، 2-4 أفريل 2006، ص 8.

[14] European Crime Prevention Network, Theoretical Paper Cybercrime; Cybercrime: A theoretical overview of the growing digital threat, February 2016 Brussels, p11

[15] مليكة عطوي، الجريمة المعلوماتية، مجلة حوليات، العدد 21، جوان 2012، ص 11.

[16] European Crime Prevention Network, Theoretical Paper Cybercrime, p11.

[17] خالد ممدوح إبراهيم، حوكمة الإنترنيت، الطبعة 01، الإسكندرية، دار الفكر الجامعي، 2011، ص 3.

[18] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة مقارنة)، المؤتمر العربي الأول لعلوم الادلة الجنائية والطب الشرعي، الرياض، 2007، ص 10.

[19] سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2014/2013، ص 18.

[20] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنيت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، ط 1، بيروت، 2007، ص 33.

[21] نائلة عادل محمد زيد قورة، مرجع سابق، ص 323.

[22] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص 62.

[23] حمزة بن عقون، مرجع سابق، ص 46 – 47.

[24] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012، ص 60 – 61، نقلا عن نهلا عبد القادر المومني، مرجع سابق، ص 90، ونقلا عن ضاح محمود الحمود ونشأت مفضي المجالي، جرائم الأنترنت، دار المنار للنشر والتوزيع، 2005، ص 31.

[25] سعيداني نعيم، مرجع سابق، ص 61 – 62.

[26] صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013/2012، ص 42.

[27] سعيداني نعيم، مرجع سابق، ص 62.

[28] أحمد سليم سعيفات، الحريات العامة وحقوق الإنسان (دراسة تاريخية وفلسفية وسياسية وقانونية مقارنة)، ج 1، منشورات الحلبي الحقوقية، لبنان، 2010، ص 40.

[29] كريم بركات، مساهمة المجتمع المدني في حماية حقوق الإنسان، مذكرة لنيل شهادة ماجستير، كلية الحقوق، جامعة بومرداس، 2005/2004، ص 27.

[30] سيد محمدين، حقوق الإنسان والرعاية اللاحقة وأثرها في البيئة الاجتماعية، ط 1، الوكالة العربية للصحافة والنشر والإعلان، القاهرة، 2007، ص 40.

[31] Union interparlementaire et les Nations Unies (Haut-commissariat aux droits de l'homme), Droits de l'homme Guide à l'usage des parlementaires. N° 26, 2016, p11.

[32] قدوس خديجة، عمتوت كمال، انتهاكات حقوق الإنسان في ظل انتشار الجريمة الإلكترونية، مجلة التدوين، المجلد 12، العدد 2، 2020، ص 130.

[33] أبو زيد أبو حسن عبد الموجود إبراهيم، التنمية الاجتماعية وحقوق الإنسان، المكتب الجامعي الحديث، مصر، 2009، ص 394.

[34] نادية خلفة، آليات حماية حقوق الإنسان في المنظومة القانونية الجزائرية، دراسة لبعض الحقوق السياسية، أطروحة دكتوراه، كلية الحقوق، جامعة باتنة، 2010/2009، ص 20.

[35] قدوس خديجة، عمتوت كمال، مرجع سابق، ص 131.

[36] سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الإنترنيت (دراسة مقارنة)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد الثالث، 2013، ص 431 – 432.

[37] مولاي براهيم عبد الحكيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، العدد 23، المجلد الثاني، دون سنة، ص 216.

[38] سوزان عدنان الأستاذ، مرجع سابق، ص 434 – 435.

[39] سوزان عدنان الأستاذ، المرجع نفسه، ص 435.

[40] قدوس خديجة، عمتوت كمال، مرجع سابق، ص 136.

[41] Glenn Curtis, Cybercrime, An Annotated Bibliography, Library of Congress-Federal Research Division, 2009, p3.

[42] طوني عيسى، التنظيم القانوني لشبكة الإنترنيت (دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية)، منشورات الحلبي الحقوقية، لبنان، 2001، ص 169.

[43] سوزان عدنان الأستاذ، مرجع سابق، ص 436.

[44] سوير سفيان، مرجع سابق، ص 34 – 35.

[45] United Nations, Étude détaillée sur la Cybercriminalité Ébauche, Février 2013, New York, p113.

[46] Naganna Chetty, Sreejith Alathur, Hate speech review in the context of online social networks, National Institute of Technology Karnataka, Surathkal, India, Aggression and Violent Behavior 40, 2018, p97

[47] Ibid, p113.

[48] United Nations, Étude détaillée sur la Cybercriminalité Ébauche, Février 2013, New York, p111

[49] Jean-Philippe Foegle, Robin Médard, La liberté d'expression sur Internet en recul, Hommes & Libertés, N°175, Septembre 2016, p111.

[50] قدوس خديجة، عمتوت كمال، مرجع سابق، 139.

[51] قدوس خديجة، عمتوت كمال، مرجع سابق، ص 137.

[52] Keith F. Durkin, Ronald L, Internet Crimes against Children, P 800.

[53] David Finkelhor, and Andrea J, Child, Victims of Stereotypical Kidnappings, Juvenile Justice Bulletin, 2016, p11

قائمة المصادروالمراجع:

أولا: باللغة العربية

1- الكتب:

- أبو زيد أبو حسن عبد الموجود إبراهيم، التنمية الاجتماعية وحقوق الإنسان، المكتب الجامعي الحديث، مصر، 2009.
- أحمد سليم سعيفات، الحريات العامة وحقوق الإنسان (دراسة تاريخية وفلسفية وسياسية وقانونية مقارنة)، ج 1، منشورات الحلبي الحقوقية، لبنان، 2010.
- خالد ممدوح إبراهيم، حوكمة الإنترنيت، الطبعة 01، الإسكندرية، دار الفكر الجامعي، 2011.
- سيد محمدين، حقوق الإنسان والرعاية اللاحقة وأثرها في البيئة الاجتماعية، ط 1، الوكالة العربية للصحافة والنشر والإعلان، القاهرة، 2007.
- ضاح محمود الحمود ونشأت مفضي المجالي، جرائم الأنترنت، دار المنار للنشر والتوزيع، 2005.
- طوني عيسى، التنظيم القانوني لشبكة الإنترنيت (دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية)، منشورات الحلبي الحقوقية، لبنان، 2001.
- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنيت (الجرائم الإلكترونية)، منشورات الحلبي الحقوقية، ط 1، بيروت، 2007.
- محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنيت، مكتبة دار الثقافة للنشر والتوزيع، عمان، ط 1، 2004.
- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004.
- نائلة عادل محمد فريد، جرائم الحاسب الاقتصادية (دراسة نظرية وتطبيقية)، القاهرة، 2004.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، طبعة 1، دار الثقافة للنشر والتوزيع، عمان، 2008.

2- مذكرات الماجستيروأطروحات الدكتوراه:

- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة، 2012/2011.
- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2013/2012.
- سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2014/2013.
- سوير سفيان، جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية، جامعة أبو بكر بلقايد، تلمسان، 2010.
- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013/2012.
- كريم بركات، مساهمة المجتمع المدني في حماية حقوق الإنسان، مذكرة لنيل شهادة ماجستير، كلية الحقوق، جامعة بومرداس، 2005/2004.
- نادية خلفة، آليات حماية حقوق الإنسان في المنظومة القانونية الجزائرية، دراسة لبعض الحقوق السياسية، أطروحة دكتوراه، كلية الحقوق، جامعة باتنة، 2010/2009.

3- القوانين:

- القانون رقم 09-04 الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 47.

4- المجلات والملتقيات:

- سوزان عدنان الأستاذ، انتهاك حرمة الحياة الخاصة عبر الإنترنيت (دراسة مقارنة)، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 29، العدد الثالث، 2013.
- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة مقارنة)، المؤتمر العربي الأول لعلوم الادلة الجنائية والطب الشرعي، الرياض، 2007.
- عسال رضا، عماد عبد الرزاق، الجريمة الإلكترونية والمجرم الإلكتروني، مقاربة مفاهيمية، مجلة بيليوفيليا لدراسان المكتبات والمعلومات، العدد 5، مارس، 2020.
- قدوس خديجة، عمتوت كمال، انتهاكات حقوق الإنسان في ظل انتشار الجريمة الإلكترونية، مجلة التدوين، المجلد 12، العدد 2، 2020.
- محمود صالح العادلي، الجرائم المعلوماتية، ماهيتها وصورها، ورشة العمل الإقليمية حول تطوير التشريعات في مجال مكافحة الجرائم الإلكترونية. مسقط، 2-4 أفريل 2006.
- معاشي سميرة، الجريمة المعلوماتية (دراسة تحليلية لمفهوم الجريمة المعلوماتية)، مجلة الفكر، العدد 17، جوان، 2018.
- مليكة عطوي، الجريمة المعلوماتية، مجلة حوليات، العدد 21، جوان 2012.
- مولاي براهيم عبد الحكيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، العدد 23، المجلد الثاني، دون سنة.
- هشام فريد رستم، جريمة الحاسب كصور من صور الجرائم الاقتصادية المستحدثة، بحث مقدم لمؤتمر الأمم المتحدة، التاسع لمنع الجريمة ومعاملة المجرمين، مجلة الأمن العام، العدد 151، سنة 1995.

ثانيا: باللغة الأجنبية

- David Finkelhor, and Andrea J, Child, Victims of Stereotypical Kidnappings, Juvenile Justice Bulletin, 2016.
- European Crime Prevention Network, Theoretical Paper Cybercrime.
- European Crime Prevention Network, Theoretical Paper Cybercrime; Cybercrime: A theoretical overview of the growing digital threat, February 2016 Brussels.
- Glenn Curtis, Cybercrime, An Annotated Bibliography, Library of Congress-Federal Research Division, 2009.
- Jean-Philippe Foegle, Robin Médard, La liberté d'expression sur Internet en recul, Hommes & Libertés, N°175, Septembre 2016.
- Keith F. Durkin, Ronald L, Internet Crimes against Children.
- Naganna Chetty, Sreejith Alathur, Hate speech review in the context of online social networks, National Institute of Technology Karnataka, Surathkal, India, Aggression and Violent Behavior 40, 2018.
- Union interparlementaire et les Nations Unies (Haut-commissariat aux droits de l'homme), Droits de l'homme Guide à l'usage des parlementaires. N° 26, 2016.
- United Nations, Étude détaillée sur la Cybercriminalité Ébauche, Février 2013, New York.

الجريمة الالكترونية وآثارها على المجتمع من منظور اقتصادي

Electronic crime and its effects on society from an economic perspective

الدكتورة طريّق مسعودة
المدرسة العليا للتسيير والاقتصاد الرقمي بالقليعة
-تيبازة - الجزائر.
مخبر الدراسات والبحوث حول الاقتصاد الرقمي
mtriek@esgen.edu.dz

ملخص :

إن التطور الكبير في مجال تكنولوجيا المعلومات قد مس جميع نواحي الحياة الاجتماعية والاقتصادية وغيرها، من خلال ما قدمته التكنولوجيا المتطورة لتسهيل الحياة للأفراد والمؤسسات وبالخصوص مستعملي الانترنت؛ الا أن هذا التطور السريع قد خلق عدة تحديات، لعل أهمها توفير قاعدة قانونية لحماية اقتصاديات المجتمعات من الجرائم الالكترونية.

نحاول من خلال هذه الورقة البحثية تسليط الضوء على الجريمة الالكترونية من منظور اقتصادي من خلال تبيان كيف يمكن للجريمة الإلكترونية ان تتسبب في خلق ازمات اقتصادية يصعب التصدي لها واظهار الآثار الاقتصادية لمثل هذه الجرائم عل المجتمعات.

الكلمات المفتاحية : الجريمة الالكترونية؛ الرقمنة؛ الجرائم الالكترونية الاقتصادية؛ جرائم الانترنت.

Abstract:

The great development in the field of information technology has touched all aspects of social, economic and other life, through what advanced technology has provided to facilitate life for individuals and institutions, especially Internet users; However, this rapid development has created several challenges, perhaps the most important of which is providing a legal base to protect the economies of societies from cybercrime.

Through this research paper, we try to shed light on cybercrime from an economic perspective by showing how cybercrime can cause economic crises that are difficult to address and show the economic effects of such crimes on societies.
Keywords: cybercrime; digitization; Economic cybercrime; Internet crimes.

مقدمة:

إن التطور الكبير في مجال تكنولوجيا المعلومات قد مس جميع نواحي الحياة الاجتماعية والاقتصادية وغيرها، من خلال ما قدمته التكنولوجيا المتطورة لتسهيل الحياة للأفراد والمؤسسات وبالخصوص مستعملي الانترنت؛ الا أن هذا التطور السريع في عالم الاتصالات والمعلومات قد خلق عدة تحديات تواجهها جميع المجتمعات، لعل أهمها الجريمة الالكترونية في جميع صورها وعلى جميع المستويات.

انطلاقا مما سبق يمكن طرح الاشكالية التالية :

كيف يمكن للجريمة الالكترونية ان تأثر على المجتمع من الناحية الاقتصادية؟

أهداف البحث

يهدف هذا البحث الي اظهار كيف تتأذى اقتصاديات الدول من الاستخدام الواسع للتكنولوجيا بطريقة غير سليمة وها هي الآثار المترتبة على ذلك، من خلال ابراز ماهية الجريمة الالكترونية أنواعها وخصائصها ثم تبيان كيف تأثر هذه الجرائم سلبا على اقتصاديات الدول .

أهمية البحث

لقد اصبحت الجرائم الالكترونية تهدد امن وسلامة ومستقبل الافراد والمؤسسات على حد السواء ومع ضرورة استعمال واستخدام المعلومات المتاحة ووسائل الاتصال الحديثة لا بد من التعرف على هذا الشكل من الاعتداء للتمكن من حصره والتعامل معه والتصدي له.

منهج البحث

من أجل معالجة الاشكالية المطروحة تم اتباع المنهج الوصفي والمنهج التحليلي.

تقسيمات البحث

تم تقسيم البحث الى ثلاثة محاور: تم معالجة في المبحث الاول كل الادبيات المتعلقة بالجريمة الالكترونية تعريفها وتصنيفها وخصائصها، اما المبحث الثاني فقد خصص للجانب الاقتصادي للجريمة الالكترونية كما خصص المحور الثالث والاخير لمعالجة كيفية معالجة الجريمة الإلكترونية.

المحور الاول: عموميات حول الجريمة الالكترونية

تعتبر الجريمة الالكترونية من أكبر التحديات التي أفرزها التطور الكبير والسريع في مجال تكنولوجيا المعلومات والاتصال، لهذا سوف نحاول من خلال هذا المبحث اعطاء صورة عامة عن الجريمة الالكترونية.

أولا: ماهية الجريمة الالكترونية

نتطرق في هذه النقطة الى تعريف الجريمة الالكترونية

1- تعريف الجريمة الالكترونية

لقد تعددت تعاريف الجريمة الالكترونية لهذا من الصعب تقديم تعريف موحد للجريمة الالكترونية، حيث اختلفت الاجتهادات في ذلك اختلافاً كبيرا، يرجع إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة، و تباين الدور الذي تلعبه هذه التقنية في الجريمة من جهة أخرى ، فالنظام المعلوماتي لهذه التقنية يكون محلاً للجريمة تارة، ويكون وسيلة لارتكابها تارة اخرى، فكلما كان البحث منصباً على الجرائم التي ترتكب ضد النظام المعلوماتي انطلق التعريف من زاوية محل الجريمة بأنها الجريمة المرتكبة بالاعتداء على النظام المعلوماتي، أما إذا كان البحث منصباً على دراسة الجرائم التي ترتكب باستخدام التقنية المعلوماتية ارتكز التعريف على الوسيلة وكان :" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب الآلي[1] .

كما عرفها خبراء من منظمة التعاون الاقتصادي والتنمية (OECD) على انها "أي سلوك غير قانوني أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة التلقائية للبيانات و / أو عمليات نقل البيانات"[2].

وحسب الأمم المتحدة، فالجريمة الإلكترونية هي "أي سلوك غير قانوني يستعمل فيه العمليات الإلكترونية للمساس بأمن أنظمة الكمبيوتر وبالبيانات المعالجة"[3].

أما المشرع الجزائري فقد قام بضبط المصطلحات الخاصة بالجريمة الالكترونية من خلال سن القانون رقم 04/09، المتعلق بالقواعد المطبقة على الجرائم المتصلة بجرائم تكنولوجيا الاعلام والاتصال ومكافحتها.[4] على غرار، الجرائم المتصلة بتكنولوجيا الاعلام

والاتصال والتي عرفها على انها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الالكترونية" وفي نفس السياق عرف المشرع الجزائري المنظومة المعلوماتية والمعطيات المعلوماتية ومقدمو الخدمات ...[5]

الجريمة الالكترونية هي أي عمل غير مشروع بدءا من عدم تسليم الخدمات أو البضائع مرورا باقتحام الكمبيوتر والتسلل إلى ملفاته؛ وصولا إلى انتهاك حقوق الملكية الفكرية، والتجسس الاقتصادي (سرقة الإسرار التجارية) والابتزاز عبر الانترنت وتبيض الأموال الدولي وسرقة الهوية. كما تعرف بالجرائم التي لا تعرف الحدود الجغرافية التي يتم ارتكابها بأداة هي الحاسوب الآلي عن طريق شبكة الانترنت وبواسطة شخص فائق الذكاء[6].

الجريمة الإلكترونية هي كل فعل غير قانوني يتسبب فاعله بالحاق الضرر بغيره (افراد او مؤسسات أو هيئات خاصة أو دولية) من خلال استعماله الأجهزة الإلكترونية وشبكة معلوماتية،

2- نبدة تاريخية عن ظهور الجرائم الالكترونية

ظهر مصطلح المعلوماتية لأول مرة من خلال البروفيسور A.L.MIKHILOV مدير المعهد الاتحادي للمعلومات والتقنية بالاتحاد السوفياتي سابقا منذ عام1966، ثم شاع استخدام هذا المصطلح على نطاق واسع و بمفاهيم مختلفة.

في نهاية الثمانينيات سجلت اولى الجرائم الالكترونية التي ارتكبت عبر الانترنيت المعروفة بدودة موريس وهو الشاب موريس الذي نشر فيروس الكتروني تمكن من مهاجمة الاف الحواسيب عبر الانترنيت، وتسبب بأضرار بالغة أبرزها، توقف الاف الأنظمة عن العمل و تعطيل الخدمة و قد قدرت الخسائر آنذاك لإعادة اصلاح هذه الأنظمة وتشغيل المواقع المصابة بحوالي مائة مليون دولار .

و قد اطلق مصطلح جرائم الانترنيت لاحقا شهر فيفري من سنة 1998 في مؤتمر انعقد في استراليا. وبعدها توالت الجرائم الالكترونية بعد اقتران الانترنت بتكنولوجيا الاعلام والاتصال[7].

ثانيا: خصائص الجريمة الالكترونية و أنواعها

تمثل الجرائم المعلوماتية نتاج لتطور تكنولوجيا المعلومات واتساع نطاق تطبيقها في المجتمع مما يضفي عليها طابعا قانونيا خاصا، و يميزها بالعديد من الخصائص الاجرامية المشتركة التي لا تتوافر في الجرائم التقليدية

1- خصائص الجرائم الالكترونية

تتميّز الجرائم الإلكترونية بعدّة خصائص، منها:

- صعوبة معرفة مرتكب الجريمة، وسهولة إخفاء معالم الجريمة وآثارها، فذكاء واحترافية مرتكب الجريمة يحولان دون تتبع اثره فهو يستطيع ان يستخدم برامج او كلمات سرية واستعمال التشفير لإخفاء أي شيء يدينه[8]. يحتاج اتباث هذه الجرائم خبرة فنية مع استخدام وسائل أمنية ذات تقنية عالية.
- بدون عنف وبأقل جهد مقارنة بالجرائم التقليدية؛ حيث سميت بالجرائم الناعمة حيث انها لا تحتاج الى جهد عضلي في ارتكابها وانما تحتاج الى من يتسم بالحكمة والتفكير بطريقة علمية مبنية على المعرفة والمهارة في استخدام الحاسوب وكل ما يتعلق بشبكة الانترنت. يقوم هؤلاء الاشخاص بارتكاب الجرائم الالكترونية بدافع تحقيق مصلحة ما وأحيانا لمجرد أثبات تفوقهم على الآلة أو بدافع اللهو والفضول[9].
- جريمة لا تتقيد بمكان أو زمان محددين؛ فهي لا تعترف بالحدود الجغرافية للدول مما خلق مشاكل حول الاختصاص القضائي فيما يخص تطبيق القانون وتسليط العقوبات على الجناة؛ إن ربط العالم بشبكة من الاتصالات من خلال الأقمار الصناعية والفضائيات والإنترنت جعل الانتشار الثقافي وعولمة الثقافة والجريمة أمرا ممكنا وشائعا لا يعترف بالحدود الإقليمية للدول ولا بالمكان ولا بالزمان أصبحت ساحة الجريمة الالكترونية العالم أجمع [10].

إضافة الى كون الجريمة الالكترونية سلوك غير أخلاقي في المجتمع، فهي تتميز أيضا بصعوبة قياس الضرر المترتب عليها، كونه ضررا يمس الكيانات المعنوية ذات القيم المعنوية أو القيم المادية أو كلاهما معا. ضف الى ذلك سهولة الوقوع فيها بسبب غياب الرقابة الأمنية.

2- أنواع الجريمة الالكترونية

لقد تباينت الصور الإجرامية لظاهرة الجريمة المعلوماتية وتشعبت أنواعها الى ثلاثة أنواع مرتبطة بدرجة خطورتها و صورة الفعل و طبيعتها.

أ- درجة خطورة الجريمة الالكترونية

الجناية: هي أكثر أنواع الجرائم خطورة، وعقابها يتراوح بين الإعدام، والأشغال الشاقة المؤبدة، أو السجن.

الجنحة: في المرتبة الثانية من حيث الخطورة، وعقابها السجن لثلاث سنوات ودفع الغرامة، أو إحدى هاتين العقوبتين. المخالفة: أبسط أنواع الجرائم، وعقوبتها السجن من يوم واحد إلى عشرة، وغرامة مالية .

ب- صورة فعل الجريمة الالكترونية

جريمة آنية: وهي الجريمة الوقتية، التي تحدث مباشرةً وتتمّ بنفس الوقت على صورة جريمة كاملة؛ كالقتل الذي يُفضي لإزهاق الروح بنفس وقت الجريمة، أو كالحريق الذي يشتعل بنفس اللحظة، كإلقاء نار على شيءٍ قابلٍ للاشتعال. الجريمة المستمرة: هي فعل جرمي يتّصف بالاستمرار والامتداد عبر الزمن، ويطول زمن ارتكابها؛ بحيث يُخفي المجرم معالم جريمته، كسرقة الأشياء وإخفائها، وكجرائم القتل التي لا يظهر فاعلها في البداية، ومثل شراء المخدّرات وإخفاء الأسلحة، واختطاف الأشخاص وحبسهم. الجريمة المتعاقبة: هي الجريمة التي يتجدّد فعلها، ويستمر المجرم باقترافها؛ كقطع الطريق، وتعذيب الأشخاص وضربهم بشكلٍ مستمر، وتكرار السرقات لأماكن وأشياء متفرقة، والاعتداء على أشخاص كثيرين، والنّصب والاحتيال عليهم بشكلٍ متكرر.

ج- طبيعة الجريمة الالكترونية

تنقسم الجريمة الالكترونية حسب طبيعتها الى ثلاثة أقسام وهي الجريمة السياسية والجريمة العسكرية والجريمة الاجتماعية، والجريمة الاقتصادية.

- **الجريمة السياسية** : الجريمة التي يتم ارتكابها لأسبابٍ سياسيةٍ؛ حيث يتم فيها الاعتداء على النظام السياسي والرموز السياسية للدولة، والجرائم التي فيها اعتداء على الدستور، وجرائم التحريض والمظاهرات ضد الدولة، وجرائم النشر والصحافة السياسية.
- الجريمة العسكرية: وهي الجرائم التي يتم فيها تعطيل المصالح العسكرية والاعتداء عليها، مثل مخالفة الأوامر العسكرية، والاعتداء على نظام الجيش والأمن.
- الجرائم الاجتماعية: وهي الجرائم التي يتمّ ارتكابها لدوافع اجتماعية نابعة من الانتقام والحقد والطمع والانتقام من الأشخاص، ومشاكل الأسرة، والقضايا الأخلاقية.
- الجرائم الاقتصادية: وهي الجرائم التي تتعلّق بالسطو على الأموال العامة للدولة، والتعدّي على الاقتصاد القومي، وإفساد عمليات الإنتاج والتوزيع الاقتصادي.

-

المحور الثاني: و اقع الجريمة الالكترونية في الميدان الاقتصادي

ان ظاهرة الجرائم الإلكترونية لم تحدث صدفة ولكنها نتاج التطور الاقتصادي الكبير الذي صاحبه التطور السريع في تكنولوجيا المعلومات والاتصالات، حيث تشهد الساحة الدولية الآن تزايد عدد الجرائم الالكترونية بشكل مخيف لا سيما في المجال الاقتصادي أين وجدت المؤسسات مهما كان حجمها نفسها امام خطر لا تعرف متى واين يمكن ان يلم بها.

أولا: أثر الجريمة الالكترونية على الاقتصاد

تهدد الجرائم الالكترونية أمن الدولة وسلامة اقتصادها؛ وهي لا تقتصر على أفراد أو مجموعات وإنما قد تمتد إلى مستوى دولي لتشمل التجسس الإلكتروني في المجال الاقتصادي لتزعزع بذلك استقرار مختلف المؤسسات المكونة للنسيج الاقتصادي للدول. وفيما يلي سنستعرف بعض آثار الجرائم الالكترونية على اقتصاد الدول.

1- الاثر على الشركات والمؤسسات الاقتصادية

تتأثر الشركات والمؤسسات بالجرائم الالكترونية التي تتعرض لها من جراء عمليات الاختراق والقرصنة المتزايدة متسببة في تعطيل مسارها وزعزعة استقرارها.

تستهدف هذه الجرائم بصورة أكثر المؤسسات المالية والاقتصادية وتخص في أغلبها البنوك والمصارف وشركات التأمين وبنسبة أقل القطاع العام وقطاع التعليم[11]. تعد الجرائم الالكترونية أحد ابرز التحديات الأمنية التي تواجهها الشركات والحكومات على المستوى الدولي وباتت تشكل خطرا لما تخلفه من خسائر كبيرة بمعدل يتجاوز النصف مليون دولار امريكي للكبريات الشركات جراء كل هجمة الكترونية أو عملية اختراق تتعرض له[12]. فيما يلي الجرائم الالكترونية التي قد تتعرض لها الشركات وتتسبب لها في خسائر مادية[13] :

- الإطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منها
- العبث بمخازن المعلومات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول إليها
- سرقة الأموال وتحويل حسابات مصرفية الخاصة بالشركة
- الغش في المعاملات الالكترونية كالتغيير في المبيعات

- عمليات الاحتيال
- التهديد والابتزاز
- اختراق الموقع الإلكتروني الخاص بالشركة

2- الأثر على عمل البنوك والمصارف

ساهمت البنوك والمصارف في انتشار الخدمات الإلكترونية، من خلال تقديم خدماته المالية والمصرفية عبر الشبكة، كخدمة تحويل الأموال، وخدمات الدفع الإلكتروني وغيرها. واستخدم بطاقات الائتمان المصرفية من أجل تأمين وصول المستخدمين إلى الحسابات المصرفية، عن طريق قنوات متعددة كالصرافات الآلية، ومواقع الانترنت، والهاتف المحمول. ادى هذا الوضع بمرتكبي الجرائم الالكترونية الى التفكير في السطو على الأموال الالكترونية، وإجراء التحويلات المالية على نحو غير مشروع. معتمدين في ذلك لا سيما على سرقة أو نسخ البطاقات المصرفية، سرقة أرقام الحسابات المصرفية عن طريق التجسس، سرقة أرقام الحسابات المصرفية من خلال مواقع وهمية، اختراق منظومة المصرف وإجراء التحويلات المالية، الترويج والتسويق غير المشروع لأسعار العملات وأسعار سوق الأسهم المالية بهدف التلاعب بها، والقيام بأعمال التجارة الالكترونية غير المرخصة والحصول على الأموال من دون تقديم الخدمات والمنتجات وغسيل الأموال عبر الانترنت.

تتمثل الجرائم الالكترونية التي قد تتعرض لها البنوك والتي تؤثر على الجانب المادي لديها فيما يلي[14]:

- السطو الإلكتروني
- العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها
- تعطيل النظام
- نقل ملكية الأسهم
- اختراق الموقع الإلكتروني الخاص بالبنك.

إن تحول المعاملات التجارية والمالية من الطابع التقليدي الى الطابع الالكتروني قد وضعت مستعملي الانترنت في معاملاتهم امام العديد من المشكلات المتعلقة بالجرائم الالكترونية وقد تسبب ذلك في خسائر كبيرة تكبدها جميع دول العالم بدرجات متفاوتة.

ثانيا: تكاليف الجرائم الالكترونية

من الصعب إجراء تقييم مالي لعواقب الجرائم الإلكترونية. في الواقع ، "لطالما كان من الصعب تقييم العواقب المالية للجرائم الإلكترونية ؛ غالبًا ما تكون الأرقام متناقضة والمصادر غير متجانسة، ولعل أحد أسباب صعوبة التقييم هو عدم الابلاغ عن الانتهاكات التي يتعرضون لها بسبب عدم ملاحظة الهجمات التي تعرضوا لها، وإحجام الشركات عن التنديد بهذه الجرائم. خوفًا من الكشف عن الأسرار الكامنة في نظام الكمبيوتر الخاص بهم ، وغياب التزام الضحايا بتقديم شكوى . وفيما يلي بعض الاحصائيات على سبيل المثال لا الحصر.

2009عقد في هونج كونج أول مؤتمر متخصص لمحاربة الجريمة الإلكترونية وقد ذكر خلاله أن الجرائم الإلكترونية كلفت العالم إلى تلك اللحظة ما يقارب 501 مليار دولار

في ذات السنة 2009 كشفت السلطات الأمريكية عمليات قرصنة وسرقة طالت أكثر من 130 مليون بطاقة ائتمان وبطاقة سحب مصرفية؛ كما أظهر تقرير نشرته "سيمانتك كوربوريشن" تزايدا مطردا في هجمات الجريمة الإلكترونية حيث رصد 100 تهديد إلكتروني في الثانية.

بينت الدراسة التي أجرتها شركة نورتن الرائدة في تطوير الحلول البرمجية الأمنية أن ثلثي مستخدمي الانترنت حول العالم تعرضوا لجريمة إلكترونية على الأقل مرة واحدة (هجمات فيروسية وتجسسيه واحتيالية لسرقة بطاقات الائتمان وسرقة الهوية أو البيانات المصرفية والشخصية الحساسة)

كما أشارت الدراسة إلى أن عملية إزالة الآثار المترتبة عن الجريمة الإلكترونية تستغرق في المتوسط 28 يوم وتكلف في المتوسط 334 مليار دولارا.

2014 قدر مركز الاستراتيجية والدراسات الدولية أن الجريمة الالكترونية كلفت العالم ما بين 345 و445 مليار دولار امريكي وهو ما يمثل 0,62 بالمئة من الناتج الاجمالي العالمي.

2015 أشار المنتدى الاقتصادي العالمي بأن ممارسات التزوير والقرصنة قد كلفت حوالي 1.77 تريليون دولار وهو ما يقارب 10% من التجارة العالمية[15].

2016 كلفت الجريمة الالكترونية الاقتصاد العالمي 600 مليار دولار وهو ما يعادل 0,8 بالمئة من الناتج الاجمالي العالمي[16].

2017 توقع تقرير صدر في نفس السنة من Cybersecurity Ventures أن أضرار برامج الفدية ستكلف العالم 5 مليارات دولار،مسجلة ارتفاعًا من 325 مليون دولار مقارنة بعام

2015، بزيادة 15 مرة في عامين فقط. وقدرت الأضرار لعام 2018 بنحو 8 مليارات دولار، وفي عام 2019 ارتفع الرقم إلى 11.5 مليار دولار. تشير أحدث التوقعات إلى أن تصل تكاليف أضرار برامج الفدية العالمية إلى 20 مليار دولار بحلول عام 2021 - أي 57 ضعفًا عما كانت عليه في عام 2015. كما توقع التقرير حدوث هجوم فدية على الشركات كل 11 ثانية، بحلول عام 2021، بعدما كان كل 40 ثانية في عام 2016 [17].

2021 توقع الخبراء تكبد الاقتصاد العالمي حوالي 6 ترليون دولار بسبب الجرائم الالكترونية وهو ضعف الخسائر المسجلة سنة 2015 والمقدرة بحوالي 3 ترليون دولار [18].

يتوقع أن تزداد تكاليف الجرائم الإلكترونية العالمية بنسبة 15 في المائة سنويًا على مدى السنوات الخمس المقبلة، لتصل إلى 10.5 تريليون دولار أمريكي سنويًا بحلول عام 2025، بعد أن كانت 3 تريليونات دولار أمريكي في عام 2015. وهذا يمثل أكبر تحويل للثروة الاقتصادية في التاريخ، وهي مخاطرة بالحوافز على الابتكار والاستثمار، فقد تعدت هذه الخسائر بشكل كبير الضرر الناجم عن الكوارث الطبيعية في عام واحد، وهي أيضا أكثر ربحية من التجارة العالمية لجميع المخدرات غير المشروعة مجتمعة[19].

المحور الثالث: مواجهة الجريمة الالكترونية

عند ظهور الانترنت لم يفكر مخترعوه في كيفية حماية المعلومات لان استعماله كان حكرا على فئة معينة، لكن سرعة انتشار استعمال الإنترنت جعلت منه مصدرا للقلق والخوف عندما اصبح يستعمل لتنفيذ ما يعرف بالجرائم الالكترونية.

أولا: معوقات اثبات الجريمة الالكترونية

1- غياب الأثر المادي وعدم القدرة على اثبات الجريمة الإلكترونية بحد ذاتها.

يتم إثبات الجريمة بالدليل المادي، ففي غياب هذا الدليل يصعب الحكم في أي قضية؛ في الجريمة الالكترونية غالبا ما يكون الدليل المادي أو الرقمي غير متوفر أو مجهول، و هذا لما توفره التكنولوجيات الجديدة من امكانيات إخفاء الدليل وحو الآثار، فمرتكبي هذا النوع من الجرائم يتصفون بتمكنهم من وسيلة الاجرام (تكنولوجيا المعلومات) لذا يصعب تتبعهم، فهم يحتاطون جيدا لذلك .

إن حيطة وحذر مجرمي الانترنت تحول دون امكانية إثبات الجريمة الالكترونية فهم يستعملون شتى الوسائل من أجل إخفاء وتدليس جرائمهم في شكل عطل أو خطأ في نظام

التشغيل أو من خلال إزالة الجريمة عن طريق التلاعب بالبيانات الرقمية خصوصا المشفرة منها.

2- تلاشي الحدود الجغرافية أمام الجريمة الالكترونية

لقد تعدى الاجرام حدود الدولة الواحدة وصار بامكان المجرم المعلوماتي المتواجد في أقصى الكرة الارضية أن يقوم بالاستيلاء على أموال غيره من الجهة الأخرى للكرة الارضية دون أن يتحرك من مكانه ودون أن يعرف الشخص المعني، دون عنف، دون تعب وحتى غالبا دون خوف.

3- حدود القضاء

-نقص الخبرة لدى جهات البحث والتحري والتحقيق بالجرائم الالكترونية.

- تنازع الاختصاص القضائي بين العالمية والاقليمية، لما يكون السلوك المادي للجريمة الاقتصادية بإقليم دولة، والنتيجة الاجرامية بإقليم دولة أخرى.

ثانيا: آليات مكافحة الجريمة الالكترونية

ان انتشار استعمال الأنترنت أظهر عيوبا حيث سجل أول اختراق للشبكة سنة 1988 حينها توقف عملها لمدة ثلاث أيام و لذلك كان لابد من إيجاد برامج أمنية و قواعد قانونية للحماية من الجرائم الإلكترونية[20]. من هذا المنطلق لا بد من ارساء قاعدة قانونية متينة والاهتمال بكل ما هو جديد في المجال التكنولوجي والتحكم فيها و لذلك لا بد من التكفل بإعداد العنصر البشري ليتولى هذه المهام الصعبة بجدية

1- ارساء قاعدة قانونية خاصة بالجريمة الالكترونية.

يجب على الدول منفردة ومجتمعة مسايرة التطورات الحاصلة على الساحة الدولية فيما يخص التكنولوجيا من أجل مواءمة انظمتها القانونية مع مستجدات الجرائم الالكترونية، والعمل على انشاء أجهزة متخصصة لمواجهتها، والاستفادة من التطور التكنولوجي فيما يخص اجراءات جمع الادلة للتصدي للمنظمات الاجرامية التي أصبحت تتحدى أجهزة العدالة الجنائية المحلية والاقليمية والدولية لافتقارها الآليات والاساليب التي تتناسب وطبيعة الجريمة الالكترونية المرتكبة [21].

2- الاهتمام بالعنصر البشري

يتميز مرتكبو الجرائم الالكترونية بالحكمة والتفكير بطريقة علمية مبنية على المعرفة والمهارة، لهذا يعتبر اكتساب أحدث التكنولوجيا من برمجيات الحماية وغيرها غير كافف في غياب الكفاءة في استخدام هذه البرمجيات لذا لا بد من من التدريب والتحسيس بالإضافة الى الاعتماد على الوسائل المتاحة من أجل القيام باليقظة بجميع انواعها على ان تكون عملية مستمرة وليست آنية.

3- مواكبة التكنولوجيا

يعد التحكم في التكنولوجيا من اولى الخطوات لمواجهة الجريمة الالكترونية والحد منها، ويتحقق ذلك بتوفير الحماية القصوى للمعلومات المتداولة (المتنقلة عبر الشبكة أو المخزنة في الحواسيب). يتعين تركيب أحدث برمجيات الحماية. اما ثاني خطوة فتتمثل في ضرورة القيام بالتحديثات من أجل فعالية البرامج، وعدم ترك أي ثغرة لمرتكبي الجرائم المترصدين بالمؤسسات[22].

بالإضافة لما سبق، يجب رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت، والاعتماد على أساليب وتقنيات متطوّرة للتمكن من الكشف عن هوية مرتكب الجريمة والاستدلال عليه بأقل وقت ممكن، و تأسيس منظمات خاصة لمكافحة الجرائم الإلكترونية والحد منها. و توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية ومخاطرها.

رغم كل الاحتياطات والتدابير للتصدي للجرائم الالكترونية الا أن السيطرة والقضاء عليها يبقى مستحيلا، ويبقى سعي الدول من خلال مؤسساتها وهيئاتها هو تجنب آثار هذه الجرائم وتحجيمها من أجل الحفاظ على نسيجها الاقتصادي من الكوارث التي قد تتعرض لها من جراء ممارسات الكترونية غير سليمة.

خاتمة

تشهد الساحة الدولية تطورات كثيرة ومتسارعة في مجال تكنولوجيا المعلومات والاتصال وهو الامر الذي ساعد على تطور أدوات وسبل الجريمة الإلكترونية بشكل أكثر تعقيدا وأشد ضراوة من قبل في جميع المجالات وبالخصوص المجال الاقتصادي، الأمر الذي يلزم الدول لتطوير آليات مكافحة هذه الجرائم وتتبع كل تطوراتها واستحداث خطوط دفاع قوية وسن قوانين وتشريعات وتوعية الناس بمستحدثات هذه الجرائم, من أجل محاولة الحد وتقليل الخسائر التي انهكت خزائن الدول.

لقد تباينت الصور الإجرامية لظاهرة الجريمة المعلوماتية وتشعبت أنواعها فلم تعد تهدد العديد من الصالح التقليدية التي تحميها القوانين والتشريعات منذ عصور قديمة ، بل أصبحت تهدد العديد من المصالح والمراكز القانونية التي استحدثتها التقنية المعلوماتية بعد اقترانها بثورتي الاتصالات و المعلومات،

في الأخير يمكن تقديم التوصيات التالية:

محاولة تحديد الجرائم الالكترونية في الميدان الاقتصادي من أجل حصرها لتسهيل عملية التعامل معها فيما يخص التجريم وتطبيق القانون.

توعية جميع الاطراف الفاعلة في الاقتصاد سواء اكانوا أفراد أو مؤسسات او شركات بأخطار الجريمة الالكترونية.

- الجريمة الالكترونية لا تعرف الحدود، وبالتالي لا بد من التعاون الدولي في هذا المجال من أجل التصدي لهذه الجرائم التي باتت تهدد اقتصاديات جميع الدول على حد السواء.

الهوامش:

[1] هشام رستم ، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992، – ص29

[2] H. ALTERMAN et A. BLOCH : La Fraude Informatique (Paris, Gaz. Palais), [3 sep. 1988] p. 530

[3] Dixième Congrès des Nations Unies, à Vienne, sous le titre « la prévention du crime et le traitement des délinquants », du 10 au 17 avril 2000, on ligne http://www.uncjin.org ,consulté le 28 juin 2022.

[4] القانون رقم 09-04 المؤرخ في 05 اوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47.

[5] المادة 2 من القانون رقم 09-04 المؤرخ في 05 اوت 2009، مرجع سابق.

[6] اسراء جبريل رشاد مرعي، الجرائم الالكترونية "الاهداف- الاسباب- طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي، على الخط، https://democraticac.de/?p=35426 ، تم الاطلاع عليه بتاريخ 1 جويلية 2022.

[7] عبد الفتاح مراد، دور الكمبيوتر في مجال ارتكاب الجرائم الإلكترونية، دار الكتب والوثائق المصرية، 2005، ص 43.

[8] محمد عبد الرحيم سلطان العلماء، جرائم الانترنت والاحتساب عليها، مؤتمر القانون والكمبيوتر والانترنت، جامعة الامارات العربية المتحدة، من 1 الى 3 ماي 2000، المجلد 3، ط 2004، ص 877.

[9] هشام محمد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني، مجلة الامن والقانون، دبي، العدد 02، ص، 24.

[10] اسراء جبريل رشاد مرعي، الجرائم الالكترونية "الاهداف- الاسباب- طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي، على الخط، https://democraticac.de/?p=35426 ، تم الاطلاع عليه بتاريخ 1جويلية 2022.

[11] محمد سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات، الهيئة المصرية العامة للكتاب، القاهرة، 2003، ص. 35.

[13] منى شاكر فراج العسبلي، مركز التميز لأمن المعلومات، على الخط، http://kenanaonline.com/users/ahmedkordy/posts/320920 تم الاطلاع عليه بتاريخ 30 جوان 2022.

[14] منى شاكر فراج العسبلي، مركز التميز لأمن المعلومات، على الخط، http://kenanaonline.com/users/ahmedkordy/posts/320920 تم الاطلاع عليه بتاريخ 30 جوان 2022.

[15] جورج فهيم، الجريمة الالكترونية تكبد الاقتصاد العالمي تريليون دولار سنويا، 2015، htt

[16] Rapport de synthèse, l'impact économique de la cybercriminalité :pas de ralentissement en vue, on ligne, https://www.mcafee.com/enterprise/fr-ca/assets/executive-summaries/es-economic-impact-cybercrime.pdf, consulté le 30 juin 2022.

[17] Steven morgan, cyberwarfare in the C-Suite, cybercrime magazine, novembre 2020, on ligne, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report- consulté le 2 juillet 2022.

[19] Steven morgan, cyberwarfare in the C-Suite, cybercrime magazine, novembre 2020, on ligne, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report- consulté le 2 juillet 2022.

[20] اسراء جبريل رشاد مرعي، الجرائم الالكترونية "الاهداف- الاسباب- طرق الجريمة ومعالجتها"، المركز الديمقراطي العربي، على الخط، https://democraticac.de/?p=35426 ، تم الاطلاع عليه بتاريخ1 جويلية 2022.

[21] نقموش محمد، ميلودية أحمد، الجريمة المعلوماتية: -حتمية تطوير آليات التعاون الدولي في مجال مكافحتها-، مجلة الدراسات القانونية والسياسية، المجلد 04، العدد 02، 2018، ص. 277.

[22] فيلالي أسماء، المجرمون المعلوماتيون: خطر حقيقي يهدد عالم المعلومات. كتاب جماعي، الجريمة المعلوماتية وأثرها على التنمية الاقتصادية، المركز الديمقراطي العربي، برلين، ألمانيا ، الجزء الأول، جويلية 2020، ص. 71.

مخاطر الجرائم الإلكترونية الممارسة ضد النساء وطرق مواجهتها

The dangers of cybercrime against women and ways to confront them

خشيبة حنان دكتوراه
كلية الحقوق- جامعة الجزائر 1
hananekhochiba@yahoo.com

ديش توريه دكتوراه
كلية الحقوق- جامعة تلمسان
touria.dich@gmail.com

ملخص :

لطالما تعرضت المرأة إلى الكثير من الاضطهاد الذي لم يختفي رغم كل التطور والتقدم، والمتمثل في القرية الإلكترونية التي لم تعد تختلف عن القرية القديمة من حيث الزمن، حيث أن صورة المرأة مازالت سلعة يتاجر بها كل من سولت له نفسه ذلك وعرض المرأة مازالت سلعة يتاجر بها كل من سولت له نفسه ذلك وعرض المرأة العربية لم يختلف كثيرا في اضطهاده على شبكات الإنترنت عن سابق الأزمان، حيث أصبحت الحسابات الإلكترونية الخاصة بالمرأة حسابات مشاع لكل قرصان أو مجرم الإلكتروني له نزوات عدوانية ضدها سواء كانت مكبوتة أو معلنة.

كما أن التهديدات المتنوعة على مختلف صفحات الويب لا تتوقف بل في تزايد مستمر حتى في الحياة الخاصة للمرأة أصبحت محل تهديد دائم، فكم من امرأة طلقت وطردت من وظيفتها بسبب هذه التحرشات الإلكترونية.

الكلمات المفتاحية: الجريمة الإلكترونية، التهديدات، التحرشات الإلكترونية، العنف الإلكتروني.

Abstract:

Women have always been subjected to a lot of persecution that did not disappear despite all the development and progress, which is represented in the electronic village, which is no longer different from the old village in terms of time, as the image of women is still a commodity traded by everyone who asked him to do so, and the display of women is still a commodity traded Everyone who asked himself that and the presentation of Arab women did not differ much in their oppression on the Internet from the past, as the electronic accounts of women

became public accounts for every pirate or cyber criminal who has aggressive whims against her, whether they are repressed or declared.

And the various threats on various web pages do not stop, but are constantly increasing, even in the private life of women has become a constant threat, how many women have been divorced and fired from their job because of these electronic harassment.

Keywords: cybercrime, threats, cyber harassment, cyber violence.

مقدمة:

يوصف العصر الحالي بأنه العصر الرقمي أو ما يسمى بالعصر الإلكتروني الرقمي، فهو يتضمن تطورات تكنولوجيا هائلة وكبيرة ومعقدة تخدم جميع المجالات العامة والخاصة داخل الإطار الضيق للدول، مما يؤدي إلى خدمة المجتمع الدولي بأكمله فالتكنولوجيا تخدم جميع مجالات الحياة، حيث بات هذا العصر يتحرك من خلال تكنولوجيا المعلومات والاتصالات، والتي واكبتها حركة إجرامية كبيرة، فانتشرت الجرائم الإلكترونية بشكل واضح وكبير في جميع دول العالم، فالجميع يستخدم الحاسب الآلي و الجميع معرض تحت تهديد هذه الجرائم، وهي دون شك جرائم من نوع فريد، ومن بين هذه الجرائم التي ذاع صيتها في البيئة المعلوماتية الجرائم الإلكترونية المرتكبة ضد المرأة والتي هي عبارة عن تهديدات وتحرشات جنسية تتعرض لها النساء عبر شبكات الإنترنت، اللازمة للحد من هذه التحرشات.

فما هي أنواع هذه الجرائم وخطورتها وطرق محاربتها؟.

أهداف الدراسة:

- ❖ البحث عن أنواع الجرائم الإلكترونية المرتكبة ضد النساء وضرورة وعيهن بتلك المخاطر.
- ❖ البحث عن سياسات وآليات تعامل المؤسسات التعليمية والاجتماعية و القانونية على مستويات الوقاية والحماية والملاحقة القانونية.
- ❖ التأثيرات النفسية والاجتماعية التي تقع على النساء والفتيات جراء تعرضهن لأشكال مختلفة من الجرائم الإلكترونية، وحماية الأسرة من الاستغلال والاعتداءات الإلكترونية.
- ❖ التعرف على كيفية تعامل النساء عند تعرضهن للجرائم الإلكترونية.
- ❖ تسليط الضوء على طرق الوقاية والحماية والملاحقة القانونية لمرتكبي لتلك الجرائم.

أهمية الدراسة:

- ❖ التطور التكنولوجي الحاصل في مختلف شبكات الإنترنت وخاصة شبكات التواصل الإجتماعي.

- ❖ زيادة نسبة إنتشار الجرائم المعلوماتية.
- ❖ خطورة الجرائم الإلكترونية بكل أنواعها التي تتعرض لها النساء في ظل عالم الرقمنة والتطور التكنولوجي الهائل.
- ❖ المساس بسمعة المرأة وتشويه صورتها.

وللإجابة على الإشكالية المطروحة سنتبع المنهج التحليلي الوصفي وذلك من خلال عرض مجموعة الجرائم الإلكترونية التي تتعرض لها النساء ووصف نوع هذه الجرائم، وعلى هذا الأساس ستقسم دراستنا كما يلي:

المبحث الأول: التعريف بالجريمة الإلكترونية وتصنيف الجرائم الواقعة على الأشخاص

المبحث الثاني: الجرائم الإلكترونية التي تتعرض لها النساء

المبحث الأول: التعريف بالجريمة الإلكترونية وتصنيف الجرائم الواقعة على الأشخاص

تعاني المجتمعات الإلكترونية في الآونة الأخيرة من انتهاك للحقوق والخصوصيات الإلكترونية، وذلك في ظل انتشار الجريمة الإلكترونية، ولدراسة ماهية الجريمة الإلكترونية أكثر لابد من تحديد تعريف دقيق لهذه الجريمة وكذا أنواعها الواقعة على الأشخاص.

المطلب الأول: التعريف بالجريمة الإلكترونية

تعرف الجرائم الإلكترونية بأنها تلك الأفعال الإجرامية الناتجة من خلال أو بواسطة استخدام المعلوماتية والتقنية الحديثة المتمثلة في الكمبيوتر والمعالجة الآلية للبيانات، أو بنقلها[1].

ولقد عرفته منظمة التعاون الاقتصادي والتنميةOECD، "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[2].

وقد نص المشرع الجزائري على هذه الجرائم في قانون09-04 واصطلح على تسميته:" الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، وعرفها بأنها:"جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأية جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية[3].

إن جرائم الكمبيوتر في نطاق الظاهرة الإجرامية المستحدثة، جرائم تنصب على معطيات الحاسوب(بيانات ومعلومات وبرامج) وتطال الحق في المعلومات، ويستخدم لإقترافها وسائل تقنية تقتضي استخدام الحاسوب بوصفه نظاما حقق التزاوج بين تقنيات الحوسبة والاتصالات، وتتم

من خلال الاتصال بالإنترنت ويكون هدفها اختراق الشبكات أو تخريبها أو التحريف أو التزوير أو السرقة والاختلاس أو القرصنة، جرائم أخلاقية، ابتزاز، تشهير وسرقة حقوق الملكية الفكرية، ولقد جرم المشرع الجزائري الأفعال الماسة بنظام المعالجة الآلية للمعطيات، وسميت بالغش ألمعلوماتي في القسم السابع مكرر من قانون العقوبات[4].

المطلب الثاني: تصنيف الجرائم الإلكترونية الواقعة على الأشخاص

فرغم الإيجابيات والفوائد التي جاءت بها الشبكة المعلوماتية والتسهيلات المقدمة للفرد، إلا أنها جعلته أكثر عرضة للانتهاك، ومنها:

أولا_ جريمة التهديد:

يقصد به زرع الخوف في النفس، بالضغط على إرادة الإنسان، وتخويفه من أضرار ما ستلحقه أو ستلحق أشخاص له بها صلة، ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعد بإلحاق الأذى ضد نفس المجني عليه أو ماله وضد نفس أو مال الغير، ولا يشترط أن يتم إلحاق الأذى فعلا أي تنفيذ الوعد، لأنها تشكل تشكل جريمة أخرى قائمة بذاتها تخرج من إطار التهديد إلى التنفيذ الفعلي، وقد يكون التهديد مصحوبا بالأمر أو طلب لقيام بفعل أو الامتناع عن الفعل، أو لمجرد الانتقام، ولقد أصبحت الإنترنت الوسيلة لارتكاب جرائم التهديد والتي في حد ذاتها تحتوي عدة وسائل لإيصال التهديد للمجني عليه لما تتضمنه من نوافذ وجدت للمعرفة كالبريد الإلكتروني أو الويب...

ثانيا_ انتحال الشخصية:

وهو استخدام شخصية الفرد للاستفادة من ماله أو سمعته أو مكانته، ولقد تميزت بسرعة الانتشار خاصة في الأوساط التجارية، وتتم بجمع قدر كبير من المعلومات الشخصية المراد انتحال شخصيته للاستفادة منها لارتكاب جرائمه عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة، كالاسم، العنوان الشخصي، رقم بطاقة الائتمان لتمكن من الوصول لماله أو سمعته...عن طريق الغش.

ثالثا_ انتحال شخصية أحد المواقع:

ويتم ذلك عن طريق اختراع أحد المواقع للسيطرة عليه، ليقوم بتركيب برنامج خاص به هناك باسم الموقع المشهور[5].

رابعا_ جرائم السب والقذف:

للمساس بشرف الغير وسمعتهم، واعتبارهم، ويكون القذف والسب كتابيا، أو عن طريق المطبوعات أو رسوم، عن البريد الإلكتروني أو الصوتي، صفحات الويب، بعبارات تمس الشرف.

فيقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية، وقد يكون شخصا طبيعيا أو معنويا، لتصل المعلومات المراد نشرها إلى أعداد كبيرة من مستخدمي شبكة الإنترنت.

خامسا_المو اقع الإباحية والدعارة:

وجود مواقع على شبكة الإنترنت تحرض على ممارسة الجنس للكبار والقصر، وذلك بنشر صور جنسية للتحريض على ممارسة المحرمات، والجرائم المخلة بالحياء عن طريق الصور، أفلام، رسائل...بالإضافة إلى انتشار الصور ومقاطع الفيديو المخلة بالآداب على مواقع الإنترنت من قبل الغزو الفكري ولكي يتداولها الشباب وإفساد أفكارهم وإضعاف إيمانهم.

وتوفر الشبكة تسهيلا للدعارة، عبر الآلاف المواقع الإباحية، وتسوق الدعارة وتستثمر لها مبالغ ضخمة مع استخدام أحدث التقنيات.

سادسا_ التشهيروتشويه السمعة:

يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فردا أو مؤسسة تجارية أو سياسية، تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوب نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين، ويضم لهذه الجرائم كذلك تشويه السمعة، الشائعات و الأخبار الكاذبة لمحاربة الرموز السياسية والفكرية وحتى الدينية من أجل تشكيك الناس في مصداقية هؤلاء الأفراد، وقد يكون الهدف من ذلك هو الابتزاز.

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي تنقلها القانون وفي مقدمته الدستور الجزائري حيث تنص المادة40 منه:"تضمن الدولة عدم انتهاك حرمة الإنسان"[6]، وعليه يمكن استخدام الشبكة المعلوماتية في الاعتداء على حرمة الفرد وحياته الخاصة، وحرمته، والحريات العامة للأفراد، وهو مخالف للقانون ومعاقب عليه.

المبحث الثاني: الجر ائم الإلكترونية التي تتعرض لها المرأة

وسنحاول من خلال ما يلي إظهار أخطر الجرائم الإلكترونية التي تتعرض لها النساء، وعرض بعض الحالات الواقعية كانت فيها نساء الجزائريات ضحية للجريمة الإلكترونية.

المطلب الأول: أنواع الجر ائم الإلكترونية التي تتعرض لها المرأة

تتعرض المرأة لعدد غير منته من الجرائم الإلكترونية، سواء كانت من مستخدمي الإنترنت والوسائل التكنولوجية أم لا من أمثلتها:

- استغلال خدمات الإنترنت بإرسال رسائل تحرش ومضايقة أو تشويه وتحقير شخص من خلال البريد الإلكتروني فضلا عن إمكانية اختراق البريد الإلكتروني و الإطلاع على معلوماته.
- المشاكل والمعاكسات الأخلاقية تتضمن شبكة الإنترنت عدد هائل من الصور أو الروايات الجنسية الخليعة، كما أن هناك معلومات تعطى لبعض المستخدمين عن عناوين بيوت الدعارة في العديد من دول العالم[7]، وغيرها من الجرائم النافية للأخلاق و المخلة بالحشمة، مثل الجرائم التي يكون البلوتوثBluetooth وسيلة لها من خلال تبادل الأشرطة العنيفة وذات المضمون غير الأخلاقي كما يمكن من خلال البلوتوث الإطلاع والتجسس وسرقة الملفات والمعلومات من جهاز الضحية من طرف المجرم الإلكتروني يهدد من خلاله الآخرين مثلا، أو الفيسبوكfacebook مسرحا لها من خلال الصدقات التي لا تكون حقيقية في الغالب ولا يبدو أن نواياها حسنة.

كما تتعرض العديد من النساء إلى سرقة بطاقات الائتمان عن طريق التحايل أو وعود العمل والزواج الزائفة أو حتى عن طريق جذبهن للمشاركة في عصابات المخدرات و الدعارة والإرهاب من خلال برامج جمع المعلوماتbots، هما أكثر جرائم الابتزاز والتهديد التي تتعرض لهن النساء خاصة في العالم العربي مقابل نشر معلومات خاصة عنهن أو فبركة صور مخلة بالحياء لهن وتهديدهن بنشرها بالإضافة إلى جرائم تشويه السمعة للأحياء و الأموات منهن فكم من فتاة تم تشويه صورتها الاجتماعية بعد نجاحها أو موتها منتحرة مثلا أو في حادث معين[8].

المطلب الثاني: بعض الحالات الو اقعية كانت فيها النساء الجز ائريات ضحية للجريمة الإلكترونية

الجرائم والانتهاكات الإلكترونية التي تتعرض لها النساء في المجتمع الجزائري عبر صفحات الويب يوميا، وسنحاول من خلال ما يلي عرض بعض الحالات الواقعية مع عدم التفصيل أكثر فيها خوفا من التعرف عليهن وهي ما تخشاه هذه الحالات:

أولا_ الاستغلال و التحرش الجنسي:

فتاة تتعرض للتحرش الجنسي (عن طريق تبادل الألفاظ والصور...) من طرف أخوها عن طريق الفيسبوك باحثة عن زوج المستقبل لتكتشف الأمر فيما بعد وهي تعيش مع أخيها في نفس البيت وقد عانا معا من حالة اكتئاب حاد، رغم أن الأخ لم يعرف الحقيقة لحد الساعة.

ثانيا_ التجسس وتسجيل المكالمات:

زوجة تطلق بعدما قام زوجها بوضع تقنية التجسس أو بتثبيت برنامج إنصات على هاتفها النقال وسمعها تتحدث عنه بسوء مع أمها و عائلتها.

ثالثا_ التهديد وتشويه السمعة:

فتاة في العشرينات ورغم عدم استخدامها للإنترنت طلب منها رجل الزواج فلما رفضت هددها بنشر صورها على الإنترنت فلم تنصع له، فقام بوضع صورة وجهها على جسد امرأة عارية بتقنية الفتوشوب، وبذلك نجح بتشويه سمعتها إلى حد كبير ولم تتجاوز هذه الفتاة آثار الجريمة إلا بعد فترة وبمساعدة الأسرة.

رابعا_ السب والشتم:

زوجة تتعرض للسب والشتم من طرف امرأة أخرى بعدما كشفت علاقتها بزوجها وكان البريد الإلكتروني والفايسبوك هو الأداة، وقد كانت هذه المجرمة تتخفى وراء اسم مزور غير حقيقي.

خامسا_ تشويه الصورة والسمعة عن طريق نشر الصور على الحائط:

حائط الفيسبوك كان مسرح الجريمة، أشخاص مجهولين ومعروفين قامو بنشر بعض الصور والتعليقات على حائط شخصية معروفة للنيل منها وإفساد مزاجها كنوع من تصفية الحساب.

سادسا_ خطيب مغشوش:

تعرفت عليه عن طريق غرفة الدردشة والشات، كان مؤدبا غنيا يريد إنشاء أسرة ويتيم بسبب موت والديه في حادث ولا يملك بيتا وجده يكرهه لأنه يكره أباه، وبعد حصوله على كل المعلومات وعنوان البيت وبعد اللقاء الأول تبين أنه فقير يريد استغلالها كونها امرأة عاملة وبدأت سلسلة التهديدات وأقر بأنه يكذب بعد 7أشهر من التعارف على الفيسبوك ولا يعطيها أية معلومة صحيحة(وقد يكون مصابا بهوس الكذب)، فأصيب بصدمة نفسية وتخلت عن العمل.

سابعا_ التحرش الجنسي بعد علاقة في الفيسبوك ثم تهديد بتشويه السمعة:

هذه كانت حالة طالبة جامعية تعرفت على شاب عبر مواقع التواصل الاجتماعي (الفيسبوك) دون استخدام خيار الإخفاء لمعلوماتها الشخصية وكان مهذبا في كلامه، وبعد فترة التعارف لمدة تقل عن شهر اتفقا على اللقاء، فتحرش بها جنسيا، وكانت الصدمة بالنسبة لها،

وهددها بأنه سيخبر الجميع بما فعله بها إن حاولت التخلي عن هذه العلاقة، لكنها استطاعت الخروج من المشكلة بسبب مساعدة الأصدقاء[9].

الخاتمة:

وفي آخر هذه الدراسة نخلص إلى أنه رغم المحاولات المستمرة لتصدي لمثل هذه الجرائم تبقى الوقاية خير من ألف مادة قانونية، إذ يبدو القانون عاجزا نوعا ما في التعامل مع هذا النوع الذي لا يتطلب أركان مادية دائما، أضف إلى ذلك الثغرات التي طالما ميزت القوانين وضيق نصوصها الذي يجد المجرم الإلكتروني وغير الإلكتروني ملاذا للهروب من تحمل تبعات جريمته.

وعليه نتائج هذه الدراسة تتلخص فيما يلي:

النتيجة التي نخرج بها من خلال هذه الدراسة أن الحماية لوحدها غير كافية بل لابد من توعية المرأة و المجتمع ككل بمدى خطورة هكذا جرائم.

وأن القانون يعاني من ضعف وثغرات قانونية عن تنوع الجرائم والوسائل الإلكترونية المستخدمة في هذا النوع من الجرائم، كما أن تطبيق القانون على المستوى المحلي فقط دون وجود اتفاقيات فعالة بين الدول لا يكفي لمحاربة مثل هذه الظواهر.

أما فيما يخص التوصيات التي نخرج بها من هذه الدراسة:

أنه مهما تعددت القوانين التي تردع مثل هذه الجرائم إلا أنها ليست بالكفاية إذ تبقى التوعية هي الأساس لابد من توعية النساء من مخاطر التعامل مع التكنولوجيا مع جهلهن بطرق التعامل مع مخاطرها واستخدامها دون الحاجة لأنها في الغالب تكون عرضة للقرصنة والاحتيال، على اعتبار النساء والأطفال أكثر استهدافا على الشبكة العنكبوتية.

الهوامش:

[1] _محمد الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية، دار النهضة العربية، القاهرة، 1994، ص07.

[2] _أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، القاهرة، 2006، ص87.

[3] _ينظر المادة2-أ من القانون09-04 المؤرخ في 5أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، المؤرخة في 16 أوت2009، العدد47.

[4] _ينظر القسم السابع مكرر، المواد من394مكرر إلى394مكرر7 من الأمر 66-156 المؤرخ في 8جوان 1966، المتضمن قانون العقوبات، المعدل والمتمم.

[5] _محمد بن عبد الله بن علي المنشاوي، جرائم الإنترنت في المجتمع السعودي، ماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص55.

[6] _ينظر المادة40/1 من الدستور1996، ج.ر، رقم76 المؤرخة في 8ديسمبر1996، المعدل والمتمم بالقانون رقم16_01 المؤرخ في6مارس2016، ج.ر، رقم14 المؤرخة في 7 مارس 2016.

[7] _الدليمي عبد الرزاق(2011)، الإعلام الجديد والصحافة الإلكترونية، الطبعة الأولى، دار وائل للنشر والتوزيع، عمان، ص64.63,62.

[8] _بن غدفة شريفة ود. القص صليحة ، الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الإنترنت وطرق محاربتها، عدد19أوت2017، جامعة سطيف2 الجزائر، مقال منشور على الموقع:"https://www.mohamah.net/law/ ، تاريخ التصفح: 2022/06/12.

[9] _بن غدفة شريفة، القص صليحة، الموقع السابق.

الجرائم الإلكترونية الماسة بأمن المعلومات

Cybercrimes that affect information security

أ. إحسان طوير

باحثة دكتوراه علوم، كلية الحقوق،

جامعة سيدي بلعباس

ihsenetouir@gmail.com

ملخص:

تعد الجريمة المعلوماتية من الجرائم الحديثة، ذلك لارتباطها بالتقنية الحديثة المتعلقة بتكنولوجيا المعلومات، لذلك نجد أن تعريفاتها يشوبها نوع من الغموض بالرغم من الجهود التي سعت إلى وضع تعريف محدد لها، لكن الفقه لم يتفق على تعريف محدد، كما نجد جانبا آخر ذهب إلى أن هذا النوع من الجرائم يعتبر تقليديا، إلا أن أسلوب ارتكابه إلكترونيا، وعليه تعد هذه الجريمة من الأصناف الجديدة للجرائم، فانتقل المجرم الذي يرتكبها من الصورة التقليدية إلى الصورة الإلكترونية التي يصعب التعامل معها، فالإشكالية تظهر في كيفية مكافحتها، لأنها تتعلق بالمكونات والمعلومات والبرامج الخاصة بالحاسوب.

الكلمات المفتاحية:

الجريمة – مجرم محترف – أمن المعلومات – البيئة الرقمية – قرصنة.

Abstract:

Information crime is one of the modern crimes, as it is related to modern technology related to information technology, so we find that its definitions are tainted with a kind of ambiguity despite the efforts that sought to develop a specific definition for it, but with diligence. We did not agree on a specific definition, and we also find another aspect that the type of crime is considered traditional, but the method of committing it electronically, and accordingly this crime is considered one of the new types of crimes, as the criminal who commits

it has moved from the traditional image to the electronic image, which is difficult to deal with. The most important conclusion that can be drawn is that international communications conducted remotely through the virtual world facilitate the commission of crimes between one state and another, making it difficult to know. Therefore, protection mechanisms need to be further developed and new challenges posed by professionals in the field of crime.

Keywords:

Crime, Professional Criminal, Information Security, Digital Environment, Hacking.

مقدمة:

تعد الجريمة المعلوماتية من الجرائم الحديثة، ذلك لارتباطها بالتقنية الحديثة المتعلقة بتكنولوجيا المعلومات، لذلك نجد أن تعريفاتها يشوبها نوع من الغموض بالرغم من الجهود التي سعت إلى وضع تعريف محدد لها، لكن الفقه لم يتفق على تعريف محدد، كما نجد جانبا آخر ذهب إلى أن هذا النوع من الجرائم يعتبر تقليديا، إلا أن أسلوب ارتكابه إلكترونيا، وعليه تعد هذه الجريمة من الأصناف الجديدة للجرائم، فانتقل المجرم الذي يرتكبها من الصورة التقليدية إلى الصورة الإلكترونية التي يصعب التعامل معها، فالإشكالية تظهر في كيفية مكافحتها، لأنها تتعلق بالمكونات والمعلومات والبرامج الخاصة بالحاسوب.

ويظهر السبب الجلي في عدم وجود تعريف فقهي جامع مانع للجريمة المعلوماتية هو التطور المستمر والسريع للعالم الإلكتروني، وعليه يترتب عن ذلك العديد من المشكلات العملية أهمها؛ صعوبة مواجهة هذه الجرائم، وعدم التمكن من مكافحتها بالسبل والحلول المناسبة.

تكمن أهمية الموضوع في دراسة تحليلية للإطار المفاهيمي للجرائم الإلكترونية التي تعتبر انتهاكا لحقوق التأليف الرقمي؛ خاصة وأنها في تطور دائم ومستمر، نظرا لتطور تكنولوجيات الاتصال والمعلومات، وكذا تعلقت الدراسة بدراسة مختلف الجرائم التي تقع على المصنف الرقمي داخل البيئة الرقمية، وعليه نطرح الإشكالية التالية: ماهي الجرائم الإلكترونية؟ كيف واكب المشرع الجزائري مختلف الاعتداءات الواقعة على المحل الإلكتروني؟

إجابة على الإشكالية اعتمدت على المنهج الوصفي من خلال تقديم مختلف المفاهيم الخاصة بالجرائم الرقمية، كذلك الخصائص المميزة لها. والمنهج التحليلي من خلال تحليل الاعتداءات التي

تشكل انتهاكا لحقوق التأليف. نناقش هذه الإشكالية من خلال المحاور الآتية:

المبحث الأول: ماهية الجريمة المعلوماتية

المطلب الأول: التعريف الفقهي للجريمة الإلكترونية

المطلب الثاني: التعريف القانوني للجريمة الإلكترونية

المطلب الثالث: خصائص الجريمة المعلوماتية وأركانها

المبحث الثاني: الجرائم المرتكبة على النشر الإلكتروني

المطلب الأول: جريمة التقليد الواقعة على المصنفات الرقمية

المطلب الثاني: المعالجة الآلية للمعطيات

المبحث الأول: ماهية الجريمة المعلوماتية

اختلفت الاتجاهات من حيث تعريف الجريمة الإلكترونية، ويرجع ذلك إلى السرعة الفائقة التي تتميز بها التكنولوجيات الراهنة؛ حيث كان من الصعب إيجاد تعريف موحد للجريمة الإلكترونية.

المطلب الأول: التعريف الفقهي للجريمة الإلكترونية

من خلال الجهود المبذولة من طرف الفقه في محاولتهم لوضع تعريف دقيق وموحد للجريمة المعلوماتية، فقد توصل إلى اتجاهين: الأول يضيق من مفهوم الجريمة المعلوماتية والآخر يوسع من مفهومها.

ومن بين التعريفات المدرجة ضمن المفهوم الضيق للجريمة المعلوماتية: «كل فعل غير مشروع، يكون العلم بتكنولوجيا الكومبيوتر بقدر كبير لازما لارتكابه من ناحية، وملاحقته من ناحية أخرى. »

كما يعرفها اتجاه آخر كما يلي: «هي التي تقع داخل جهاز الكومبيوتر، أو داخل نظامه فقط. » أو هي:« نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكومبيوتر، أو تلك التي يتم تحويلها عن طريقه. »[1]

بينما يعرفها أصحاب الاتجاه الموسع: «كل سلوك إجرامي يتم بمساعدة الكومبيوتر. » أو هي كل جريمة تتم في محيط أجهزة الكومبيوتر، أو هي كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات، أو بنقلها.

عرفها الفقيه فان دير هيلست يونيف، بقوله: هناك غياب لتعريف عام، وإطار نظري متسق في هذا الحقل من الجريمة، وفي أغلب الأحيان تستخدم مصطلحات الافتراضية، والحاسوب، والإلكترونية، والرقمية، وكلها تعكس فجوات مهمة في التعريف. [2] كما عرفها الفقيه تادي مان، بقوله: كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب. [3]

كما عرفها مكتب تقييم التقنية في الو م أ، بأنها الجريمة التي تلعب فيها بيانات الكومبيوتر، والبرامج المعلوماتية دورا رئيسيا. [4]

الملاحظ من هذه التعريفات أن الجريمة المعلوماتية هي النشاط الإجرامي الذي يؤدى داخل نظام الكومبيوتر مشكلا بذلك جريمة. ونجد جانبا آخر من الفقه عند وضعهم لتعريف الجريمة المعلوماتية يراعون عدة اعتبارات هامة وهي:

- أن يكون هذا التعريف مقبولا ومفهوما على المستوى العالمي.
- أن يراعى في وضع التعريف؛ التطور السريع والمتلاحق لتكنولوجيا المعلومات والاتصالات.
- أن يحدد التعريف الدور الذي يقوم به الجهاز الكومبيوتر، وذلك لإتمام النشاط الإجرامي. [5]

المطلب الثاني: التعريف القانوني للجريمة الإلكترونية

اتجهت بعض التشريعات إلى وضع تعريفات لنظام المعلومات؛ حيث عرفها قانون اليونسترال بشأن التجارة الإلكترونية لسنة 1996 من خلال نص المادة 02: النظام الذي يستخدم لإنشاء رسائل البيانات، أو إرسالها، أو استلامها، أو تخزينها، لتجهيزها على أي وجه آخر. [6]

عرفها قانون المعاملات الإلكترونية الأردني رقم 85، لسنة 2001، من خلال نص المادة 02، فقرة 10، حيث عرف نظام المعالجة الآلية للمعطيات: النظام الإلكتروني المستخدم بإنشاء رسائل المعلومات، أو إرسالها، أو تسلمها، أو معالجتها، أو تخزينها، أو تجهيزها، على أي وجه آخر. [7]

عرفها قانون إمارة دبي الخاص بالمعاملات، والتجارة الإلكتروني، رقم 02، لسنة 2002، من خلال نص المادة 02، فقرة 06، بأنه: نظام إلكتروني لإنشاء أو استخراج، أو إرسال، أو استلام، أو تخزين، أو عرض، أو معالجة المعلومات، أو الرسائل إلكترونيا. [8]

عرف التشريع الجزائري الجريمة الإلكترونية ضمن القانون رقم 09-04، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، في نص المادة 02 منه: يقصد في مفهوم هذا القانون... جرائم المساس بأنظمة المعالجة الآلية للمعطيات، المحددة في قانون

العقوبات، أو أي جريمة أخرى ترتكب، أو يسهل ارتكابها، عن طريق منظومة معلوماتية، أو نظام للاتصالات الإلكترونية.

- منظومة معلوماتية: أي نظام منفصل، أو مجموعة من الأنظمة المتصلة ببعضها البعض، أو المرتبطة، يقوم واحد منها الأكثر لمعالجة آلية للمعطيات، تنفيذا لبرنامج معين.

- معطيات معلوماتية: أي عملية عرض للوقائع، أو المعلومات، أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية؛ بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

المطلب الثالث: خصائص الجريمة المعلوماتية وأركانها

تتسم الجريمة المعلوماتية بمجموعة من الخصائص تميزها عن الجريمة التقليدية والتي سنستعرضها من خلال الفروع التالية.

الفرع الأول: خصائص الجريمة المعلوماتية

أولا: الجريمة المعلوماتية جريمة عابرة للحدود

نظرا للطابع العالمي الذي تتسم به شبكة الأنترنت، وما يترتب عن ذلك الاتصال الدولي بين الأشخاص، وهذا ما يجعل الجريمة المعلوماتية تكون ذات طابع دولي، ونجد أن هذه الاتصالات الدولية التي تتم عن بعد عن طريق العالم الافتراضي، تسهل ارتكاب الجرائم بين دولة ودولة أخرى، فالجريمة المعلوماتية لا تحدد بالنطاق الجغرافي، وهي تعتبر عابرة للحدود الدولية، وهذا ما يميزها عن الجريمة العادية.

كما يمكن القول إن من أهم الخصائص التي تميز هذه الجريمة هي تخطيها للحدود الجغرافية، وبالتالي اكتسابها الطابع الدولي. كما يطلق عليها البعض؛ أنها جرائم ذات طبيعة متعدية للحدود، فمع بداية عصر التكنولوجيا أو العصر الافتراضي، لم تعد الحدود الجغرافية تشكل عائقا أمام الاتصال الدولي، وعليه يتوفر عامل قصور المسافات والسرعة مهما كان الموقع الجغرافي لارتكاب الجريمة، وهو ما يميز الجريمة الإلكترونية عن الجريمة التقليدية [9].

وقد أثار الطابع الدولي لهذه الجريمة تساؤلا حول القانون الواجب التطبيق في التعامل مع الجريمة المعلوماتية فيما يتعلق بجمع وقبول الأدلة.

لذلك بات من الضروري تشجيع التعاون الدولي لمواجهة جرائم المعلوماتية، فيجب أن يشمل

هذا التعاون على تبادل المعلومات، تسليم المجرمين، وضمان الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى، وتتمثل الوسيلة المثلى للتعاون الدولي في إبرام الاتفاقيات الدولية [10].

لمواجهة هذه الجريمة مواجهة فعالة، يجب تجريم صورها في القانون الوطني للمعاقبة عليها، وأن يكون هناك تعاون، وتضامن دولي، لمواجهة مشاكلها من حيث مكان وقوعها، واختصاص المحاكم بها، وجمع المعلومات، والتحريات عنها، والتنسيق بين الدول في المعاقبة عليها، وتحديد صورها، وقواعد التسليم فيها، وإيجاد الحدود لمشكلاتها الأساسية [11].

ومما يثار في هذا النطاق من إشكال؛ النطاق المحلي إذا ما وقعت الجريمة بين أكثر من دولة، ومن حيث النطاق الزمني، فتختلف المواقيت بين الدول، لذا يقع التساؤل حول القانون الواجب التطبيق على هذه الجريمة، والإجراءات الجنائية.

ثانيا: صعوبة إثبات الجريمة المعلوماتية

تختلف الجرائم المعلوماتية عن الجرائم العادية؛ حيث إن هذه الأخيرة تعتبر سهلة الاكتشاف والإثبات، أما جرائم الأنترنت فهي صعبة الاكتشاف لتمتعها بخصائص تحول دون اكتشافها وأهمها:

1-جريمة لا عنف فيها؛ حيث إنه يقال لا يوجد شعور حقيقي بعدم الأمان في مواجهة الجريمة المعلوماتية، كالذي يوجد بصورة دائمة في مواجهة غيرها من الجرائم.

2-جريمة لا تترك أثرا؛ حيث يقوم الجاني بجرمه في وقت وجيز، دون أن يترك أي أثر مع تمكنه من إخفاء أثر الجريمة.

3-جريمة تعتمد على تغيير الأرقام والبيانات أو محوها من ذاكرة الحاسب الآلي، وبالتالي يصعب القبض عن الجاني في حالة تلبس.

4-غموض حدود هذه الجريمة مع صعوبة الاحتفاظ بآثارها؛ إذ يستطيع المجرم المعلوماتي في أقل من ثانية، أن يمحو أو يحرف أو يغير البيانات والمعلومات الموجودة في الكومبيوتر. [12]

5-صعوبة التحقيق في الجريمة المعلوماتية؛ حيث يتطلب هذا النوع من الجرائم العلم الكافي بتقنيات الكومبيوتر، ونظم المعلومات، من أجل المتابعة القضائية.

6-عدم شعور الجاني بأنه يقوم بفعل ماس بالأخلاق التي ينص عليها المجتمع الذي يأويه، فالمختصون في المعلوماتية لا يجدون العيب أو الحرج في الدخول إلى نظام الحاسوب بطريقة غير مشروعة، أو نسخ البرنامج بدلا من شراءه، لكن هذا لا يزيح صفة الجريمة في هذا الفعل، فهو

يشكل ابتداء على محل يحميه القانون.[13]

7-أسلوب ارتكاب الجريمة يعتمد على التضليل والخداع، مما يساعد على صعوبة التعرف على مرتكبها، ومن أسباب صعوبة إثبات هذه الجريمة ترجع إلى الجاني وإلى وسيلة تنفيذها؛ حيث تتم هذه الجريمة بشكل منظم من إقليم دولة واحدة باستخدام الأنترنت.

ضف إلى ذلك أن المجرم المعلوماتي هو مجرم محترف ذكي، لا يترك آثارا جانبية للجريمة مما يصعب إثباتها، كما أن المجني عليهم لا يقومون بعملية الإبلاغ عنها في حالة اكتشافها، بفقد ثقة عملائهم فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات، لمدة قد تقل عن الثانية الواحدة.

فعلى سبيل المثال أحصت وزارة الداخلية في فرنسا سنة 1986، حوالي 1200 جريمة معلوماتية، في حين كان هناك حوالي 53600 جريمة ضد الأشخاص، و18900 جريمة تندرج تحت وصف جرائم الآداب، و3مليون جريمة ضد الأموال، وفي أحدث التقارير لمركز شكاوى احتيال الأنترنت؛ الأمر الذي أظهره التحليل الشامل للشكاوى التي قدمت للمركز خلال سنة 2004، قد بلغت 6348 شكوى، من ضمنها 5273 حالة تتعلق باختراق الكومبيوتر عبر الأنترنت، و814 حالة تتعلق بوسائل الدخول والاقتحام الأخرى، كالدخول عبر الهاتف، أو الدخول المباشر إلى النظام بشكل مادي، مع الإشارة إلى أن هذه الحالات هي فقط التي تم الإبلاغ عنها، فلا تمثل الأرقام الحقيقية لعدد حالات الاحتيال الفعلي.[14]

إضافة إلى ارتفاع الخسارة الناجمة عن الجرائم المعلوماتية مقارنة بالجرائم التقليدية؛ إذ حسب تقرير المركز الوطني للبيانات NCCCDإجمالي الخسائر الناجمة في الشهر بلغت حوالي 810000 دولار، أي ما يساوي 800 بليون دولار سنويا.

وتوصل مكتب التحقيقات الفيدرالي FBI إلى أن متوسط الخسارة التي تخلفها الجريمة المعلوماتية يبلغ حوالي 500000 دولار، في حين لا تزيد الخسارة التي تخلفها جرائم السرقة العادية 3500دولار.[15]

ثالثا خصوصية مجرم المعلومات

المجرم المعلوماتي يكون ذو اختصاص وخبرة عالية، ومعرفة في مجال المعلوماتية، وقد تم تصنيف مجرمي الجرائم الإلكترونية إلى المخترقين والمحترفين والحاقدين.

1-المخترقون؛ مثل الهاكرز، فيعد شخصا مختصا في استخدام الحاسب الآلي، ويتمتع بخبرة في التسلل إلى حسابات الآخرين بطرق مضللة.

2-المحترفون؛ وهم الفئة الأكثر خطورة بين مجرمي الأنترنت؛ حيث تنقسم إلى فئتين؛ فئة مادية والغرض من دخولها غير المشروع هو غرض مادي مالي مثل الدخول في حسابات البنوك، والفئة الثانية؛ فئة سياسية، وهذه الفئة تختص بالتعبير عن آرائهم، ومواقفهم في مجال سياسي معين.

3-الحاقدون؛ وهم من تحركهم نزوة الرغبة والانتقام والتأثر، ولا يملكون أية أسباب للجريمة سواء مادية أو سياسية. [16]

رابعا: الجريمة المعلوماتية جريمة مستحدثة

تعتبر الجرائم الإلكترونية من الجرائم الحديثة؛ نظرا للتقدم الذي أحدثته الأنترنت والكومبيوتر في العصر الحالي، فهي ترتكب عن طريق أجهزة حديثة، وفي بيئة حديثة، وتعد هذه الأخيرة بمثابة مجتمع مصغر، وعليه نظرا للأجهزة والقدرات التي ترتكب بواسطتها؛ فإنها تتعدى الرقابة الدولية، وبالتالي صعوبة تطبيق العقاب على مرتكبيها.

فالجريمة المعلوماتية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، فلا غرابة أن تعد الجرائم الإلكترونية سواء التي تتعرض لها أجهزة الكومبيوتر، أو التي تسخر تلك الأجهزة في ارتكابها من الجرائم المستحدثة؛ ذلك أن التقدم التكنولوجي الذي تحقق من خلال السنوات القليلة الماضية، جعل العالم بمثابة قرية صغيرة؛ حيث يتجاوز هذا التقدم بقدراته وإمكاناته أجهزة الدولة الرقابية؛ بل إنه أضعف من قدراتها في تطبيق قوانينها الذي أصبح يهدد أمنها وأمن مواطنيها. [17]

المبحث الثاني: الجرائم المرتكبة على النشر الإلكتروني

المطلب الأول: جريمة التقليد الواقعة على المصنفات الرقمية

أولا: **الركن الشرعي لجنحة التقليد**

لقد جرم المشرع الجزائري في المادتين 151/152، من الأمر 03-05، مجموعة من الأفعال، والتي صنفها في صور الاعتداء على حق، فقد أدرج المشرع الجزائري جل جرائم الاعتداء على حقوق المؤلف تحت وصف التقليد، كما أنه لم يعرف التقليد في الأمر05-03، واكتفى بالنص على الأفعال التي تدخل ضمن هذه الجنحة، وذلك في المادة 151 من الأمر نفسه.

وقصد منع الغش والتقليد قام المشرع الجزائري بحماية حقوق المؤلف، وعليه نصت المادة 151 المذكورة سالفا على الآتي: «يعد مرتكبا لجنحة التقليد كل من يقوم بالأعمال التالية:

- الكشف غير المشروع للمصنف، والمساس بسلامة المصنَّف، أو الأداء لفنان مؤد أو عازف.
- استنساخ أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة.
- استيراد أو تصدير نسخ مقلدة من مصنف أو أداء.
- بيع نسخ مقلدة لمصنف أو أداء.
- تأجير ووضع رهن التداول لنسخ مقلدة لمصنف أو أداء. »

1.الكشف غير المشروع للمصنف الرقمي:

يتمثل في نشر الفعل المقلد علنا بواسطة وسائل سلكية أو لاسلكية بطريقة تمكن أيا كان من الجمهور الاطلاع على ذلك من مكان وزمان يختارهما.[18]

كما أنه تعددت سبل الكشف عن البرمجيات، وذلك بسبب تطور تكنولوجيات كسر الحماية مقارنة مع مواكبة طرق الحماية للبرمجيات، ومن طرق الدخول غير المشروع هو الحصول على الشفرة السرية التي تتبع الدخول للبرمجية واستغلالها كأنه ملك للمستعمل، ومن بين الطرق أيضا قرصنة الرقم التسلسلي للنسخة من البرمجية، وهو رقم تضعه الشركة المصنعة للبرمجية من أجل ضمان عدم تقليد برمجياتها أو استنساخها بطريقة لا شرعية، ومن المعروف أن الكشف غير المشروع عن البرمجيات يشكل ضررا كبيرا للمؤلف أو الناشر على حد سواء. »[19]

2.المساس بسلامة المصنَّف:

يحمي المشرع الجزائري حق مؤلف برنامج حاسوب، أو قواعد بيانات حق إذاعة هذا الأخير أو نشره أو تعديله أو تغيير أو حذف أو إضافة في برنامجه، ولا يمكن اعتراض الغير مالم يكن فيه إخلال أو مساس بمصالحهم، فمؤلف البرنامج له الحق في التعديل دون تغيير وإدخال ما يراه ملائما أثناء عملية صنع الدعامة، وهذا ما نصت عليه المادة 89، من الأمر 05-03.

كما أنه لا يمكن لأي كان أن يدخل تعديلات على المصنَّف بتصحيح أو إضافة أو تعديل أو حذف إلا بموافقة من المؤلف المادة 90 من الأمر 05-03.[20] وعليه فإن المشرع الجزائري يحمي حق المؤلف في هذا المجال من تعديل أو تصوير أو تغيير أو إجراء أو حذف أو إضافة ترد على البرامج أو قاعدة البيانات من شخص آخر دون إذن المؤلف، فمن يرتكب أحد الأفعال السابقة يتوافر في حقه

النشاط الإجرامي لجريمة التقليد.

3.استنساخ البرنامج بأي أسلوب من الأساليب في شكل نسخ مقلدة:

فقد يتم استنساخ البرمجيات في عدة صور وأشكال باختلاف الدعامة والمصدر المتواجد فيها، ويقصد بالاستنساخ هو كل فعل يهدف إلى التعدي على برامج محمية بأي طريقة كانت، فقد اعتبر المشرع الجزائري في المادة 27، ف02، من الأمر 10-97، المؤرخ في 06/03/1997، أن المؤلف أو مالك الحقوق المادية على المصنَّف هو الوحيد المخول بنسخ المصنَّف بأي وسيلة كانت، فيكون الاستنساخ دون رضا المؤلف، وهو إعادة نسخ المصنَّف بأي أسلوب كان، ويعد هذا النوع من النسخ تقليدا بالنسبة للمشرع الجزائري.[21]

ويقصد بالاستنساخ عمل نسخة من المصنَّف بأي وسيلة تقنية تسمح بنقله إلى الجمهور، فهو القيام بنسخة مطابقة للمصنف الأصلي، وعليه فإن استنساخ المصنَّف بدون علم المؤلف يشكل جنحة التقليد، فالمشرع الجزائري كان واضحا في تحديده للاستنساخ بالنسبة للبرمجيات وحددها في حالات استثنائية معينة، فلابد أن يرافق هذا السلوك عدم موافقة المؤلف.[22]

ثانيا: الركن المعنوي لجنحة التقليد

يشترط في جنحة التقليد لقيامها القصد الجنائي العام، فالجاني أثناء قيامه بفعل الاعتداء لم يقصد إلحاق الضرر بالمؤلف، فيكفي أن يكون الجاني على علم مسبق بأنه بصدد التعدي على مؤلف خاص بشخص آخر، ومع ذلك تتجه إرادته إلى تحقيق الفعل الإجرامي، وهي تعتبر من الجرائم العمدية، وهو ما يقصد به توافر العلم والإرادة لدى الجاني أثناء قيامه بسلوك الاعتداء محققا بذلك النتيجة الإجرامية.[23]

وقد حقق المشرع الجزائري عقوبات كافية لتحقيق جزاء لجنحة التقليد بموجب المادة 153، من الأمر 03-05 السالف الذكر، كعقوبة أصلية لمرتكب جنحة التقليد بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة من 500ألف دينار جزائري إلى مليون دينار جزائري سواء تمت عملية النشر في الجزائر أو في الخارج، ويعاقب بنفس العقوبة كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف طبقا لنص المادة 154، من الأمر نفسه.

المطلب الثاني: المعالجة الآلية للمعطيات

أولا: مفهوم نظام المعالجة الآلية للمعطيات

تتسم المعالجة الآلية للمعطيات إلى آلية، تتميز بتوفير المعلومات اللازمة ومعالجتها، فقد نص المشرع على المعالجة الآلية للمعطيات، وذلك للدلالة على مصطلح الجريمة المعلوماتية؛ حيث إن المشرع اضطر إلى مواكبة التطور التكنولوجي للمعلومات في الوقت الراهن؛ الذي أدى بدوره إلى ابتكار نظام المعالجة الآلية، نجم ذلك عن اندماج تقنية نظام المعلومات، وتقنية الاتصالات عن بعد.

وتعرف المعالجة الآلية للمعلومات بأنها عبارة عن آلية وإجراءات منظمة، تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها من ثم تحويلها إلى معلومات يسترجعها الإنسان عند الحاجة ليتمكن من إنجاز عمل، أو اتخاذ قرار، أو القيام بأي وظيفة عن طريق المعرفة التي يحصل عليها من المعلومات المسترجعة من النظام.[24]

تعتبر أنظمة المعالجة الآلية للمعطيات من بين الجرائم الإلكترونية في القانون الجزائري؛ حيث إنه يتكون من ألفاظ مركب، وتقنيات تنتمي إلى بيئة أخرى، وهي البيئة الإلكترونية، تختلف عن بيئة القانون.

نجد الفقه الفرنسي في هذا النطاق من خلال المقرر الفرنسي الصادر في 22ديسمبر1981، قد قسم أنظمة المعالجة الآلية للمعطيات في تعريفه إلى لفظين؛ المعالجة الآلية/ المعطيات، فقد عرف المعالجة الآلية: «مجموعة من العمليات الموجزة عن طريق وسائل آلية، تتعلق بجمع المعطيات، تسجيلها، تحضيرها، تعديلها، حفظها، إتلافها، نشرها، وبوجه عام استغلالها.» [25] كما عرف المعطيات: «عرض معلومة في شكل اصطلاحي مخصص لتسهيل معالجتها.» [26] هذا ما يبين أن أنظمة المعالجة الآلية للمعطيات تتكون من ألفاظ تدل على معناها، بأنها معطيات تعالج بصورة آلية.

كما عرفت المعطيات المعلوماتية في القانون الجزائري في نص المادة 02[27]، من القانون 04-09، ف ج: «أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها. »

كما أنه لم يرد أي تعريف لها ضمن قانون العقوبات الجزائري بالرغم من أنها تشكل جريمة.

اعتبر الدستور الجزائري المعدل بمقتضى قانون 01-16، المؤرخ في 06 مارس2016 ، أنه تعتبر حماية المعطيات ذات الطابع الشخصي بمثابة حق أساسي يضمنه القانون، ويعاقب على انتهاكه، ذلك من خلال نص المادة 46، فـ04، من الدستور الجزائري، واعتبر أن الإخلال بأنظمة المعالجة

الآلية للمعطيات ذات الطابع الشخصي من الوقائع الإجرامية.

فعملية معالجة المعطيات تحتاج إلى آلية منظمة تتولى عمليات جمع وتوفير المعلومات اللازمة ومعالجتها، هو الأمر الذي دفع إلى إيجاد إجراءات مناسبة تساعد على ذلك، فظهر نتيجة لذلك مصطلح نظم المعلومات المبنية على الحاسبات الآلية، أو ما يسمى بنظام المعلومات المحوسبة.[28]

1. تعريف الدخول:

لم يحدد المشرع الجزائري تعريفا دقيقا للدخول، كما لم يبين الوسائل التي يتم بها الدخول، لذا يمكن الدخول إلى النظام المعلوماتي بأية وسيلة كانت؛ لكن اشترط أن يتم الدخول بغير رضا صاحب النظام؛ حيث إنه جرم أي طريقة يتم بها الدخول؛ سواء طريقة مباشرة أو غير مباشرة، كما يرى الفقه الفرنسي بأن الدخول يملك معنيين:

دلالة معنوية: حيث إنه يشبه الدخول هنا إلى نظام معالجة البيانات، أو النظام المعلوماتي أو النظام الإلكتروني، يشبه الدخول إلى ذاكرة الإنسان.

دلالة مادية: يعتبر الدخول غير مشروع إذا تم بطريقة غير مشروعة، يعتبر كذلك الفعل مجرما إذا مسموحا للشخص بالدخول إلى جزء من النظام فقط، إذا تجاوز ذلك إلى جزء آخر غير مسموح له، نكون بصدد جريمة الدخول غير المصرح بها. كما يجب أن يعرض النظام أمام الجمهور، ويتم الولوج إليه عن طريق اختراق الأرقام أو الكلمات أو أية وسيلة استعملت لغرض حمايته.[29]

2.تعريف البقاء:

هو تواجد الجاني داخل النظام المعلوماتي، ويكون غير مسموح له بذلك من طرف صاحب النظام، كما يعتبر فعل البقاء مجرما إذا كان الدخول مسموحا به، أو البقاء غير جائز، أو كان مرتبطا بفعل الدخول غير المشروع.[30]

ويعرف البقاء: «كل تواجد غير عادي كالاتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي؛ أي الدخول والنظر فيه، وفي المعطيات التي يتضمنها، وغيرها من التصرفات غير المسموح بها، والتي تشكل بدورها بقاء احتيالي. »[31]

ثانيا: أركان جريمة الدخول والبقاء في النظام المعلوماتي

تنقسم جريمة المعالجة الآلية للمعطيات كغيرها من الجرائم إلى ركن مادي، وركن معنوي، وركن شرعي، سنركز في هذه الدراسة على الركن المادي، والركن المعنوي للجريمة.

1.الركن المادي:

يتحدد الركن المادي لجريمة الدخول بكون الركن المادي لكل جريمة بأنه ذلك النشاط الإيجابي أو السلبي الذي يجرمه القانون؛ حيث يتطلب الركن المادي في هذه الجريمة، نشاطا إيجابيا، لكن الإشكال المطروح في هذا النطاق؛ هل تعتبر كل الأنظمة الافتراضية متمتعة بالحماية القانونية؟ وهل يعتبر كل دخول لها مخالفا للقانون؟

نص المشرع الجزائري عن الفعل المادي لفعل الدخول عن طريق الغش إلى أنه لم يقدم تعريفا، ذلك من خلال نص المادة 394، مكرر من قانون العقوبات الجزائري:« ... كل من يدخل أو يبقى عن طريق الغش. » حيث إن نص المادة ورد على سبيل العموم، ولم يحدد المشرع الجزائري على سبيل الحصر طرقا معينة للدخول أو البقاء غير المشروعين في جزء أو كل، لنظام المعالجة الآلية للمعطيات.

إن الدخول المشروع يكون بإذن من صاحب النظام، ويتم بطريقة مشروعة، وقد يكون الدخول مباشرا بنظام المعلوماتي يقصد به الدخول في النظام دون الحاجة إلى شبكة اتصال معلوماتي أو إلكتروني لتحقيق الجريمة؛ أي أن فعل الدخول يتم بتواجد الجاني في نفس المكان الذي وجد فيه النظام، وما عليه سوى استعمال الطرق الاحتيالية كفك الشفرات بالطريقة غير المشروعة، والولوج إلى النظام أو التلاعب بنظام المعلومات، وإجراء تعديلات عليه بهدف تسهيل عملية الدخول.

وقد يكون الدخول عن بعد، ويكون الدخول عن طريق استخدام الشبكات المعلوماتية؛ سواء السلكية أو اللاسلكية، ولا يشترط أن يتواجد الجاني في نفس مكان وجود جهاز الحاسب محل الجريمة.

فإذا ما تحقق فعل الدخول سواء مباشرة إلى الجهاز الذي يحتوي على النظام، أو تم الدخول عن بعد عن طريق الاتصال بشبكة المعلومات، وتم ذلك عن طريق الغش أو الاحتيال، فإن ذلك يشكل قيام الركن المادي لجريمة الدخول إلى النظام؛ حيث إن المشرع اعتبر أن كل دخول يتم عن طريق الغش في كل أو جزء من المنظومة المعالجة، أو يحاول ذلك؛ يعتبر فعلا يعاقب عليه القانون.

يتحدد الركن المادي لجريمة البقاء بحيث نص المشرع الجزائري على البقاء غير المشروع

ضمن المادة 394 مكرر في الفقرة الأولى من قانون العقوبات بقوله: «كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات...» .

يعتبر فعل البقاء مجرما إذا ما اتخذ البقاء صورة فعل غير مشروع؛ حيث إنه يبقى الجاني داخل النظام ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق وقوع دخول غير مشروع، وبقاء غير مشروع معا؛ ذلك إذا لم يكن للجاني الصفة، وكان مخولا للدخول إلى النظام، وبالرغم من ذلك دخل إليه عن طريق الغش أو الاحتيال، ثم يبقى داخل النظام بعد ذلك، فهنا يكون قد جمع الجاني بين الركن المادي لجريمة الدخول، والركن المادي لجريمة البقاء.

وتعتبر هذه الجريمة من الجرائم المستمرة، فهي تعتبر كذلك كلما زاد بقاء الجاني داخل المنظومة المعلوماتية، كما لا تشترط هذه الجريمة توافر نية الإضرار بالنظام لدى الجاني، فمتى كان البقاء داخل النظام غير مشروع؛ فإن ذلك يشكل فعلا يعاقب عليه القانون.[33]

2. الركن المعنوي:

إضافة إلى الركن المادي للجريمة، يجب أن تقترن أيضا بالركن المعنوي حتى تكتمل عناصرها؛ حيث يتكون القصد الجنائي من عنصري العلم والإرادة، ويتحقق متى كانت إرادة الجاني واضحة في تحقيق فعل الدخول بمحض إرادته، وليس صدفة، وكان على دراية بأنه يلج إلى نظام معلوماتي خاص بالغير، وقد يتحقق في نوع هذه الجرائم القصد العام الذي يهدف إلى مباشرة السلوك الإجرامي أو القصد الخاص الذي يعتبر الهدف من تحقيق النتيجة.

يتحدد الركن المعنوي لجريمة الدخول إذا كان الجاني على دراية بأنه مرتكب لفعل غير مشروع، يعاقب عليه القانون، وبالرغم من ذلك اتجهت إرادته إلى تحقيق ذلك، فلا يمكن أن ينكر دراية بما قام به؛ أي أنه بمجرد قيامه بالفعل، يعتبر أنه قد حقق قصد جنائي عام، والذي يرد غالبا على جميع صور الجرائم المعلوماتية، أو الإلكترونية، لكن نجد بعض الجرائم في هذا النطاق تقتصر على القصد الخاص.

ويتحدد الركن المعنوي لجريمة البقاء غير المشروع؛ حيث يتحقق الركن المعنوي لجريمة البقاء متى كان الجاني على دراية تامة بأنه متواجد داخل منظومة إلكترونية، وهو على دراية تامة بأنه محظور من البقاء داخلها، وبالرغم من ذلك يستمر فعل البقاء عنده.

ويتحدد الركن المعنوي لجريمة المعالجة الآلية للمعطيات بكونه يجب توافر نية الجاني أنه

يدخل إلى منظومة إلكترونية غير مسموح له بالدخول إليها، ولا تشترط نية توقيع ضرر بالنظام جراء الدخول، ويعتبر دخولا غير مشروع عندما يكون النظام مستقرا مثلا؛ أي أن صاحب النظام يحظر الدخول إلا لمن سمح لهم بذلك، أو كان النظام غير مجاني، إذ يجب دفع مصاريف الدخول حتى يسمح بذلك، واستعمل الجاني طرقا احتيالية، وقام بالدخول إلى النظام مجانا، بهذا يتحقق الدخول غير المشروع.[34] يشترط توفر عنصر العلم والإرادة في هذه الجريمة، وهو توجه علم الجاني إلى واقعة محمية قانونا؛ حيث إنه على علم بأنه غير مصرح له بالدخول؛ سواء في كل المنظومة أو جزء منها.

ثالثا: العقوبات المقررة لجريمة الدخول والبقاء في النظام المعلوماتي

نص المشرع على عقوبات بسيطة لجريمة الدخول أو البقاء؛ حيث يعاقب على هذه الجريمة في الصورة المبسطة؛ أي إذا كان الدخول أو البقاء لم يرتب ضررا بالنظام المعلوماتي وعقوباته المشددة إذا ما تم الإضرار بالمنظومة المعلوماتية، كما قسم قانون العقوبات، عقوبات على الشخص الطبيعي، وعقوبات على الشخص المعنوي.

- **خص المشرع الجزائري العقوبات المقررة للشخص الطبيعي** من خلال نص المادة 394 مكرر من قانون العقوبات الجزائري؛ حيث نص على العقوبات الخاصة بالجريمة المتعلقة بنظام المعاجلة الآلية للمعطيات إلى عقوبات أصلية، تمثلت في الحبس من ثلاثة أشهر إلى سنة، والغرامة من 50 ألف دينار إلى 200 ألف دينار، ومع التعديل الذي وقع على قانون العقوبات سنة2006، قام المشرع بالرفع من الغرامة من 100 ألف دينار كحد أقصى، إلى 200 ألف دينار.

أما إذا نجم عن الدخول أو البقاء عن طريق الغش، حذف أو تغيير المعطيات، تضاعف العقوبة، فتكون أدنى عقوبة للحبس مقررة بستة أشهر، والقصوى بسنتين، والغرامة من 100 ألف دينار جزائري، إلى 400ألف جزائري. أما إذا نتج عن الدخول أو البقاء تخريب للنظام، فترفع عقوبة الحبس من ستة أشهر إلى سنتين، أما الغرامة فيثبت حدها الأدنى عند 50 ألف دينار جزائري، في حين حدها الأقصى عند 300 ألف دينار جزائري.[35]

أما العقوبات التكميلية نصت عليها المادة 394 مكرر 06:« ... مع الاحتفاظ بحقوق الغير حسن النية بحكم بمصادرة الأجهزة، والبرامج، والوسائل المستخدمة» ، وترد المصادرة في الجرائم المعلوماتية للأجهزة والبرامج والوسائل المستعملة، ويقصد بها كل وسيلة مهما كانت طبيعتها ونوعها

تستخدم في ارتكاب الجريمة؛ غير أن المشرع الجزائري قيد المصادرة بعدم المساس بحقوق الغير حسن النية، وهو الأشخاص الذين لم يكونوا محل متابعة أو إدانة من أجل الوقائع التي أدت إلى المصادرة، ولديهم سند ملكية، أو حيازة صحيح.

أما الغلق فقد نص عليها المشرع ضمن المادة 394، مكرر، كما يلي:« ...مع إغلاق المواقع التي تكون محلا للجريمة من الجرائم المعاقب عليها، وفقا لهذا القسم، علاوة على إغلاق المحل، أو مكان الاستغلال، إذا كانت الجريمة قد ارتكبت بعلم مالكها. » حيث إن المشرع نص على إغلاق محل أو مكان الاستغلال، وهي المواقع التي تكون محلا للجريمة.

أما الاستغلال فهو المكان الذي يستعمله المتهم في ارتكاب جريمة، فضبط فيه، وهو يحتوي على الوسائل الإلكترونية الكافية واللازمة لتحقيق عملية الدخول غير المشروع، ولم تحدد المادة 396 مكررة مدة الغلق.[36]

- **تتحدد العقوبات المطبقة على الشخص المعنوي** كما نصت عليه المادة 394، مكرر03:« يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم، بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي. » وقع المشرع الجزائري عقوبات على الأشخاص المعنوية، وقد استثنى من ذلك؛ الأشخاص المعنوية العامة من الخضوع للمسؤولية الجنائية، كما بين المشرع مجمل العقوبات الموقعة عليه، والمتمثلة في:

-حل الشخص المعنوي.

-غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات.

- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.

- المنع من مزاولة نشاط أو عدة أنشطة مهنية، أو اجتماعية بشكل مباشر، أو غير مباشر نهائيا، أو لمدة لا تتجاوز خمس سنوات.

- مصادرة الشيء الذي استعمل في ارتكاب الجريمة، أو نتج عنها.

- نشر وتعليق حكم الإدانة.

- الوضع تحت التصرف لمدة لا تتجاوز خمس سنوات، وتنصيب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة، أو الذي ارتكبت الجريمة بمناسبته.

كما ألزمت المادة 394، مكرر 04، من قانون العقوبات القاضي على تطبيق الحد الأقصى

للغرامة المساوي لخمس أضعاف ما قررته للشخص الطبيعي. أما إذا ارتكبت الجريمة على الجهات العامة، فتضاعف الغرامة مرتين عما هو مقرر للشخص الطبيعي.[37]

نتائج الدراسة:

1- إن الجريمة المعلوماتية هي ذلك النشاط الإجرامي الذي يؤدى داخل نظام الكومبيوتر؛ مشكلا بذلك جريمة.

2- إن الاتصالات الدولية التي تتم عن بعد عن طريق العالم الافتراضي، تسهل ارتكاب الجرائم بين دولة ودولة أخرى، مما يصعب معرفتها.

3- إن المجرم المعلوماتي هو مجرم محترف ذكي، لا يترك آثارا جانبية للجريمة مما يصعب إثباتها.

4- تعد الجريمة المعلوماتية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة.

5- تعتبر أنظمة المعالجة الآلية للمعطيات من بين الجرائم الإلكترونية في القانون الجزائري.

6- تنقسم جريمة المعالجة الآلية للمعطيات كغيرها من الجرائم إلى ركن مادي، وركن معنوي، وركن شرعي.

قائمة المصادروالمراجع:

-أحسن بوصقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، الجزائر.

-إلياس الشيخاني، الاعتداء على حقوق المؤلف والحقوق المجاورة في قانون حماية الملكية الأدبية والفنية، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2008.

-القانون رقم 04-09 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية، عدد47، المؤرخة في 16 أوت2009.

-بدرة عمارة، الحماية الجنائية للمعلومات الالكترونية، دراسة في القانون 15-04، مجلة البحوث القانونية والسياسية، جامعة الطاهر مولاي، سعيدة، عدد02، 2014.

-بسمة مامن، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، مجلد09، عدد01، 2022.

-بهاء فهمي الكبيجي، مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، 2013.

-حديدان سفيان، الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، عدد08، مجلد02، ديسمبر 2017، جامعة قالمة.
-خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009.
-خالد ممدوح إبراهيم، حوكمة الأنترنت، دار الفكر الجامعي، الإسكندرية، 2011.
-خثير مسعود، الحماية الجنائية لبرامج الكومبيوتر، دار الهدى، عين مليلة، الجزائر، 2010.
-رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أدرار، العدد41.
-سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، 2012.
-عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية، جامعة الشرق الأوسط، 2014، مقال منشور على شبكة الأنترنت بتاريخ 21/06/2021، Meu.edu.jo
-عميمر عبد القادر، الحماية الجنائية لحق المؤلف، مذكرة لنيل شهادة ماجستير، الفرع الجنائي، كلية الحقوق، جامعة الجزائر01، 2012/2013.
-عنية باطلي، الجريمة الالكترونية؛ دراسة مقارنة، الدار الجزائرية، الجزائر، 2015.
-قارة آمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه، الجزائر، ط2، 2007.
-محمد حجازي، جرائم الحاسبات والأنترنت، المركز المصري للملكية الفكرية، القاهرة، 2005.
-محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والأنترنت، دار الفكر الجامعي، الإسكندرية.
-نائلة عادل محمد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان، 2005.
-نشناش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية، جامعة بسكرة، 2015.
-Arreté du 22 decembre 1981 relatif à l'enrichissement du vocabulaire de L'informatique, bulletin des bibliothéque de France, 1982, n06.
-John Eoton Djermy smithers amanagers, guid to information technology, London, Philip Allan, 1982.
-Rose philipe, la criminalité informatique à l'horizon 2005, Analyse prospective l'armatan, 1992.

[1] خالد ممدوح إبراهيم، حوكمة الأنترنت، دار الفكر الجامعي، الإسكندرية، 2011، ص357.

[2] محمد حجازي، جرائم الحاسبات والأنترنت، المركز المصري للملكية الفكرية، القاهرة، 2005، ص08.

[3] رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، جامعة أحمد دراية، أدرار، العدد 41، ص435.

[4] المرجع نفسه، ص435.

[5] المرجع السابق، ص358.

[6] نشناش منية، مداخلة حول الركن المفترض في الجريمة المعلوماتية، جامعة بسكرة، 2015، ص03.

[7] المرجع نفسه، ص03.

[8] قانون إمارة دبي رقم 02، لسنة 2002، متعلق بالمعاملات والتجارة الإلكترونية، صدر في 12فبراير، 2002.

[9] نائلة عادل محمد، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان، 2005، ص50.

[10] المرجع السابق، ص50.

[11] خالد ممدوح إبراهيم، المرجع السابق، ص362.

[12] محمود عبد الرحيم الديب، الحماية القانونية للملكية الفكرية في مجال الحاسب الآلي والأنترنت، دار الفكر الجامعي، الإسكندرية، ص56-55.

[13] John Eoton Djermy smithers amanagers, guid to information technology, London, Philip Allan, 1982 P263.

[14] نائلة عادل محمد فريد، المرجع السابق، ص49.

[15] Rose philipe, la criminalité informatique à l'horizon 2005, Analyse prospective l'armatan, 1992, P49.

[16] خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط1، 2009، ص78-79.

[17] عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية، جامعة الشرق الأوسط، 2014، مقال منشور على شبكة الأنترنت بتاريخ 21/06/2021، ص26.Meu.edu.jo

[18] إلياس الشيخاني، الاعتداء على حقوق المؤلف والحقوق المجاورة في قانون حماية الملكية الأدبية والفنية، المؤسسة الحديثة للكتاب، طرابلس، لبنان، 2008، ص20.

[19] خثير مسعود، الحماية الجنائية لبرامج الكومبيوتر، دار الهدى، عين مليلة، الجزائر،2010، ص90.

[20] المرجع نفسه، ص91.

[21] المرجع نفسه، ص94.

[22] عميمر عبد القادر، الحماية الجنائية لحق المؤلف، مذكرة لنيل شهادة ماجستير، الفرع الجنائي، كلية الحقوق، جامعة الجزائر01، 2012/2013، ص54.

[23] خثير مسعود، المرجع السابق، ص96.

[24] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة ماجستير في العلوم القانونية، جامعة الحاج لخضر، باتنة، 2012، ص42.

[25] Arreté du 22 decembre 1981 relatif à l'enrichissement du vocabulaire de L'informatique, bulletin des bibliothéque de France, 1982, n06, p335.

[26] Op, cit, p336.

[27] القانون رقم 04-09 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة رسمية، عدد47، المؤرخة في 16 أوت2009.

[28] سعيداني نعيم، مرجع سابق، ص42.

[29] بهاء فهمي الكبيجي، مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط، 2013، ص26.

[30] عنية باطلي، الجريمة الالكترونية؛ دراسة مقارنة، الدار الجزائرية، الجزائر، 2015، ص160.

[31] بسمة مامن، جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، مجلد09، عدد01، 2022، ص480.

[32] قارة آمال، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومه، الجزائر، ط2، 2007، ص43.

[33] أحسن بوصقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، الجزائر، ص43.

[34] بدرة عمارة، الحماية الجنائية للمعلومات الالكترونية، دراسة في القانون 15-04، مجلة البحوث القانونية والسياسية، جامعة الطاهر مولاي، سعيدة، عدد02، 2014، ص438.

[35] حديدان سفيان، الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، عدد08، مجلد02، ديسمبر 2017، جامعة قالمة، ص682.

[36] المرجع نفسه، ص688.

[37] حديدان سفيان، مرجع سابق، ص683-684.

جريمة التزوير في المحررات الالكترونية كأداة لانتهاك حقوق الإنسان في البيئة الرقمية

The crime of forgery in electronic edits as a tool for violating human rights in the digital environment

د. كركوري مباركة حنان، أستاذة محاضرة "ب"

كلية الحقوق، جامعة الجزائر -1- بن يوسف بن خدّة (الجزائر)

البريد الالكتروني: m.karkouri@univ-alger.dzkarkouri.hanane39@gmail.com /

ملخص:

تعالج هذه الدراسة موضوع جريمة التزوير في المحررات الالكترونية كأداة لانتهاك حقوق الإنسان في البيئة الرقمية؛ حيث تتجلى من خلال البحث في التأصيل المفاهيمي لجريمة التزوير في المحررات الالكترونية عن طريق تحديد مختلف التعريفات الفقهية والتشريعية لجريمة التزوير في المحرر الالكتروني، فضلا عن تبيان الخصوصيات التي تتميز بها هذا من ناحية؛ ومن ناحية أخرى تتجلى في كيفيات ارتكاب جريمة التزوير في المحرر الالكتروني في مختلف الوسائل التي يتم بواسطتها ارتكاب هذه الجريمة، فقد تكون هذه الوسائل مادية متمثلة في اصطناع المحرر أو تزوير التوقيع أو القيام بعملية الحذف أو الإضافة أو التغيير للحقيقة الواردة فيه، كما قد تكون وسائل معنوية متمثلة أساسا في جعل واقعة مزورة في صورة واقعة صحيحة، وهو الأمر الذي يتطلب توقيع المشرع الجزائري للعقوبات الجزائية اللازمة على مرتكبي هذه الجريمة طبقا للأحكام الواردة في قانون العقوبات في القسم الخاص بالمساس بأنظمة المعالجة الآلية للمعطيات.

الكلمات المفتاحية: التزوير الالكتروني؛ الإطار المفاهيمي؛ وسائل التزوير؛ التشريع الجزائري؛ البيئة الرقمية.

Abstract:

This study addresses the crime of forgery in electronic edits as a tool for violating human rights in the digital environment; it manifests itself through research into the conceptual rooting of the crime of forgery in electronic edits by identifying various doctrinal and fragmented definitions of the crime of forgery in the electronic editor, as well as clarifying the specifics that characterize this; On the other hand, it is reflected in the ways in which the electronic editor commits the offence of forgery in the various means by which the crime is committed, which may be material, such means as the fabrication of the editor, forgery of the signature, the deletion,

addition or change of the truth contained in it, and may be moral means, mainly in making a false incident in the form of a valid fact, This requires the Algerian legislator to impose the necessary criminal penalties on the perpetrators of this crime in accordance with the provisions of the Penal Code in the section on the violation of automated data processing systems.
Key words: Electronic forgery; conceptual framework; means of forgery; Algerian legislation; digital environment.

مقدمة:

يعتبر مصطلح التزوير في المحررات الإلكترونية مفهوماً حديث النشأة ظهر للتماشي مع التطورات التكنولوجية في مجال تكنولوجيا المعلومات والاتصالات التي يشهدها العالم اليوم، وللتوصل إلى تحديد مفهوم هذا النوع من الجرائم التي تختلف عن جريمة التزوير في المحررات التقليدية، وعليه كان لابد من تبيان الإطار المفاهيمي لجريمة التزوير في المحررات الالكترونية في التشريع الجزائري فضلا عن تبيان خصوصية ارتكاب هذا النوع من الجرائم المستحدثة والتي يعتبر ارتكابها بمثابة انتهاك مباشر لحقوق الإنسان في البيئة الرقمية هذا من جهة؛

ومن جهة أخرى تسليط الضوء على كيفيات ارتكاب هذه الجريمة التي تتم بواسطة مجموعة من الوسائل الالكترونية المتطورة التي لا يمكن حصرها، وكذا تبيان مختلف الآثار المترتبة عن ارتكاب جريمة التزوير في المحرر الالكتروني المرتكبة من طرف فرد واحد أو عدة أفراد، ذلك أن ارتكاب هذه الجريمة لا يقتصر على فرد معين فقط أو على مؤسسة ذات طابع عام أو خاص أو على الدولة الواحدة، وإنما يتجاوز ارتكاب هذه الجريمة كافة الحدود الإقليمية للدولة، باعتبار إنها جريمة الكترونية تقع في بيئة افتراضية غير ملموسة وغير محددة المعالم.

وبالتالي كان لزاماً على المشرع الجزائري فرض ترسانة قانونية بغية فرض الحماية الخاصة على حقوق الإنسان في البيئة الافتراضية الرقمية، وكذا توقيع العقاب على مرتكبي هذا النوع من الجرائم المستحدثة والمنصوص عليه في مضمون أحكام قانون العقوبات والتوقيع والتصديق الالكترونيين وكذا القوانين ذات الصلة التي تنص على إجراء التزوير الالكتروني.

وعليه ومما سبق ذكره، فإن الإشكالية المطروحة هي: ما هو أساس قيام جريمة التزوير في المحررات الالكترونية وما هي انعكاساته على حقوق الأفراد في البيئة الرقمية المعلوماتية؟

للإجابة على هذه الإشكالية المطروحة تم اعتماد المنهج الوصفي والتحليل أداة له؛ وذلك من خلال وصف وتحليل مختلف المعطيات والآراء الفقهية وكذا النصوص القانونية

والتشريعية في القانون الجزائري مع الإشارة في بعض المواضع من الدراسة إلى بعض التشريعات المقارنة المتعلقة بارتكاب جريمة التزوير في المحرر ذات الطبيعة الالكترونية التي تم الاعتماد عليها في الدراسة، والمقسمة بدورها إلى مبحثين أساسين؛

ركز المبحث الأول منه على تحديد التأصيل المفاهيمي لجريمة التزوير في المحررات الالكترونية باعتبارها من أكثر الجرائم تهديدا لحقوق الأفراد في البيئة الرقمية أو المعلوماتية، ثم خصوصية ارتكاب جريمة التزوير في المحرر حتى يتم الاعتداد بمعيار وجود فعل التزوير وارتكاب الجريمة في النظام المعلوماتي، في حين ركز المبحث الثاني على كيفيات ارتكاب جريمة التزوير في المحررات الالكترونية من خلال تبيان مختلف الوسائل المادية والمعنوية المستخدمة في ارتكابها؛ ثم التوصل إلى تبيان موقف المشرع الجزائري من هذه الجرائم عن طريق توقيعه لجملة من العقوبات المتمثلة في الحبس والغرامات المالية على كل من ارتكب فعل التزوير على المحرر في البيئة الرقمية، وسيتم التفصيل في جميع هذه المسائل تباعا في المباحث الآتية:

المبحث الأول: الإطار المفاهيمي لجريمة التزوير في المحررات الالكترونية

إن جريمة التزوير المرتكبة في المجال التكنولوجي تعتبر من أخطر صور الغش المعلوماتي والسبب في ذلك يعود للدور الهام والخطير الذي أصبح يقوم به الحاسب الآلي لأنه اقتحم كافة المجالات حيث أصبح يجرى من خلاله كم هائل من المعطيات ذات الآثار القانونية الهامة والخطيرة والتي لا يصدق عليها وصف المحرر التقليدي المكتوب.

ولهذا كان للتدخل الفقهي والتشريعي دور بالغ الأهمية في تحديد تعريف لجريمة التزوير في المحرر الالكتروني، وذلك لاعتبارها إحدى أهم الجرائم الإلكترونية وأكثرها تعقيدا نظرا لاتصالها بالثقة العامة والتي من شأنها إلحاق الضرر بالحقوق أو المراكز القانونية للأفراد في البيئة الرقمية (المطلب الأول)، والجدير بالذكر أن لهذه الجريمة خصوصيات تتميز بها؛ حيث تتمثل على وجه الخصوص في إمكانية ارتكاب جريمة التزوير في أي من مراحل تشغيل النظام، فضلا عن انعدام الأثر المادي لها واعتبارها جريمة لا تتم إلا بعد التخطيط المسبق (المطلب الثاني)، وبناء على ما سبق سنتعرض إلى تعريف جريمة التزوير في مجال المحررات الإلكترونية ثم إلى خصوصية ارتكابها في المطالب الموالية:

المطلب الأول: تعريف جريمة تزوير المحرر الالكتروني

تعتبر جريمة التزوير من أهم الجرائم المستحدثة ذات الوصف الدقيق باعتبار أنها تحتاج في معالجتها إلى عناية خاصة بسبب تباين سبل وكيفيات التزوير وتطورها، حيث لم تقتصر جريمة التزوير على المفهوم التقليدي الواقع على المحررات الورقية بل تطورت هذه

الجريمة وظهر بما يُعرف بالتزوير الالكتروني؛ وهو الأمر الذي استدعى العديد من التشريعات إلى التنصيص على أحكام جريمة التزوير في شكلها الجديد وذلك في مضامين تشريعاتها العقابية بغية إضفاء الحماية الجزائية على المعلومات أو البيانات الخاصة بالأفراد والموجودة في البيئة الرقمية أو الشبكة الإلكترونية، والتي تتعلق أساسا بإثبات حقوق أو مراكز قانونية معينة.

وعليه يمثل التصرف المادي المتمثل في التزوير في المحرر الإلكتروني صورة لا تقل أهمية عن التزوير في المحررات التقليدية الورقية[1]، فأي مساس بمحتواه وتغييره يمكن أن يتم في أي وقت، ولا يمكن كشفه أو الوقوف عليه أو إقامة الدليل على وقوعه، بالتالي فإن خطورة التزوير في المحررات الإلكترونية يتجاوز التزوير في المحررات الورقية المعروفة في الأدلة الكتابية الخطية، إلا أن هذا التزوير يتحد معه في المفهوم الوظيفي بالنسبة لتحريف الحقائق أو البيانات.

ويعرف التزوير في اللغة بأنه الزور والباطل والكذب والتقليد والمحاكاة والبعد عن الحق، وهو أيضاً لفظ مشتق من كلمة مزور وهو الكذب والتلفيق وادخال الباطل، وهو معنى واسع شامل لكل صنوف الغش والتحايل[2]، وقد حظي تعريف التزوير في مجال المحررات الإلكترونية باهتمام فقهي وتشريعي واسع، وبناء على ذلك سنتطرق إلى تبيان التعريف الفقهي والقانوني لجريمة التزوير بشيء من التفصيل في الفروع الموالية:

الفرع الأول: التعريف الفقهي لجريمة التزوير

يُعرف الفقهاء التزوير عموما بأنه عبارة عن عملية مادية وصورة من صور الكذب التي يقوم بها شخص بغرض تغيير الحقيقة في محرر أو سند عمومي أو سند رسمي بإحدى الطرق المحددة في القانون، وشأنه إلحاق الضرر بالحقوق أو المراكز القانونية لأحد أو بعض أطراف السند أو المحرر محل الادعاء بالتزوير[3].

وقد اختلف الفقه حول مدى جواز تطبيق النصوص المقررة على الأفعال التي تشكل تغييرا للحقيقة في البيانات المخزونة إلكترونيا في الحاسبات الآلية، والتي يتحقق بها وجود الركن المادي لجريمة التزوير الإلكتروني، إلا أنه ومع ضيق نطاق النصوص المقررة في قانون العقوبات، فإنه من الضروري تعديل أحكام هذا القانون بشكل يستوعب جريمة التزوير الإلكتروني، وذلك لتوفير الحماية للمحررات الإلكترونية أيا كانت طبيعتها، لاسيما بعد أن تزايد الاعتماد على هذه المحررات في المعاملات الالكترونية[4].

وبناء على ذلك عرف جانب من الفقه العربي التزوير المعلوماتي بأنه "تغيير الحقيقة بأي وسيلة كانت سواء كان ذلك محرر أو دعامة أو سند طالما أن هذه الدعامة ذات أثر في إنشاء حق، أو لها شأن في إحداث نتائج معينة"[5]، وهناك من عرف التزوير في مجال المحررات الإلكترونية بأنه "تغيير الحقيقة في المحررات المعالجة آليا، والمحررات الإلكترونية، وذلك بنية استعمالها"[6].

في حين عرف الأستاذ عبد الفتاح بيومي الحجازي جريمة التزوير بأنها "تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في ورقة مكتوبة أو مرسومة عن طريق الرسم ويستوي في المحرر الإلكتروني أن يكون باللغة العربية أو بأية لغة أخرى لها دلالتها، وربما تتمثل في صورة مخرجات غير ورقية بشرط أن تكون محفوظة على دعامة معلوماتية كبرنامج منسوخ على أسطوانة، وبشرط أن يكون المحرر المعلوماتي ذات أثر قانوني في إثبات حق أو التزام، وأن يكون قابلا للاستخدام"[7]، وبالرجوع إلى الفقه المقارن نجد بأن الفقيه الفرنسي ايميل جارسون قد عرف جريمة التزوير بأنها "تغيير الحقيقة بقصد الغش في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه أن يسبب ضررا"[8].

ومن خلال التعريفات الفقهية الواردة أعلاه يمكننا القول بأن جريمة التزوير في المحررات الالكترونية هي عبارة عن القيام بتغيير الحقيقة الموجودة في المحرر الالكتروني المكتوب أما باللغة العربية أو بلغة أجنبية بواسطة أجهزة الحاسب الآلي بأي طريقة كانت وذلك بقصد الغش فيما أعد المحرر لإثباته، تغييرا من شأنه أن يسبب ضررا للغير إذا حصل بقصد جنائي أو بسوء نية.

الفرع الثاني: التعريف التشريعي لجريمة التزوير

لقد أدرجت العديد من التشريعات العربية والأجنبية جريمة التزوير عموما في مختلف النصوص العقابية؛ حيث أقرت هذه النصوص في مجملها تجريم فعل التزوير بوصفه سلوكا مجرما ليشمل التزوير فيما بعد كافة صور المحررات الورقية والالكترونية على وجه الخصوص[9]؛ وفي هذا الصدد نصت المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بأن جريمة التزوير عبارة عن "استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييرا من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة"[10].

وبالرجوع إلى القانون الجزائري نجد بأن المشرع الجزائري قد نص بصفة صريحة على جريمة تزوير المحررات في المواد 214 إلى 229 من قانون العقوبات، حيث قسم هذه الجريمة

إلى ثلاثة أقسام، قسم خاص بتزوير المحررات الرسمية، قسم خاص بتزوير المحررات العرفية والتجارية أو المصرفية، وقسم أورد فيه تزوير بعض الوثائق الإدارية والشهادات[11].

أما بالنسبة المشرع المصري فقد جرم في قانون التوقيع الإلكتروني تزوير المحررات الإلكترونية بأشكاله المختلفة، حيث نص في مضمون المادة الرابعة -04- من قانون التوقيع الإلكتروني بأنه "مع عدم الإخلال بأية عقوبة أشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من أتلف أو عيب توقيعا أو وسيطا أو محررا إلكترونيا، أو زور شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر، أو أستعمل توقيعا أو وسيطا أو محررا إلكترونيا معيبا أو مزورا مع علمه بذلك"[12].

وبالإشارة إلى القانون الأردني نجد بأن قانون العقوبات الأردني رقم 16 لسنة 1960 في نص المادة 260 بأن التزوير هو عبارة عن "تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد إثباتها بصك أو مخطوط يحتج بهما أو يمكن أن ينجم عنه ضرر مادي أو معنوي أو اجتماعي"[13]، أما بالنسبة لقانون العقوبات العراقي رقم 111 لسنة 1969 نجد المادة 286 منه قد عرفت الجريمة نفسها بأنها عبارة عن "تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر أخر بإحدى الطرق المادية أو المعنوية التي بينها القانون تغييرا من شأنه إحداث ضرر بالمصلحة العامة أو بشخص من الأشخاص"[14].

في حين أن القانون الفرنسي بوصفه تشريعا أجنبيا؛ فقد اعتبر جريمة التزوير في المحررات الإلكترونية من أخطر صور الغش في نطاق المعلوماتية[15]، بسبب خطورة الدور الذي يقوم به الحاسب الآلي في الوقت الحاضر وفي كل المجالات فقد أصبحت تتم من خلاله عمليات هائلة ترتب آثار قانونية خطيرة، وهو الأمر الذي أكد عليه في المادة 221 من قانون العقوبات الفرنسي.

المطلب الثاني: خصوصية جريمة التزوير في المحرر الالكتروني

تعتبر جريمة تزوير المحرر الإلكتروني في البيئة الرقمية من بين أخطر الجرائم الواقعة في البيئة الرقمية والماسة بحقوق الإنسان في هذا الفضاء وسواء كان فردا أو يمثل شخصا معنويا عاما أو خاصا، خاصة إذا تعلق الأمر بتزوير محررات رسمية تمت على يد موظف مكلف بتحريرها مثل العقود، أو وثيقة إدارية تخص جهة حكومية لأن ذلك يمس بالثقة العامة في مثل هذه الوثائق، وهو الأمر الذي يترتب عليه إنفراد هذا النوع من الجرائم

المستحدثة بخصوصية تزيد من خطورتها ومن الآثار الخطيرة التي تترتب على قيامها، وفي الفروع الآتي بيانها سنذكر أهم الخصائص التي تنفرد بها جريمة التزوير الالكتروني:

الفرع الأول: إمكانية ارتكاب جريمة التزوير في أي من مراحل تشغيل النظام

يمكن ارتكاب جريمة التزوير في أية مرحلة من مراحل تشغيل نظام المعالجة الآلية وهي مرحلة الإدخال، المعالجة، الإخراج، ففي مرحلة الإدخال تترجم المعلومات إلى لغة مفهومة من قبل الآلة يسهل إدخال معلومات غير صحيحة أو عدم إدخال الوثائق الأساسية والمعلومات المطلوبة[16]، لذلك يمكن تصور التزوير المعنوي بإدخال معلومات غير صحيحة للاعتداد بها على أنها معلومات صحيحة، أو ترك إدخال معلومات أساسية وذلك من أجل إحداث تغيير للحقيقة، كقيام موظف بإدراج أسماء أشخاص على محرر الكتروني لكنهم غير موجودين في الحقيقة[17].

أما في مرحلة المعالجة فيمكن إدخال تعديلات على برامج الحاسب الآلي لتحقق الهدف الإجرامي عن طريق التلاعب في برامج النظام المعلوماتي، كما يمكن تغيير النتائج عند مرحلة الإخراج بعد أن تم إدخال المعطيات ومعالجتها بطريقة صحيحة، بالدخول إلى نظام المعالجة الآلية من أجل تزييف الحقيقة[18].

الفرع الثاني: انعدام الأثر المادي في جريمة التزوير في المحرر الإلكتروني

ما يميز جريمة التزوير في المحرر الإلكتروني عن غيرها من الجرائم هو انعدام الأثر المادي الواقع على المحرر الذي وقعت عليه عملية التزوير؛ حيث تتم عملية التزوير عن طريق إحداث التغيير إما بالإضافة أو الحذف باستخدام أدوات أو مواد كيميائية، باعتبار أنها جريمة فنية غير ملموسة[19]، يصعب اكتشافها والجدير بالذكر أن إثبات الجرائم الالكترونية راجع لعدة أسباب، متمثلة في وسيلة التنفيذ التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد.

ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات، وبالتالي يصعب العثور على دليل مادي ملموس مثبت لوقوع الجريمة والسبب الرئيسي في ذلك يعود لسلوك المجرم المعلوماتي الذي يستخدم وسائل فنية وتقنية معقدة أثناء ارتكابه للجريمة[20].

الفرع الثالث: ارتكاب جريمة التزوير عن طريق التخطيط المسبق

يتطلب ارتكاب جريمة التزوير في المحرر الالكتروني تجنيد مختلف العلوم والمعارف الفنية والتقنية والتطورات الحادثة فيها، فهي جرائم تحتاج إلى عمليات ذهنية وعقلية

ومعلومات فنية ومهارات خاصة، وبالتالي فإن هذه الجرائم لا يمكن أن ترتكب بالصدفة، وإنما هي جرائم يخطط لها بخبرة أشخاص ذوي مهارات عالية.

وفي هذا الصدد نجد بأن اتفاقية بودابست قد نصت في المادة السابعة -07- بأن " يلتزم كل طرف بتجريم الأفعال التالية إذا ما أقترف عمدا دون وجه حق إدخال، تغيير، حذف أو حجب لبيانات الحاسب الآلي، بما يؤدي إلى إيجاد بيانات غير صحيحة بقصد جعلها تأخذ شكل البيانات الصحيحة عند استخدامها استخداما مشروعا، ويتم التجريم بغض النظر عن كون هذه البيانات مقروءة أو مفهومة"[21]، حيث يتضح لنا جليا من نص المادة المذكورة آنفا أن التزوير الإلكتروني يرِد على محررات إلكترونية يتم الحصول عليها بوسائل إلكترونية، فتكون ناشئة عن جهاز إلكتروني أو كهرومغناطيسي أي طبع ممغنط، بالتالي يمكن اعتبار المحررات الإلكترونية محررات تطبق عليها جريمة التزوير، بالنظر إلى الغاية والهدف من تجريم التزوير، لأن الهدف من تجريم أفعال التزوير هو حماية الثقة العامة بالمحررات بغض النظر عن طبيعتها.

المبحث الثاني: كيفيات ارتكاب جريمة التزوير في المحررات الالكترونية

تتجلى كيفيات ارتكاب جريمة التزوير في المحرر الالكتروني من خلال النشاط الإجرامي المتمثل في ارتكاب سلوك مجرّم وهو فعل تزوير المحرر في البيئة الرقمية الإلكترونية، بإحدى الوسائل التي يتم بواسطتها ارتكاب هذه الجريمة، فقد تكون وسائل تزوير مادية لا تتحقق إلا من خلال اصطناع المحرر أو تزوير التوقيع أو القيام بعميلة الحذف أو الإضافة أو التغيير للحقيقة الواردة فيه فتغيير الحقيقة يعني استبدالها بما يخالفها، الأمر الذي لا يعتبر معه تغييرا للحقيقة ذلك التغيير الذي يعدم المحرر أو يمحو عنه قيمته في مخرجات الحاسب الآلي، أي البيانات والمعلومات الخارجة منه، وقد تكون هذه الوسائل معنوية متمثلة أساسا في جعل واقعة مزورة في صورة واقعة صحيحة فأي تغيير أو تعديل في أي من بيانات يعتبر تزويرا (المطلب الأول).

وفيما يتعلق بمسالة العقوبات المقررة على ارتكاب هذه الجريمة، نجد أن المشرع الجزائري قد تناول جميع المسائل الخاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات واستعمال الإعلام الآلي، في القسم السابع مكرر من قانون العقوبات والذي جاء حصرا تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، بحيث كيّف النصوص القانونية الواردة في هذا القسم على أنها جنح وقد حصرها في الجرائم المتمثلة في إدخال المعطيات والدخول أو البقاء في المنظومة الآلية للمعطيات وننشر المعطيات المخزنة أو المرسلة (المطلب الثاني)،

وعليه سنتعرض إلى تبيان كيفيات ارتكاب جريمة التزوير في مجال المحررات الإلكترونية في المطالب الموالية:

المطلب الأول: وسائل ارتكاب جريمة التزوير في المحرر الالكتروني

تتمثل وسائل ارتكاب جريمة التزوير في المحرر الالكتروني في تغيير الحقيقة الواردة في المحرر الالكتروني إما عن طريق التزوير المادي أو المعنوي، ويستوي في ذلك أن يتم التزوير بوضع إمضاءات أو أختام مزورة، أو تغيير المحرر والأختام والإمضاءات، أو زيادة كلمات أو وضع أسماء أشخاص آخرين مزورة، أو التقليد بصفة عامة أو تغيير إقرار أصحاب الشأن في المحرر أو جعل واقعة مزورة في صورة واقعة صحيحة، أو جعل واقعة غير معترف بها في صورة واقعة معترف بها، أو التزوير عن طريق الترك؛ وفيما يلي سنتعرض بشيء من التفصيل في تحديد وسائل التزوير المادي والمعنوي في المحرر الالكتروني في الفروع الموالية:

الفرع الأول: التزوير المادي

يُعرف الفقهاء التزوير المادي بأنه تغيير للحقيقة بصورة ملموسة في محرر رسمي أو عمومي؛ حيث يتم ذلك بطريقة مادية تترك أثرا ماديا سواء بزيادة أو بحذف أو بتعديل أو بإنشاء محرر لا وجود له في الأصل، وهناك من يعرف التزوير المادي أيضا بأنه "كل تغيير للحقيقة ينصب على مصدر المحرر بأنه ينسب المحرر إلى غير منشئه، أو يتناول بالتعديل صلب المحرر بعد،إنشائه من محرر حقيقي"[22]، وتجدر الإشارة إلى أن المشرع الجزائري قد نص في أحكام قانون العقوبات على صور التزوير المادي في المواد من 214 إلى 216 ويمكن حصرها في ثلاث صور[23]؛

تتمثل الصورة الأولى في اصطناع محرر؛ حيث يقصد بالاصطناع خلق محرر بأكمله ونسبه إلى محررة، أو بتعبير آخر إنشاء محرر سواء بتقليد خط المنسوب إليه أو بدون تقليد لخطه، أي دون ضرورة تعمد تقليد محرر بالذات أو خط إنسان معين، والأصل لا يكون للمحررات قيمة إلا إذا حملت توقيعا من صاحب الشأن أي توقيع الشخص الذي أصدرها ومن ثم يقترن الاصطناع في الغالب باصطناع محرر أو أختام مزورة[24].

في حين أن الصورة الثانية فتتمثل في توقيع مزور أو وضع ختم مزور على مخرجات الحاسب الآلي؛ حيث يعرف التوقيع بأنه كل تصرف إداري يقصد به التعبير عن موافقة الموقع على مضمون السند أو بعبارة أخرى التعبير عن انطباق إراداته الداخلية على التصريحات الواردة فيه والتزامه بها[25]، وتقتضي هذه الطريقة من طرق التزوير المادي أن يوقع المزوّر على محرر بإمضائه هو ينسبه إلى شخص آخر لم يصدر عنه[26].

وفي هذا الصدد نصت المادة 214 من قانون العقوبات بأن "يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته إما بوضع توقيعات مزورة، وإما بإحداث تغيير في المحررات أو الخطوط أو التوقيعات، وإما بانتحال شخصية الغير أو الحلول محلها، وإما بالكتابة في سجلات أو غيرها من المحررات العمومية أو بالتغيير فيها بعد إتمام أو قفلها"[27]، وهذا الحكم ينطبق على المحررات الالكترونية في حالة التقاضي الالكتروني ووجود المستندات الالكترونية.

أما الصورة الثالثة والأخيرة فتتمثل في حذف أو إضافة أو تغيير مضمون المحرر؛ حيث تعني هذه الطريقة كل أساليب التشويه المادي التي يمكن أن تقع على المحرر بعد الفراغ من تحريره، ويستهدف المزور بهذه الطريقة الإيهام بأن المحرر كان له منذ تحريره المظهر والفحوى اللذان صارا له بعد التغيير[28]، وأهمها تفترضه هذه الطريقة أنه يشمل كل تغيير مادي يمكن إحداثه في المحرر بعد تمام المحرر، أما الذي يحصل أثناء تحرير المحرر فهو من طرق التزوير المعنوي.

الفرع الثاني: التزوير المعنوي

لقد نصت المادة 215 من قانون العقوبات على مضمون التزوير المعنوي؛ وقد اعتبرته بأنه مجموعة من الأفعال المتعلقة بتزييف جوهر المحررات الرسمية أو ظروفها بطريق الغش، وكتابة اتفاقيات مخالفة لتلك التي تم تدوينها أو أمليت من قبل الأطراف، فضلا عن تقرير وقائع كاذبة بصورة وقائع صحيحة وغيرها من التصرفات؛ وفي هذا الصدد أقر نص المادة المذكورة صراحة بأن "يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية قام أثناء تحريره محررات من أعمال وظيفته بتزييف جوهرها أو ظروفها بطريقة الغش وذلك إما بكتابة اتفاقيات أو أمليت من الأطراف أو بتقريره وقائع يعلم أنها كاذبة في صورة وقائع صحيحة أو بالشهادة كذبة أو بأن الوقائع قد اعترف بها أو وقعت في حضوره أو بإسقاطه أو بتقديره عمدا الإقرارات التي تلقتها"[29].

وفي نفس السياق وبالإشارة إلى التشريعات العربية المقارنة نجد المادة 23 من قانون التوقيع الإلكتروني الصادر عن جمهورية مصر العربية[30]؛ قد أوردت صور التزوير الإلكتروني التي تكون محلا للمساءلة الجنائية، وبالتالي يمكن الإدعاء بها أمام القضاء، فإذا توافرت إحدى الصور المذكورة في هذه المادة أمكن الإدعاء بتزوير المحرر أو التوقيع الإلكتروني، على أن تطبق في شأن هذا الإدعاء الأحكام المنصوص عليها في قانون الإثبات الخاصة بالإدعاء بالتزوير.

وتجدر الإشارة إلى أن وسيلة التزوير في المحررات الالكترونية تتم بطريقة أسهل وأسرع مقارنة بالتزوير الواقع في المحررات العادية، لأنه لا يحتاج إلى إزالة باستخدام الأدوات والمواد الكيماوية لتغيير معاني الكلمات أو كشط توقيعات سابقة، ولكنه يحتاج فقط إلى إدخال كلمات أو تغيير معاني كلمات بالحذف أو الإضافة أو التعديل عليها، وبذلك يصدر المحرر النهائي مطابقا للأصل، وإن كان مزورا في مضمونه[31].

ذلك أن إمكانية وقوع التزوير في المحررات الإلكترونية بالطرق المعنوية وارد بصورة أكبر من التزوير المادي والسب الحقيقي في ذلك هو جوهر أو حقيقة التزوير المعنوي، والذي يتحقق بتشويه المعاني التي يجب أن يعبر المحرر عنها، فهو تزوير يؤدي إلى تغيير مضمون أو دلالة المحرر ذاته[32]، فضلا عن ذلك اعتباره غير متضمن لأي أثر ذات طبيعة مادية تشير بكل بوضوح إلى العبث به، ولذلك لا يستدل عليه إلا إذا تم التوصل إلى حقيقة ما كان يجب إثباته، فضلا عن ذلك أيضا اعتبار التزوير المعنوي مصاحب لإنشاء المحرر المزور ذاته.

وتتمثل صور التزوير المعنوي على وجه الخصوص في تغيير إقرارات أولي الشأن؛ بحيث يمكن من خلال انتشار استخدام الحاسب الآلي في كافة مجالات الحياة، أن تقع تلك الطريقة من طرق التزوير باستخدام النظام المعلوماتي في القيام بها، ففي مجال المحررات يتم مثلا استخدام النظام المعلوماتي ممثلا في الحاسب الآلي، بحيث يقوم الشخص المسؤول عن هذا النظام والذي يتعامل مع الجمهور، على خلاف الحقيقة بما يريد إثباته بالمخالفة لإقرار ذوي الشأن، بالمخالفة للثقة التي أولاها الجمهور للنظم المعلوماتية وما يصدر عنها من بيانات[33].

ويمكن أن تتمثل أيضا في جعل واقعة مزورة في صورة واقعة صحيحة؛ بحيث يمكن أن تقع تلك الطريقة من خلال الاتصالات الإلكترونية، وذلك من خلال التلاعب بها بنسبة وقائع مزيفة إلى الغير، طالما أن النظام المعلوماتي يتم استخدامه محل النظم التقليدية السابقة التي كانت محلا للتزوير المعنوي بالطرق التقليدية[34]، لأن دخول النظام المعلوماتي جعله أيضا محلا لتلك الطرق في ارتكاب جرائم التزوير باستخدام النظم المعلوماتية كوسيلة تتلاءم مع التغيير الذي شهدته المجتمعات في ارتكاب هذه الجريمة التي تنتهك حقوق الإنسان في هذه البيئة الرقمية.

وفي الأخير يمكننا القول بأن درجة الخطورة في ارتكاب جرائم التزوير في المحررات الإلكترونية تتجاوز حجم خطورة التزوير في المحررات الورقية المعروف في الأدلة الكتابية الخطية، وإذا كان التزوير يتحد معه في المفهوم الوظيفي، إلا أنه من الناحية التقنية لا يقتصر فقط على معالجة الدعامات الورقية، بل يتطلب ذلك إلماما بتقنية المعلوماتية

ومختلف العناصر المكملة لها وهو الأمر الذي يؤدي إلى انتهاك البيانات الخاصة بالفرد في البيئة المعلوماتية أو الرقمية.

المطلب الثاني: توقيع العقوبات على مرتكبي جريمة التزوير في المحرر الالكتروني

في البداية يجدر القول بأن مختلف المعلومات المخزنة في ذاكرة الحاسوب أو في الأقراص الممغنطة، أو المدرجة المحمولة عليه، أو على دعامة مادية ليست مقرؤءة، على اعتبار أنه لا يمكن قراءة المعلومات المحمولة عليه، وبالتالي فإنها تفتقر لصفة المحرر[35]، وبناء على ذلك يثور الإشكال المتمحور حول المحررات الالكترونية باعتبارها غير مصنفة ضمن المحررات التقليدية، والجدير بالذكر أيضا أن المواد من 214 إلى 222 من قانون العقوبات الجزائري قد نصت على جريمة تزوير المحررات بصفة عامة، بحيث لم ينص المشرع صراحة على تطبيق هذه الأحكام عل جريمة تزوير المحررات الالكترونية[36]؛

وهو الأمر الذي أكده في نص المادة 222 من قانون العقوبات[37]، حيث تنص هذه الأخيرة بأن "من قلد أو زور أو زيف رخصا أو شهادات أو كتابات أو بطاقات أو نشرات أو إيصالات أو جوازات سفر أو أوامر خدمة أو وثائق سفر أو تصاريح مرور أو غيرها من الوثائق سفر أو تصاريح مرور أو غيرها من الوثائق التي تصدرها الإدارات العمومية بغرض إثبات حق أو شخصية أو صفة أو منح إذن، يعاقب بالحبس من 06 أشهر إلي 03 سنوات وبغرامة من 20.000إلى 100.000 دينار جزائري"، وعليه نلاحظ من نص المادة المذكورة آنفا بان المشرع الجزائري لكي نص على تطبيق أحكامها على المحرر الالكتروني وإنما كرس مبدأ المادية البحتة في مفهوم المحرر، حيث اشترط صراحة وجود عنصر الكتابة فى المحرر، غير أن الفقه قد وسع من مفهوم النص المذكور رأى بأنه يمكن استخراج المحرر الالكتروني في شكل مادي ملموس، وبالتالي يمكن تطبيق نصوص قانون العقوبات عليه.

وتجدر الإشارة إلى أن المشرع الجزائري قد تناول المسائل الخاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات واستعمال الإعلام الآلي، في القسم السابع مكرر من قانون العقوبات والذي جاء تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات"، بحيث كيّف النصوص القانونية الواردة في هذا القسم على أنها جنح وقد حصرها في الجرائم التي سيتم التفصيل فيها في الفروع الآتي بيانها:

الفرع الأول: جريمة إدخال المعطيات في منظومة المعالجة الآلية

تعتبر مستخرجات الحاسوب من المحررات أو المستندات المعلوماتية الالكترونية مشمولة بالنص الخاص في قانون العقوبات الجزائري، أما مستخرجات الحاسب الآلي الأخرى

كدعامة والأشرطة الممغنطة اشترط المشرع أن تكون في شكل محرر ذات شكل مكتوب أو عبارات خطية[38]، خاصة وأن المستند الالكتروني هو المفهوم الحديث للمحرر في جريمة التزوير، حيث نلاحظ جليا تجريم فعل كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية، أو أزال معلومة أو غيرها بتعديل".

وهو الأمر الذي أقرته صراحة المادة 394 مكرر 01 من قانون العقوبات؛ حيث نصت على أنه "يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات، وبغرامة من 500.000 إلى 4000.000دج كل من يدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[39].

الفرع الثاني: جريمتي الدخول أو البقاء في المنظومة عن طريق الغش وتصميم أو نشر المعطيات المخزنة أو المعالجة أو المرسلة

لقد نصت على أحكام هذه الجريمة المادة 349 من قانون العقوبات الجزائري[40]، وبناء على الأحكام الواردة فيها فإن عملية الدخول غير المرخص به وعن طريق الغش للمنظومة المعلوماتية وسواء تعلق بالدخول أو البقاء بصفة كلية أو جزئية من المنظومة، ويكفي إثبات المحاولة لتطبيق أحكام المادة، ولا يشترط لقيام هذه الجريمة إلحاق ضرر بالمنظومة المعلوماتية، أما فيما يتعلق بمسألة العقوبات المقررة على ارتكاب هذه الجريمة فإنها تتراوح بين ثلاث أشهر وسنة كاملة حبسا نافذا، وبغرامة تقدر من 50.000 إلى 200.000 دج، والجدير بالذكر أن العقوبة قد يتم مضاعفتها في حالة حذف أو تغيير المعطيات[41].

أما فيما يتعلق بجريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار بمعطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في أحكام المادة 394 مكرر، وكذا حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

وبناء على ذلك فإنه يعاقب كل من قام بتلك الأفعال بالحبس من شهرين إلى ثلاث سنوات، وبغرامة مالية تتراوح من 1000.000 دج إلى 10.000.000 دج كل من يقوم عمدا وبطريق الغش بالأفعال السابقة الذكر، وطبقا لمقتضيات المادة 394 مكرر 05 يعاقب كل مساهم في هذه الجرائم ويستوي في ذلك أن يكون فاعلا أصليا أو شريك، كما يعاقب أيضا وطبقا لنص المادة 394 مكرر 07 على مجرد الشروع في ارتكاب الجريمة السالفة الذكر ويجد ذلك أساسه في مصطلحي "التحضير" و"الأفعال المادية"[42].

الخاتمة:

وفي ختام هذه الدراسة موضوع جريمة التزوير في المحررات الالكترونية كأداة لانتهاك حقوق الإنسان في البيئة الرقمية؛ عن طريق تبيان التأصيل المفاهيمي لجريمة التزوير في المحررات الالكترونية إضافة إلى تبيان خصوصية ارتكاب هذه الجريمة ثم كيفيات ارتكابها باستخدام مختلف الوسائل المادية المتمثلة في اصطناع المحرر أو تزوير التوقيع أو القيام بعميلة الحذف أو الإضافة أو التغيير للحقيقة الواردة فيه، إضافة إلى الوسائل المعنوية والمتمثلة في جعل واقعة مزورة في صورة واقعة صحيحة، وفي الأخير تسليط الضوء على العقوبات الجزائية المقررة على مرتكبي جريمة التزوير، وقد توصلنا بهذا الخصوص إلى جملة من النتائج نوردها فيما يلي:

1- إن جريمة التزوير المرتكبة في المجال التكنولوجي تعتبر من الجرائم والسبب في ذلك يعود للدور الهام والخطير الذي يلعبه الحاسب الآلي في كافة المجالات العلمية والتعليمية والإدارية والصحية..إلخ وغيرها المجالات، حيث أصبح يجرى من خلاله كم هائل من المعطيات ذات الآثار القانونية الهامة والخطيرة والتي لا يصدق عليها وصف المحرر الورقي المكتوب.

2- تتمثل خصوصيات هذه الجريمة في إمكانية ارتكاب جريمة التزوير في أي من مراحل تشغيل النظام، فضلا عن انعدام الأثر المادي لها واعتبارها جريمة لا تتم إلا بعد التخطيط المسبق.

3- تتعدد وسائل ارتكاب جريمة التزوير في المحرر الالكتروني فقد تكون وسائل تزوير مادية لا تتحقق عن طريق اصطناع المحرر أو تزوير التوقيع أو القيام بعميلة الحذف أو الإضافة أو التغيير للحقيقة الواردة في المحرر كما قد تكون هذه الوسائل معنوية تتمثل في جعل واقعة مزورة في صورة واقعة صحيحة فأي تغيير أو تعديل في أي من بيانات يعتبر تزويرا.

4- توقيع المشرع الجزائري لجملة من العقوبات الخاصة على الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات واستعمال الإعلام الآلي، في القسم السابع مكرر من قانون العقوبات والذي جاء تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات.

ومن خلال النتائج المتوصل إليها لابد من اقتراح توصيات علمية وعملية تتمثل في:

1- التفعيل الحقيقي للأحكام الواردة في قانون العقوبات في نظر جريمة التزوير في المحرر الالكتروني من خلال تشديد العقوبات الجزائية على مرتكبي هذه الجرائم.

2- استحداث نصوص قانونية خاصة تتناسب وطبيعة جريمة التزوير في المحرر الالكتروني فضلا عن استحداث أحكام خاصة للتعويض للأفراد ضحايا الانتهاك في البيئة الرقمية.

3- عقد دورات وندوات تكوينية لفائدة المختصين في مجال تكنولوجيا المعلومات والاتصالات للتقليل من حدوث جرائم التزوير وفرض حماية حقيقية وفعلية للبيانات الخاصة بالأفراد في البيئة الرقمية.

الهوامش:

[1] زين الدين وبلال أمين، جرائم نظم المعالجة الآلية للبيانات، ط 1، دار الفكر الجامعي، الإسكندرية 2008، ص 334.

[2] زين الدين وبلال أمين، المرجع والموضع نفسه.

[3] سعد عبد العزيز، جرائم التزوير وخيانة الأمانة واستعمال المزور، ط 1، دار هومة، الجزائر 2005، ص 14.

[4] عباس العبودي، تحديات الإثبات بالسندات الالكترونية ومتطلبات النظام القانوني لتجاوزها، منشورات الحلبي الحقوقية، بيروت 2010، ص 104.

[5] -عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية 2009، ص 140.

[6] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية 2004، ص 63، وانظر أيضا: عمر عبد السلام حسين الجبوري، جريمة التزوير الإلكتروني في التشريع الأردني، مذكرة مقدمة للحصول على شهادة الماجستير، تخصص القانون العام، جامعة الشرق الأوسط، الأردن 2017، ص 31.

[7] عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الإلكترونية، دار الفكر الجامعي، الإسكندرية 2002، ص 306.

[8] عبد الرحمان إبراهيم الحوطي، نطاق تجريم الشهادات والتقارير الطبية في القانون الأردني والكويتي، مذكرة مقدمة للحصول على شهادة الماجستير، تخصص القانون العام، جامعة الشرق الأوسط، الأردن 2012، ص 19.

[9] -علي محمود، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، مداخلة علمية مقدمة ضمن فعاليات المؤتمر العلمي الأول حول: الجوانب القانونية والأمنية للعمليات الالكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، الإمارات العربية المتحدة 2003، ص197.

[10] لمزيد من التفصيل ينظر: نص المادة 11 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الموقع الالكتروني: www.moj.gov.j، تاريخ الاطلاع: 2022/06/22، وقت الاطلاع: 06:13.

[11] لمزيد من التفصيل ينظر: المواد من 214 إلى 229 من الأمر رقم 156/66 المعدل والمتمم المتضمن قانون العقوبات الجزائري.

[12] انظر: نص المادة 23 من القانون رقم 15 لسنة 2004 المتعلق بإصدار اللائحة التنفيذية لقانون التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات المصري، الجريدة الرسمية لجمهورية مصر العربية، العدد 17، المؤرخة في 22 أفريل 2004.

[13] قانون العقوبات الأردني رقم 16 لسنة 1960.

[14] قانون العقوبات العراقي رقم 111 لسنة 1969.

[15] عبد الفتاح بيومي حجازي، التجارة الإلكترونية وحمايتها القانونية، دار الفكر الجامعي، الإسكندرية 2006، ص 165.

[16] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية وأزمة الشرعية الجزائية، مقال منشور في مجلة مركز دراسات الكوفة، العدد 07، جامعة الكوفة، العراق 2008، ص 115.

[17] حنان براهمي، جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة مقدمة للحصول على شهادة الدكتوراه، قسم حقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة- الجزائر، السنة الجامعية 2015، ص 193.

[18] عادل يوسف عبد النبي الشكري، المرجع السابق، ص 117.

[19] عمر عبد السلام الجبوري، المرجع السابق، ص 18.

[20] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة للحصول على شهادة الماجستير، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة- الجزائر، السنة الجامعية 2013، ص 25 وما يليها.

[21] المادة 07 من اتفاقية بودابست: الموقع الالكتروني: https://rm.coe.int/budapest-convention-in-arabic/، تاريخ الاطلاع: 2022/06/20، وقت الاطلاع: 00:29.

[22] انظر: كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت 2003، ص 253.

[23] لمزيد من التفصيل ينظر: المواد من 214 الى 216 من قانون العقوبات.

[24] عباس حفصي، عباس، جرائم التزوير الالكتروني، أطروحة مقدمة للحصول على شهادة الدكتواره، كلية العلوم الإنسانية والعلوم سياسية، جامعة وهران 1- الجزائر، السنة الجامعية 2014، ص 25.

[25] لامية مجدوب، جريمة التزوير في المحررات الرسمية أو العمومية في التشريع الجزائري، دار الفكر الجامعي، الإسكندرية 2014، ص 76.

[26] -أحمد خليفة الملط، الجرائم المعلوماتية، ط 2، دار الفكر الجامعي، الإسكندرية 2006، ص 76.

[27] المادة 214 من قانون العقوبات.

[28] أحمد حسن سعيد خليل، جريمة التزوير في التشريع الفلسطيني، رسالة مقدمة للحصول على شهادة الماجستير، تخصص القانون العام، الجامعة الإسلامية غزة- فلسطين، السنة الجامعية 2015، ص 160.

[29] -المادة 215 من قانون العقوبات.

[30] للمزيد من التفصيل ينظر: المادة 23 من قانون التوقيع الالكتروني الصادر عن جمهورية مصر العربية.

[31] عادل يوسف عبد النبي الشكري، المرجع السابق، ص 115.

[32] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، المرجع السابق، ص 222.

[33] انظر: أحمد حسن سعيد خليل، المرجع السابق، ص 170.

[34] إيهاب فوزي السقا، جريمة التزوير في المحررات الالكترونية، دار الجامعة الجديدة، الإسكندرية 2008، ص 57.

[35] انظر: حمزة بن عقون، السلوك الإجرامي للمجرم لمعلوماتي، أطروحة مقدمة للحصول على شهادة الماجستير في العلوم القانونية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة-الجزائر، السنة الجامعية 2012، ص 278، وانظر أيضا: حسام محمد نبيل الشنراقي، جرائم الاعتداء على التوقيع الالكتروني: دراسة تطبيقية مقارنة، دار الشتات للنشر والتوزيع، مصر 2015، ص 98.

[36] لمزيد من التفصيل ينظر: المواد من 214 إلى 222 من قانون العقوبات.

[37] المادة 222 من قانون العقوبات.

[38] انظر: نهلا عبد القادر المرضي، الجرائم المعلوماتية، ط1، دار الثقافة، عمان 2010، ص 149.

[39] المادة 394 مكرر 01 من قانون العقوبات.

[40] المادة 349 من قانون العقوبات.

[41] راضية لالوش، أمن التوقيع الالكتَّروني، مذكرة مقدمة للحصول على شهادة الماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو- الجزائر، ص 167.

[42] المادة 394 مكرر 05 و07 من قانون العقوبات.

عنوان المقال، **مفهوم جرائم التمييز وخطاب الكراهية في القانون الوطني والدولي**

لقب وإسم المؤلف حافظي سعاد
مؤسسة الانتماء – جامعة أبو بكر بلقايد كلية حقوق وعلوم سياسية
البريد الالكتروني hafdi.souad@yahoo.fr

الملخص:

الملخص ***صدر في العدد الأخير من الجريدة الرسمية، القانون رقم 20-05 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، والذي يتضمن إنشاء المرصد الوطني للوقاية من التمييز وخطاب الكراهية.***

ويحدد القانون المهام الموكلة لهذا المرصد الذي يوضع لدى رئيس الجمهورية، والمتمثلة في اقتراح عناصر الاستراتيجية الوطنية للوقاية من التمييز وخطاب الكراهية، والمساهمة في تنفيذها بالتنسيق مع السلطات العمومية المختصة ومختلف الفاعلين في هذا المجال والمجتمع المدني، إلى جانب الرصد المبكر لأفعال التمييز وخطاب الكراهية وإخطار الجهات المعنية بذلك. هدا وقد صدر في الجزائر قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حيث يجوز مراقبة المعلومات الالكترونية في حالةالمسائل المتعلقة بالارهاب المخالفة للنظام العام وتنشأ هيئة عليا للوقاية من جرائم تكنولوجيا الاعلام والاتصالات وحتى في حالات جرائم خطاب كراهية وتمييز .

وقد صدر مؤخرا المرسوم الرئاسي 19-172 المؤرخ في 3 شوال 1440 الموافق ل6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال

ومكافحتها صدر مرسوم رئاسي 21-439 يتضمن إعادة تنظيم هيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال تتشكل من مجلس التوجية المديرية

الكلمات المفتاحية المرصد الوطني خطاب الكراهية العنصرية التمييز الفضاء الرقمي

Abstract: Law No. 20-05 of April 28, 2020, related to the prevention and combating of discrimination and hate speech, was promulgated in the latest issue of the Official Gazette, which includes the establishment of the National Observatory for the Prevention of Discrimination and Hate Speech.

The law defines the tasks assigned to this observatory, which is placed with the President of the Republic, which is to propose elements of the national strategy for the prevention of discrimination and hate speech, and to contribute to its implementation in coordination with the competent public authorities and various actors in this field and civil society, in addition to early monitoring of acts of discrimination and hate speech and notifying the relevant authorities. concerned with that. In Algeria, Law 09-04 has been issued that includes special rules for the prevention and control of crimes related to information and communication technology, where electronic information may be

monitored in the case of issues related to terrorism that violate public order, and a higher authority is established for the prevention of information and communication technology crimes, even in cases of hate speech and discrimination crimes.

Presidential Decree 19-172 of Shawwal 3, 1440 corresponding to June 6, 2019 was recently issued specifying the composition of the National Authority for the Prevention and Control of Crimes Related to Information and Communication Technologies. directorate direction

Keywords National Observatory, hate speech, racism, discrimination, digital space

مقدمة

الكراهية مصطلح حقوقي[1] فضفاض[1] يمكن أن يُعرف بكونه أي "عبارات تؤيد التحريض على الضرر (خاصة التمييز أو العدوانية أو العنف (حسب الهدف الذي تم استهدافه وسط مجموعة اجتماعية أو] سُكانية"[1] وتكون هذه المجموعات عادة من الضعفاء والأقليات.[2] ويندرج خطاب الكراهية في مركبات" حرية التعبير وحقوق الأفراد والجماعات والأقليات ومبادئ الكرامة والحرية والمساواة."[1] ويأتي مصطلح خطاب الكراهية لأن العالم، بقوانينه الدولية والمحلية، يفرق بين حق الرأي وحق التعبير عن الرأي، فإن العالم لا يضع أي قيد على حق الرأي و يجعله مطلقاً ولكنه يضع قيوداً وضوابط على التعبير عن هذا الرأي[3] فهناك قيود منها احترام حقوق الآخرين وحماية الأمن القومي.[4] لذا، ينبع مسوغ قوانين خطاب الكراهية بكون الخطاب المفعم بالكراهية يتعارض وقيم التسامح والعيش المشترك التي تحتاجها الجماعات البشرية.[5]

تعمل القوانين الحديثة على ضمان حماية المساواة بين الناس وتحظر خطاب الكراهية[6]، وتذكر الفقرة 2 من المادة 20 من العهد الدولي الخاص بالحقوق المدنية والسياسية ما يلي:

"تُحظر بالقانون أية دعوة إلى الكراهية القومية أو العنصرية أو الدينية تُشكل تحريضاً على التمييز أو العداوة أو العنف" [7]

تشمل هذه القوانين منع استخدام عبارات الإهانة، أو الألقاب، لتعيين أفراد من المجتمع بناءاً على عرقهم أو دينهم أو توجههم الجنسي.[8] وتزداد أهمية قوانين مكافحة خطاب الكراهية في المجتمعات الحديثة المتعددة الثقافات.[9] ويبدو بأن الإنترنت صارت مرتعاً واسعاً لخطاب الكراهية لعدد من الأسباب[10] منها ما توفره الشبكة من إمكانية لنشر خطاب الكراهية باسم مستعار، أو مجهول أحياناً.[1]

هذا، وتتباين التعريفات القانونية عبر الدول[11]، وأحياناً تتعارض التعريفات مع مبادئ حرية التعبير والمساواة[12]، وأن "المعايير التطبيقية [لقوانين مكافحة خطاب الكراهية] تكون متضاربة، ... ويستحيل توافقها مع مبادئ اليقينية القانونية المطلوب وجودها بالأحكام القانونية، وأن هذه المعايير عرضة لإساءة الاستخدام مما يجعلها تقوض حريات التعبير ذات الأهمية الكبرى، وخصوصاً الخطاب السياسي."[13] بالإضافة إلى ذلك، فإن "قوانين مواجهة

خطاب الكراهية ومكافحة 'الإساءة' هي أدوات بيد هؤلاء الذين سيقيدون الحريات الدينية لأقصى حد."[13]

بينما تستغل بعض الدول والجماعات هذا المفهوم، الفضفاض لتمرير قوانين تحد من الحريات العامة[14]، كالدينية.[13] ولأن أصول قوانين مكافحة خطاب الكراهية "ينبع من أنظمة شمولية هدفت إلى "تقييد الديموقراطيات"[15]، تصبح هناك قوانين خفارة (بوليسية) على اللغة يشبهها البعض بلغة نيوسبيك برواية جورج أورويل.[16] بالإضافة إلى ذلك، "يمكن للقيود المتعلقة بمنع خطاب الكراهية أن تقوض شرعية قوانين مكافحة التمييز، سواءاً على مستوى القبول الشعبي أو - ولربما هذا الأكثر أهمية - فيما يتعلق بأخلاقيات تنفيذها."[17] فهي أداة قانونية قوية قد تدمج مع عقيدة رقابية التي هي "أسوأ العقائد الأيديولوجية"[18]

في بعض البلدان، قد يكون التعريف الفضفاض مدخلاً للإساءة لحرية التعبير[19] ومنعها تجاه رموز الدول[20][14] أو ما يعتبره المشرع عنصراً من عناصر الوطن. مثلاً، يمكن أن يسوغ قانون العقوبات بتعريفٍ فضفاضٍ لخطاب الكراهية بوضع التعبير عن الرأي جريمة[14] يسميها بجريمة إطالة اللسان، في الأردن مثلاً، حين يقوم أحدهم بشتم الحاكم رمز من رموز الدولة أو الدين. وحتى في الدول الديموقراطية، فأن قوانين عقوبة خطاب الكراهية قد تضع بعض الجماعات فوق النقد، مثلاً قوانين معاداة السامية تستخدم أحياناً لقمع نقد إسرائيل[21] والحركة الصهيونية[22] أو ممارسات جيش الاحتلال ضد الفلسطينين.[24][23] وكذلك، يوجه البعض[25] النقد للجماعات اليسارية الغربية، كالنسوية[26]، التي تتقدم المطالبين بهكذا قوانين[27] ورقابتها على لغة مواقع التواصل الاجتماعي واستخدامها لمفهوم خطاب الكراهية لنعت كل ما لا يعجبها، يكون بعضه، أي الخطاب، جزءاً أساسياً من حرية التعبير القانونية فتمنع الرقابة الحوار الاجتماعي البناء[28] مما يؤدي إلى ديكتاتورية لغوية اجتماعية لا ديموقراطية.[29] بمعنى آخر، تظهر مشاكل تطبيق مفهوم خطاب الكراهية بشكل قانون نتيجة لتباينات بالقيم والأخلاقيات بنفس الدول أو المجتمع[30]، أي الاختلاف فيما يعرفه الناس بكونه مناسب وغير مناسب.[31]

المبحث الأول خطاب الكراهية وفضاء رقمي

بتاريخ 31مايو2016 ، وافقت شركات فيسبوك وجوجل ومايكروسوفت وتويتر على مدونة ضبط السلوك التابعة للاتحاد الأوروبي[32]، وقدمت هذه الشركات تعاريفها الخاصة بما يشكل خطاباً مفعماً بالكراهية لمتنع أشكاله على منصاتها.[33] مثلاً يشمل خطاب الكراهية حسب فيسبوك:

لا يُسمح بالمحتوى الذي يهاجم الأشخاص على أساس عرقهم الفعلي أو المتصور أو السلالة أو الأصل القومي أو الديانة أو الجنس أو النوع أو الهوية الجنسية أو التوجه الجنسي أو الإعاقة أو المرض. ولكننا في الوقت ذاته نسمح بالتعبيرات التي تُنشر على سبيل الدعابة أو السخرية والتي قد يعتبرها البعض تهديدًا أو هجومًا. ويتضمن هذه المحتوى الذي قد يعتبره العديد من الأشخاص مفتقدًا إلى الذوق (مثال: النكات أو الأعمال الكوميدية القصيرة أو كلمات الأغاني الشعبية، وما إلى ذلك).[34]

ويتضح التناقض في تعريف فيسبوك سريعاً، فما هو معيار التعبيرات الساخرة من التعبيرات الجدية أو المستترة؟[1]، وهذا بالطبع يعتمد على النوايا، والنوايا جوانب من غير ممكن الوصول إليها بسهولة كما يتضح من الدراسات اللغوية في تحليل الخطاب. فالدراسات بنظرية التهذيب تخبرنا بأن المتحدثين لا يرتدون نواياهم[35]، أي لا يمكن للشخص المقابل، المتلقي، معرفة النوايا من النظر، سواءاً إلى المتكلم أو إلى كتاباته[35]، على الفيسبوك مثلاً.

ولكون الفيسبوك مرآة للتواصل البشري المباشر، فلقد سجلت بسنة 2012 جريمة بكل 40 دقيقة مرتبطة بالموقع، يتعلق الكثير منها بما يمكن وصفه بخطاب الكراهية.[36] هذا، وغيره من وسائل الجدال، يستخدمها البعض لرفض مفهوم" المساحة الآمنة "التي يرغب الفيسبوك، وبعض التيارات الفكرية اليسارية مثلاً، بتوفيرها وحمايتها. والفيسبوك، كغيره من مواقع التواصل الاجتماعي، موقع خصب للتنمر والهجوم اللفظي[37] الذي يقع، حسب التعريف، ضمن خطاب الكراهية.

المطلب الأول قوانين خطاب الكراهية]

ينص العهد الدولي الخاص بالحقوق المدنية والسياسية" :تُحظر بالقانون أية دعوة إلى الكراهية القومية أو العنصرية أو الدينية تشكل تحريضاً على التمييز أو العداوة أو العنف."[38] ووفقاً للاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري فيعتبر "كل نشر للأفكار القائمة على التفوق العنصري أو الكراهية العنصرية، وكل تحريض

على التمييز العنصري وكل عمل من أعمال العنف أو تحريض على هذه الأعمال يُرتكب ضد أي عرق أو أية جماعة من لون أو أصل أثني آخر، وكذلك كل مساعدة للنشاطات العنصرية، بما في ذلك تمويلها، جريمة يعاقب عليها القانون".[39] قامت المفوضية السامية للأمم المتحدة لشؤون اللاجئين بتمويل مؤتمرات لنقاش مدى انطباق حرية التعبير على فضاء الإنترنت.[40]

التطبيق

يمكن تقسيم تشريعات وأنظمة خطاب الكراهية إلى نوعين: الأول وضِع بهدف حفظ النظام العام، أما النوع الثاني فوضع لأجل حماية الكرامة الإنسانية. تطلب تشريعات النوع الأول الموضوعة لحماية النظام العام في كثير من البلدان حدوداً أعلى في حال انتهاكها، لذلك لا يتم تطبيقها بصورة محددة في أكثر الحالات. فمثلاً لم يُحاكم في أيرلندا الشمالية بحلول عام 1992 سوى شخص واحد بتهمة خرق تشريع من هذا القبيل. أما قوانين النوع الثاني الموضوعة لحماية الكرامة الإنسانية فحدود تطبيقها أدنى بكثير من قوانين النوع الأول، فعادةً ما يجري تطبيقها بكثرة في ألمانيا والدنمارك وكندا وفرنسا وكندا وهولندا.[41]

يتداخل تطبيق القوانين المتعلقة بخطاب الكراهية في الولايات المتحدة مع حق حرية التعبير الذي يضمنه دستور البلاد تبعاً لما جاء في التعديل الأول .غالباً ما يجب إعادة فحص قرارات المحكمة للتحقق من عدم إخلال الحكم الصادر بالدستور الأمريكي.[42]

قوانين خطاب الكراهية حسب البلد]

أستراليا

تختلف قوانين خطاب الكراهية في أستراليا تبعاً للاختصاص القضائي، وتسعى بصورة خاصة إلى منع خلق الضحية بناءً على العرق.

ألمانيا]

يعد "التحريض على الكراهية) "بالألمانية (Volksverhetzung :جريمة يعاقب عليها القانون في ألمانيا تبعاً لما جاء في الفقرة 130 من القانون الجنائي الألماني، وقد تبلغ عقوبتها السجن لما يصل إلى 5 سنوات.[43] تُجرم الفقرة 130 التحريض العلني على الكراهية ضد فئات سكانية أو الدعوة للعنف أو الدعوة للتدابير التعسفية ضدهم أو إهانتهم أو توجيه الطعن أو الذم العدائي بطريقة تنتهك كرامتهم الإنسانية (المحمية دستورياً). وعليه مثلاً من غير القانوني

إطلاق تسميات مثل "الطفيليين النفعيين" على مجموعات إثنية ما بصورة علنية.[44] تُعاقب ألمانيا مرتكبي جريمة "التحريض على الكراهية" في البلاد حتى إن لم يكونوا ألماناً أو كانوا في الخارج، وذلك شريطة وقوع تأثير التحريض ضمن الأراضي الألمانية بموجب ما يحدده "مبدأ كلية الوجود" الوارد في القانون الجنائي.[45]

أقرت ألمانيا بتاريخ 30 يونيو 2017 قانوناً يُجرم خطاب الكراهية على مواقع التواصل الاجتماعي. ينص القانون على تغريم مواقع التواصل الاجتماعي بمبلغ مالي قد يصل إلى 50 مليون يورو في حال الفشل المستمر لموقع ما من إزالة المحتوى غير القانوني في غضون أسبوع واحد.[46]

بلجيكا]

القانون البلجيكي لمكافحة العنصرية هو قانون ضد خطاب الكراهية والتمييز أقره البرلمان الاتحادي في بلجيكا عام 1981، مما جعل من غير القانوني القيام بأعمال معينة تُرتكب بدوافع العنصرية أو رهاب الأجانب.[47]

يحظر قانون إنكار الهولوكوست البلجيكي الصادر بتاريخ 23 مارس عام 1995، إنكار الهولوكوست علانيةً. ويحظر القانون بوجه خاص "إنكار أو التقليل من أهمية أو تبرير أو الموافقة على الإبادة الجماعية المرتكبة من قبل نظام ألمانيا النازية خلال الحرب العالمية الثانية ."قد تصل العقوبة إلى السجن عاماً واحداً مع دفع غرامة تصل إلى 2,500 يورو.[48]

البرازيل]

ينص الدستور البرازيلي على أن "ممارسة العنصرية لا يفرج عن مرتكبها بكفالة ولا تسقط بالتقادم وتعاقب بالسجن بموجب أحكام القانون."

كند]

في كندا، يعتبر الدفاع عن الإبادة الجماعية ضد أي "مجموعة يمكن تحديدها" جريمة مدانة بموجب القانون الجنائي ويتسبّب بعقوبة أقصاها السجن لمدة خمس سنوات، ولا يوجد حدّ أدنى للحكم .

التحريض علناً على الكراهيّة ضدّ أي مجموعة قابلة للتعيين هو أيضاً جريمة. ويمكن مقاضاتها إما كجريمة اتّهاميّة يمكن الحكم عليها بعقوبة أقصاها السجن لمدة سنتين، أو

كإدانةٍ بإجراءاتٍ جزائيّة مع حكم بالسجن لمدة ستّة أشهر كحدٍّ أقصى، ولا يوجد حدّ أدنى للحكم في كلتا الحالتين.[52] هناك بعض الاستثناءات حول "جريمة التحريض العلني على الكراهيّة" في حال كانت التصريحات حقيقيّة أو متعلّقة بموضوعات النقاش العامّ والعقيدة الدينيّة. وكان القرار القضائي البارز بشأن دستوريّة هذا القانون هو R v Keegstra الصادر عام 1990).

يتم تعريف "المجموعة القابلة للتعيين" في كلّ جرائم "خطاب الكراهية" على أنّها أيّ جزءٍ من الشعب يتميّز بلون بشرة معين أو أصل قومي أو عرقي أو عمر أو جنس أو ميول جنسية أو هوية جندرية أو تعبير جنسي أو بأيّ عجزٍ عقليّ أو جسديّ.

تشيلي[]

يعاقَب بغرامة كبيرة -حسب المادة 31 من قانون "Ley sobre Libertades de Opinión e Información y Ejercicio del Periodismo"(قانون حرّيّة الرأي والمعلومات وأداء الصحافة)- أولئك الذين يستخدمون أي وسيلة من وسائل التواصل الاجتماعي لنشر منشورات أو إرسال رسائل تهدف إلى التشجيع على الكراهية أو العداء تجاه شخص أو مجموعة من الأشخاص بسبب عرقهم أو دينهم أو جنسهم أو جنسيّتهم وقد تمّ تطبيق هذا القانون على المصطلحات المرسلة عبر الإنترنت. وهناك أيضًا قانون بزيادة العقوبات على الجرائم التي حدثت بدافع الكراهية التمييزية.

كرواتيا[]

يضمن الدستور الكرواتيّ حرّيّة التعبير، لكن وبالمقابل يحظر قانون العقوبات في البلاد التمييز، ويُعاقِب أيّ شخص يقوم بانتهاك حقوق الإنسان والحريات الأساسية التي يعترف بها المجتمع الدولي على أساس اختلاف العرق، الدين، اللغة، المعتقد، السياسي أو أي معتقدٍ آخر، أو على أساس الثروة، أو الولادة أو مستوى التعليم أو المركز الاجتماعي أو الممتلكات المادّيّة أو الجنس أو لون البشرة أو القومية أو الانتماء العرقي

الدنمارك[]

تحظر الدنمارك الخطاب الذي يحضّ على الكراهية، وتُعرّفه بأنّه تصريحات علنيّة تتعرّض مجموعةٌ ما من خلالها للتهديد (trues) أو الإهانة (trues) أو التقليل من الشأن

(nedværdiges)وذلك بناءاً على العرق أو لون البشرة أو الأصل العرقي أو القومي أو العقيدة أو الميول الجنسيّة.

أوروبا[]

قام مجلس أوروبا (Council of Europe) بدعم حركة "لا لخطاب الكراهية" التي تعمل بنشاطٍ على زيادة الوعي تجاه خطاب الكراهية من أجل المساعدة في مكافحة هذه المشكلة. في حين أنّ المادة العاشرة من الاتفاقية الأوروبية لحقوق الإنسان لا تحظر القوانين الجنائيّة ضدّ المراجعات التاريخيّة كنكران أو تقليل من شأن الإبادات الجماعيّة أو الجرائم ضدّ الإنسانيّة، كما تفسّرها المحكمة الأوروبية لحقوق الإنسان(ECtHR) ، فقد ذهبت لجنة وزراء مجلس أوروبا أبعد من ذلك وأوصت في عام 1997 بأن تقوم الحكومات الأعضاء في المجلس بـ"اتّخاذ الخطوات المناسبة لمكافحة خطاب الكراهية" بموجب توصيتها .R (97) 20 لا تقدم المحكمة الأوروبية لحقوق الإنسان تعريفاً مقبولاً لـ"خطاب الكراهية"، ولكنّها تقدّم فقط مُحدّداتِ يمكن من خلالها للنائب العام أن يقرّر إمكانية اعتبار "خطاب الكراهية" حرّيّة تعبير.

وقد نتج عن البرامج التعليمية في المدارس -التي حثّت على الإبلاغ عن حوادث خطابات الكراهية- وعيٌ متزايد حول هذا الموضوع. كما أنشأ مجلسُ أوروبا المفوضيةَ الأوروبية لمناهضة العنصريّة والتعصّب وهي التي تصدر تقارير خاصّة بكلّ بلد، وتصدر أيضاً عدّة توصياتٍ حول السياسات العامّة في البلدان الأوروبيّة، على سبيل المثال معاداة الساميّة والتعصّب ضدّ المسلمين

فنلندا

]

كان هناك جدل كبير حول تعريف "خطاب الكراهية (vihapuhe)" في اللغة الفنلندية .

في حال كان يقصد بـ"خطاب الكراهية" التحريضَ العرقي، فإنّه محظور في فنلندا وتم تعريفه - في المادة 11 من قانون العقوبات، وجرائم الحرب والجرائم ضد الإنسانية- على أنّه أيّ نشرٍ للمعلومات أو نشر لرأي أو بيان يهدّد أو يهين مجموعة ما، بناءً على عرقها أو جنسيتها أو أصلها القومي أو دينها أو قناعاتها أو توجّهها الجنسيّ أو بناءً على عجز جسديّ يميّزها أو أي سمة مماثلة. يُعاقب مرتكب جريمة التحريض العرقي في فنلندا بغرامة ماليّة أو بالسجن لمدّة تصل

إلى سنتين، أو من 4 أشهر إلى 4 سنوات إذا زادت خطورة ما يدعي إليه (كالتحريض على الإبادة الجماعية) .

يزعم بعض المنتقدون أنّه يمكن أن يستخدمَ إطلاقُ صفة "خطاب كراهية" على بعض الآراء والتصريحات –في السياقات السياسية- لإسكات الآراء غير الملائمة أو الحرجة ولقمع النقاشات. بعض السياسيّين الفنلنديّين، بما فيهم عضو البرلمان وزعيم الحزب الفنلنديّ Finns Partyجوسي هالا آهو Jussi Halla-aho ، يعتبرون مصطلح "خطاب الكراهية" مصطلحاً إشكاليّا بسبب الاختلافات حول تعريفه.

فرنسا

يحظر قانونُ العقوبات الفرنسيّ وقوانينُ الصحافةِ، الاتّصالاتِ العامّةَ والخاّصةَ التي تنطوي على تشهيرٍ أو إهانة، أو تحرّض على التمييز أو الكراهية أو العنف ضدّ شخصٍ أو جماعة ما بسبب مكان المنشأ أو العرق أو عدم معرفتهما، أو الجنسية أو العرق أو الدين الخاصّ، أو الجنس أو التوجه الجنسيّ أو العجز الجسديّ. يحظر القانون الفرنسي أيضاُ الإعلانات التي تبرّر أو تنكرُ الجرائمَ ضدّ الإنسانيّة - على سبيل المثال، الهولوكوست (قانون غايسوت) .

ألماني

في ألمانيا، يُعدّ التحريض على الكراهية أو بالألمانيّة "Volksverhetzung" جريمةً يُعاقب عليها بموجب المادة 130 من القانون الجنائي الألماني (Strafgesetzbuch) ويمكن أن يؤدّي إلى السجن لمدّة تصل إلى خمس سنوات.[1] فالقسم 130 يُجرِّمُ التحريضَ علناً على الكراهية ضد مجموعاتٍ معيّنة من السكّان، أو الدّعوة إلى اتّخاذ تدابير عنيفة أو تعسّفيّة بحقّهم أو إهانتهم أو الافتراء عليهم أو تشويه سمعتهم بطريقة تنتهك كرامتهم الإنسانية (المحميّة دستورياً)، فعلى سبيل المثال، من غير القانوني أن نطلق علنًا على بعض الجماعات العرقية ألقاب "اليرقات" أو "المستعبِدين." يُعاقب مرتكب جرم التحريض على الكراهية في ألمانيا حتّى إذا ارتكب جرمه خارج البلاد وحتّى إذا ارتكبه مواطنون غير ألمان، في حال حدث التحريض داخل الأراضي الالمانيّة، فعلى سبيل المثال، تمّ التعبير عن المشاعر التحريضية في الكتابة أو الخطاب الألماني وجعلها نافذة في ألمانيا) مبدأ "الوجود في كلّ مكان Principle of Ubiquity "في القانون الجنائي الألماني، القسم 9 § 1 والقسم 3 والقسم 4.(

في 30 حزيران 2017، وافقت ألمانيا على مشروع قانون يجرّم خطاب الكراهية على مواقع التواصل الاجتماعي. ينصّ القانون على أنّه قد يتم تغريم مواقع التواصل الاجتماعي بما يصل إلى 50 مليون يورو (56 مليون دولار أمريكي) إذا أخفقوا في إزالة محتوى غير قانوني في غضون أسبوع، بما في ذلك "الأخبار المزيفة" التشهيريّة .

الولايات المتحدة الأمريكية[

لا تمتلك الولايات المتحدة الأمريكية قوانين لخطاب الكراهية، ويعود ذلك إلى أن المحاكم الأمريكية قضت مراراً وتكراراً بأن القوانين التي تجرم خطاب الكراهية تنتهك بذلك ضمان حرية التعبير الواردة في التعديل الأول للدستور الأمريكي.[ ] على الرغم من ذلك، هناك عدة فئات من الخطابات غير خاضعة لحماية التعديل الدستوري الأول، مثل الخطاب الذي يدعوا إلى حدوث عنف وشيك على شخص أو مجموعة. ومع ذلك، قضت محكمة الولايات المتحدة العليا بأن خطاب الكراهية لا يندرج تحت هذه الفئات .

زعم أنصار تشريع خطاب الكراهية في الولايات المتحدة بأن حرية التعبير تضعف من التعديل الرابع عشر للدستور الأمريكي وذلك من خلال دعم الخطاب القمعي والذي بدوره يحط من المساواة ومن هدف التعديل في الأصل، والذي هو ضمان حماية متساوية بموجب القانون.[68]

الهند[]

تتمتع حرية الخطاب والتعبير بالحماية بموجب المادة 19 (1) من دستور الهند، ولكن بموجب المادة 19 (2) يمكن فرض "قيود منطقية" على حرية الخطاب والتعبير لصالح "سيادة الهند وسلامتها أو أمن الدولة أو العلاقات الودية مع الدول الأجنبية أو النظام العام أو الآداب أو الأخلاق، أو فيما يتعلق بازدراء المحكمة أو التشهير أو التحريض على جريمة." [69]

نيوزيلندا[]

تحظر نيوزيلندا خطاب الكراهية بموجب قانون حقوق الإنسان لعام 1993. المادة 61 (التنافر العنصري) تجعل من غير القانوني نشر أو توزيع "تهديد أو مسيء أو مهين ... مسألة أو كلمات من المرجح أن تثير العداء ضد أي مجموعة من الأشخاص.

على أساس اللون أو العرق أو الأصول الإثنية أو القومية لتلك المجموعة من الأشخاص ".
تنص المادة 131 (التحريض على التنافر العنصري) على الجرائم التي يخلق "التنافر العنصري" المسؤولية الناتجة عنها

صدر في العدد الأخير من الجريدة الرسمية، القانون رقم 20-05 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، والذي يتضمن إنشاء المرصد الوطني للوقاية من التمييز وخطاب الكراهية.

ويحدد القانون المهام الموكلة لهذا المرصد الذي يوضع لدى رئيس الجمهورية، والمتمثلة في اقتراح عناصر الاستراتيجية الوطنية للوقاية من التمييز وخطاب الكراهية، والمساهمة في تنفيذها بالتنسيق مع السلطات العمومية المختصة ومختلف الفاعلين في هذا المجال والمجتمع المدني، إلى جانب الرصد المبكر لأفعال التمييز وخطاب الكراهية وإخطار الجهات المعنية بذلك.

كما يتولى المرصد تبليغ الجهات القضائية المختصة عن الأفعال التي تصل إلى علمه والتي يحتمل أنها تشكل جريمة من الجرائم المنصوص عليها في هذا القانون، ويتولى أيضا تقديم الآراء أو التوصيات حول أي مسألة تتعلق بالتمييز وخطاب الكراهية.

وتقوم ذات الهيئة بالتقييم الدوري للأدوات القانونية والإجراءات الإدارية في مجال الوقاية من التمييز وخطاب الكراهية ومدى فعاليتها، مع تحديد مقاييس وطرق الوقاية من التمييز وخطاب الكراهية، وتطوير الخبرة الوطنية في هذا الميدان.

ويتكفل المرصد بوضع البرامج التحسيسية وتنشيط وتنسيق عمليات التوعية بمخاطر التمييز وخطاب الكراهية وآثارهما على المجتمع، وجمع ومركزة المعطيات المتعلقة بالتمييز وخطاب الكراهية، بالإضافة إلى إنجاز الدراسات والبحوث في مجال الوقاية من التمييز وخطاب الكراهية، ويقدم أي اقتراح من شأنه تبسيط وتحسين المنظومة القانونية الوطنية للوقاية من التمييز وخطاب الكراهية.

ويحرص أيضا على تطوير التعاون وتبادل المعلومات مع مختلف المؤسسات الوطنية والأجنبية العاملة في هذا المجال، ويمكن له أن يطلب من أي إدارة أو مؤسسة أو هيئة أو مصلحة كل معلومة أو وثيقة ضرورية لإنجاز مهامه، عليها الرد على مراسلاته في أجل أقصاه 30 يوما.

وحسب المادة 11 من ذات القانون، فإن المرصد الوطني يتشكل من ستة أعضاء من بين الكفاءات الوطنية، يختارهم رئيس الجمهورية ويتم تعيينهم بموجب مرسوم رئاسي لعهدة مدتها 5 سنوات قابلة للتجديد مرة واحدة، ويمثل هؤلاء الأعضاء كل من المجلس الأعلى للغة العربية، المحافظة السامية للأمازيغية، المجلس الوطني لحقوق الإنسان، الهيئة الوطنية لحماية وترقية الطفولة، المجلس الوطني للأشخاص المعوقين وسلطة ضبط السمعي البصري، بالإضافة إلى أربعة ممثلين للجمعيات الناشطة في مجال تدخل المرصد يتم اقتراحهم من الجمعيات التي ينتمون إليها.

وينتخب الأعضاء فورتنصيبهم، رئيس المرصد الذي تتنافى عهدته مع ممارسة أي عهدة انتخابية أووظيفة أوأي نشاط مهني آخر.

وحسب المادة 14 من القانون، فإن المرصد يرفع إلى رئيس الجمهورية تقريرا سنويا يضمنه لا سيما تقييم تنفيذ الاستراتيجية الوطنية للوقاية من التمييز وخطاب الكراهية واقتراحاته وتوصياته لتعزيز وترقية الآليات الوطنية المعمول بها في هذا المجال، ويتولى نشره وإطلاع الرأي العام على محتواه وفقا للكيفيات المحددة في نظامه الداخلي.

من المفترض أن أية اتفاقية دولية من اتفاقية دولية من اتفاقيات حقوق الانسان تتضمن بندا خاصا بالمساواة وعدم التمييز دلك ان المساواة وعدم التمييز وهي من المبادئ الاساسية للقانون الدولي لحقوق الانسان عموما ، والمتمتع بسائر الحقوق المحمية خاصة وهو بمثابة حق عاغم يتفرع عنه العديد من حقوق الانسان الاخرى وهو نقطة اليه أية أو الانطلاق لكافة الحقوق والحريات الاخرى[1].

ورد مبدأ المساواة صراحة في ميثاق الأمم المتحدة في مواضيع عديدة وفي الاعلان العالمي لحقوق الانسان في مقدمته والمادة الأولى منه كما أقر الاعلان بعض مظاهر أو تطبيقات المبدأ العام للمساواة مثل المساواة في الاشتراك في ادارة الشؤون العامة للدولة ، وفي تقلد الوظائف العامة وفي حق التصويت المادة 21 وتضيق المادة 7 منه النص على أن الناس جميعا سواء امام القانون وهو متساوون في حق التمتع بحماية القانون دونما تمييز كما يتساوون في حق التمتع بالحماية من أي تمييز ينتقد هذا الاعلان ومن أي تحريض على مثل هذا التمييز وقد تضمنت الاتفاقية الدولية العامة

1انظر ، الطاهر بن خرف الله ، مدخل الى الحريات وحقوق الانسان ،ج.2 ، التعبير الدستوري للحريات والحقوق ، طاكسيج كوم ، للدراسات والنشر والتوزيع ، 2009 ؛

لحقوق الانسان نصوصا متفرقة تتناول المبدأ العام وتطبيقاته في مجال الحقوق المحمية وهي نصوص تثير جملة من الأسئلة حول مفهوم التمييز وعدم المساواة وحدود المبدأ ومتى يكون التمييز جائزا ومتى يكون محظورا ؟ وماهي صور التمييز المحظور ؟وعلى هذا الأساس سأتناول هذا المطلب من خلال : مبدأ تحريم التمييز في الصكوك الدولية لحقوق الانسان

صدر في العدد الأخير من الجريدة الرسمية، القانون رقم 20-05 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، والذي يتضمن إنشاء المرصد الوطني للوقاية من التمييز وخطاب الكراهية.

ويحدد القانون المهام الموكلة لهذا المرصد الذي يوضع لدى رئيس الجمهورية، والمتمثلة في اقتراح عناصر الاستراتيجية الوطنية للوقاية من التمييز وخطاب الكراهية، والمساهمة في تنفيذها بالتنسيق مع السلطات العمومية المختصة ومختلف الفاعلين في هذا المجال والمجتمع المدني، إلى جانب الرصد المبكر لأفعال التمييز وخطاب الكراهية وإخطار الجهات المعنية بذلك.

كما يتولى المرصد تبليغ الجهات القضائية المختصة عن الأفعال التي تصل إلى علمه والتي يحتمل أنها تشكل جريمة من الجرائم المنصوص عليها في هذا القانون، ويتولى أيضا تقديم الآراء أو التوصيات حول أي مسألة تتعلق بالتمييز وخطاب الكراهية.

وتقوم ذات الهيئة بالتقييم الدوري للأدوات القانونية والإجراءات الإدارية في مجال الوقاية من التمييز وخطاب الكراهية ومدى فعاليتها، مع تحديد مقاييس وطرق الوقاية من التمييز وخطاب الكراهية، وتطوير الخبرة الوطنية في هذا الميدان.

ويتكفل المرصد بوضع البرامج التحسيسية وتنشيط وتنسيق عمليات التوعية بمخاطر التمييز وخطاب الكراهية وآثارهما على المجتمع، وجمع ومركزة المعطيات المتعلقة بالتمييز وخطاب الكراهية، بالإضافة إلى إنجاز الدراسات والبحوث في مجال الوقاية من التمييز وخطاب الكراهية، ويقدم أي اقتراح من شأنه تبسيط وتحسين المنظومة القانونية الوطنية للوقاية من التمييز وخطاب الكراهية.

ويحرص أيضا على تطوير التعاون وتبادل المعلومات مع مختلف المؤسسات الوطنية والأجنبية العاملة في هذا المجال، ويمكن له أن يطلب من أي إدارة أو مؤسسة أو هيئة أو مصلحة كل معلومة أو وثيقة ضرورية لإنجاز مهامه، عليها الرد على مراسلاته في أجل أقصاه 30 يوما.

وحسب المادة 11 من ذات القانون، فإن المرصد الوطني يتشكل من ستة أعضاء من بين الكفاءات الوطنية، يختارهم رئيس الجمهورية ويتم تعيينهم بموجب مرسوم رئاسي لعهدة مدتها 5 سنوات قابلة للتجديد مرة واحدة، ويمثل هؤلاء الأعضاء كل من المجلس الأعلى للغة العربية، المحافظة السامية للأمازيغية، المجلس الوطني لحقوق الإنسان، الهيئة الوطنية لحماية وترقية الطفولة، المجلس الوطني للأشخاص المعوقين وسلطة ضبط السمعي البصري

، بالإضافة إلى أربعة ممثلين للجمعيات الناشطة في مجال تدخل المرصد يتم اقتراحهم من الجمعيات التي ينتمون إليها.

المبحث الثاني الاجراءات التشريعية للوقاية من جر ائم المعلوماتية خطاب كراهية وتمييز في فضاء رقمي كنموذج

هدا وقد صدر في الجزائر قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حيث يجوز مراقبة المعلومات الالكترونية في حالةالمسائل المتعلقة بالارهاب المخالفة للنظام العام وتنشأ هيئة عليا للوقاية من جرائم تكنولوجيا الاعلام والاتصال [2]

ويهدف القاون 09-04 الى حماية أنظمة المعالجة الية للمعطيات وحمايتها من الجرائم كماله مجال في التحقيق فمع مراعاة لسرية الاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزماته التحريات أو التحقيقات مراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها والقيام باجراء التفتيش أو الحجز داخل أنظمة المعلومات كما يمكن مراقبة الاتصالات الالكترونية في اعمال ارهابية لمقتضيات تمس أمن الدولة ومؤسساتها والدفاع الوطني وكدلك لمقتضيات التحقيق في قضية بحيث يصعب الوصول الى نتيجة دون اللجوء الى المراقبة الالكترونية يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية ادنا لمدة 6 أشهر قابلة للتمديد ودلك على أساس تقرر يبين طبيعة الترتيبات التقنية المستعملة اضافة الى قواعد خاصة بعملية التفتيش

أنظر القانون 09-04 المؤرخ فيي 14 شعبان 1430 الموافق ل5 غشت2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها جر العدد47 [2]

وطلب مساعدة دولة أجنبية من أجل تفتيش منطومة معلوماتية موجودة بالخارج تطبيقا لمبدأ المعاملة بالمثل . وكدلك حجز معطيات وبيانات ومنع الوصول الى المعطيات محتوى الجرم وحفظ المعطيات المتعلقة بحركة السير حسب المادة 10 من القانون 09-04 اضافة الى التزامات مقدم الخدمة بالتعاون مع السلطات القضائية ويعاقب الشخص الطبيعي من من 6 أشهر الى 5 سنوات وبغرامة من 50.000دج الى 500.000دج اضافة الى التزامات مقدمي خدمة الأنترنت بمنع الوصول الى بيانات المخالفة للنظام العام والتي تشكل جرما عن طريق سحب محتوياتها وضع ترتيبات تقنية بمنع الوصول اليها حسب المادة 12 من القانون 09-04 كما تنشئ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحنه حيث تتولى التنسيق وتنشيط عمليات الوقاية من جرائم الاعلام ومساعدة السلطات القضائية ومضالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بالاعلام وهدا حسب المادة 14 من قانون 09-04 السالف الدكر ويكون الاختصاص للمحاكم الجزائرية ادا كانت الجرائم مرتكبة خارج الاقليم الجزائري عندما يكون مرتكبيها اجنبيا وتستهدف مؤسسات الدولة ويمكن طلب مساعدة قضائية دولية بشرط عدم المساس بسيادة مع اجراء التحفظ اما عن طريق الفاكس أو البريد الالكتروني .

اضافة الى أنه صدر القانون 16-02 المؤرخ في 8 يونيو 2016 قانون العقوبات حيث نصت المادة 87 منه يعاقب بالسجن المؤقت من 5الى 10 سنوات وبغرامة من 100.000دج الى 500.000دج كل جزائري أو أجنبي مقيم بالجزائر بطريقة شرعية أو غير شرعية يسافر أو يحاول السفر الى دولة أخرى بغرض ارتكاب أفعال ارهابية أو تدبيرها واضافت الفقرة الأخيرة يستخدم تكنولوجيا الاعلام والاتصال لارتكاب الأفعال المدكورة ونصت المادة 87 مكرر 12 يعاقب بالسجن المؤقت من 5سنوات الى 10عشر 10 سنوات وبغرامة من 100.000دج الى 500.000دج كل من يستخدم تكنولوجيا الاعلام والاتصال لتجنيد الأشخاص لصالح ارهابي أو جمعية أو تنظيم أو جماعة أو منظمة يكون غرضها أو تقع أنشطتها تحت طائلة أحكام هدا القسم أو ينظم شؤونها أو يدعم أعمالها أو أنشطتها أو ينشر أفكارها وتنص المادة 394 مكرر 8 دون الاخلال بالعقوبات الادارية المنصوص عليها يعاقب بالحبس من سنة الى ثلاث سنوات وبغرامة من من 2.000.000دج الى 10.000.000دج أو باحدى هاتين العقوبتين فقط مقدم خدمة

الأنترنت بمفهوم المادة 2 من القانون 09-04 المؤرخ في 5 غشت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها التي لا يقوم رغم اعداره من الهيئة الوطنية المنصوص عليها في القانون المدكور أو صدور أو حكم قضائي يلزمه بدلك بالتدخل الفوري لسحب أو تخزين المحتويات التي يتيح الاطلاع عليها أو جعل الدخول اليها غير ممكن عندما تتضمن محتويات تشكل جرائم منصوص عليها قانونا ، بوضع ترتيبات تقنية تسمح بتخزين أو بسحب المحتويات المتعلقة بالجرائم المنصوص عليها في الفقرة ا أو جعل الدخول اليها غير ممكن[3] و قد صدر مؤخرا قرار وزاري مشترك مؤرخ في 17 ديسمبر 2017 يحدد التنظيم الداخلي لهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وتشمل مصالح الادارة العامة وتشمل مكتب الموارد البشرية مكتب الماليبة والوسائل مكتب الوقاية والامن وهناك مديرية الملراقبة الوقائية واليقظة الالكترونية وتشمل مصلحة المراقبة الالكترونية مصلحة المتابعة والتحليل والتعاون ويلحق به مركز العمليات التقنية والملحقات ومصلحة المراقبة الالكترونية مكتب تنسيق النشاطات مكتب مراقبة الاتصالات ومكتب مراقبة شبكات الاتصالات السلكية واللاسلكية مكتب مراقبة شبكة الانترنت وهناك مصلحة المتابعة التحليل والتعاون مكتب جمع معلومات ومكتب الوقاية والمتابعة ومكتب الاتصال والتعاون ويشتمل مركز العمليات التقنية على مكتب انظمة المراقبة الهاتفية ومكتب انظمة مراقبة الانترنت ومكتب أنظمة التموقع الجغرافي ومراقبة الاتصالات ومكتب الدعم التقني وتشمل الملحقة الجهوية مكتب الادارة العامة ومكتب المراقبة الالكترونية وتشمل مصلحة المتابعة التحليل والتعاون مكتب جمع ومركزة استغلال المعلومات ومكتب الوقاية والمتابعة ومكتب الاتصال والتعاون ويشتمل مركز العمليات التقنية مكتب الطمة المراقبة الهاتفية مكتب مراقبة الانترنت مكتب انظمة التموقع الجغرافي ومراقبة الاتصالات مكتب الدعم الفني وتشمل الملحقة الجهوية مكتب الادارة والمراقبة والمتابعة والتحليل والعمليات التقنية وتشمل مديرية التنسيق مصلحة الدراسات والخبرات القضائية ومصلحة منطومة الاعلام ومصلحة الدراسات والخبرات مكتب التقنيات

3

القانون 16-02 المؤرخ في14 رمضان 1437الموافق ل 19 يونيو 2016 قانون العقوباتيعدل ويتمم الأمر 66—156 المؤرخ في 18 صفر 1386 الموافق ل8 يونيو 1966 والمتضمن قانون العقوبات جر العدد37

الرقمية وقاعدة المعطيات ومكتب الدراسات وتشمل مصلحة منطومة الاعلام مكتب الابحاث مكتب ادارة شبكة الاعلام مكتب امن منظومة الاعلام [4]

وقد صدر مؤخرا المرسوم الرئاسي 19-172 المؤرخ في 3 شوال 1440 الموافق ل6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها فالهيئة ممؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة وزارة الدفاع الوطني ويحدد مقر الهيئة بمدينة الجزائر تتشكل من مجلس التوجيه ويتشكل من ممثلي وزارات وزارة الدفاع الوطني الوزارة المكلفة بالداخلية وزارة العدل الوزارة المكلفة بالمواصلات السلكية واللاسلكية وتتكلف حول مسائل تطوير التعاون مع المؤسسات والقيام دوريا بتقييم حالة التهديد في مجال جرائم المتصلة بتكنولوجيا الإعلام والاتصال تقييم أياقتراح اقتراح كل نشاط يتصل بالبحث دراسة التقرير السنوي لنشاطات الهيئة إبداءالرأي في كل مسالة تتصل بمهام الهيئة المساهمة في ضبط المعايير القانونية في مجال اختصاصه اما المديرية العامة فتسهر على حسن سير الهيئة وإعداد مشروع الميزانية وإعداد وتنفيذ برنامج عمل الهيئة وتنشيط وتنسيق ومتابعة ومراقبة أنشطة هياكل الهيئة تنشيط وتنسيق ومراقبة أنشطة هياكل الهيئة تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة ، تحضير اجتماعات مجلس التوجيه وإعداد التقرير السنوي لنشاطات الهيئة وتضم المديرية مديرية تقني مديرية الادارة والمصالح وتقنية تقوم بمساعدة شرطة قضائية ووضع وسائل والاجهزة للمراقبة في مجال جرائم الارهابية والتخريبية [5]

وقد صدر مرسوم رئاسي 21-439 يتضمن إعادة تنظيم هيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال تتشكل من مجلس التوجية المديرية العامة مديرية المراقبة الوقائية واليقظة الالكترونية مديرية الإدارة والوسائل مصلحة الدرسات والتلخيص مصلحة التعاون واليقظة الالكترونية .

10-انشاء القطب الجزائي المختص لمكافحتها

---

[4] انظر القرار الوزاري المشترك 17 ديسمبر 2017 يحدد التنظيم الداخلي للهياكل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ج ر العدد14 لسنة 2018

أنظر المادة من 2 الى15المرسوم الرئاسي 19-172 المؤرخ في 3 شوال 1440 الموافق ل6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من جرائم المتصلة

[5] بتكنولوجيات الاعلام والاتصال ومكافحتها وتنظيمها وكيفيات سيرها جر العدد37

وقد صدر قانون الإجراءات الجزائية 21-11 يقصد في مفهوم هذا القانون الجريمة الالكتلرونية أي جريمة يسهل ارتكابها يسهل استعمالها باستعمال تكنولوجيا معلومات وتنص المادة 211 مكرر23 يمارس وكيل الجمهورية لدى القطب الجزائي لمكافحة جرائم التصالات وتنص المادة 211 مكرر 24 يخنص وكيل الجمهورية لدى القطب الجزائي ورئيس القطب الجزائي اختصاص النظر في الجرائم تكنولوجيا معلومات واتصال وكذا النظر في الجرائم التالية جرائم امن الدولة جرائم نشر وترويج اخبار كاذبة تمس بامن الدولة ونشر اخبار كاذبة تمس بالنظام العمومي عبر الحدود الوطنية وتنص المادة 211 مكرر 25من قانون إجراءات الجزائية يختص وكيل الجمهورية بنظر وتحقيق وحكم في الجرائم الالكترونية ويقصد بجرائم تكنولوجيا اكثر تعقيدا الجريمة بالنظر الى تعدد مشاركين وفاعلين ومتضررين او بالنظر الى اتساع الرقعة الجغرافية واتساع مكان او خبرة فنية متخصصة او لجوء الى تعاون دولي قضائي وتنص المادة 211 مكرر 28 اذا تزامن اختصاص القطب الجزائي باختصاص القطب الاقتصادي ومالي يؤول الاختصاص وجوبا الى هذا القطب واذا تزامن اختصاص القطب الجزائي باختصاص القطب محكمة منعقدة بمقر مجلس القضائي يؤول اختصاص الى هذا القطب [6]

خاتمة

صدر في العدد الأخير من الجريدة الرسمية، القانون رقم 20-05 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، والذي يتضمن إنشاء المرصد الوطني للوقاية من التمييز وخطاب الكراهية.

ويحدد القانون المهام الموكلة لهذا المرصد الذي يوضع لدى رئيس الجمهورية، والمتمثلة في اقتراح عناصر الاستراتيجية الوطنية للوقاية من التمييز وخطاب الكراهية، والمساهمة في تنفيذها بالتنسيق مع السلطات العمومية المختصة ومختلف الفاعلين في هذا المجال والمجتمع المدني، إلى جانب الرصد المبكر لأفعال التمييز وخطاب الكراهية وإخطار الجهات المعنية

هدا وقد صدر في الجزائر قانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حيث يجوز مراقبة المعلومات الالكترونية

[6] انظر امر 21-11 المؤرخ في25 غشت متضمن قانون إجراءات جزائية جر العدد 652021

في حالةالمسائل المتعلقة بالارهاب المخالفة للنظام العام وتنشأ هيئة عليا للوقاية من جرائم تكنولوجيا الاعلام والاتصالات

وقد صدر مؤخرا المرسوم الرئاسي 19-172 المؤرخ في 3 شوال 1440 الموافق ل6 يونيو 2019 يحدد تشكيلة الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها صدر مرسوم رئاسي 21-439 يتضمن إعادة تنظيم هيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال تتشكل من مجلس التوجية المديرية العامة مديرية المراقبة الوقائية واليقظة الالكترونية مديرية الإدارة والوسائل مصلحة الدرسات والتلخيص مصلحة التعاون واليقظة الالكترونية .

وتنظيمها

قائمة المصادر والمراجع

الاتفاقيات الدولية

القانون رقم 20-05 المؤرخ في 28 أبريل 2020، المتعلق بالوقاية من التمييزوخطاب الكراهية ومكافحتهما، والذي يتضمن إنشاء المرصد الوطني للوقاية من التمييزوخطاب الكراهية.

مراجع[↑ تعدى إلى الأعلى ل:أ ب ت ث ج ح *Iginio, Gagliardone; Danit, Gal; Thiago, Alves; Gabriela, Martinez (2015-11-16). مكافحة خطاب الكراهية في الانترنت. UNESCO Publishing.ISBN 9789236000404. الأصل في 13 مؤرشف من فبراير 2020.*

1. ^ *حرية التعبير: مقدمة قصيرة جدًّا. Kalimat. 2013. ISBN 9789777192071. الأصل في 23 مؤرشف من ديسمبر 2017. اطلع عليه بتاريخ أغسطس 2020.*
2. ^ *Howard, Erica (2017-07-28). Freedom of Expression and Religious Hate Speech in Europe (باللغة الإنجليزية). Routledge. ISBN 9781351998789. الأصل في 13 فبراير 2020 مؤرشف من.*
3. ^ *"ضرورة تطوير قوانين الإعلام لمعالجة خطاب الكراهية والعنف". جريدة الدستور الاردنية. مؤرشف من الأصل في 13 فبراير 2020. اطلع عليه بتاريخ 22 ديسمبر 2017.*
4. ^ *"أكاديميون مغربيون: خطاب الكراهية بمواقع التواصل يهدّد قيم التسامح في المملكة". رأي اليوم (باللغة الإنجليزية). مؤرشف من الأصل في 10 يناير 2018. اطلع عليه بتاريخ 22 ديسمبر 2017.*
5. ^ *الاديان وحرية التعبير: اشكالية الحرية في مجتمعات مختلة. مركز القاهرة لدراسات حقوق الإنسان،. 2007. الأصل في 13 فبراير 2020 مؤرشف من.*

6. ^ Paul, Daudin Clavaud; Toby, Mendel; Ian, Lafrenière (2014-12-22). Maintien de l'ordre et respect de la liberté d'expression: manuel pédagogique. UNESCO Publishing. ISBN 9789236000305. الأصل مؤرشف من 2020 فبراير 14 في.
7. ^ Wolfson, Nicholas (1997). Hate Speech, Sex Speech, Free Speech (باللغة الإنجليزية). Greenwood Publishing Group. ISBN 9780275957704. الأصل مؤرشف من 2020 فبراير 13 في.
8. ^ Weber, Anne (2014-01-01). Manual on hate speech (باللغة الإنجليزية). Council of Europe. ISBN 9789287178770. الأصل مؤرشف من 2020 فبراير 14 في.
9. ^ للمزيد أنظر: Foxman, Abraham H.; Wolf, Christopher (2013-06-04). Viral Hate: Containing Its Spread on the Internet (باللغة الإنجليزية). St. Martin's Press.ISBN 9781137356222. مؤرشف الأصل من 2020 فبراير 13 في.
10. ^ UNESCO (2015-12-07). Keystones to foster inclusive knowledge societies: access to information and knowledge, freedom of expression, privacy and ethics on a global internet. UNESCO Publishing. ISBN 9789236000428. الأصلمؤرشف من 2017 ديسمبر 27 في.
11. ^ Gelber, Katharine; Stone, Adrienne Sarah Ackary (2007). Hate Speech and Freedom of Speech in Australia (باللغة الإنجليزية). Federation Press.ISBN 9781862876538. الأصل مؤرشف من 2020 فبراير 14 في.
12. ↑ تعدى إلى الأعلى ل: أ ب ت Mchangama, Jacob (2015-01-02). "The Problem with Hate Speech Laws". The Review of Faith & International Affairs. **13** (1): 75–82.doi:10.1080/15570274.2015.1005919. ISSN 1557-0274. الأصل مؤرشف من 2020 فبراير 24 في.
13. ↑ تعدى إلى الأعلى ل: أ ب ت Beaumont, P. (1994). Striking a Balance: Hate Speech, Freedom of Expression and Non-Discrimination. Edited by ColiverSandra.[London: Article 19 International Centre against Censorship/Human Rights Centre, University of Essex. 1992]. ix+ 417 pp. ISBN 1-870798-76-7.£ 9· 95. *International & Comparative Law Quarterly*, *43*(2), 476-478.نسخة محفوظة 27 على موقع واي باك مشين 2017 ديسمبر.
14. ^ "THE SOVIET ORIGINS OF HATE-SPEECH LAWS - ProQuest".search.proquest.com. مؤرشف الأصل من 2020 فبراير 13 في. اطلع عليه بتاريخ 2017 ديسمبر 27.
15. ^ "George Orwell meets the OIC | Human Events". Human Events مؤرشف). (باللغة الإنجليزية الأصل من 2019 فبراير 15 في. اطلع عليه بتاريخ 2017 ديسمبر 22.
16. ^ Weinstein, James. "Hate Speech Bans, Democracy, and Political Legitimacy Symposium: Hate Speech and Political Legitimacy 32 Constitutional Commentary 2017". heinonline.org. صفحة 527. مؤرشف الأصل من 2020 فبراير 14 في. اطلع عليه بتاريخ 2017 ديسمبر 27.
17. ^ "The Harm in Hate Speech: A Critique of the Empirical and Legal Bases of Hate Speech Regulation 43 Hastings Constitutional Law Quarterly 2015-2016". heinonline.org. مؤرشف الأصل من 2020 فبراير 14 في. اطلع عليه بتاريخ 2017 ديسمبر 27.
18. ^ Paul, Daudin Clavaud; Toby, Mendel; Ian, Lafrenière (2014-12-22). Maintien de l'ordre et respect de la liberté d'expression: manuel pédagogique. UNESCO Publishing. ISBN 9789236000305. الأصل مؤرشف من 2020 فبراير 14 في.
19. ^ Berkeley Journal of International Law (باللغة الإنجليزية). University of California Press. 1996. الأصل مؤرشف من 2020 فبراير 14 في.
20. ^ Mearsheimer, John J.; Walt, Stephen M. (2008-06-26). The Israel Lobby and US Foreign Policy (باللغة الإنجليزية). Penguin Books Limited. ISBN 9780141920665. الأصل مؤرشف من 2020 فبراير 13 في.

21. ^ The Middle East: Abstracts and index (باللغة الإنجليزية). Northumberland Press. 2006. مؤرشف من الأصل في 13 فبراير 2020.
22. ^ Adel, Ahmed. "الكتاب . بهـدوء معـاداة السـامية في وسائل الإعلام الإسرائيلية بقلم : إبراهيم نافع". www.ahram.org.eg. مؤرشف من الأصل في 23 ديسمبر 2017. اطلع عليه بتاريخ 22 ديسمبر 2017.
23. ^ Asad, Talal; Brown, Wendy; Butler, Judith; Mahmood, Saba (2013). Is Critique Secular?: Blasphemy, Injury, and Free Speech (باللغة الإنجليزية). Fordham University Press. ISBN 9780823251681. مؤرشف من الأصل في 14 فبراير 2020.
24. ^ Robertson, Eleanor (2016-03-10). "Language policing and Twitter wars: why modern feminism is failing us (again)". The Guardian (باللغة الإنجليزية). ISSN 0261-3077. مؤرشف من الأصل في 2 يونيو 2019. اطلع عليه بتاريخ 22 ديسمبر 2017.
25. ^ Establishment, The (2016-06-14). "How About We Stop Policing Women's Language?". Huffington Post (باللغة الإنجليزية). مؤرشف من الأصل في 5 أكتوبر 2017. اطلع عليه بتاريخ 22 ديسمبر 2017.
26. ^ Braun, Stefan (2004). Democracy Off Balance: Freedom of Expression and Hate Propaganda Law in Canada (باللغة الإنجليزية). University of Toronto Press. ISBN 9780802086365. مؤرشف من الأصل في 13 فبراير 2020.
27. ^ "How Language Policing And Hyper-Sensitivity Are Ruining Social Dialogue". Thought Catalog. مؤرشف من الأصل في 11-02-2014. اطلع عليه بتاريخ 22 أغسطس 2018 (باللغة الإنجليزية). في 13 ديسمبر 2017.
28. ^ Phyak, Prem (2015-11-01). "(En)Countering language ideologies: language policing in the ideospace of Facebook". Language Policy (باللغة الإنجليزية). **14** (4): 377–395. doi:10.1007/s10993-014-9350-y. ISSN 1568-4555. مؤرشف من الأصلفي 2 يونيو 2018.
29. ^ Brown, Alex (2015-03-05). Hate Speech Law: A Philosophical Examination(باللغة الإنجليزية). Routledge. ISBN 9781317502364. مؤرشف من الأصل في 14 فبراير 2020.
30. ^ Tatchell, Peter (2007-10-10). "Hate speech v free speech". The Guardian(باللغة الإنجليزية). ISSN 0261-3077. مؤرشف من الأصل في 14 أكتوبر 2018. اطلع عليه بتاريخ 22 ديسمبر 2017.
31. ^ Hern, Alex (2016-05-31). "Facebook, YouTube, Twitter and Microsoft sign EU hate speech code". The Guardian (باللغة الإنجليزية). ISSN 0261-3077. مؤرشف منالأصل في 14 أبريل 2019. اطلع عليه بتاريخ 22 ديسمبر 2017.
32. ^ "فيسبوك تحذف 66 ألف منشور أسبوعيا". قناة الحرة. مؤرشف من الأصل في 28 يونيو 2017. اطلع عليه بتاريخ 21 ديسمبر 2017.
33. ^ "ما الحديث الذي يعتبره فيسبوك يحض على الكراهية؟ / مركز مساعدة فيسبوك | فيسبوك". www.facebook.com. مؤرشف من الأصل في 17 يونيو 2017. اطلع عليه بتاريخ 21 ديسمبر 2017.
34. ↑ تعدى إلى الأعلى ل:أ ب Bousfield, Derek (2008). Impoliteness in Interaction (باللغة الإنجليزية). John Benjamins Publishing. ISBN 9027254117. مؤرشف من الأصل في 13 فبراير 2020.
35. ^ "A Facebook crime every 40 minutes: From killings to grooming as 12,300 cases are linked to the site". Mail Online. مؤرشف من الأصل في 22 ديسمبر 2018. اطلع عليه بتاريخ 21 ديسمبر 2017.
36. ^ Scheinbaum, Angeline Close (2017-09-14). The Dark Side of Social Media: A Consumer Psychology Perspective (باللغة الإنجليزية). Routledge. ISBN 9781351683807. مؤرشف من الأصل في 24 فبراير 2020.

37. ^ *العهد الدولي الخاص بالحقوق المدنية والسياسية* 23 ، مكتبة حقوق الإنسان، جامعة منيسوتا، اطلع عليه بتاريخ فبراير 2017 على موقع واي باك مشين 02 ديسمبر 2017 نسخة محفوظة.
38. ^ الاتفاقية الدولية للقضاء على جميع أشكال التمييز العنصري(أ)، المادة 4، البند .، نسخة محفوظة 11 يناير 2020 على موقع واي باك مشين.
39. ^ *Report of the High Commissioner for Human Rights on the use of the Internet for purposes of incitement to racial hatred, racist propaganda and xenophobia, and on ways of promoting international cooperation in this area*, Preparatory Committee for the World Conference Against Racism, Racial Discrimination, Xenophobia, and Related Intolerance, UN GAOR, UN Doc. A/CONF. 189/PC. 2/12 (2001), 27 April 2001
40. ^ *Bell, Jeannine (Summer 2009). "Restraining the heartless: racist speech and minority rights". Indiana Law Journal. **84**: 963–79. اطلع عليه بتاريخ 9 أكتوبر 2014. في 16 مارس 2020 مؤرشف من الأصل.*
41. ^ *O'Neil, Partick M. (2016). "Hate Speech". Encyclopedia of American Studies. في مؤرشف من الأصل 29 مارس 2019.*
42. ↑ تعدى إلى الأعلى ل:أ ب *"Strafgesetzbuch §130 (1)". في 19 مايو 2019 مؤرشف من الأصل.*
43. ↑ تعدى إلى الأعلى ل:أ ب StGB §130 (2) 1. c)
44. ^ Section 9 §1 Alt. 3 and 4 of the Strafgesetzbuch
45. ^ *News, ABC. "ABC News". ABC News. في 5 يوليو 2017 مؤرشف من الأصل.*
46. ^ Véronique Lamquin, Moureaux : « Le politique n'ose plus aller à contre-courant »,*Le Soir*, 31 July 2011[وصلة] نسخة محفوظة [مكسورة] 2 أبريل 2012 على موقع واي باك مشين.
47. ^ Act of 23 March, 1995 on punishing the denial, minimisation justification or approval of the genocide perpetrated by the German National Socialist Regime during the Second World War نسخة محفوظة 12 أكتوبر 2006. على موقع واي باك مشين (ترجمة إنجليزية غير رسمية)
(بالفرنسية) Loi tendant à réprimer la négation, la minimisation, la justification ou l'approbation du génocide commis par le régime national-socialiste allemand pendant la seconde guerre mondiale نسخة محفوظة 29 مارس 2009. على موقع واي باك مشين (official French text)
(بالهولندية) Wet tot bestraffing van het ontkennen, minimaliseren, rechtvaardigen of goedkeuren van de genocide die tijdens de tweede wereldoorlog door het Duitse nationaal-socialistische regime is gepleegd نسخة محفوظة March 12, 2007, على موقع واي باك مشين. (official Dutch text)
48. ^ "1988 Constitution made racism a crime with no right to bail", Folha de S.Paulo, 15 April 2005. نسخة محفوظة 11 ديسمبر 2018 على موقع واي باك مشين.
49. ^ دستور البرازيل الصادر عام 1988 شاملا تعديلاته لغاية عام 2014، ترجمة المؤسسة الدولية للديموقراطية والانتخابات؛ تحديث مشروع الدساتير المقارنة، المادة الخامسة، الفصل الأول، البند رقم 42 تحت عنوان "حظر تطبيق العقوبات بأثر رجعي" صفحة 9
50. ^ *Criminal Code*, RSC 1985, c C-46, s 318, "Advocating Genocide". نسخة محفوظة 19 فبراير 2019 على موقع واي باك مشين.
51. ^ RSC 1985, c C-46, s 319 "Public incitement of hatred" and "Wilful promotion of hatred". نسخة محفوظة 19 فبراير 2019 على موقع واي باك مشين.
52. ^ *Paúl Díaz, Álvaro (2011). "Alvaro Paúl Díaz, The Criminalization of Hate Speech in Chile in Light of Comparative Case Law (IN SPANISH), Rev. chil. derecho, 2011, vol.38, n.3, pp. 573–*

609". Revista Chilena de Derecho. **38** (3): 573–609. doi:10.4067/S0718-34372011000300007. اطلع عليه بتاريخ 10 أكتوبر 2014. في 23 أكتوبر 2017 مؤرشف من الأصل.

53. ^ Paúl Díaz, Álvaro (2011). "Alvaro Paul Díaz, The Criminalization of Hate Speech in Chile in Light of Comparative Case Law (In Spanish), Rev. chil. derecho, 2011, vol.38, n.3, pp. 573–609". Revista Chilena de Derecho. **38** (3): 573–609. doi:10.4067/S0718-34372011000300007. اطلع عليه بتاريخ 10 أكتوبر 2014. في 23 أكتوبر 2017 مؤرشف من الأصل.
54. ^ Article 174. of Croatian penal code on Croatian Wikisource
55. ^ Sharon, Alina Dain (February 28, 2013). "A Web of Hate: European, U.S. Laws Clash on Defining and Policing Online Anti-Semitism". ذا ألجيمباينر جورنال [لغات أخرى]. الأصل مؤرشف من 12 أبريل 2019.
56. ^ "TV2:n Vihaillassa ei päästy yksimielisyyteen vihapuhe-käsitteestä".Helsing Sanomat (باللغة الفنلندية). 20 September 2011. الأصل مؤرشف من 2 يوليو 2014. في 27 سبتمبر 2011. اطلع عليه بتاريخ 27 سبتمبر 2011.
57. ^ "Vihapuheen määritelmästä ei yksimielisyyttä". YLE Uutiset (باللغة الفنلندية). YLE. 21 September 2011. الأصل مؤرشف من 2 فبراير 2012. في 27 سبتمبر 2011. اطلع عليه بتاريخ 27 سبتمبر 2011.
58. ^ Finnish Penal code Rikoslaki/Strafflagen Chapter 11, section 10 Ethnic agitation / Kiihottaminen kansanryhmää vastaan نسخة محفوظة 05 واي باك مشين على موقع 2018 أكتوبر.
59. ^ Loi 90-615 du 13 juillet 1990
60. ^ Jordans, Frank (30 June 2017). "Germany passes law against online hate speech". ABC News. Associated Press. الأصل مؤرشف من 01 يوليو 2017. في 01 يوليو 2017.
61. ^ Must We Defend Nazis?. NYU Press. 2018-01-31. 162–135 صفحات.ISBN 9781479827756. الأصل مؤرشف من 16 مارس 2020. في 16 مارس 2020.
62. ^ Patrick M. (2017-07-12). Rediscovering a Lost Freedom. Routledge. 113– صفحات 130. ISBN 9781315128184. الأصل مؤرشف من 24 فبراير 2020. في 24 فبراير 2020.
63. ^ "Brandenburg v. Ohio (1969)". Encyclopedia of the First Amendment. 2300 N Street, NW, Suite 800, Washington DC 20037 United States: CQ Press. ISBN 9780872893115. الأصل مؤرشف من 24 فبراير 2020. في 24 فبراير 2020.
64. ^ The Encyclopedia of Civil Liberties in America. Routledge. 2015-04-10. 769– صفحات 770. ISBN 9781315699868. الأصل مؤرشف من 24 فبراير 2020. في 24 فبراير 2020.
65. ^ Berry, Vanessa A. (2011-05-05). "Snyder v. Phelps: Public Servant or Private Citizen?". Fort Belvoir, VA. الأصل مؤرشف من 24 فبراير 2020. في 24 فبراير 2020.
66. ^ ""Matal v. Tam"". IIC - International Review of Intellectual Property and Competition Law. **48** (6): 749–751. 2017-08-22. doi:10.1007/s40319-017-0624-8. ISSN 0018-9855. مؤرشف الأصل من 16 مارس 2020. في 16 مارس 2020.
67. ^ Downs, Daniel M.; Cowan, Gloria (2012-6). "Predicting the Importance of Freedom of Speech and the Perceived Harm of Hate Speech: PREDICTORS OF FREE SPEECH AND HATE SPEECH". Journal of Applied Social Psychology(باللغة الإنجليزية). **42** (6): 1353–1375. doi:10.1111/j.1559-1816.2012.00902.x. الأصل مؤرشف من 24 فبراير 2020. في 24 فبراير 2020.
68. ^ "Original PDF". dx.doi.org. الأصل مؤرشف من 7 أبريل 2020. في 10 نوفمبر 2019. اطلع عليه بتاريخ 10 نوفمبر 2019.

Jacque –henri STAHL, principe de l'egalite et stabilite des situations juridiques a propos des delais dr recours contentieux regis par la lois du 12 avril 2000 ,R.F.D.A. ,sept-oct,2004 ,p.398

Mario BETTATI,L'incrimination sous la presidence de monsieur Jean KAHN ,president de la commission nationale consultative des droits de l'homme ,La lutte contre le racisme et la xenophobie 1997 ,exlusion et droits de l'homme , la documentation francaise ,paris ,1998 ,pp.152 et s.

;Lnigui CONDORELLI ,Les sources intrenationales et le devenir du concept ,op.cit.,pp.174 et s

. ;La discrimination dans la jurisprudence de la cour de cassation ,rapport annuel ,la documentation francaise 2008 ,p.83

. ;Mohamed KAHLOULA , Les droits fondamentaux du justiciable dans le procés civil a la lumiere de la refonte du code algeriens de procédure civil ;

Dominique BREILLAT , convention europeenne des droits de l'homme et l' »islame etude de droit melanges en hommage a abdellah BENHAMOU , ouvrage publié avec le soutien de recteur de l'universite a kounouze edition .Vincent BERGER,Jurisprudence de la cour europeenne des droits de l'homme ,12 ed.,edit .D. ,2011,preface par Louis –EDMOND PETTILI,p.7 ;BERTRAND Mathieu,Michel VERPEAUX ,Contentieux constitutionnel des droits fondamentaux ,edit.L.G.D.J. ,p.3 ;XAVIER Bioy,Droits fondamentaux et libertes publiques ,edit.L.G.D.J. ,Montchrestien ,2011,p.3 ;Jacques ROBERT ,Le juge constitutionnel , juge des libertes , libertes et droits fondamentaux, preparation au C.R.F.P.A ,montchrestien,1999,p.7 ;

KAHLOULA Mohamed , Le droit algerien face a la pollution de la mer par les navires pétroliers ;

HANAFI Louisa , Droit et respect la vie priveé de la persnne ; Djillali TCHOUAR , Droit algerien de la famille quels principes d'égaliité ; Dalila ZENNAKI ? égalité homme et femme en algérie et conformité au x normes internationales le cas de la convention sur liélimination de toutes les formes de discrimination de toutes les formes de discriminations a l'égard des femme ;

; Bachir YELLES CHAOUCHE , Les réformes politiques en algerie ou l'art de réformer pour changer etat de droit et économie ; Madjid BENCHIKH , Les R2FORMES POLITIQUES EN ALGERIE ou l'art de réformer sans changer ; Lahcer OULHAJ , De la constitution économiquee marocaine ; Massoudi MENTRI Réflexion sur la question dadaptation des institutions de l'union africaine aux défis de paix et de développement ; ABDELKADER kacher , L'alternance not chef pour sortir de la crisr de gouvernnance en algerie melanges en hommage a abdellah BENHAMOU , ouvrage publié avec le soutien de recteur de l'universite a kounouze edition

.Vincent BERGER,Jurisprudence de la cour europeenne des droits de l'homme ,12 ed.,edit .D. ,2011,preface par Louis –EDMOND PETTILI,p.7 ;

BERTRAND Mathieu,Michel VERPEAUX ,Contentieux constitutionnel des droits fondamentaux ,edit.L.G.D.J. ,p.3 ;XAVIER Bioy,Droits fondamentaux et libertes publiques ,edit.L.G.D.J. ,Montchrestien ,2011,p.3

;Jacques ROBERT ,Le juge constitutionnel , juge des libertes , libertes et droits fondamentaux, preparation au C.R.F.P.A ,montchrestien,1999,p.7 ; KAHLOULA Mohamed , Le droit algerien face a la pollution de la mer par les navires pétroliers ;

[1] Cf.Mario BETTATI,L'incrimination sous la presidence de monsieur Jean KAHN ,president de la commission nationale consultative des droits de l'homme ,La lutte contre le racisme et la xenophobie 1997 ,exlusion et droits de l'homme , la documentation francaise ,paris ,1998 ,pp.152 et s. ;Lnigui CONDORELLI ,Les sources intrenationales et le devenir du concept ,op.cit.,pp.174 et s. ;La discrimination dans la jurisprudence de la cour de cassation ,rapport annuel ,la documentation francaise 2008 ,p.83. ;Mohamed KAHLOULA , Les droits fondamentaux du justiciable dans le procés civil a la lumiere de la refonte du code algeriens de procédure civil ; Dominique BREILLAT , convention europeenne des droits de l'homme et l' »islame etude de droit melanges en hommage a abdellah BENHAMOU ,

دليلة مباركي ، حرمة الحياة الخاصة كحق من ; ouvrage publié avec le soutien de recteur de l'universite a kounouze edition الحقوق اللصيقة بالشخصية م ع ق ا العدد 6 لسنة 2008 ؛ صديقي نبيلة ، حماية الحق في الخصوصية م ع ق ا العدد 6 لسنة 2008 ؛ تشوار الجيلالي ، حق الشخص في التصرف في جسمه الرتق العذري والتغيير الجنسي نموذجا م ع ق ا العدد 6 لسنة 2008 ؛ نهار مالطي ، حماية الجسم البشري والدين أية علاقة ؛م ع ق ا العدد 6 لسنة 2008 ؛ فريد بلفراق ، حق التصرف في الجسد بين الشريعة والقانون ، م ع ق ا العدد 6 لسنة 2008 ؛ قاشي علال ، التصرف الوارد على جسم الانسان ومدى مشروعيتها ، م ع ق ا العدد 6 لسنة 2008 ؛ شمامة خير الدين ، الاتستنساخ م ع ق ا العدد 6 لسنة ؛ مرنيز فاطمة ، جريمة الاعتداء على البيانات الشخصية عبر شبكة الأنترنت م ع ق ا العدد 6 لسنة 2008 ؛ مراد بدران ، القيود الواردة على الحقوق الشخصية في طل الطروف الاستثنائية ، 62008 م ع ق ا العدد 6 لسنة دايم بلقاسم ، الرقابة القضائية على الملائمة وأثرها على الحقوق والحريات م ع ق ا العدد 6 لسنة 2008؛ BENHAMOU Abdallah ,Les droits politiques et condition de mise en œuvre ; BENHAMOU Abdallah , Constitution religion et democratie , ; BENAISSA Salima ,L'autorité en question ; BOURICHE Riadh BENAAME Youcef ?,Le système d'évaluation des incidences environnement a les des projets de develloppement

[1] انظر ، Samuel PISON ,Paroles des victimes , la lutte contre le racisme et la xenophobie 1997 exlusion et droit de l'homme , p.162 ;Marcel COLIN ,La relation genocidaire aspects psychiatriques ,op.cit.,p.165 ;Michel masse ,Le crime contre l'humanite en droit francais ,op.cit.,p.163

[1] Cf.Caroline PICHERAL,Discrimination raciale et convention europeenne des droits de l'homme,REV.TRIM.DR.H.2001,pp.517 et s. ;Le droit de l'homme a la nom discrimination raciale , ,REV.TRIM.DR.H.2001,pp.666

[1] Cf.Jean RIVERO ,Les libertes publiques ,T.2,P.U.F.,pp.22et s.

[1] Cf.Michel levinet,La CEDH,socle de la protection des droits de l'homme dans le droitconstitutionnel europeen ,R.F.D.C. ,PUF,Avril,2011 N86 P.

[1] Cf.Armel PECHEUL ,au source du principe ,les droits fondamentaux a l'epreuve de la mondialisation , acte du collogue international organise par le centre de recherches hannah arendt les 16 17 mars 2006 ,pp.8 ets ;Ibrahim SOUSS,L'universalite des droits de l'homme,op.cit.,pp.28 ets ;Alain BRUN ,Les droits fondamentaux et le citoyen europeen ,op.cit.,pp47ets ;Henri D.BOSLY ,Droits de l'homme et droits de l'individu ,op.cit.,pp.82 ;Challa RAMAKRISHNA , Fundamental human rights in the recent economic evolution in indla and the social effects therof ,op.cit., pp.103ets ;

62[1]

[1] Cf.Jean –Luc CHABOT,Droit naturel ou morale naturelle ,Droit naturel et droits de l'homme , societe d'histoire du droit journees internationales 2009 grenoble –vizille texte reunis par MARTIAL MATHIEU preface de Jean Marie carbasse ,P.U.G .,fevrier ,2011 ,p.23. ;Paulina SWIECIKA , Reflexion sur la structure de l'argumentation juridique basee sur la naturalis ratio d'apres les juristes romains ,op.cit., p.55 ;Martial MATHIEU ,Not chariity but a right les droits sociaux dans l'œuvre de thomas paine ,op.cit.,pp139et s. ;Brigitte BASDEVANT GAUDEMET ,Religion et declarations des droits en occident et dans le monde arabe,op.cit.,p189 ;Rosine LETINIER DE ARVIZU, engagement des moines et defense de leurs droits dans l'Espagne wisigothique et du haut moyen age ,op.cit.,pp.206et s. ;Fernando DE ARVIZU,La protection de l'homme et de ses biens dans les fors espagnols du moyen age quelques exemples illustratifs ,op.cit.,pp.217et s ; Frederic CHARLIN ,La nature juridique de l'affranchissement de l'esclave dans les colonies francaises :d'une liberte octroyee vers un droit a la liberte ,op.cit.,pp.262 et s . ;Francois JANKOWIAK ,Droits fondamentaux et question romaine sous le magistere de pie ix,op.cit.,pp270et s ;Pierre LEGAL,Liberte d'enseignement et loi injuste le recours au droit naturel 1920-1960, op.cit., pp.290ets ;Constance Chevallier –COVERS , Le droit naturel et la protection internationale des droits de l'homme , op.cit.,pp.334ets ;Hafida BELRHALI BERNARD ,L a responsabilite administrative au service de la protection des droits de l'homme ,op.cit.,p359

[1] Cf.Jacque –henri STAHL, principe de l'egalite et stabilite des situations juridiques a propos des delais dr recours contentieux regis par la lois du 12 avril 2000 ,R.F.D.A. ,sept-oct,2004 ,p.398

Samuel PISON ,Paroles des victimes , la lutte contre le racisme et la xenophobie 1997 exlusion et droit de l'homme , p.162 ;Marcel COLIN ,La relation genocidaire aspects psychiatriques ,op.cit.,p.165 ;Michel masse ,Le crime contre l'humanite en droit francais ,op.cit.,p.163

[1] Cf.Caroline PICHERAL,Discrimination raciale et convention europeenne des droits de l'homme,REV.TRIM.DR.H.2001,pp.517 et s. ;Le droit de l'homme a la nom discrimination raciale , ,REV.TRIM.DR.H.2001,pp.666

[1] Cf.Jean RIVERO ,Les libertes publiques ,T.2,P.U.F.,pp.22et s.

[1] Cf.Michel levinet,La CEDH,socle de la protection des droits de l'homme dans le droitconstitutionnel europeen ,R.F.D.C. ,PUF,Avril,2011 N86 P.

[1] Cf.Armel PECHEUL ,au source du principe ,les droits fondamentaux a l'epreuve de la mondialisation , acte du collogue international organise par le centre de recherches hannah arendt les 16 17 mars 2006 ,pp.8 ets ;Ibrahim SOUSS,L'universalite des droits de l'homme,op.cit.,pp.28 ets ;Alain BRUN ,Les droits fondamentaux et le citoyen europeen ,op.cit.,pp47ets ;Henri D.BOSLY ,Droits de l'homme et droits de l'individu ,op.cit.,pp.82 ;Challa RAMAKRISHNA , Fundamental human rights in the recent economic evolution in indla and the social effects therof ,op.cit., pp.103ets ;

62[1]

[1] Cf.Jean –Luc CHABOT,Droit naturel ou morale naturelle ,Droit naturel et droits de l'homme , societe d'histoire du droit journees internationales 2009 grenoble –vizille texte reunis par MARTIAL MATHIEU preface de Jean Marie carbasse ,P.U.G .,fevrier ,2011 ,p.23. ;Paulina SWIECIKA , Reflexion sur la structure de l'argumentation juridique basee sur la naturalis ratio d'apres les juristes romains ,op.cit., p.55 ;Martial MATHIEU ,Not chariity but a right les droits sociaux dans l'œuvre de thomas paine ,op.cit.,pp139et s. ;Brigitte BASDEVANT GAUDEMET ,Religion et declarations des droits en occident et dans le monde arabe,op.cit.,p189 ;Rosine LETINIER DE ARVIZU, engagement des moines et defense de leurs droits dans l'Espagne wisigothique et du haut moyen age ,op.cit.,pp.206et s. ;Fernando DE ARVIZU,La protection de l'homme et de ses biens dans les fors espagnols du moyen age quelques exemples illustratifs ,op.cit.,pp.217et s ; Frederic CHARLIN ,La nature juridique de l'affranchissement de l'esclave dans les colonies francaises :d'une liberte octroyee vers un droit a la liberte ,op.cit.,pp.262 et s . ;Francois JANKOWIAK ,Droits fondamentaux et question romaine sous le magistere de pie ix,op.cit.,pp270et s ;Pierre LEGAL,Liberte d'enseignement et loi injuste le recours au droit naturel 1920-1960, op.cit., pp.290ets ;Constance Chevallier –COVERS , Le droit naturel et la protection internationale des droits de l'homme , op.cit.,pp.334ets ;Hafida BELRHALI BERNARD ,L a responsabilite administrative au service de la protection des droits de l'homme ,op.cit.,p359

134[1]

[1] Cf.Vincent BERGER,Jurisprudence de la cour europeenne des droits de l'homme ,12 ed.,edit .D. ,2011,preface par Louis –EDMOND PETTILI,p.7 ;BERTRAND Mathieu,Michel VERPEAUX ,Contentieux constitutionnel des droits fondamentaux ,edit.L.G.D.J. ,p.3 ;XAVIER Bioy,Droits fondamentaux et libertes publiques ,edit.L.G.D.J. ,Montchrestien ,2011,p.3 ;Jacques ROBERT ,Le juge constitutionnel , juge des libertes , libertes et droits fondamentaux, preparation au C.R.F.P.A ,montchrestien,1999,p.7 ; KAHLOULA Mohamed , Le droit algerien face a la pollution de la mer par les navires pétroliers ; HANAFI Louisa , Droit et respect la vie priveé de la persnne ; Djillali TCHOUAR , Droit algerien de la

famille quels principes d'égaliité ; Dalila ZENNAKI ? égalité homme et femme en algérie et conformité aux normes internationales le cas de la convention sur liélimination de toutes les formes de discrimination de toutes les formes de discriminations a l'égard des femme ; ; Bachir YELLES CHAOUCHE , Les réformes politiques en algerie ou l'art de réformer pour changer etat de droit et économie ; Madjid BENCHIKH , Les R2FORMES POLITIQUES EN ALGERIE ou l'art de réformer sans changer ; Lahcer OULHAJ , De la constitution économiquee marocaine ; Massoudi MENTRI Réflexion sur la question dadaptation des institutions de l'union africaine aux défis de paix et de développement ; ABDELKADER kacher , L'alternance not chef pour sortir de la crisr de gouvernnance en algerie melanges en hommage a abdellah BENHAMOU , ouvrage publié avec le soutien de recteur de l'universite a kounouze edition

1

droit interne tunisien et le discours identitaire, collogue Tunis 13-16 janvier 1988 , preface de professeur Mohamed ARKOUN ,centre d'etude de recherches et de publications universite de tunis , 1989 ;Soukeina BOURAOUI, Les reserves des Etats parties a la convention de copenhague ,op.cit .,p27 ;Hafidha CHAKER,Les reserves de la tunisie ,op.cit.,p43 ;BEN ACHOUR Sana ,Laghmani slim ,Droit international droit interne et droit musulman ,op.cit.,p.55 ;Mohamed ARKOUN,De l'ijtihad a la critique de la raison islamique l'exemple du statut de la femme dans la shari a ,op.cit.,p.73 ;BENNANI Ferida , La tutelle dans le mariage :Droit realite et perspectives d'avenir ,op.cit.,pp.141-142 ;EBEIDMONA Makram,Conception laique et conception religieuse dans le domaine des droits de l'homme,op.cit.,p.143 ;BEN ACHOUR Rafaa, Femme et constitution,op.cit.,p.155 ;JEMMAA F ethi Femme et droits fondamentaux,op.cit.,p.171 ;HATEM Kotrane,Les discriminations sexuelles dans l'emploi,op.cit.,p.183 ;Mahfoudh DORRA,Les femmes universitaires entre le carriere et la vie familiale en Tunisie,op.cit.,p.195 ;BEN MILED Emna, MAOUIA Alia,HORCHANI-ZAMITI Melika,Education familiale et acces a la citoyennete,op.cit.,p.211 ;TRIKI Souad,Le travail invisible des femmes,op.cit.,p223 ;GALLALI Slaheddine,Droit de la femme statut de l'homme la question ,op.cit.,p.237 :SAMENDI Zeineb ,Fondamentalisme modernisme-laic :sens d'un antagonisme,op.cit.,p.243 :Bochra BEL HADJ Hamida ,Le statut legal de la femme tunisienne a travers l'exercice de son droit au divorce ,op.cit.,p.285 ;Khayat GHITA,Lavortement et le planning familial ,op.cit.,p.287 ;CHERIF khediija , Ilhem MARZOUKI,Les facteurs socio-culturels defavorisant les femmes en matiere de succession ,op.cit.,p.301 ;BAFFOUN Alia,Les strtegies nom discursives de la reproduction de l'ordre sexuel inegalitaire,op.cit.,p.327 ;NILUFER Gole,Le statut de la femme turque comme enjeu des projets sociaux,op.cit.,p.335 ;BELHAJ Yahia Emna,Discours islamiste radical et droits des femmes,op.cit.,p.369 ;BEN ACHOUR Yadh,Rapport de synthese,op.cit.,p377

1

[1]- Les libertes publiques sont libertes enimerees par la declaration de 1789 et par le preambule de la constitution 1946 sont ainsi oublie les libertes auxquelles notre doit positif,la definition trop extansives .....les libertes publiques sont l'ensemble des droits fondamentaux qui dans un etats moderne et liberale sont indispensable a une veritable libertees les fondement ideologiques des libertes publiques le positivisme juridique nie la realite des droits naturels c'est a dire de droits qui escis teraient independomment .....Cf.Gille LEBRETON ,op.cit.,p.11

[1]La dialictique des rapports qui entrtiennent le principe de legalite et l'exigence de stabilite des situation juridiques est trop comme ici pour que l'on entreprenne d'en faire le tours ,votre jurisprudence a fait application des regles issues des articles 5 et 9 de ce decret par la suite ,le legislateur a entendre Cf.Jacque –Henri STAHL,Principe de legalite et stabilite des situations juridiques (a propos des delais de recours contentieux regis par la lois du 12 avril 2000) R.F.D.A. ,sept_octo,2004

[1] L'institue meme de la matere libertes publique ne voi pas de soi et demande quelque eclaircrissants qui engagent des debats de fond le mot liberte donne bien a des emploi si abusifs et deprouvus ....Cf.Patrik WACHSMAN,Libertes publiques ,1ed.,2002

7[1]

[1] Cf. Erika ROYSTON,Les violences obstericales,Jacqueline DES FORTS , Violences et corps des femmes du tiers-monde , le droit de vivre pour celles qui donnent la vie ,edit. ANEP ,2003 ,p. 19 ; Valerie BERAL ,Les violences demographiques l'envers de la medaille ,op.cit.,p 81 ;Wassyla TAMZALI,Les violences sexuelles le corps feminin a le droit d'etre respecte ,op.cit.,pp.136 ets. ;Marie –Victoire LOUIS ,Marchandisation de la violence sexuelle halte au business du corps humain ,op.cit.,pp173 et s. ; Dalila ALOULA , Violences et descolarisation feminine ,op.cit.,p..137

[1] Cf.Samuel PISON ,Paroles des victimes , la lutte contre le racisme et la xenophobie 1997 exlusion et droit de l'homme , p.162 ;Marcel COLIN ,La relation genocidaire aspects psychiatriques ,op.cit.,p.165 ;Michel masse ,Le crime contre l'humanite en droit francais ,op.cit.,p.163

[1] Cf.Caroline PICHERAL,Discrimination raciale et convention europeenne des droits de l'homme,REV.TRIM.DR.H.2001,pp.517 et s. ;Le droit de l'homme a la nom discrimination raciale , ,REV.TRIM.DR.H.2001,pp.666

[1] Cf.Jean RIVERO ,Les libertes publiques ,T.2,P.U.F.,pp.22et s.

[1] Cf.Michel levinet,La CEDH,socle de la protection des droits de l'homme dans le droitconstitutionnel europeen ,R.F.D.C. ,PUF,Avril,2011 N86 P.

[1] Cf.Armel PECHEUL ,au source du principe ,les droits fondamentaux a l'epreuve de la mondialisation , acte du collogue international organise par le centre de recherches hannah arendt les 16 17 mars 2006 ,pp.8 ets ;Ibrahim SOUSS,L'universalite des droits de l'homme,op.cit.,pp.28 ets ;Alain BRUN ,Les droits fondamentaux et le citoyen europeen ,op.cit.,pp47ets ;Henri D.BOSLY ,Droits de l'homme et droits de l'individu ,op.cit.,pp.82 ;Challa RAMAKRISHNA , Fundamental human rights in the recent economic evolution in indla and the social effects therof ,op.cit., pp.103ets ;

62[1]

[1] Cf.Jean –Luc CHABOT,Droit naturel ou morale naturelle ,Droit naturel et droits de l'homme , societe d'histoire du droit journees internationales 2009 grenoble –vizille texte reunis par MARTIAL MATHIEU preface de Jean Marie carbasse ,P.U.G .,fevrier ,2011 ,p.23. ;Paulina SWIECIKA , Reflexion sur la structure de l'argumentation juridique basee sur la naturalis ratio d'apres les juristes romains ,op.cit., p.55 ;Martial MATHIEU ,Not chariity but a right les droits sociaux dans l'œuvre de thomas paine ,op.cit.,pp139et s. ;Brigitte BASDEVANT GAUDEMET ,Religion et declarations des droits en occident et dans le monde arabe,op.cit.,p189 ;Rosine LETINIER DE ARVIZU, engagement des moines et defense de leurs droits dans l'Espagne wisigothique et du haut moyen age ,op.cit.,pp.206et s. ;Fernando DE ARVIZU,La protection de l'homme et de ses biens dans les fors espagnols du moyen age quelques exemples illustratifs ,op.cit.,pp.217et s ; Frederic CHARLIN ,La nature juridique de l'affranchissement de l'esclave dans les colonies francaises :d'une liberte octroyee vers un droit a la liberte ,op.cit.,pp.262 et s . ;Francois JANKOWIAK ,Droits fondamentaux et question romaine sous le magistere de pie ix,op.cit.,pp270et s ;Pierre LEGAL,Liberte d'enseignement

et loi injuste le recours au droit naturel 1920-1960, op.cit., pp.290ets ;Constance Chevallier –COVERS , Le droit naturel et la protection internationale des droits de l'homme , op.cit.,pp.334ets ;Hafida BELRHALI BERNARD ,L a responsabilite administrative au service de la protection des droits de l'homme ,op.cit.,p359

015أنظر الملحق الخامس

NAFI Louisa , Droit et respect la vie priveé de la persnne ; Djillali TCHOUAR , Droit algerien de la famille quels principes d'égaliité

; Dalila ZENNAKI ? égalité homme et femme en algérie et conformité aux normes internationales le cas de la convention sur liélimination de toutes les formes de discrimination de toutes les formes de discriminations a l'égard des femme ; ;

Bachir YELLES CHAOUCHE , Les réformes politiques en algerie ou l'art de réformer pour changer etat de droit et économie ;

Madjid BENCHIKH , Les R2FORMES POLITIQUES EN ALGERIE ou l'art de réformer sans changer ;

Lahcer OULHAJ , De la constitution économiquee marocaine ; Massoudi MENTRI Réflexion sur la question dadaptation des institutions de l'union africaine aux défis de paix et de développement

; ABDELKADER kacher , L'alternance not chef pour sortir de la crisr de gouvernnance en algerie melanges en hommage a abdellah BENHAMOU , ouvrage publié avec le soutien de recteur de l'universite a kounouze edition

الملتقى الوطني حقوق الإنسان في العصر الرقمي

المحور الثالث: استعمال التكنولوجيات الرقمية كأداة لانتهاك حقوق الإنسان

التنمر الالكتروني على مواقع التواصل الاجتماعي و انعكاساته على المواطنة الرقمية

مشاهر زهرة ، مخبر الدراسات والبحوث الاجتماعية في الجزائر- جامعة الجيلالي اليابس سيدي بلعباس zahramechahar@gmail.com

هني زينب، مخبر الدراسات والبحوث الاجتماعية في الجزائر- جامعة الجيلالي اليابس سيدي بلعباس hennizineb113@gmail.com

الملخص:

ما ينفك الباحث في فهم التغير المتسارع الذي أحدثته التقنية خاصة في مجال التكنولوجيا الرقمية في المجتمعات المستهلكة ، حتى يجد نفسه في مأزق فهم وتحديد مظاهر الاستخدام السيئ لشبكات التواصل الاجتماعي ، ومن بين أشكال الاستخدام السيئ لهذه الشبكات التي نسعى للبحث فيها ، التنمر الالكتروني الذي أصبح ظاهرة متنامية تؤرق الباحثين و الساعيين للحفاظ على السلم و التعايش المشترك ، لذلك تهدف هذه الورقة البحثية إلى إبراز اثر الاستخدام السيئ لمواقع التواصل الاجتماعي كالتنمر الالكتروني و أشكاله المختلفة ، عدم تقبل الآخر و انتشار الكلمات العنصرية و الجهوية مثل "القهوي"التعبير الذي ظهر مؤخرا على مواقع التواصل و تأثيره على المواطنة الرقمية في ظل العيش المشترك.

الكلمات المفتاحية: التنمر الالكتروني، مواقع التواصل الاجتماعي, المواطنة الرقمية, المواطن الرقمي.

Abstract:

The researcher strives to understand the rapid change brought by technology, especially in the field of digital technology in consumer societies.

Until he finds himself in the dilemma of understanding the manifestations of the misuse of social networks

Among the forms of misuse of social networking sites, such as electronic bullying and its various forms, such as rejection of the other and the spread of racist and regional words such as “Kahoei", which means brown, the expression that appeared recently on social networking sites and the impact of this digital citizenship and coexistence.

Keywords: electronic bullying,CitizenshipDigital,digital citizen,Social Media.

مقدمة:

إن امتلاك الوسائل الالكترونية و فتح حسابات حقيقة أو وهمية أصبح ميزة العصر، و أصبح استخدام تلك المو اقع و ما يبث فيها محل اهتمام أغلب أفراد المجتمع باختلاف مستواهم التعليمي، وباختلاف أعمارهم ، كل يستخدم مو اقع التواصل الاجتماعي حسب اهتمامه و هدفه من الاستخدام، فالتكنولوجيا حولت العالم إلى قرية صغيرة، وأصبحت العلاقات الاجتماعية افتراضية في كل أنحاء العالم باختلاف القيم والعادات والتقاليد ، وتعد القيم واحدة من القضايا التي دار حولها جدل كبير نتيجة التغيرات السريعة التي يشهدها المجتمع ،ولاسيما مع تنامي موجات العولمة وما ر افقها من تطورات هائلة في تكنولوجيات الإعلام و الاتصال ، التي وضعت على بساط البحث والتحليل والمقارنة الثقافات والهويات والمنظومات الاجتماعية و القيمية ... ’فمع كل هذا التطور في وسائل الاتصال الرقمي ظلت القيم هي الأكثر عرضة للهدم وإعادة البناء من جديد ، والعالم كله يسير في اتجاه نوع من التفسخ والتكون القيمي، وتنعكس سلبياتها على الفرد نفسيا واجتماعيا خاصة عندما تمس وتخل بقيم و قو انين المجتمع خاصة عندما تمس قيم المواطنة على اختلاف صورها وأشكالها ما يمثل مشكلة كبرى تواجه المجتمعات الحديثة، وخطراً حقيقيا يهدد مستقبل أجيالها، لذا فقد زاد حرص المجتمعات المتطورة على تعليم قيم المواطنة خاصة المواطنة الرقمية لأبنائها وترسيخ مفاهيمها، بهدف مواجهة تنامي مشكلات ،التنمر الالكتروني، خطاب الكراهية، العنف الرقمي ، ولتدعيم منظومة القيم وقواعد السلوك الرشيد في المجتمع، وهذا الحرص ليس بمحض الاختيار، بل هو واجب وطني و فردي , خصوصا و أنه أصبح لا يوجد فرد لا يستخدم مو اقع التواصل الاجتماعي , فعلى كل مستخدم الوعي بأهمية الاستخدام الأمثل للتقنية في الفضاء الافتراضي من أجل تحقيق مواطنة رقمية فعالة، وكما قال "مارتن لوثر كينغ " يجب علينا أن نتعلم العيش معا كإخوة، أو نهلك جميعا كالحمقى..."، لذلك وجب التحرك بشكلٍ جديّ لمُواجهة هذا النوع من الخِطاب من خلال إعادة النظر في ضو ابط الإعلام ومضمونه ، وهذا ما يفرض علينا كباحثين الاهتمام ودراسة هذه التحديات ونتائج هذه التكنولوجيا وما تطرحه هذه الثورة من تحولات وتغييرات على مستوى مجتمعاتنا العربية و الإسلامية ، دراسة علمية منتظمة ، وتأتي أهمية هذه الورقة البحثية من أهمية موضوعها فالعالم يعيش اليوم ثورة ضخمة في تكنولوجيا الاتصال التي بدأت تدفع إنسان اليوم إلى رحلة اغتراب جديدة يخبو فيها الإحساس بالزمن ويتصدع لها الوجدان ، وتتضمن هذه الورقة البحثية :

1. مدخل مفاهيمي
2. التنمر الالكتروني عبر مو اقع التواصل الاجتماعي
3. انعكاسات التنمر الالكتروني على المواطنة الرقمية

1. مفاهيم الدراسة:

1.1 التنمر الالكتروني:

يعبر التنمر ظاهرة موجودة في جميع المجتمعات منذ زمن بعيد لدى الأفراد حيث تمارس أشكال مختلفة بدرجات متفاوتة عندما تتوفر الظروف المناسبة ، و يعد التنمر الالكتروني من أنواع التنمر الحديثة التي تحول فيها التنمر من البيئة الاجتماعية إلى البيئة الافتراضية عبر أدوات التواصل الاجتماعي المختلفة، فتحولت الظاهرة إلى نطاق واسع و أشد خطورة نظرا للانفتاح الشديد و الغموض و المجهولية المتاحة للشخص المتنمر مما جعل التنمر الالكتروني يأخذ موقع الصدارة في مظاهر التنمر المتنوعة[i].

عرف بلبيسلي و هو أول من صاغ مصطلح التنمر الالكتروني بأنه" استخدام تقنيات المعلومات و الاتصالات لدعم سلوك متعمد و متكرر وعدائي، من قبل فرد أو مجموعة التي تهدف الى إيذاء أشخاص آخرين , أو هو مضايقات و تحرشات عن بعد باستخدام وسائل الاتصال الالكتروني من طرف متنمر يقصد بها إيجاد جو نفسي لدى الضحية يتسم بالتهديد و القلق"[ii].

و يعرف التنمر **Bulliyin** بصفة عامة على انه أفعال عدوانية متعمدة تقوم بها مجموعة أو فرد بشكل متكرر ضد ضحية لا تستطيع الدفاع عن نفسها بسهولة ، و يتخذ التنمر حسب " الووس" شكلين مختلفين هما:[iii]

-التنمر المباشر يشمل الاعتداءات التي ترتكب علنا ضد الضحية هي اعتداءات جسدية أو لفضية أو نفسية كالاهانة و الضرب و التهديد ،السخرية الإذلال.

-التنمر النفسي فهو الأكثر ضررا ، فانه يعمل على مستوى العلاقات و يتميز بالاستبعاد من المجموعة الإقصاء الاجتماعي أو العزلة الاجتماعية.

-ويعرف التنمر الالكتروني بأنه: " شكل من أشكال العدوان، يعتمد على استخدام وسائل الاتصال الحديثة وتطبيقات الانترنت) الهواتف الذكية، الحاسب المحمول، الألواح، كاميرات الفيديو، البريد الالكتروني، صفحات الواب، في نشر منشورات 'بوستات' أو تعليقات تسبب التنكيد للضحية، أو الترويج لأخبار كاذبة أو إرسال رسائل إلكترونية للتحرش بالضحية، بهدف إرباكه وإصابته بحالة من التنكيد المعنوي و المادي"[iv].

2.1..مو اقع التواصل الاجتماعي :

مصطلح يطلق على مجموعة من المواقع على شبكة الإنترنت ظهرت مع الجيل الثاني للويب ، أو ما يعرف باسم الويب 0.2 تتيح التواصل بين الأفراد في بيئة مجتمع افتراضي يجمعهم حسب مجموعات اهتمام أو شبكات انتماء (بلد ، جامعة ، رسائل ، مدرسة ، شركة) ، كل هذا يتم عن طريق خدمات كالتواصل المباشر مثل إرسال الرسائل أو الإطلاع على الملفات الشخصية للآخرين ، ومعرفة أخبارهم ومعلوماتهم التي يتيحونها للعرض..

- ويعرف كل من Nicole Ellison و danah Boyd مواقع التواصل الإجتماعي بأنها " خدمات داخل الشبكة تسمح للأفراد ببناء ملف يعرضونه على جميع المستخدمين الذين يختارونهم ، يتم ذلك في إطار نظام إلكتروني محدد ، يحمل هذا الملف أو الحساب قائمة من المستخدمين الذين يختارهم صاحبه ليطلعوا على محتويات ملفه [vi]

وهي عبارة عن مواقع أو تطبيقات تبدأ بإنشاء الشخص المستخدم حسابا على أحد مواقع التواصل الاجتماعي ، فيسبوك، تويتر ..، ضمن نطاق شبكة الإنترنت العالمية،وينتج له قاعدة بيانات شخصية ومنصة انطلاق و وجود إلكتروني وشخصية افتراضية،لنشر البيانات و التعليقات و الوثائق و الرسائل و الصور و الأفلام و الفيديو ..، ومن ثم الانتقال إلى مرحلة التشارك مع الأصدقاء.[vii]

- إنها شبكات اجتماعية تفاعلية توفر للمستخدمين فرصة إنشاء ملفات تعريفية شخصية، تسهل بينهم عملية الاتصال والتفاعل الاجتماعي مع إمكانية جمع أكبر عدد من الأصدقاء الجدد والقدامى ضمن مجال تشاركي متعدد يتاح في تبادل الملفات، الصور، الفيديوهات ...وما إلى ذلك من أغراض، وفي الوقت نفس تجعل من الفرد مستقبل أو مرسال أو صانع للرسالة العالمية وهو ما يتيح فرصة التعبير، الإخبار، الاحتجاج ضمن حرية نسبية [viii].

-تمثل مواقع التواصل الاجتماعي تحولا راديكاليا في الثقافة المعاصرة، حيث تتوسع الكثير من الأنشطة الاجتماعية والإنسانية، في ظل قيام هذه الوسائل على فكرة دمقرطة المضامين وتكريس نموذج متعدد الأطراف، أي دور الأفراد في إنتاج المضامين وتقاسمها وبثها، وسقوط نموذج الاتصالالعمودي؛ فهي تحول فكرة البث الأحادي الجانبي إلى نموذج التبادل الجماعي، الذي يجد مشروعيته في الشكل التحاوري القائم بين صاحب الفكرة و المتفاعلين معه.

3.1.المواطنة الرقمية:

1.3.1 مفهومها : المواطنة الرقمية هي قواعد السلوك المناسبة والمسؤولية المتعلقة باستخدام التكنولوجيا، وتشمل محو الأمية الرقمية وأخلاقيات التعامل وآداب السلوك والسالمة على الإنترنت، والقواعد المنظمة، والحقوق، والمسؤوليات، وغيرها من الأمور المتعلقة بالأساليب المثلى للاستخدام التكنولوجيا الحديثة ، والمواطنة الرقمية الصالحة تحدث عند الاستخدام الإيجابي الأمثل لأجهزة الكمبيوتر والإنترنت والأجهزة الجوالة، وهذا سوف يعزز بيئة إلكترونية إيجابية أكثر أمنا وسالمة للجميع، وتعد إدارة ومراقبة سلوكيات الفرد على الإنترنت من العناصر المهمة في المواطنة الرقمية الجيدة، فمع التكنولوجيا الحديثة المتاحة الآن للعديد من الأفراد وخاصة الأطفال والمراهقين، أصبح هناك طلب متزايد لإعداد أبنائنا لاستخدام هذه التكنولوجيا بأمان وبصورة قانونية وأخلاقية في الأنظمة المدرسية والجامعية وفي جميع نظم ومهن المجتمع.[ix]

تستمد "المواطنة"أسلوب تطبيقها تبعا لطبيعة المرحلة التي ترافقها، وما تتضمنه هذه المرحلة من متغيرات، وعليه فان "المواطنة" تتخذ أشكال ، وصور مختلفة تنسجم و طبيعة العصر ، و مع ظهور التقنيات الرقمية، و سيطرة العالم الافتراضي الرقمي الذي شكل مجتمعا رقميا خاصا لدى الفرد الذي يعيش فيه وسط أجواء

إيجابية كسهولة الحصول على المعلومة، سهولة التواصل الرقمي مع الآخرين ، وعليه فإن هذه التطورات وما رافقها من بروز ثقافة التواصل الاجتماعي جعلت من مفهوم "المواطنة" والمفاهيم المرتبطة بها كالوطن والمواطن يأخذون صفة جديدة وصورة حديثة تختلف عما كانت عليه قبل هذه التطورات.[x]

2.3.1.أسباب الاهتمام بمواطنة الرقمية: ينبغي الاهتمام بمواطنة الرقمية في الفترة الحالية والقادمة للأسباب التالية:[xi]

*ظهور بعض العادات السلبية المرتبطة باستخدام وسائل التكنولوجيا الحديثة.

*الإدمان الالكتروني.

*الأمراض النفسية مثل العزلة والانطواء لدي بعض مستخدمي أجهزة التواصل الحديثة بدرجة مبالغ فيها .

*ازدياد معدلات الجرائم المرتبطة باستخدام أجهزة التكنولوجيا الحديثة، مثل التنمر الالكتروني اختراق حسابات البنوك، والتطرف والإرهاب الالكتروني، والجاسوسية باستخدام التكنولوجيا.

*إهدار معظم الوقت أمام الشاشات الالكترونية مما أثر على الناتج العام.

*إهمال المهام الاجتماعية

*عرض المواد الإباحية على شبكة الانترنت .

*التقاط صور فوتوغرافية غري مناسبة باستخدام كاميرات الهواتف .

* استخدام مواقع الانترنت في تهديد الأفراد وعمليات النصب والسرقة وإجراء بعض العمليات التخريبية.

4.1. المواطن الرقمي:

في ظل الطفرة الرقمية المتسارعة، برز مصطلح المواطن الرقمي، الذي أطلقه الأستاذ الجامعي مارك برينسكي، ليشير إلى الأفراد الذين ولدوا و ترعرعوا في عصر التكنولوجيا المتقّدمة التي شكلت أجهزة الكمبيوتر و ألعاب الفيديو والهواتف المحمولة أبرز الملامح المميزة له، ولفت إلى أن الأشخاص" الأشخاص الرقميين"اليوم يمثلون الشباب الملمين باستخدام التكنولوجيا الحديثة على نطاق واسع في إطار الحياة اليومية سواء لإغراض الدراسة أو التواصل الاجتماعي أو الترفي أو التسلية، والمواطن الرقمي هو الذي لديه القدرة على استخدام الانترنت في أعمال بشكل منتظم وفعال، و يعرف المواطن الرقمي بأنه شخص لديه وعي ومعرفة بالتكنولوجيا، مع القدرة على تطبيق تلفك المعرفة إلى سلوكيات وعادات وأفعال، يمكن من خلالها التعامل بشكل لائق مع الآخرين [xii].

كما أصبح لزاما على "المواطن الرقمي" الإفادة من الحرية المتاحة له على "الشبكات الاجتماعية"، لغرض إرساء الدعائم الأخلاقية ، وذلك عن طريق:

- تحمل مسؤولياته الأخلاقية اتجاه المتداول الرقمي في المجال العام الافتراضي .

-ممارسة اهتمامات مشتركة مع الآخرين.

- مراعاة المنظومة الثقافية للمجتمع الذي ينتمي إليه المستخدم الرقمي زمانيا ومكانيا .

-العمل على خدمة المجال العام بصورة هادفة.

وعلى ضوء ذلك فإن الجمع بين المهارات المعرفية ، و الوجدانية، و ة النفسية و الاجتماعية، و التكنولوجية، وتفاعلها ينتج مواطنا رقميا مثاليا للقرن الحادي والعشرين.[xiii]

2. التنمر الالكتروني على مو اقع التواصل الاجتماعي :

يعتبر التنمر الالكتروني من أخطر أنواع التنمر من حيث الصعوبة في اكتشافه و قد يتولد عنه أثار جسيمة، و هو استخدام الوسائل الالكترونية لإيذاء الضحية مثل وسائل التواصل الاجتماعي و حيث يتم نشر معلومات شخصية عن الضحية أو إرسال رسائل تهديديه و تخويفية عبر تلك الوسائل[xiv].

1.2.أسباب التنمر الالكتروني:

يمكن تلخيص أهم الأسباب التي أدت إلى انتشار ظاهرة التنمر الالكتروني والتي يمكن تقسيمها إلى أسباب ذاتية وأخرى اجتماعية وأسباب مرتبطة بالإعلام والثورة التقنية في النقاط التالية:

1.1.2.الأسباب الذاتية: وتتلخص أهم الأسباب الذاتية في الغضب من الآخرين والانتقام والإحباط والغيرة من الأقران، بالإضافة إلى الرغبة في جدب الانتباه ودلك من اجل قبول من أقرانهم وفي بعض الأحيان يقومون بدلك من اجل المتعة والترفيه،ذلك لأنهم يشعرون بالملل نظرا لوجود وقت فراغ غير مستثمر .

2.1.2.الأسباب الاجتماعية: وتتمثل في :

*المناخ الأسري: تساهم الأسرة في تشكيل شخصية الأطفال والمراهقين وتؤثر على خبرتهم المستقبلية ، إلا أن انشغال بعض الأسر من متابعة ومراقبة بعض سلوكيات أبناءها وتربيتهم التربية السليمة قد يؤدي التنمر الالكتروني إلى ظهور بعض السلوكيات التي تتسم بالعنف والعدوان اتجاه الآخرين ، وخصوصا إذا كان الجو الأسري المحيط يتسم بالصراعات والعنف النفسي والمادي وسوء المعاملة للمراهق، مما يزيد احتمال إقدامه على ممارسة العنف والتنمر على الآخرين، وكذلك وجود المراهق بين والدين يعانون من اضطرابات ومشكلات نفسية وسلكية يزيد من مقدار تعرضه للتنمر التقليدي والالكتروني، ومن الملاحظ أن متابعة الأسر للأنشطة التي يمارسها أبنائهم عبر الأجهزة الحديثة ومعرفتهم للمواقع التي يتصفحونها ويقضون معظم أوقاتهم بها تساعد في انخفاض فرص تعرضهم للتنمر الالكتروني.[xv]

*مجموعة القران: تساهم مجموعة الأقران في كثير من الحالات من فرص تعرض المراهق للتنمر الالكتروني، ودلك نتيجة لنوعية العلاقات وأساليب المعاملة داخل هده المجموعة فالمعايير والأنظمة التي تحكم الجماعة ترتبط بالممارسات التي يقوم بها أفرادها، مما قد يزيد من فرص العدوان والعنف وعدم تقبل بعض الأفراد

المنتمين لها وكراهيتهم، فالأقران من الممكن أن يكونوا من ضمن المشاهدين للأساليب ووسائل التنمر التي تمارس على الضحية عبر الوسيلة الالكترونية فهناك تفاعلات غير مسؤولة وذات طابع سلبي موجود بين الأقران تؤدي إلى زيادة مستويات التنمر الالكتروني[xvi].

3.1.2.الأسباب الفردية:

التي تتعلق بالمتنمر من جهة ومن جهة أخرى بالضحية، فمن جهة المتنمر يلجئ للعنف للتعويض عن التوتر والقلق الذي ينتج عن عدم الثقة بالنفس، وبالنسبة للضحية فإن عدم الثقة بالنفس تزيد من نسبة استهداف الآخرين له لعدم قدرته على الرد، كما يمكن إرجاعه للتنشئة الأسرية و طريقة التربية حيث أن التساهل في التربية وعدم عقاب الأطفال على أخطائهم، والتذبذب في اتخاذ القرارات وعدو الاتفاق على أسلوب معين في الثواب والعقاب بين الوالدين الذي يؤدي إلى الاختلاف على القوانين في المنزل، والقسوة والعنف في التربية و استخدام العقاب الجسدي كأسلوب للعقاب من قبل الأهل ، كما تؤدي إلى وجود أطفال متنمرين مع أقرانهم في المدارس .

-إضافة إلى ذلك فإن المستوى التعليمي للوالدين يأثر في انتشار ظاهرة التنمر الالكتروني، حيث أظهرت الدراسات أن انخفاض المستوى التعليمي للوالدين له أثر سلبي على سلوكيات أطفالهم في المدارس إما كمتنمرين أو ضحايا، كما تلعب المدرسة دورا في انتشار التنمر الالكتروني ، فالطلبة والمراهقون يتسمون بكثرة النشاط و الحركة أكثر من غيرهم، لذلك يجب استثمار هذا النشاط في أمور إيجابية وأنشطة تحفز مهاراتهم الحياتية والتقنية، حيث أظهرت الدراسات أن البيئة الدراسية التي تفتقر إلى لأنشطة التي تستثمر أوقات الفراغ عند الطلبة وتلبية احتياجاتهم النفسية و الاجتماعية ينتج عنها طلبة يلجئون إلى العنف كوسيلة لتفريغ الشحنات السلبية و الضغط النفسي .[xvii]

كما أظهرت الدراسات أن الرفقة السيئة ورغبة الطالب في الانتماء لمجموعات معينة من الأقران تؤثران على تحديد سلوكياته، كما أن مشاهد العنف وخاصة مشاهد المصارعة الحرة والأفعال العنيفة التي توحي بأن هذه السلوكيات تزيد من قوة الشخص وهيبته أمام الناس وشعوره بالبطولة، بالإضافة إلى ألعاب الفيديو والكمبيوتر التي تجسد مظاهر العنف ، وحوادث إطلاق النار و التفجيرات تلعب دورا في زيادة نسبة العنف في المدارس ومنها ممارسة التنمر والتنمر الإلكتروني[xviii]

- أشارت دراسة ريتشارد " أن التنمر الالكتروني وليد تكنولوجيا الاتصالات الحديثة التي نشرت مشكلات التنمر، لتصبح من المشكلات التي يجب مواجهتها و مراجعة القوانين و تعديلها للتخفيف من أثار التنمر الالكتروني و وضع الخطط للمدارس و الجامعات و الأسر لتأسيس استخدام امن لوسائل الاتصالات ، و هو ظاهرة اجتماعية مرفوضة من المجتمع و تنشر العنف و العدوانية فيه.[xix]

2.2. النظريات المفسرة للتنمر الالكتروني:

لما كان التنمر الإلكتروني هو نوع من السلوك العدواني الذي قد يأخذ شكل أو أكثر من أشكال الإيذاء كقصد إيذاء شخص آخر، باستخدام وسائل أو أفعال كاستخدام تكنولوجيا المعلومات والاتصالات لدعم سلوك متعمد ومتكرر وعدائي، بهدف إيذاء فرد أو مجموعة أفراد يكون الغرض منها هو الإيذاء والعدوانية، كما يتطلب المهارة في استخدام وسائل الاتصال الحديثة وهي ظاهرة تحدث في كل أنحاء العالم، ويمتلك المتنمر قوة يمتاز فيها عن المتنمر عليه تتمثل في إمكانية التخفي وصعوبة ملاحقة المتنمر في كثير من الحالات، لذا سنقوم بعرض الاتجاهات النظرية المفسرة للتنمر الالكتروني و نذكر منها:

*نظرية الإحباط أو العدوان

:أشهر علماء هده النظرية" نيل ميلر"،"روبرت سيزر"،"جون دولارد"،"سبينسي" وينصب اهتمام أصحاب هده النظرية على الجوانب الاجتماعية للسلوك الإنساني، والمبدأ الجوهري في هده النظرية وجود علاقة سببية بين الإحباط والعدوان بحيث أن مثير الإحباط يمثل عاملا مسببا لاستجابة العدوان، فاذا منع الإنسان من تحقيق هدف معين شعر بالإحباط وتولدت لديه استجابة العدوان التي ينقلها مصدر آخر سواء بطريقة مباشرة أو غير مباشرةأكد" دولارد وميلر وسيرز" أن الإحباط ينتج دافعا عدوانيا يستثير سلوك إيذاء الآخرين وأن هذا الدافع ينخفض تدريجيا بعد إلحاق الأذى بالشخص الأخر ، حيث تسمى هذه العملية بالتنفيس أو التفريغ لأن الإحباط يسبب الغضب والشعور بالظلم ما يجعل الفرد مهيأ للقيام بالعدوان، و ترى هذه النظرية أن سلوك العدوان ينتج عن الإحباط أي أن الإحباط هوالسبب الذي يسبق أي سلوك عدواني.[xx]

*نظرية التعلم بالملاحظة:

يعد" ألبرت باندورا "رائد هده النظرية ويرى أن العدوان سلوك متعلم مثله مثل غيره من أنواع السلوك الأخرى،ويشير إلى أن أساليب التنشئة الاجتماعية والتربية تلعب دورا مهما في تعلم الأفراد الأساليب السلوكية التي يتمكنون عن طريقها من تحقيق أهدافهم، فالسلوك متعلم ويعزى ذلك إلى أن الفرد يتعلم الكثير من أنماطه السلوكية عن طريق مشاهدتها عند غيره، فالأطفال يتعلمون السلوك العدواني عن طريق ملاحظة النماذج العدوانية عند أبائهم ومدرسيهم وأصدقائهم وغيرها من النماذج، ومن ثم يقومون بتقليدها ، ويميز أصحاب هذه النظرية بين اكتساب الفرد للسلوك وتأديته له، فاكتساب الفرد للسلوك لا يعني بالضرورة انه سيؤديه وأن تأديته للسلوك النموذج تتوقف على توقعاته من نتائج التقليد وعلى نتائج السلوك،فاذا توقع أن تقليده لسلوك النموذج سيعود عليه بنتائج سلبية بمعنى انه سيعاقب على سلوكه فانه لا يميل إلى تقليده لهدا السلوك،إما إذا توقع الفرد أن تقليده لسلوك النموذج سيعود عليه بنتائج ايجابية فان احتمالات تقليده لهدا السلوك تزداد[xxi].

كما **ترى** هذه النظرية أن العدوان والتنمر الإلكتروني هو نوع من العدوان الذي يعتبر سلوكا مكتسبا، فعندما يعتاد الفرد على مشاهدة سلوكيات تعكس التنمر بأشكاله المختلفة ومنها الإلكتروني، سوف يقوم بتقليد ذلك وهذا هو ما يؤدي إلى شيوع سلوك التنمر الالكتروني لدى الأفراد.

3.2. أشكال التنمر الالكتروني :

يعتبر التنمر الالكتروني من الظواهر الحديثة نسبيا التي نشأت من استخدام العالم الافتراضي (الانترنت) لتكوين علاقات اجتماعية و ممارسة أنشطة الحياة، و يجب دراستها و تسليط الضوء عليها لما لها من أثار نفسية و اجتماعية تعود على الشخص المتنمر و الضحية في نفس الوقت و كذلك على المجتمع ، و انتشار هذه الظاهرة تؤدي إلى وجود أنماط سلوكية غير سوية في المناخ الاجتماعي وتظهر على صور و أشكال متعددة نذكر منها:

***الرسائل العدائية**: وتشير إلى معارك على الانترنيت باستخدام الرسائل الإلكترونية مع لغة غاضبة ومبتذلة.

***المضايقة:** وتشير إلى إرسال رسائل مسيئة ومهينة وقاسية للضحية عبر البريد الإلكتروني.

***تشويه السمعة**: إرسال شائعات بهدف تشويه سمعة الضحية.

***انتحال الشخصية**: يتظاهر المتنمر الإلكتروني بأنه شخص أخر و يقوم بإرسال و نشر المواد الالكترونية لجعل الضحية في ورطة.

***إفشاء الأسرار**: وتشير إلى تقاسم أسرار شخص ما أو معلومات محرجة أو الصور عبر الانترنت.

***الاستبعاد**: ويشير إلى قيام المتنمر بعمد وقسوة باستثناء شخص من جماعة على الانترنيت.

***المضايقة الإلكترونية**: تشير إلى المضايقات المتكررة والشديدة والتشويه الذي يتضمن تهديدات أو يخلق خوف كبير، كان يقوم باختراق الحساب الشخصي للضحية ويقوم بإرسال الشائعات السيئة إلى أصدقاء الضحية، وصور جنسية موحية أنها تم تبادله معه شخصيا عبر المناقشة، وذلك جنبا إلى جنب مع عنوان البريد الالكتروني و رقم الهاتف الخلوي للضحية.[xxii]

المتأمل لتركيبة المجتمع الجزائري يلاحظ مدى تنوع واختلاف ثقافته، لغته، أسلوب عيشه من منطقة لأخرى, و يلاحظ ظاهريا ممارسات توحي بالتسامح وقبول الآخر و احترام خصوصيته الثقافية ,لكن الملاحظ لبعض الممارسات على مواقع التواصل الاجتماعي تنفي تماما هذا الطرح،فقد أصبح الفيسبوك مثلا منبر لممارسة العنف و التنمر الالكتروني و فضاء لبث خطابات و ممارسات تنم عن العنف و الكراهية و السب و الشتم وانتهاك خصوصية الغير ، والنظر إلى كل من يختلف عن الآخر من حيث الولاية أو لون البشرة على انه أقل منه شأنا و متخلف و دوني , فينعته بعبارات "العروبي", " القليط", " القهوي", و التمييز على أساس الهوية أو اللون أو النسب أو الجنس ، فأصبح يلجئ المستخدم غير سوي للفيسبوك لممارسة التنمر الالكتروني الذي قد يخشى ممارسته في الواقع خوفا من العقاب القانوني فيلجئ إلى التنمر الالكتروني كحل بديل ، فقد عرفت مثل هذه الممارسات انتشارا أكثر في الفضاء الافتراضي حيث أصبح منصة لنشر رسائل معادية و مضامين التنمر الالكتروني، وهذه نماذج منها :

منشور Ikram Bendjillali

Wissem Mechri
رقصة الجواري بنكهة 2022
يوم الأحد أعجبني رد ١

Kaprisa Kaprisa
تعيفي
الخميس أعجبني رد ٢

Ladybug Ladybug
نعلق قبل ما ينوضوا هذوك القهوين لي ضاربين الصاروخ و الكاشيات و يتبع في جارتو الصغيرة أمبعد كي ينوض يقولك إتقى الله في يوم الجمعة يا اختاه شعب غيور على اكرام
الخميس أعجبني رد ٨

عرض الردود السابقة (٩)

Walid Medkou... Rodrigo Alvaro

Fatiha Boudrafe
La khti chawhtina Allah ya3tik mosiba
يوم الأحد أعجبني رد ١

منشور ميلة جوهرة الشرق

يوم الأحد أعجبني رد ٢

Rä Hïm
زعما برك اسخايلو معايا كون جاو تع ميلة تابعين ل قسنطينة 😁 و يبدا ميلي يقول حنا كسنطينة عاصمة الشرق و كرارم و شلغوم مهم هانا عيشناكم حلم تعكم في سطر دكا نرجعو الكلمة أولا .... 😁
يوم الأحد أعجبني رد ٩

Mb Bk ربي يشافيك صديقي Rä Hïm

Ïbřâ Hïm Hãlí Mï
نتاع ميلة كي يروحو لجيجل 🤣🤣🤣🤣

يوم الأحد أعجبني رد ١٢

عرض الردود السابقة (٤)

Ïbřâ Hï... Abdelkrim Bouslimane

منشور شرات ومعاني مقصودة

الاقربون اولى
٢٣ ساعة أعجبني رد ١٤٠

عرض الردود السابقة (٥)

Hamza Ben لا... Lakhfar Nessah

جلول الرحمانى
يظهر لي مصطلح القهوي راه انتشر بزاف في المجتمع الجزائري بحيث أصبح كل من سلك سلوكا سيئا ينادى بالقهوي وهذا من التنابز بالالقاب
المنهي عنه الذي من شأنه احداث الضغائن وإغارة
الصدور وتغيير المنكر لا يكون بالسخرية من الآخرين والتشهير بهم الله يهدينا
يوم الأحد أعجبني رد ٦٧

عرض الردود السابقة (٩)

Marwa Ouali جلول الرحمانى كلمة ي...

Mimti Benti
عيب عليك حاسب روحك حاجة جايح أنت وبهلول واصلا اديت الأذن منو باش تصورو ياربي نشوفوك في كاش لايف
٢١ ساعة أعجبني رد ٢٣

منشور ميلة جوهرة الشرق

ميلة جوهرة الشرق ...نتي س Lou Bna

Jøšhûá Røšší
قالك تاع ميلة كي يحب يزوخ يقولهم انا من قسنطينة سيرتو تاع شلغوم
٢٣ ساعة أعجبني رد ٦

Jøšhûá Røš... Moussa Bouzeraa

Souheïl Öz
نتوما تاع ميلة تحلو عينيكم الصباح تجيو تجريو لكسنطينة تباتو تحلمو بيها وكي تروحوا تحكيو لصحابكم وتجي تضحك عليها تحير
يوم الأحد أعجبني رد ٣٠

Sof Bougie
اماجينو قسنطينة لوكان عندهم لبحر شاف ربي لصلاح يازح 😂😂😂
يوم الأحد أعجبني رد ٣

Siradje Kerroud
قالك تع ميلة مزالو يصورو ب سويت سالفي
يوم الأحد أعجبني رد ٢٣

Rðwânë Ŕđẁâñe
يحصراه قسنطينة كبيرة عليكم بزاف
يوم الأحد أعجبني رد ٢

3. التنمر الالكتروني و الاستخدام السيئ لمو اقع التواصل الاجتماعي و تأثيره على المواطنة الرقمية:

رغم الآفاق الواعدة لتكنولوجيا الاتصالات والمعلومات في العصر الرقمي في العديد من المجالات و التي غيرت وشكلت حياتنا وعلاقاتنا بشكل كبير، سواء مع أنفسنا أو مع الآخرين فإنها قد قللت من الأنماط المباشرة للاتصالات والمحادثات البشرية، وتسببت في العديد من الآثار السلبية، نتيجة إساءة الكثيرين استخدامها، فهناك حاليا شبكة الإنترنت، والأجهزة والهواتف الذكية الحديثة المزودة بالكاميرات، ومواقع التواصل الاجتماعي، مثل الفيسبوك و التويتر وخدمة الرسائل النصية وغرف الدردشة و تبادل الرسائل عبر البريد الالكتروني، التي قد أثرت على علاقاتنا الإنسانية وتواصلنا واتصالنا المباشر ودفعت الأفراد إلى الاقتراب أكثر إلى أجهزة الكمبيوتر والإنترنت والهواتف الجوالة ،والابتعاد عن بعضهم البعض فمثال الهواتف الجوالة الذكية التي نحملها في كل مكان، تكون أول شيء بين أيدينا في الصباح وآخر شيء في المساء ، وفي الآونة الأخيرة بدأ البعض في إساءة استخدام الحرية المتاحة على المواقع الإلكترونية ومواقع التواصل الاجتماعي على شبكة الإنترنت، من خلال نشر معلومات مضللة أو تغريدات مسيئة تتعمد الإهانة أو الإساءة لشخصيات أو مؤسسات الدولة، من خلال إرسال رسائل تهديد أو تشهير إلكترونية أو تعليقات مسيئة، أو الحصول على معلومات أو صور من أجل ابتزاز الآخرين، الأمر الذي يؤدي إلى عواقب وخيمة تضر بالفرد وبالصالح العام، أو الدخول على المواقع الإلكترونية غير اللائقة وغير أخلاقية، أو المواقع الإلكترونية التي تتضمن محتويات وتيارات فكرية ضارة تمثل تهديدا للهوية الثقافية ، و في ظل غياب المسؤولية وعدم وجود عقوبات صارمة ورادعة، وصل الحد لدى ضعاف النفوس إلى استخدام كاميرا الأجهزة والجوالات الذكية الحديثة في التقاط بعض الصور للنساء والفتيات سواء في الأماكن العامة أو المدارس والجامعات،ونشرها عبر مواقع التواصل الاجتماعي، والتي تؤدي إلى مخاطر ومشاكل إلى ما لا يحمد عقباها.

كما تأخر المشرع الجزائري في تقنين الجرائم المتعمقة بالتحريض على الكراهية ونشر العنف عبر موقع التواصل الاجتماعي التي أضحت لغة العصر، لكن استخدامها وانعدام الرقابة هو الذي يفتح الباب واسعا لتأويلات التي لا طائل من ورائها خاصة ما حدث بمواقع التواصل الاجتماعي خلال الحراك الشعبي بالجزائر وأيضا خلال الانتخابات الرئاسية التي انعقدت في 12 ديسمبر 2019 ،متناسين وعي الشعب وإصراره على التغيير، فالمشرع الجزائري لم يقم إلا بتعريف خطاب الكراهية ولا بإيجاد وسائل رادعة و قوانين قمعية لوسائل التواصل الاجتماعي.[xxiii]

-كل هذه الأمور والآثار السلبية لسوء استغلال أجهزة الاتصالات والتكنولوجيا الحديثة،أصبحت في حاجة عاجلة إلى نشر برامج ودروس جادة في التربية الرقمية المتمثلة في ثقافة وآداب التعامل المناسب والأمثل مع مثل هذه التقنيات، من خلال تنظيم محاضرات وندوات وحلقات نقاشية وورش عمل لجميع أفراد المجتمع، وخاصة بين الأطفال والشباب في المدارس والجامعات، تتناول إيجابيات وسلبيات الاتصال وكيفية الاستفادة المثلى من التقنيات الحديثة وآداب التعامل معها، وذلك من حيث الحماية والحفاظ على الحياة الخاصة للآخرين، والمسؤولية وحدود حرية الفرد، ومراعاة حقوق الآخرين، والتثبت من صحة المعلومات المتاحة على شبكة

الإنترنت، وحقوق الملكية الفكرية، واحترام القوانين، مع ضرورة استخدام هذه الأجهزة والهواتف الذكية الحديثة في إرسال رسائل توعوية للأفراد، لاستخدامها الأمثل، وتجنب استخدامها في إيذاء وتتبع وانتهاك خصوصية الآخرين والتجسس عليهم.

-إن الكثير من الجرائم المعلوماتية يتم ارتكابها عن جهل بالقواعد والنظم أو تتم من دون قصد الإساءة،وذلك للاستخدام الخاطئ لأجهزة الاتصال الحديثة، فالكثير من الأفراد قد يقومون بالاطلاع الكافي على ما ستقدمه البرامج والتطبيقات المختلفة بالأجهزة و الهواتف الذكية من خدمات، وتكون المفاجأة أن هذه التطبيقات والبرامج قد تتوغل أكثر في خصوصياته، وتصبح متاحة على الإنترنت ولتحقيق هذه الأهداف، ظهر في الآونة الأخيرة مصطلح المواطنة الرقمية Citizenship Digital كمفهوم حديث في التربية الرقمية، يهدف إلى إيجاد الأساليب والطرق والبرامج والأنظمة المثلى لتوجيه وحماية جميع مستخدمي التكنولوجيا، وخصوص الأطفال والمراهقين، وذلك بتحديد، من البداية، الأمور الصحيحة والخاطئة في التعامل مع التكنولوجيا الحديثة، لتشكل جدار حماية لجميع الأفراد، وخاصة أن التحكم فيما يطلع عليه الأطفال والمراهقون على الإنترنت وأجهزة الهواتف الجوالة قد أصبح أمراً مستحيلاً عمليا.. وذلك سوف يؤدي إلى خلق المواطن الرقمي الذي يحب وطنه ويسعى ويفكر لخدمته ومصلحته وحمايته، فهو يستخدم التكنولوجيا الحديثة بصورة أمثل، وخاصة مواقع التواصل الاجتماعي، لخدمة وحماية مجتمع هو وطنه بعيدا عن الإساءة والتشهير بالآخرين.[xxiv]

-إن التطور الكبير الذي يشهده العالم من الناحية الرقمية والتكنولوجية أدى إلى ثورة تقنية حقيقية، فقد أصبحت التقنية من أساسيات الحياة كما بات التعايش معها ضرورة وحاجة ملحة لا غنى عنها، و أنتج هذا التطور جيلا نشأ وتربى على هذه التقنيات وهم ما نسميهم بالمواطنين الرقميين، كما صاغ مارك برينسكي Marc Prenskyوهو خبير تقنية أمريكي مصطلح**(المواطن الرقمي)** كونه ولد في العصر الرقمي و تعايش مع هذه التقنيات منذ طفولته فأصبحت جزءا رئيسا من حياته،
أما مستخدمي التقنية الذين تبنوا العديد من الجوانب التكنولوجية، فقد نسميهم المهاجرين الرقمين بالرغم من إتقانهم لها، لكنهم كمن يتعلمون لغة جديدة في مرحلة متأخرة من حياتهم، وبما أن المواطنين الرقميين هم من فئة الشباب والمراهقين ومعظمهم من الطلبة نجد أن التقنية تجذب انتباههم و تثير اهتمامهم ولهذا فهم الأكثر تمسكاً وتعلقاً بها، هناك نماذج كثيرة لسوء الاستخدام والاستغلال المتعلق بالتكنولوجيا سواء كانت في البيت أو المدرسة أو المجتمع بشكل عام، وفي ضوء هذه الاستخدامات السيئة تبرز الحاجة إلى تحديد الممارسات الملائمة وغير الملائمة، و وضع مبادئ وأسس صريحة و واضحة عند استخدام هذه التقنيات الرقمية لوجود عدد كبير من التحديات التي تواجه المواطنين الرقميين.

خاتمة:

أصبحت ظاهرة التنمر الإلكتروني من الظواهر الخطيرة التي تشهدها المجتمعات العربية منها الجزائر، حيث أصبحت تشكل هاجسا وقلقا للباحثين و الساعيين للحفاظ على السلم و التعايش المشترك، و لكافة أفراد المجتمع لما للتنمر الالكتروني من آثار نفسية و صحية و اجتماعية على الضحية ولما للتنمر الالكتروني من تهديد

للمواطنة الرقمية الأمر الذي ينعكس سلبا على المواطنة الفعلية في المجتمع ، لذا وجب الوعي بأهمية الاستخدام الأمثل لهذه المواقع و الوعي بأهمية المواطن الرقمي فنشر ثقافة المواطنة الرقمية أصبح ضرورة ملحة نتيجة لتزايد مستخدمي التقنية يوماً بعد يوم، فأصبحت التقنية من الأولويات كما تحولت حياتنا إلى حياة رقمية، وبسبب هذا التحول الرقمي في كافة ميادين الحياة تزداد الحاجة لتعزيز المواطنة الرقمية سواء كانت للمواطنين أو المهاجرين الرقميين في ظل انتشار سلوكيات غير ملائمة كالجرائم الإلكترونية بمختلف أنواعها مثل: انتشار المواقع الإباحية، جرائم التهديد والتحرش والابتزاز الإلكتروني، والتشهير الإلكتروني و يشمل السب والشتم, انتحال الشخصية، الاحتيال المالي، اختراق المواقع وسرقة البيانات، التطرف والإرهاب، الاستغلال الجنسي للقاصرين، ومن خلال ما مر معنا يمكن الخروج بالتوصيات التالية:

1-على مستوى الدولة يجب سن قوانين تجرم التنمر الالكتروني و العمل على تطبيق القوانين بحزم مثل قانون 05/20ضمن المادة 02 الذي يجرم كل أشكال التمييز ، وكذا تسخير الإمكانيات اللازمة لأجهزة العدالة ،و الحرص على متابعة عمل الآليات التي وضعتها الدولة للحفاظ على حقوق الإنسان ، من بينها المرصد الوطني للوقاية من التمييز و خطاب الكراهية .

2-على مستوى الشركاء الاجتماعيين بالأخص المجتمع المدني ،على الجمعيات العمل على تعزيز مبدأ احترام حقوق و حريات الآخرين على المستوى الرقمي كما على مستوى الواقع الفعلي ، بالعمل على ترسيخ ثقافة الاستخدام الأمثل للانترنت ، و ترسيخ ثقافة التسامح و العيش الرقمي المشترك، و بإجراء أيام تحسيسية حول أخطار الانترنت و نشر ثقافة المواطنة الرقمية.

3- على مستوى البحث العلمي و الجامعات يجب تفعيل التعاون بين الجامعات و المنظمات و مراكز البحث،بإجراء العديد من البحوث و الدراسات لمعرفة مستوى التنمر الالكتروني و أثاره المترتبة على المجتمع ككل، كما يحسب ملتقى حقوق الإنسان في المجتمع الرقمي واحد من الجهود البذولة من طرف الجامعة لدراسة و التوعية بأخطار الانترنت.

4-على مستوى الأسرة يجب على الوالدين الحرص على التنشئة الاجتماعية السليمة للأطفال بتربيتهم على قيم الدين الإسلامي ، و تجنب العنف في التربية لما له من أثار على الطفل ، و تحديد الفترة التي يقضيها الطفل و المراهق على شبكة الانترنت بالإضافة إلى مراقبة ما يشاهدونه على الانترنت ، و تربيتهم على ثقافة الإبلاغ خاصة فيما يتعلق بالتنمر و التحرش الالكتروني.

5- على المدرسة الجزائرية الحرص على تربية النشئ على أهمية المواطنة الرقمية و المواطن الرقمي بإدراجها في المناهج التربوية.

6-على مستوى الأفراد يجب أن يعي كل مستخدم للانترنت بأهمية سلوكياته الرقمية و تأثيرها على الآخرين ، فيتجنب الإساءة للآخرين و احترام حقوق الأفراد في المجتمع الرقمي.

7- على مستوى المنصات و المواقع الالكترونية خاصة بالنسبة لمسيري المنصات و المواقع و المجموعات على

صفحات التواصل الاجتماعي عليهم تقديم البلاغات على المحتويات التي تنشر التمييز و خطاب الكراهية و التنمر الالكتروني.

الهوامش :

[i] درويش محمد أحمد درويش و الليثي احمد حسن، (2017)، فاعلية بيئة تعلم معرفي سلوكي قائمة على المفضلات الاجتماعية في تنمية استراتجيات مواجهة التنمر الالكتروني لطلاب المرحلة الثانوية ،مجلة العلوم التربوية ، عدد04، مجلد 01، جامعة حلوان ، القاهرة ، ص352.

[ii] -خالد بن هايف خلف الرقاص،(2021)، التنمر الالكتروني و علاقته بالاتجاه نحو التطرف لدى عينة من طلاب الجامعة، كلية الآداب و العلوم الإنسانية، المجلة العربية للنشر العلمي ، العدد29، جامعة الملك عبد العزيز، المملكة العربية السعودية، ص449

[iii] -اقروفة صفية، (2022) ، برامج محاربة التنمر في الوسط المدرسي –برنامج كيفا ضد التنمر المدرسي نموذجا–، مجلة الرسالة للدراسات و البحوث الإنسانية، المجلد7،العدد4،ص352

[iv] -حاسي مليكة ،(2019)، التنمر الالكتروني دراسة في الأبعاد و الممارسات ، مجلة الإعلام والمجتمع، المجلد 04 ،العدد01،الجزائر، ص69

[v] - وائل مبارك ، خضر فضل الله ،(2010)، أثر الفيسبوك على المجتمع،مدونة شمس النهضة ، مصر ، ص 06

[vi] -Dominique, C. (2013). Réseaux sociaux de l'internet,. Consulté le 10 04, 201 , sur 9 http://formation.communautique.qc.ca/sites/default/files/document-identite-numerique.

[vii] – صونيه شتوان، يوسف بومدين، (2017)، اثر مواقع التواصل الاجتماعي على سلوكيات المستهلك اتجاه الأزياء الاسلامية، الأكاديمية للدراسات الاجتماعية والإنسانية ، العدد 02 ، المجلد 09 ،الجزائر ،ص31.

[viii] –نورية سوالمية، كلثوم صدراتي، (2021)، محددات العيش المشترك في ظل مواقع التواصل الاجتماعي،دراسة ميدانية على عينة من الطلبة الجامعيين، مجلة العلوم الإنسانية،المجلد10، العدد01، جامعة وهران، ص 38-39

[ix] –علي حسن بن شمس ندى ،(2017)، المواطنة في العصر الرقمي نموذج مملكة البحرين ، معهد البحرين للتنمية و السياسة ،البحرين، ص61

[x] –جيدور حاج بشير(2017) ،اثر الثورة الرقمية والاستخدام المكثف لشبكات التواصل في رسم الصورة الجديدة لمفهوم المواطنة من المواطن العادي إلى المواطن الرقمي ، مجلة دفاتر السياسة والقانون،العدد15 ، الجزائر ، ص798

[xi] -الملاح تامر المغراوي، (2017)،المواطنة الرقمية، دار السحاب للنشر و التوزيع، القاهرة ،ص 33

[xii] –عبد العزيز الأحمدي إيمان، (2020)، متطلبات إعداد المواطن الرقمي في ضوء رؤية المملكة العربية السعودية ، المجلة الأكاديمية للأبحاث والنشر العلمي، العدد17، ص 501.

[xiii] –جيدور حاج بشير ، مرجع سابق ، ص736

[xiv] –نورة بنت سعد القحطاني ، (2016) ،نورة بنت سعد القحطاني ، التنمر المدرسي و برامج التدخل ، مجلة ميادين ، كلية التربية جامعة الملك سعود ، الرياض ، العدد211، ص 120

[xv] – الصبان عبير محمد وآخرون،(2020) ، التنمر الإلكتروني لدى الطلبة المراهقين في بعض مدارس المرحلة المتوسطة والثانوية في مدينة جدة، المجلة العلمية، المجلد36 ، العدد التاسع ، جامعة أسيوط،مصر ،ص327

[xvi] – المرجع نفسه، ص328

[xvii] ––بن دادة سهيلة ، فريحة محمد كريم، (2021)، واقع ظاهرة التنمر الإلكتروني لدى المراهق الجزائري، مجلة المواقف للبحوث والدراسات في المجتمع والتاريخ،المجلد17، العدد01، جامعة برج باجي مختار ، الجزائر. ص355-356

[xviii]–المرجع نفسه ، ص 357

[xix]–حنان السيد عبد القادر زيدان، (2020)، التنمر الالكتروني و علاقته بالانتماء لدى عينة من طلاب كلية التربية النوعية ، مجلة كلية التربية، المجلد الثلاثون، العدد الرابع ، جامعة الاسكندرية، مصر ،ص263.

[xx]– محمود سعيد ابراهيم الخولي ،(2020) ،فعالية الإرشاد الانتقالي التكاملي في خفض مستوى سلوك التنمر الإلكتروني لدى طلاب ذوي الاحتياجات الخاصة، المجلة العربية لعلوم الاعاقة و الموهبة،العدد04،المجلد14، ص366

[xxi]– الدسوقي مجدي محمد،(2016)، مقياس التعامل مع السلوك التنمري، جوانا للنشر والتوزيع، القاهرة ،ص32

[xxii]– بن دادة سهيلة, فريحة محمد كريم، مرجع سابق ،ص354

[xxiii]–عبد المجيد عائشة، (2021)، تأثير مواقع التواصل الاجتماعي على انتهاك الخصوصية و انتشار خطاب الكراهية" ,دراسات حقوق الإنسان ، المجلد 05، العدد02، جامعة الطارف،الجزائر، ص70

[xxiv]علي حسن بن شمس ندى ، مرجع سابق ، ص60-61

تداعيات الأنترنت المظلم على الأمن الفردي والوطني

Les répercussions du darknet sur la sécurité individuelle et nationale

بوقاسم محمد أستاذ محاضر ب
جامعة الجزائر 02 – الجزائر
mohamed.boukacem@univ-alger2.dz

بوسنة وسيلة أستاذة محاضرة ب
جامعة البليدة 02 – الجزائر
Boucenna.awyy@gmail.com

الملخص:

لقد اتسم عصر المعلومات بتشكل مجتمعات وسلوكيات افتراضية، مما أدى إلى انتقال التفاعلات البشرية من الواقع المادي إلى الواقع الإفتراضي، وبالرغم من إيجابيات هذا الواقع الجديد، إلا أنه ينطوي في داخله على مخاطر تفوق كافة التصورات في إنتهاك حقوق الإنسان من أهمها تهديد أمنه الفردي، ولقد زاد الشعور بعدم الأمان في العديد من الدول بتزايد استعمالات الأنترنت المظلم في السنوات الأخيرة، حيث أنه يكفي بلمسة واحدة لشخص أو مجموعة أشخاص أن يلحقوا خسائر مادية وبشرية كبيرة، وأن يهددوا حياة الكثير من الأبرياء، إذ أصبح بإمكان المنظمات الإجرامية تبيض و غسل الأموال الناجمة عن أنشطتها، حتى أنهم لجؤوا إلى العملات الإفتراضية، وهذا ما ألحق الضرر بالأمن الاقتصادي للدول، بالإضافة إلى جرائم الإنتحار الجماعي للمراهقين وتجارة المخدرات والأسلحة، التي مست الأمن الاجتماعي للشعوب، من هذا المنطلق ارتأينا التطرق في هذه المداخلة إلى مختلف مجالات الأنترنت المُظلم ومحاولة معرفة كيف يمكن لها أن تؤثر على الأمن الفردي والوطني من خلال سرد حقائق معتمدين في ذلك على المنهجين التاريخي والوصفي التحليلي، وتفسيرها وتحليلها من أجل إدراك وفهم الحاضر على ضوء الأحداث السابقة والشواهد ، وكل هذا من خلال الإجابة على التساؤل المحوري التالي: كيف يؤثر الأنترنت المُظلم على الأمن الفردي والوطني ؟ وماهي الإجراءات الواجب اتخاذها للتقليل من هذه المخاطر؟

الكلمات المفتاحية: المجتمعات الافتراضية؛ الأنترنت المظلم؛ الأمن الفردي والوطني؛ الجرائم الإلكتروني.

Abstract

The age of information noticed a creation of virtual societies and behavior. This made humans move from reality to virtual reality, even if

this new reality has positive sides but it has also dangerous sides especially what concerns humans Rights and self security. people feel they're not safe these last years especially with the wide use of the deep web. It can cause a lot of damage to people and companies. Gangs for example use the dark web for their dirty business, they even use virtual currency which affects the economy, they can even use the dark web in weapons trade and drugs.

This leads to talk about different sides of the dark web and how it can affect the national security and self security so we can understand what's going on and try to answer the main question: How does the dark web affect national and self security and what procedures to take to limit its dangers?

Key words: virtual societies; dark web; national and self security; cyber crime.

مقدمة:

أولا - إشكالية الدراسة:

في إطار التعريف بموضوع الدراسة الحالية ، قامت العديد من الدراسات السابقة بإثبات وجود أثر للأنترنت المُظلم على الأمن، ولكن مجالات الأنترنت المُظلم كثيرة و قد اختلفت الدراسات في ما بينها من دراسة مجال واحد والتعمق فيه إلى دراسة بعض المجالات وضمها لمفهوم الأنترنت المُظلم، وباعتبار الأمن مفهوم واسع مرتكز على عدة أبعاد، فهناك دراسات تطرّقت إليه بصفة جزئية لمعالجة زاوية معينة وأخرى بصفة كلية،وللمواصلة في مسار البحث العلمي بالنسبة لهذا الموضوع فقد إرتأينا لفتح دراسة تضم مختلف مجالات الانترنت المُظلم ومحاولة معرفة كيف يمكن لها أن تؤثر على الأمن الفردي و الوطني من خلال أبعاده الأربعة، وذلك بطرح إشكالية جاءت صياغتها في السؤال الرئيسي التالي: **كيف يؤثر الأنترنت المُظلم على الأمن الفردي والوطني ؟** حيث تندرج تحت هذا السؤال المحوري مجموعة من التساؤلات الفرعية التالية:

1- هل يؤثر التجنيد الإرهابي عن طريق الأنترنت المُظلم سلبا على الأمن العسكري للوطن؟

2- هل تؤثر حرية التعبير والنشاطات السياسية عن طريق الأنترنت المظلم سلبا على الأمن السياسي للوطن؟

3- هل يؤثر تبييض الموال وبيع السلع الغير مشروعة عن طريق الأنترنت المُظلم سلبا على الأمن الاقتصادي للوطن؟

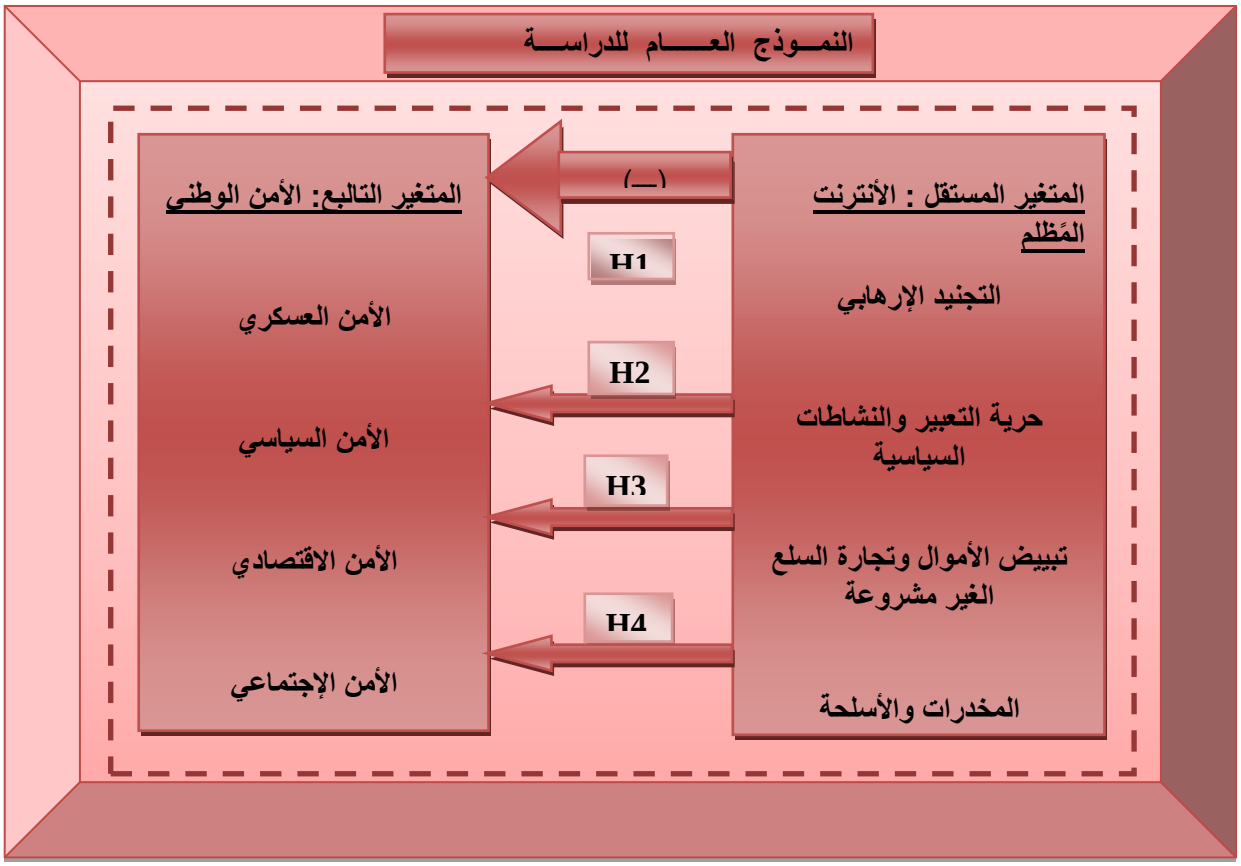
4- هل يؤثر بيع المخدرات والأسلحة عن طريق الأنترنت المُظلم سلبا على الأمن الفردي والاجتماعي للوطن؟

ثانيا – الفرضيات الرئيسية للدراسة:

بناءا على إشكالية الدراسة والتساؤلات الفرعية تمّ وضع الفرضيات التالية:

- ✓ **الفرضية الرئيسية الأولى :** يؤثر التجنيد الإرهابي عن طريق الأنترنت المُظلم سلبا على الأمن العسكري للوطن.
- ✓ **الفرضية الرئيسية الثانية:** تؤثر حرية التعبير والنشاطات السياسية عن طريق الأنترنت المظلم سلبا على الأمن السياسي للوطن.
- ✓ **الفرضية الرئيسية الثالثة:** يؤثر تبييض الموال وبيع السلع الغير مشروعة عن طريق الأنترنت المُظلم سلبا على الأمن الاقتصادي للوطن.
- ✓ **الفرضية الرئيسية الرابعة:** يؤثر بيع المخدرات والأسلحة عن طريق الأنترنت المُظلم سلبا على الأمن الفردي و الاجتماعي للوطن .

ثالثا - نموذج الدراسة :



إعتمدنا في الجانب النظري من الدراسة على المنهج الوصفي، الذي تمّ من خلاله عرض مختلف المفاهيم والتعاريف المتعلّقة بالظاهرة المدروسة والتي جمعناها من مصادر متنوعة.فيما يخصّ الجانب التطبيقي للدراسة اعتمدنا على المنهج التاريخي الاستنباطي يعني أننا انطلقنا من سرد وتحليل الأحداث الماضية لتداعيات الأنترنت المظلم على الأمن وذلك بأخذ شواهد من مختلف دول العالم،وصولا إلى استنباط خاص من خلال إسقاط ما تم تحليله في العام على دولة الجزائر كإطار خاص .

خامسا-حدود الدراسة:

وقع الاختيار على أهم الأحداث المشهودة في التاريخ، حيث تم أخذهم كإطار عام للإلمام بجميع الأحداث التي وقعت في العالم، والتي خصت تداعيات الأنترنت المظلم على أمن الدول، وباعتبارنا أننا اعتمدنا على المنهج التحليلي الاستنباطي، فإننا أخذنا دولة الجزائر كحدود مكانية، أما بالنسبة للحدود الزمنية فإن المنهج التاريخي يستوجب علينا الأخذ بالتسلسل الزمني للأحداث منذ بداية ظهور الأنترنت المظلم إلى يومنا هذا.

I. الإطار النظري للدراسة:

من أجل ضبط الدراسة نظريا وجب علينا التطرق إلى أبرز المصطلحات التي تم تداولها في مداخلتنا بالتعريف وقد جاءت كالآتي:

1. الأمن:

يعتبر الأمن حاجة أساسية في حياة الإنسان والتي من الضروري إشباعها حتى ينعم الفرد بحياة مستقرة، وهذا ما فطره الله علينا في قانونه الكوني ، حيث أن ترتيب حاجات خلقه الأساسية جاءت واضحة في كتابه الكريم لقوله تعالى " *فليعبدوا رب هذا البيت (3) الذي أطعمهم من جوع (4) وآمنهم من خوف (5)*" سورة قريش، وقوله تعالى " ادخلوها بسلام آمنين " آية 46 من سورة الحجر، وقول رسولنا الكريم "من أصبح منكم معافى في جسده، آمنا في سربه ، عنده قوت يومه فكأنما حيزت له الدنيا".

2. تعريف الأمن:

يُعرف الأمن من الناحية اللغوية أنه نقيض الخوف و يعني السلامة ، كما تعرفه أغلب القواميس على أنه" التحرر من الخوف والقلق"،وقد توصل ماسلوMaslow في نظريته حول هيكلة الحاجات، أنه يمكن ترتيب الحاجات على شكل هرمي، في قاعدته أقوى الحاجات

الإنسانية وأنه كلما أشبعت حاجة معينة، تطلع الفرد إلى إشباع حاجة أكثر تدرج منها، والشكل التالي يوضح موقع الحاجة للأمن بالنسبة لمجمل الحاجات الإنسانية.

الشكل رقم 01: تدرج الحاجات وفق هرم ماسلو

La source : Maslow Abraham : **Eupsychian Management**
Dorsey-Irwin ,Homewood, 1965

أما تعريف الأمن اصطلاحا فقد اختلف وتعدد حيث صعُب على الباحثين إعطاء مفهوم واحد وثابت، وذلك لإختلاف البيئة الأمنية للمفكرين واختلاف نوع التهديد وحدته، فلابد من إعادة تعريف الأمن في كل مرة يهدد فيها.حيث عرفه هنري كيسنجر بأنه " أي تصرف يسعى المجتمع عن طريقه لتحقيق حقه في البقاء"[1] ، كما عرف روبرت ماكنمارا الأمن " هو التنمية وبدون التنمية لا يمكن أن يوجد أمن ، والدول التي لا تنمو في الواقع ، لا يمكن أن تضل آمنة "[2]

2.1. مستويات الأمن:

يجب الإشارة أن الأمن ينطلق من الأمن الفردي للأشخاص ثم الأمن الجماعي لهم، ويمتد لضمان الأمن الوطني، وفيما يلي أهم تدرجات الأمن:

1.2.1 المستوى الأول: الأمن الداخلي Individual Security:

هو أدنى درجات الأمن وأساسها أيضا، وهو يعني بالحالة التي يوجد عليها الفرد من استقرار وطمأنينة، وهو ذو مظهرين، أحدهما مادي وهي مجالات الأمن الأساسية لدى الفرد من مأكل ومشرب وملبس ومسكن دائم والاطمئنان على حياته وأسرته من اعتداء الآخرين، أما المظهر الثاني فهو معنوي، يحقق الحاجات النفسية للإنسان من الاعتراف بوجوده وفائدته للمجتمع ، ونجد جوانب أخرى للأمن الفردي وهي عدم استغلال الإنسان لأخيه الإنسان ومحاربة الحريات[3]،وهو من مسؤوليات الدولة في تحقيق الأمن للشعب كأفراد و جماعات تربطهم علاقات (قرابة، جيرة،عمل....).

2.2.1. المستوى الثاني: الأمن الوطني National Security:

هو "توفير الحماية للمواطنين والأفراد المتواجدين على أراضي الدولة، ويُعرف أيضا بأنه استخدام الوسائل الأمنية للمحافظة على سير الحياة بشكل صحيح بعيدا عن وقوع أزمات تتسبب بأضرار بشرية ومادية للوطن"[4]، كما تم تعريفه أيضا بأنه " مجموعة من السياسات والتدابير المتخذة لسلامة إقليم الدولة والدفاع عن مكتسباتها ومواجهة الأعداء سواء كان ذلك في الداخل أو في الخارج وبغض النظر عن طبيعة التهديدات"[5].فهو مستوى مركب من عدة جزئيات فالأمن الداخلي لهذا المستوى يسمى الأمن المحلي والأمن الذاتي هو جزء من الأمن المحلي.

3.1. أبعاد الأمن الوطني :

يتميز الأمن الوطني بالشمولية، فهو ظاهرة مركبة متعددة الأبعاد، حيث تختلف قوة كل بعد منها باختلاف خصائص الدولة، وفيما يلي تقديم لأهم أبعاد الأمن الوطني:

1.3.1. البعد العسكري للأمن الوطني:

هو البعد الذي يعتمد على دور قوات الجيش ولا يسمح بضعفه أبدا، لأن ضعفه يُعرضه لأخطار وتهديدات قد تصل إلى حد وقوعه تحت الاحتلال الأجنبي، ومن أهم المؤشرات التي يمكن الاستناد إليها كمقياس لتحديد قوة الأمن الوطني من وجهة النظر العسكرية هي[6]: حجم الجيش، العوامل الجغرافية، القاعدة الصناعية العسكرية، مستوى التعليم والتدريب واللياقة البدنية التي يتمتع بها المقاتلون بالإضافة إلى قدراتهم الاستيعابية للسرعة الهائلة التي تتطور بها التكنولوجيا،حجم ونوعية الأسلحة.

2.3.1. البعد السياسي للأمن الوطني:

هو الذي يُحدد كيفية تنظيم وإدارة قوى الدولة ومواردها، فهو يرتكز على السياسة الداخلية والخارجية للدولة، فالمطلب الأساسي الذي تسعى السياسة الداخلية لتحقيقه هو الاستقرار في إطار الشرعية الدستورية وتوجيه التنافس للقوى الداخلية والإتجاهات السياسية لصالح الدولة، وضمان التماسك السياسي وعدم تشتته داخليا، أما السياسة الخارجية هدفها تأمين متطلبات السيادة الوطنية ومد نفوذها في المجتمع الدولي دون الخضوع لأي ضغوط خارجية، ولهذا يستوجب على الدولة إقامة علاقات دولية وإقليمية وعضوية أحلاف وعقد معاهدات و اتفاقيات، بما يخدم الأهداف الوطنية للدولة[7].

3.3.1. البعد الاقتصادي للأمن الوطني:

يرتكز هذا البعد على عدد من المؤشرات وهي[8]: حجم الناتج الإجمالي ،متوسط نصيب الفرد من الناتج القومي الإجمالي، حجم القاعدة الصناعية للدولة، حجم إنتاج مصادر الطاقة، حجم إنتاج المعادن الإستراتيجية أهمها(الحديد، النحاس ، الكروم ، المنغنيز...)، نسبة الأراضي المزروعة إلى حجم السكاني فهو يشكل دليل على نسبة الاكتفاء الذاتي، كما يشتمل على عناصر كثيرة تساهم في تحقيق مقومات الأمن كالأمن الغذائي والصحي والأمن المالي.

4.3.1. البعد الاجتماعي للأمن الوطني:

يدخل في إطار أمن المجتمع عدة عوامل وهي[9]: تلعب درجة التماسك الاجتماعي دور مهم في الوقوف كسد منيع في وجه القوى الطامعة ،المستوى الثقافي والتعليمي لأفراد المجتمع حيث أن المجتمع المتعلم والمُثقف يكون قادر على استخدام معطيات العلم والاستجابة للتطورات التقنية المختلفة ،الإرث الحضاري والتاريخي فالتاريخ المشترك عامل من عوامل الأمن الاجتماعي،مستوى الوعي وإدراك أهمية الأمن من قبل الأفراد.

2. الأنترنت المظلم:

قُسم الفضاء الافتراضي إلى مستويات وهذا التقسيم يحدث بالفعل وفقا لإمكانية الوصول إلى المحتوى، إنطلاقا من المستوى الأول الذي يمثل الأنترنت السطحي والذي يمكن الولوج فيه دون مشاكل عن طريق كلمات مفتاحية بسيطة في محركات البحث المشهورة، والمستوى الثاني الذي يمثل الأنترنت العميق والذي يتكون من محتوى غير مفهرس أو خاص

يصعب الوصول إليه، وصولا إلى الأنترنت المظلم الذي يمثل الأنترنت الخفي المكون من شبكات مظلمة متنوعة، والتي يمكن التعبير عنها من خلال رسم الجبل الجليدي التالي:

الصورة رقم 01 : تمثيل مستويات الأنترنت في الجبل الجليدي

1.2. تعريف الأنترنت المظلم:

الأنترنت المظلم هو محتوى الشبكة العنكبوتية العالمية الموجودة في الشبكات المظلمة الذي يستخدم الأنترنت، ولكنه يحتاج إلى برمجيات خاصة وتفويض خاص للولوج إليه، ويشكل الأنترنت المظلم جزء صغير من الأنترنت العميق الذي لا تفهرسه محركات البحث، حيث تتكون الشبكات المظلمة والتي تؤلف الأنترنت المظلم من شبكات صغيرة من نوع P2P ند للند، و شبكات ذات شعبية كبيرة مثل Tor و Freenet و I2P و يديرها أفراد أو منظمات عامة، حيث يعبر عن شبكة الأنترنت العادية باسم Clearnet الشبكة النظيفة الغير مشفرة، أما شبكات الأنترنت المظلم فتعمل على نظام التشفير.

2.2. محتويات الأنترنت المظلم:

للأنترنت المظلم عدة عناصر لعل أبرزها:

1.2.2. محركات البحث للأنترنت المظلم:

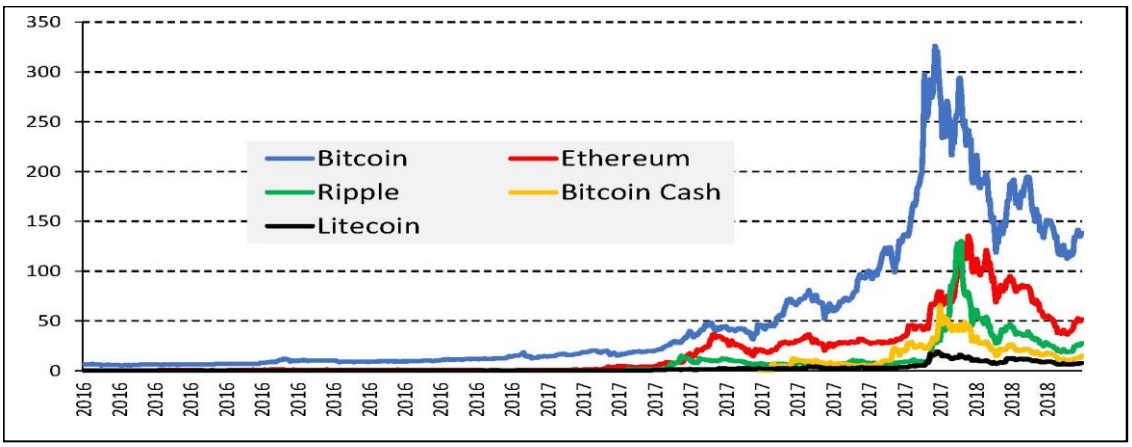
هي محركات بحث متخصصة في فهرسة مواقع الويب المظلم،ترتبط بالعديد من المواقع المخفية والخدمات المجهولة منها Not Evil الذي يعتبر أكبر محرك بحث في darknet بأكثر من

19 مليون صفحة مفهرسة[10]، و Grams الذي يعمل بنظام تصنيف لجلب أفضل المنتجات[11]، بالإضافة إلى محرك البحث World wide science وهو علمي مصمم لتسريع اكتشاف وتبادل المعرفة العلمية، يتيح الوصول إلى مجموعة متنوعة من الموارد المسجلة في شبكة الويب العميقة.

2.2.2. العملات الإفتراضية:

أصبحت العملات الإفتراضية تتحدى الأنظمة المالية بسبب عدم الكشف عن هويتها وطابعها العالمي ، وعدم إمكانية القيام بعملية فرض ضرائب على عمليات البيع والشراء للشركات والرسوم على الأفراد، مما يحد من دور المحاسبة وصعوبة تسجيل العمليات[12]، تُعرف الهيئة المصرفية الأوروبية العملات الإفتراضية بأنها " تمثيل رقمي للقيمة لا يصدر عن مصرف مركزي أو سلطة عامة ولا يرتبط بالضرورة بعملة (تقليدية)ويقبله الأشخاص الطبيعيون أو المعنويون كوسيلة للتبادل ويمكن تحويله أو تخزينه أو تداوله إلكترونيا"، أكثرها تداول عملة البيتكوين(Bitcoin) ، عملة الإثيريوم (Ethereum) صدرت في أواخر 2013 من طرف ButerinVitalik، عملة الريبل (Ripple)،عملة البيتكوين كاش (Bitcoin Cash)، عملة لايتكوين (Litecoin)[13].

الشكل رقم 02: قيمة العملات الإفتراضية في الأسواق الإستثمارية الكبرى بمليارات الدولارات الأمريكية من سنة 2016 إلى 2018



La source :Marek Dabrowski and Lukasz Janikowski : **Virtual currencies and their potential markets and monetary policy**, op-cit ,p20.

3.2.2. الأسواق السوداء (Cryptomarkets):

توجد على شبكة الويب المظلمة،حيث يمكنهم من الوصول إليها باستخدام برامج خاصة مثل متصفح Tor الذي يخفي موقع وهوية المستخدم،تستعمل هذه الأسواق خدمات البصل لاستضافة واجهات المحلات ومنتديات لمناقشة السلع والخدمات،كما أن إخفاء الهوية الذي توفره هذه الشبكة المظلمة للأسواق تجعلها نقاط ساخنة لتبادل غير قانوني للسلع، حيث يظهر كل سوق مشفر كواجهة ويب للمستخدم ويقوم بعرض فئات المنتجات للسلع المسروقة أو المقلدة ولأنشطة أخرى غير قانونية كالإرهاب والعقاقير الغير مشروعة والمخدرات والأسلحة والخدمات المتعلقة بالاحتيال وقائمة لكل منها، يوضح الجدول التالي أشهر سبعة أسواق سوداء:

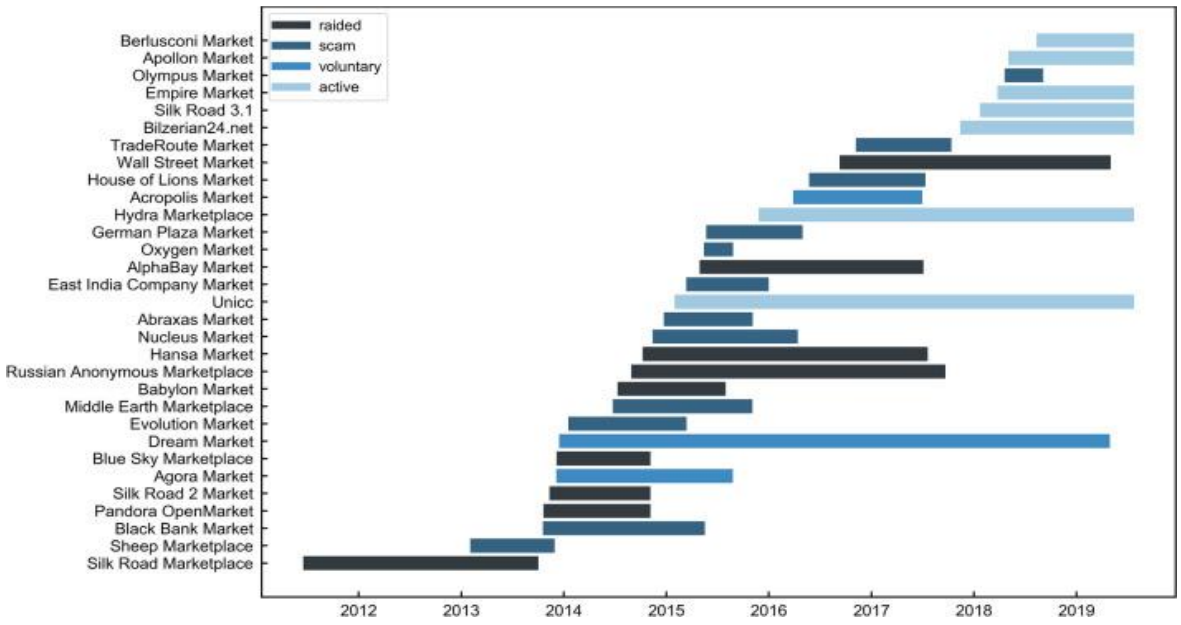
الجدول رقم 01 : أشهر أسواق السوداء في الأنترنت المظلم

Cryptomarkets	Listnings	Pourcentage
Dream	92,388	77,03
Wall street	8,902	7,42
Empire	9,947	8,42
Silkroad	718	0,60
Berlusconi	6,007	5,01
Tochka Point	1,442	1,02
Valhala	503	0,44

La source : Thero Carr,JunZuhuang,Dwight Sablan: **Into the Reverie: Exploration of the Dream Market**,
International conference of big data,2019,Cerist, p1434.

إن أهمية إخفاء هوية منشئي و مستخدمي وبائعي الأسواق المظلمة تؤثر على أعمار الأسواق المظلمة، حيث أن معظم منشئي الأسواق يلجئون إلى غلق المنصات الإفتراضية الخاصة بهذه الأسواق وفتح أخرى بأسماء مختلفة، والشكل المُبين أدناه يُحدد أعمار أهم الأسواق المُظلمة:

الشكل رقم 03: أعمار الأسواق المظلمة



La source :andrettiAbeerELBahrawy,LauraAlessandretti,**Collective Dynamics of Dark Web Market places**,12 janvier 2020, p05

I. الجانب التطبيقي للدراسة:

لقد عرض الأنترنت المظلم أمن الدول للخطر المادي والمعنوي،حيث أصبحت العلاقة بين التطور والتهديدات في المجال الالكتروني تتناسب طرديا، كلما زاد التطور زادت التهديدات، فضلا على أن الإنترنت المظلم عبارة عن ساحة فارغة من المراقبة والمتابعة يفر بها المجرمون بأفعالهم، ويتفقون على تنفيذها بدون أي رقابة أو تردد من أي جهة حكومية أو دولية،حيث تصاعدت عمليات الإجرام الالكتروني بشكل كبير في الفترة الأخيرة، وفيما يلي سرد للأهم الأحداث التي تُظهر لنا تداعيات الأنترنت المظلم من خلال مجالات استخدامه على الأمن الفردي والوطني:

1. تداعيات الأنترنت المظلم على الأمن العسكري:

1.1. الحرب السيبيرانية:

تمثل الحروب السيبرانية مدخلاً جديدا على نطاق الصراع الذي يمتد عبر مجالات اقتصادية وسياسية واجتماعية وعسكرية، إذ أصبحت الجيوش العسكرية في أنحاء العالم تهتم بحرب المعلومات أو ما يسمى بالحرب الإلكترونية التي لا تقل أهمية عن الحرب العسكرية، يمكننا القول بأن المعركة الإلكترونية تعزز الإتجاه إلى الهجوم، هذا الأسلوب من

شأنه أن ينمي فرص تصعيد الأزمات إلى حروب، وأن يجعل من فرضية كبح الحروب أكثر صعوبة مما يؤدي إلى تهديد الأمن العسكري الوطني،كما أن تكاليف دخولها منخفضة وفرص نجاحها عالية نسبيا ، تجعل من الأسلحة السيبيرانية وسيلة فعالة.ومن أبرز الأمثلة على ذلك عام 2008،هاجم المتخصصون في اختراق أنظمة الحاسوب مواقع الحكومة الجورجية على شبكة الأنترنت في الأسابيع التي سبقت اندلاع الصراع المسلح، وهذا الصراع بين روسيا وجورجيا يمثل أولى الهجمات السيبرانية (الإلكترونية) التي تصاحب صراعاً مسلحاً.وفي نفس العام انطلقت واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأمريكي، من خلال وصلةUSBبسيطة متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، ولم يتم اكتشاف انتشار برامج التجسس في كلا من الأنظمة السرية والغير سرية، وقد شكل هذا ما يشبه جسر رقمي، تم من خلاله نقل الآلاف ملفات البيانات إلى خوادم خارجية، كما نذكر كذلك مهاجمة منشآت نووية في إيران عام 2010 باستخدام فايروس "ستاكسنت"، وكانت كل الإشارات تدل على أن الولايات المتحدة وإسرائيل هي المسؤولة عن تلك المهاجمة ".[14]

2.1. المنظمات الإرهابية:

في 10 مارس 2007، تم نشر مقطع لأيمن الظواهري على أحد المواقع الشبكية،ينذر فيه حكومتي ألمانيا والنمسا بمواجهة العواقب في حال عدم سحب قواتها من بعثات دعم السلام في أفغانستان، حيث تم كشف مخططات لتنفيذ هجمات إرهابية في أوروبا[15]، ومن جهة أخرى استعمل الأنترنت المظلم لغرض تمويل هذه الجماعات الإرهابية التي ترصد الجمعيات الخيرية عن طريق أشخاص يمثلون واجهة لهذه التنظيمات، يقومون بجمع التبرعات لصالحهم ومن ثم تحويلها إلى عملات افتراضية يصعب تتبع أثار تحويل هذه الأموال، كما أشارت الخبيرة الاقتصادية و المحللة السياسية في مجال تمويل الجماعات الإرهابية Loretta Napoleoni ، أن الاقتصاد الجديد للإرهاب قدر ب 5,1 تريليون دولار من خلال التحويلات القانونية و الغير مشروعة و غسيل الأموال.

ومن خلال سرد الحقائق تم تأكيد الفرضية التي تنص على أن التجنيد الإرهابي يؤثر سلبا على الأمن العسكري.

2. تداعيات الأنترنت المظلم على الأمن السياسي:

1.2. حرية التعبير:

يمكن القول بأن حرية استخدام الأنترنت تجعل الحكومة أكثر عرضة للمساءلة أمام مواطنيها، كما تساهم في دمج المواطنين في عملية صنع السياسات، ومن أهم مستخدمي الإنترنت النشطاء السيبيرانيون الذين يستخدمون المواقع المحجوبة لتعبئة الآخرين وراء سبب معين أو للنهوض بجدول أعمال محدد[16].

ويكمن خطر حرية التعبير في هذا السياق بـ[17]:

- ✓ **الجهل بالهوية:** فالإنترنت تتيح لمستخدمي الرسائل ومنشئيها التستر خلف هوية مجهولة، وهذا يُسهل كثيرا من إنتاج واستهلاك مواد زائفة وغير قانونية وخطيرة، مثل المواد الإباحية وخطابات الكراهية والتحريض والكلام المسيء والاستفزاز التي قد تقوم بخلق العنف والتمييز والتأثير على الجمهور للتصرف بطرق معينة تخدم إتجاهات محددة.[18]
- ✓ **غياب مراقبة الجودة:** فبإمكان أي شخص تقريبًا نشر أي شيء على الإنترنت وخاصة المواقع المظلمة، حيث تنشر الادعاءات الواهية بنفس الدرجة من السهولة التي تنشر بها المقالات العلمية،كما لوحظ إطلاق مواقع شكاوى الغرض منها التعبير عن الشحناء بصورة تشهيرية التي لايمكن ظهورها في الصحف نتيجة الرادع القانوني.
- ✓ **الجمهور المحتمل الضخم:** فالإنترنت المظلم والمواقع المشفرة توفر الوصول إلى عدد كبير من القراء والمشاهدين المحتملين في جميع أنحاء العالم، ويمكن لهذا الأمر أن يزيد من حجم أي ضرر ناجم عن الكلام أو تعبير عن رأي.
- ✓ **عثور المعادين للمجتمع على أصدقاء لهم:** فبوسع ذوي الآراء الغريبة والغير المعتادة والدعايات الهدامة والخطيرة أن يعثر بعضهم على بعض بسهولة أكبر عبر الإنترنت المظلم، من خلال الانتساب إلى هذه المواقع، حيث أصبح لدى هؤلاء الأشخاص الشجاعة للتعبير عن آرائهم والإيمان بأفكارهم والتصرف على أساسها.

2.2. الصحافة:

تنبع أهمية الصحافة في تتبع شبكات الإجرام والفساد من سياسيين ورجال أعمال و فضحهم لدى العدالة والرأي العام من خلال استخدام الإنترنت المظلم كمصدر للمعلومات

والصفقات المخفية عن القانون ، أين ألف الصحافي الهولندي الشاب دانييل فيرلان 31 عاما كتابا تحت عنوان " أعرف كلمة مرورك" الصادر أخيرا في أمستردام فقد سبق لفيرلان المتخصص في الصحافة الاستقصائية الإلكترونية القيام بحملات صحافية جريئة في عالم الإنترنت المظلم و مجرميه ،حيث ألف كتابا يعتمد كل منها على قصة حقيقية من الحملات الصحافية الاستقصائية التي قام بها لصالح تلفزيون " RTLNews" الهولندي وأثبت دانييل فيرلان من خلال تحقيق استقصائي له أن نتائج الانتخابات الهولندية كانت سهلة الاختراق وأنه تم التلاعب إلكترونيا بنتيجة التصويت ما أدى إلى إعادة فرز جميع الأصوات يدويا، وفي 2018 نجح في اختراق شبكة إباحية انتقامية و أوقع أكثرهم في أيدي العدالة[19].

3.2. قراصنة الأنترنت المظلم:

تختلف الأسباب التي تدعوهم إلى القرصنة من مجرد الهواية إلى تحقيق مكاسب مادية دون بذل أي مجهود منها الاستيلاء على المخزونات النقدية للبنوك فضلا عن القرصنة الانتقامية التي غالبا ما تكون بين دول على إثر خلاف سياسي منها تهديد المنشآت الحيوية للدول كالمفاعلات النووية والقرصنة السياسية التي تتم من قبل ناشطين للسيطرة على مواقع سياسية وسرقة البيانات الحكومية والتي بدورها تعد إحدى آليات الاحتجاج السياسي ، حيث تعتبر مجموعة "أنونيموسAnonymous " على رأس مجموعات القرصنة لأغراض سياسية وهي منتشرة حول العالم تنتمي لجنسيات مختلفة تأسست عام 2003 تعمل في مجال النضال عبر الإختراق البرمجي وتتبنى مبدأ المعارضة الشديدة للرقابة على الإنترنت حيث اخترقت مواقع حكومية إسرائيلية وأمريكية وبريطانية وتركية واتخذت مواقف لثورات "الربيع العربي " 2010 ، فشنت هجمات إلكترونية انتقامية ضد مواقع رسمية تابعة لحكومات عربية[20]، كما اتهمت الولايات المتحدة روسيا بالتدخل في الانتخابات الأمريكية، وذلك عن طريق إنشاء مواقع وهمية على الإنترنت، تشبه البوابات الإلكترونية، واستغلال وسائل التواصل الاجتماعي، كما أعرب مسؤولون في قطاع الأمن الوطني في الولايات المتحدة الأمريكية أن إيران أيضا كانت مسؤولة عن إرسال تهديدات عبر البريد الإلكتروني للناخبين الديمقراطيين قبيل انتخابات الرئاسة الأمريكية 2020 ، كما أن التسريبات التي قام بها عميل الاستخبارات الأمريكية السابق إدوارد سنودن أعطت معلومات مفصلة عن أنشطة التجسس السيبراني، وسلطت هذه التسريبات التي عُرفت بوثائق ويكيليكس الضوء على أساليب وكالة الأمن القومي الأمريكي للتجسس داخل البلاد وخارجها، والتي شملت التنصت على دوائر حكومية

فيبلدان أخرى وزعماء أجانب، وأظهرت الوثائق قيام الاستخبارات الأمريكية بالتنصت على هاتف المستشارة الألمانية أنجيلا ميركل، ما تسبب بأزمة سياسية بين البلدين[21].

ومن خلال ماذكرنا سابقا تم تأكيد الفرضية الثانية التي تنص على أن حرية التعبير والنشاطات السياسية عن طريق الأنترنت المظلم تؤثر سلبا على الأمن السياسي.

3. تداعيات الأنترنت المظلم على الأمن الإقتصادي:

1.3. تجارة المخدرات:

إن معظم أعمار المتعاطين للمخدرات هم من فئة الشباب، مما سيؤدي إلى نقص كبير في الإنتاجية الفردية أو اضمحلالها، ويؤدي تعاطي المخدرات إلى إنفاق الكثير من الدخل العام للأسرة و الفرد، الذي يؤثر على الدخل المتاح للإنفاق على السلع و الخدمات المشروعة، وبذلك يعد نقصا في الإنفاق العام،مما يخلق حالة كساد في الإقتصاد الوطني، ويعتبر تعاطي المخدرات أيضا سببا من أسباب البطالة لدى الأفراد. إن تجارة المخدرات تستنزف أموالا طائلة من الدولة من حيث مجال مكافحتها من طرف الأجهزة المعنية كالشرطة و الجمارك وحرس الحدود، التي تسعى إلى منع عبورها إلى حدود الدولة ، وتتبع البائعين والمستهلكين ومصادر التجارة والترويج،ولقد صرحت "إيلفا يوهانسون" المفوضة الأوروبية للشؤون الداخلية أنه "حيثما تشيع الجرائم المرتبطة بالمخدرات، فغالبًا ما تكون هناك جرائم منظمة، وتنشط 5000 منظمة إجرامية في أوروبا، أكثر من ثلثها متورط في تجارة المخدرات كما أن الإتّجار بالمخدرات يموّل الجريمة المنظمة بمبالغ مالية تصل قيمتها إلى 30 مليار يورو سنويا والاتجار الغير مشروع بالمخدرات هو أكبر سوق للمنظمات الإجرامية داخل دول الاتحاد الأوروبي".كما أوضح تقرير للأمم المتحدة أن "جائحة فيروس كورونا قد دفعت بالمتاجرين في المخدرات إلى إيجاد طرق وأساليب جديدة، فمن المحتمل أن تزداد الأنشطة الغير مشروعة عبر الإنترنت وتهريب المخدرات ضمن شحنات بواسطة البريد.[22]

2.3. غسيل الأموال:

تعتبر عملية المغسلة الروسية أشهر جريمة لغسل الأموال كشف عنها المهربون في تحويل مايقارب 200 مليار دولار إلى خارج روسيا خلال الفترة 2010-2014 عن طريق شبكة من البنوك العالمية ،حيث شملت عملية الغسل 70 ألف عملية مصرفية مع 1920 شركة معظمها وهمية في بريطانيا والولايات المتحدة الأمريكية[23].

وعليه تم تأكيد الفرضية الثالثة التي تنص على أن تبييض الأموال والسلع الغير مشروعة تؤثر سلبا على الأمن الاقتصادي.

4. تداعيات الأنترنت المظلم على الأمن الإجتماعي:

1.4. تجارة الأسلحة:

قال Lyburd"إن شراء مسدس جلوك كان أشبه بشراء قطعة من الشوكولاتة" كان هذا من التقرير حول Liam Lyburd18 سنة الذي أعد للقيام بمجزرة في مدرسته السابقة و قتل زملائه في نيو كاسل (أخبارBBC News) 30 جويلية 2015 وقد تم تحذير الشرطة من قبل صديق بشأن رسائلLyburdعلى الفايسبوك تحت الإسم المستعار Felix Burns والتي أشارت إلى خططه حيث داهمت الشرطة سكنه واكتشفت مسدس الجلوك ومئة طلقة وقد تم الحصول عليه من الأنترنت المظلم على السوق المشفرة Evolution. يأتى السلاح بأنواعه المختلفة فى المرتبة الثانية على مواقع الإنترنت المظلم ويتم تصنيفه داخل قوائم متعددة بداية من المسدسات الصغيرة إلى الكلاشنكوف والبنادق الآلية والقنابل الصغيرة ، كما يوجد صفحات لبيع الذخيرة بأنواعها وأشكالها، فالإنترنت المظلم يساعد فى ترويج السلاح بين المواطنين خاصة فى الدول التى تفرض قواعد صارمة على بيع وامتلاك سلاح لهذا أصبح المواطنون يلجئون لتلك الموقع التى تضم عشرات الآلاف من الصفحات الخاصة بالسلاح، وكل ما على المستخدم فعله الدخول والبحث والدفع عن طريق زر الشراء.[24]

2.4. المخدرات الرقمية:

هناك مواقع متخصصة تقوم ببيع هذه النغمات على مواقع الإنترنت وللأسف الشديد لا توجد رقابة رسمية عليها في الوقت الحالي حيث عرف العالم العربي المخدرات الرقمية عام 2012م وانتشرت تحديدا في دولة لبنان والمملكة العربية السعودية أين تناقلت الأوساط السعودية خبرا عن تسجيل أول حالة وفاة جراء تعاطي "المخدرات الرقمية " على الرغم أن الدولة رفعت مستوى التأهب للحد من وصول هده المخدرات إلى المجتمع عبر الإنترنت وفي الوقت ذاته نوهت الحكومة اللبنانية بضرورة زيادة وعي الأهالي لمثل هده الأنواع من المخدرات كما دعت جهات حكومية لبنانية مختلفة لحجب المواقع الإلكترونية التي تقوم بتسويق وبيع هده الموسيقى[25].

3.4. المنظمات الإرهابية:

"برينتونتارنت" شاب البالغ من العمر 28 عاما ،كان عضوا نشطا في مجتمع اليمين المتطرف على الإنترنت في منصة تسمى 8 chan، وهي عبارة عن منتدى غير مراقب ينشر صورا تحث على الكراهية والعنصرية الساخرة، حيث قام بشن هجوم إرهابي أطلق النار من خلاله مستهدفا مسجدين في مدينة كرايستشيرش جنوبنيوزيلندا والذي أسفر عن مقتل 49 شخصا .وعليه تم التأكد من الفرضية الرابعة التي تنص على أن بيع الأسلحة والمخدرات عن طريق الأنترنت المظلم يؤثر سلبا على الأمن الاجتماعي. كما أن التجنيد الإرهابي والتحريض يؤثر أيضا سلبا على الأمن الاجتماعي. إضافة إلى ما سبق ذكره توجد هناك مجالات أخرى لم نتطرق إليها بالتفصيل كتجارة الأعضاء البشرية ومنتديات القمار وفيديوهات التعذيب والإتجار بالبشر والطقوس الدينية والدعارة.

الخاتمة:

إن سرد أحداث ووقائع تاريخية مرتبطة بالدراسة، ساعدتنا في إظهار وتأكيد علاقة الأثر التي سمحت لنا بالإجابة عن التساؤلات الفرعية من خلال إختبار الفرضيات المشتقة من نموذج الدراسة؛ وقد توصلنا من خلال هذه الدراسة إلى جملة من النتائج لعل أبرزها:

- يعمل الأنترنت المظلم في مجال تقني خاص به بعيد عن كل حالات المراقبة والمتابعة.
- يلجأ الأفراد إلى هذا الأنترنت لأنه يتيح لهم امكانية التخفي والقيام بالأعمال التي تعود عليهم بمكاسب مالية أو انتقامية أو غيرها من الدوافع.
- يتضمن الأنترنت حالات كثيرة من الجرائم والتهديدات الإلكترونية التي تهدد أمن الفرد والدولة.
- يمثل أمن الفرد الكترونيا أمن الدولة، لأن أمن الدولة مقترن بأمن الفرد.
- أصبحت العلاقة بين التطور التكنولوجي والتهديدات في المجال الإلكتروني تتناسب طرديا، حيث أنه كلما زاد التطور التكنولوجي زادت التهديدات الأمنية.
- تؤثر سلبا كل مجالات إستخدام الأنترنت المظلم على أبعاد الأمن الوطني.
- تداخل الأثر بين مجالات استخدام الأنترنت المظلم وأبعاد الأمن، حيث نجد مجال استخدام معين يؤثر على أكثر من بعد.

من أهم التوصيات والإقتراحات التي تصب في سياق الموضوع نجد:

يجب اتباع بروتوكول خاص أي نهج منتظم في التحقيق في الجرائم المرتكبة و اختراق الشبكات المظلمة وذلك بـ:

✓تشخيص السوق من خلال خلق قواعد بيانات لتجار الشبكة المظلمة ، ففي كثير من الأحيان هم نفس التجار الذين ينتقلون بين أسواق المخدرات المختلفة أو المختصة في تجارة الأعضاء البشرية وعندها يمكن بناء الملفات الشخصية للأفراد (البروفايلات تدريجيا) .

✓وضع مواقع مزيفة على الشبكة المظلمة لاستدراج الأشخاص الراغبين بخدمات غير شرعية.

✓ جمع البيانات عبر أساليب التحقيق التقليدية و البحث عن معلومات إضافية متاحة عبر خدمات الإنترنت بالإضافة إلى تقديم طلبات خادم بروتوكول الإتصال الصوتي عبر الأنترنت.

✓ القيام بالتعطيل على الإنترنت من أجل التسلل إلى الأسواق المشفرة وإقفالها.

✓ توفير حوافز أو مكافآت مغرية من أجل تشجيع الأشخاص الذين شاركوا في مجموعات إجرامية منظمة على التعاون مع وكالات إنفاذ القانون من خلال توفير الرؤى والمعلومات المفيدة كما هي في الواقع أي في الساحة الملموسة.

✓فرض التنظيم الرقابي لمقاهي الإنترنت وذلك بتطبيق تدابير تشريعية أو تنظيمية مخصصة تلزم مشغلي مقاهي الإنترنت بالحصول على وثيقة هوية تحمل صورة فوتوغرافية من زبائنهم إضافة إلى عناوين إقامتهم وبيانات الاستخدام والاتصال الخاصة بهم والاحتفاظ بكل ما سبق وتقديمه إلى جهات إنفاذ القانون عند الطلب.

✓يجب إتباع نهج وقائي استبقائي يعني قبل حدوث الكارثة الإجرامية.

✓وجوب توعية المجتمع المدني على أخطار الأنترنت المظلم بمختلف مجالاته ، والتي تمس كافة أبعاد الأمن الوطني.

الهوامش:

[1] Henry Kissinger ,Nuclear Weapons and foreign policy, wild field and Nicholson, London,1969, p. 46.

[2] McNamara ,The essence of security Harper press , New York, 1966, p.149.

[3] Tashtoush, Hayel Abdel-Mawla , National Security and elements of state power under the new world order , first edition, Dar al-hamid for publishing and distribution , Amman Jordan, 2012,p 22.

[4] خالد علي محمد الأميري و أحمد فلاح العموش، الأمن الوطني : المفهوم، الأبعاد و النظريات، مجلة الآداب، العدد 133، 2020 ، ص529.

[5] عبد المعطي زكي، الأمن القومي قراءة في المفهوم والأبعاد، المعهد المصري للدراسات السياسية والإستراتيجية ، فيفري 2016 ، ص2.

[6] هايل عبد المولى طشطوش ، الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد، سلطنة عمان ، الطبعة 2013 ، ص 66-69.

[7] Ghali Boutrous , Issa Mahmoud Khairy : Introduction politics, First edition, The Anglo Egyptian library, Cairo, 2010, p244.

[8] هايل عبد المولى طشطوش ، الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد ، مرجع سابق الذكر ، ص 81-83.

[9] هايل عبد المولى طشطوش، الأمن الوطني وعناصر قوة الدولة في ظل النظام العالمي الجديد ، مرجع سابق الذكر ، ص 144-146.

[10] Sécurité informatique , www.funinformatique.com , 13.06.2022

[11] https://www.wired.com. 13.06.2022.

[12] بن عوالي الجيلالي ،بلمشري بشرى، المحاسبة عن العملات الإفتراضية (نماذج مقترحة)، مجلة البحوث في العلوم المالية و المحاسبة، مجلد05، العدد 01 ، 2020، ص164.

[13] بن عوالي الجيلالي ،بلمشري بشرى، المحاسبة عن العملات الإفتراضية (نماذج مقترحة)، مرجع سابق الذكر ، ص 165-166.

[14] أولاف تايلور، التهديدات الجديدة (الأبعاد الإلكترونية)، مجلة الناتو، دون سنة نشر، www.nato.int/docu/review/2011/11- september 08 جوان 2022.

[15] مكتب الأمم المتحدة المعني بالمخدرات والجريمة بالتعاون مع فرقة العمل التابعة للأمم المتحدة المعنية بتنفيذ تدابير مكافحة الإرهاب، استخدام الإنترنت في أغراض إرهابية، الأمم المتحدة نيويورك، جوان 2013 ،ص. 86

[16] Olesya Tkacheva,LowellH.Schwarts and others, Internet Freedom and Political Space , National Defense Research Institute, US Department Of State

[17] نايجل ووربيرتن، حرية التعبير، مؤسسة هنداوي للنشر، القاهرة، 2013. ص. 80

[18] نجاة السعيد ، حرية التعبير والأمن القومي والقانون، 12مارس 2019، حرية التعبير والأمن القومي والقانون | الحرة (alhurra.com) ، 04 جوان 2022.

[19] عماد فؤاد ،الشبكة العميقة مرتع القراصنة والجريمة الإلكترونية ،27 نوفمبر 2020 ، الشبكة العميقة: مرتع القراصنة والجريمة الإلكترونية(alaraby.co.uk) ، 03 جوان 2022.

[20] مجلة الأيام السورية ، القرصنة الإلكترونية (الوجه المظلم للتطور التقني) ، 21فيفري 2019، القرصنة الإلكترونية.. الوجه المظلم للتطور التقني - الأيام السورية(ayyamsyria.net) ، 07 جوان 2022.

[21] مجلة العلوم و التكنولوجيا، الحرب السيبيرانية تهديدات حقيقية من العالم الإفتراضي، 15 مارس 2019، الحرب السيبرانية.. تهديدات حقيقية من العالم الافتراضي(aa.com.tr) 10 جوان 2022.

[22] يورونيوز، تجارة المخدرات عرفت انتشارا عبر البيع بواسطة الانترنت في أوروبا، 23 سبتمبر 2020 https://arabic.euronews.com/my-europe/2020/09/23/report-finds-abundant-supply-of-illicit-drugs-in-eu، 15 جوان،2022

[23] شادي الزعيم، فضيحة غسيل أموال تفوق 200 مليار دولار تهز بنوكا عالمية، 22 نوفمبر 2018، فضيحة غسيل أموال تفوق 200 مليار دولار تهز بنوكا عالمية(alarabiya.net) ، 17 جوان 2022

[24] جوديث ألدريدج وأخرون، خلف الستار(التجارة عير المشروعة بالأسلحة النارية و المتفجرات و الذخيرة على الأنترنت المظلم)، مؤسسة Euorpe Rand للنشر والتوزيع،2017 ،ص1-3

[25] مستشفى الأمل للطب النفسي وعلاج الإدمان، علاج إدمان المخدرات الرقمية، علاج إدمان المخدرات الرقمية(hopehospital.com.eg) ، 15، جوان، 2022.

الرقابة الرقمية بين الأمن والقمع

Digital Surveillance between Security and Repression

عيساوي فاطمة
أستاذة محاضرة أ/ جامعة البويرة
fatmaaissaoui550@gmail.com

عبد العزيز حكيمة
أستاذة محاضرة ب/ جامعة بومرداس
abdelaziz.abdelaziz5216@gmail.com

ملخص

أحدث التطور التكنولوجي تحولا في النظام القانوني لبعض الحريات المكرسة قانونا، ولعل أظهر الحريات تعرضا للتحول حرية التعبير وحرية الرأي وحرية التجمع السلمي، والحق في الخصوصية، حيث سمحت الوسائل الرقمية بتغيير النظام القانوني لممارستها، سواء من حيث مدى الحرية ونظام المسؤولية الذي يخضع له الناشر وصاحب الموقع، أو من حيث الحدود التي تقع على ممارستها بدافع حماية النظام العام والأمن القومي؛ فالمجال الرقمي ليس مجالا خارج القانون، إنما يخضع لسلطة الدولة التي تُخضِع النشاط الرقمي للرقابة، لكن قد تكون هذه الرقابة وسيلة للقمع والاستبداد الذي يتخذ الأمن بمدلوله الواسع وغير المنضبط حجة له.

تعالج هذه الورقة إشكالية الرقابة التي تقيمها الدولة على النشاط الرقمي باسم الأمن، وتجيب عن إشكالية غموض الحد الفاصل بين الحفاظ على الأمن والقمع. وتكتسي دراسة الموضوع أولوية لتزايد حجم الرقابة الرقمية وتسببها بالنتيجة في تقليص الحيز المدني الذي تتيحه التكنولوجيات الحديثة، لذلك بات الموضوع من الشواغل المستعجلة للمهتمين بحقوق الإنسان سواء على المستوى المؤسسي أو على مستوى الأفراد، بهدف المساهمة في خلق التراكم المطلوب للتقييد القانوني الملزم للرقابة الرقمية، لاسيما تلك الممارسة ضد الصحفيين والمعارضين السياسيين.

الكلمات المفتاحية: الرقابة الرقمية؛ البيانات الرقمية؛ الحقوق الرقمية، الأمن الرقمي.

Abstract

Technological development has brought about a transformation in the legal system for some of the legally enshrined freedoms, and perhaps the freedoms that have been subject to transformation have shown freedom of expression, freedom of opinion,

freedom of peaceful assembly, and the right to privacy, as digital means have allowed to change the legal system for its exercise, both in terms of the extent of freedom and the responsibility system to which the publisher and owner are subject. Geographical domain, internal domain, is subject to the authority of the State you enter to display the commercials, but this page is running and the internal review which entails security with a disciplined broad scale argument for it.

This paper addresses the problem of state control over digital activity in the name of security, and answers the problem of the ambiguity of the boundary between maintaining security and repression. The study of the subject is a priority due to the increasing volume of digital surveillance and its consequent reduction in the civil space provided by modern technologies. Therefore, the subject has become an urgent concern for those interested in human rights, whether at the institutional level or at the individual level, with the aim of contributing to creating the required accumulation of legal binding restrictions on digital surveillance, especially That practice against journalists and political opponents.
Key Words : Digital Surveillance; Numeric Control; Digital Data ; Digital Rights; Digital Security.

مقدمة

تطرح الرقمنة إشكالات عدة في مجال حقوق الإنسان من حيث محتوى هذه الحقوق ومداها ونظامها القانوني، فقد دعمت الرقمنة حرية التعبير وإبداء الرأي لدى الأفراد، بينما قيدت حريات وحقوق أخرى كالحق في الحياة الخاصة والحق في الأمن، وأنتجت حقوقا جديدة لم تكن قبلها وهي الحق في الولوج إلى الأنترنت، والحق في حماية البيانات الشخصية بعد أن أتيح للشركات وللدول الوصول إلى كميات غير مسبوقة من البيانات عن الأشخاص والهيئات، بعد تيسّر الاتصالات الرقمية ودمج آليات التتبع والمراقبة على نطاق مذهل في توسعه وعمقه.

وسّعت التكنولوجيات الحديثة مساحة "الحيز المدني" بحيث أصبح متاحا لكل متصل بالأنترنت المشاركة في الحياة المجتمعية، بإبداء الرأي وتوجيه النقد للسياسات المتبعة في كل المجالات وعلى جميع المستويات، والتعبئة لتنظيم الاحتجاجات السلمية، وبناء الشبكات والتحالفات، واطلاع العامة عليها وأسباب إطلاقها من أجل الدفع نحو التغيير الاجتماعي والسياسي، لاسيما بعد حملة المظاهرات التي شهدها العالم العربي منذ 2011، والعالم بأسره منذ 2019 لأسباب مختلفة ومعقدة يدرج بعضها في إطار التصدي للتمييز العرقي وأخرى في إطار السعي لتغيير الظروف الاجتماعية والاقتصادية والسياسية، وحتى لمقاومة الاحتلال في بعض المواضع من العالم. لكن بالموازاة لذلك، وعلى الجانب

الآخر، أتاحت هذه التكنولوجيات تقييد حقوق المستعملين وانتهاكها، ومراقبتهم وتعقّبهم، وانتهاك خصوصيتهم، بانتهاج سياسات مختلفة منها حجب الانترنت وإضعاف التدفق؛ استخدام المراقبة الاقتحاميّة عبر الإنترنت؛ اختراق حسابات الناشطين والصحفيين على مواقع التواصل الاجتماعي؛ استخدام تكنولوجيا التعرّف الآلي على الوجه خصوصا في المظاهرات والاحتجاجات العامة ما يتيح مراقبة المحتجين وتعقّبهم فيحجم الأفراد لذلك عن ممارسة حقهم في التعبير وحقهم في التظاهر السلمي خشية تحمّل العواقب التي قد/ تترتب عن ذلك.

ونظرا لتزايد حجم الرقابة الرقمية وتسببها بالنتيجة في تقليص الحيز المدني الذي تتيحه التكنولوجيات الحديثة، بات الموضوع من الشواغل المستعجلة للمهتمين بحقوق الإنسان سواء على المستوى المؤسسي أو على مستوى الأفراد، ويشكل مبحثا من المباحث التي يجب أن تسترعي نظر الباحث الأكاديمي وهذا ما كان مسوغا للورقة التي تنصب على تأثير الرقمنة على الحقوق والحريات العامة، لا من حيث اتساع نطاقها وتغير نظامها القانوني، وإنما من زاوية الحد الواقع عليها من السلطة العامة بفرض رقابة قد تتحول إلى قمع رقمي لا يختلف عن أوجه القمع الممارسة على الوسائل التقليدية، بالداعي الأمني غالبا، **فما ضابط الرقابة الرقمية المبررة والرقابة التعسفية القمعية؟**

تُبحَثُ هذه الإشكالية لبيان الحد الفاصل بين الرقابة المبررة ذات الهدف المشروع وبين الرقابة غير المبررة، بل وغير المشروعة في مبتغاها (قمع الحريات) وفي وسائلها (الاعتداء على الخصوصية) وذلك بهدف تقييدها ومنع بعض أشكالها، بخطة تخدم هذا الهدف، تنطلق من تحديد مفهوم الرقابة الرقمية لبيان تقاطعها مع جملة حقوق وحريات يثير فرضية تحولها إلى وسيلةِ قمعٍ للحريات (المحور الأول)، ثم الدواعي التي قد تتأسس عليها وحدودها التي إما تبقيها في إطار المشروع أو تتصدى لها بالردع عند خروجها عنه (المحور الثاني)، ليتسنى الحكم على سلامة الفرضية المنطلق منها وهي تحوّل الرقابة الرقمية إلى وسيلة قمع للحريات.

المحور الأول

الرقابة الرقمية وورود فرضية انتهاكها للحقوق والحريات

تثير الرقابة الرقمية بمختلف صورها جملة مخاوف مردها إلى تقاطعها مع جملة من الحقوق والحريات المكفولة نصا، وأبرزها: الحق في الخصوصية، الحق في التعبير وإبداء الرأي، الحق في التجمع السلمي وإنشاء الجمعيات (أولا)، وهذا باستخدام وسائل متعددة (ثانيا).

أولا- تقاطع الرقابة الرقمية وحقوق الإنسان وحرياته

"الرقابة الرقمية على الاتصالات تشمل المراقبة والاعتراض والجمع والحصول على أو تحليل أو استخدام أو حفظ أو الاحتفاظ أو التدخل في أو الولوج أو أي أفعال مماثلة متخذة تتعلق بالمعلومات التي تتجلى في طلب أو تتعلق باتصالات أي شخص في الماضي أو الحاضر أو المستقبل. وتشمل "الاتصالات" الأنشطة والتفاعلات والمعاملات المنقولة بالوسائل الإلكترونية، مثل محتوى الاتصالات وهوية أطرافها وتحديد الموقع الجغرافي والمعلومات بما في ذلك عناوين IP ووقت ومدة الاتصالات ومعرّفات المعدات المستخدمة في الاتصالات".[1] ويعني هذا المفهوم أن من شأن الرقابة تعقب الفرد ذاته في اتصالاته الرقمية أو محتوى مراسلاته ومنشوراته على المواقع والمنصات ووسائل التواصل الاجتماعي باستعمال تقنيات تجسس متطورة، كما قد تتخذ الرقابة الرقمية شكلا وقائيا وذلك بقيام الدولة بحجب بعض المواقع والمنصات ومواقع التواصل الاجتماعي لأغراض مختلفة، قد تكون أخلاقية، أمنية أو سياسية أو اقتصادية. ولغرض هذه الورقة نقصد فيها الرقابة التي يكون مصدرها الدولة، مهما كانت الجهة الممثلة لها: الهيئة الإدارية بما تملكه من اختصاص الحفاظ على النظام العام؛ السلطة القضائية بما تملكه من سلطة التحري والتحقيق في الجرائم وتتبع المجرمين[2]، وغيرها من الأجهزة الرسمية من شرطة ودرك وجهاز الاستعلام والاستخبار، حيث السعي إلى إيجاد توازن بين المهام الموكولة لها وبين الحقوق والحريات، لأن من طبيعة الرقابة إليكترونية كانت أم تقليدية أن تمس بشكل مباشر جملة من الحقوق والحريات، لكنها أظهرُ في الرقابة الإليكترونية لاتساع مداها ولورود تحولها لوسيلة حقيقية للقمع، ما يجعل قبولها والتسليم لها كليا أمرا يصعب استساغته، إلا أن تُؤطر تأطيرا قانونيا على وجه الاستعجال.

فإذا كان التطور التكنولوجي الرقمي قد أحدث الحق في حماية البيانات الشخصية والحق في الوصول إلى الانترنت[3]، وعدّل النظام القانوني للكثير من الحقوق والحريات[4]، فإنه فتح في المقابل مخاطر جديدة على أمن الأشخاص بما يخوله للبوليس الإداري والقضائي وجهاز الاستعلام من وسائل للرقابة، فإذا كان المسلم به اليوم أن النشاط على الفضاء الرقمي ليس خارجا عن رقابة الدولة كما كان يدعيه البعض عند ظهور الانترنت[5]، فإن ذلك لا يعني قبول تحول الرقابة إلى قمع للحريات. فقد ورد في التقرير السنوي لمفوضة الأمم المتحدة السامية لحقوق الإنسان في 2014 بشأن الحق في الخصوصية في العصر الرقمي، أن الرقابة الرقمية تنتهك الحق في الخصوصية، وحقوقا أخرى غير منفكة عنه كالحق في الحياة العائلية والحق في الصحة، والحق في حرية التجمع وفي تكوين الجمعيات، والحق في حرية الرأي

والتعبير وفي التماس المعلومات وتلقيها وإذاعتها[6]، لأن الحق في الخصوصية لا ينفك لا عن حرية الرأي وحرية التعبير ، إذ يعتبر مدخلا لممارستهما، وغالبا ما ينظر إليه على أنه شرط أساسي لإعمال الحق في حرية التعبير، فقد يعيق التدخل في الخصوصية ممارسة حرية التعبير خوفا من رد الفعل، "فالقيود المفروضة على إغفال الهوية في الاتصالات، على سبيل المثال، لها أثر سلبي واضح على ضحايا كافة أشكال العنف وسوء المعاملة، الذين قد يترددون في الإبلاغ خوفاً من الوقوع ضحية مرتين"[7]. ويترابط الحق في الخصوصية مع الحق في حرية التعبير ويعتمد كل منهما على الآخر بصورة متبادلة؛ ويمكن لانتهاك أحدهما أن يكون سبباً لانتهاك الآخر ونتيجة له[8]. وأكثر المعرضين لذلك فئة الصحفيين، فكثيرا ما يخضع هؤلاء للرقابة التي تعيق العمل الإعلامي وتصعب الوصول إلى مصدر المعلومة[9]. ويكفي استقراء الواقع للتدليل على أثر الرقابة الرقمية على الحقوق والحريات، فقد وقعت حالات تعذيب وسوء معاملة باستخدام التكنولوجية الرقمية في جمع البيانات، وكذا في تحديد أهداف دقيقة لضربات فتاكة شنتها طائرات دون طيار[10]، وفي تعقب الصحفيين والمعارضين واعتقالهم[11]، بل وتصفيتهم جسديا، إذ كثيرا ما يلجأ المعارضون للفضاء الرقمي للتعبير عن آرائهم وإبداء تعليقاتهم ونقدهم لأنظمة الدول[12]، خصوصا بالنسبة للمعارضين الأحرار الذين لا ينتمون لحزب أو تنظيم معتمد، فتكون الرقابة الرقمية بصورها المختلفة وسيلة لإسكات هؤلاء وحجبهم عن الجمهور.

ثانيا- تنوع وسائل الرقابة الرقمية

ساهمت الأزمات الدولية والداخلية سواء كانت أمنية، اقتصادية أو صحية في توسيع وتسريع عملية الرقابة الرقمية وتطويرها، فعقب أحداث 11 سبتمبر 2001 أطلقت وكالة الأمن القومي الأمريكية NSA برامج رقابية جديدة مثل Total Information Awareness، كما ألزمت دول الاتحاد الأوروبي متعاملي الاتصالات تخزين البيانات الوصفية لكل الاتصالات لعموم الجمهور[13] بالتوجيه الصادر في 2006 (قبل إلغائه بقرار من محكمة العدل الأوروبية في سنة 2014)، وتعممت هذه الإجراءات الرقابية على الدول إما بشكل مؤطر قانونا وإما في شكل سري غير مؤطر وحتى مخالف للقانون، وتتخذ أشكالا متعددة، تتخذ بعض الدول استراتيجية عامة للتحكم في الأنترنت، ومن الوسائل:

- **حجب الأنترنت:** وهو أن تعمد الدولة بشكل وقائي إلى حجب مواقع إليكترونية عن مواطنيها، ومثالها حجب الحكومة المصرية النفاذ إلى الأنترنت على المستوى الوطني بعد منتصف الليل في الساعات الأولى من يوم الجمعة 28 جانفي 2011، لتوقيف تعبئة المواطنين

للمشاركة في المظاهرات ضد الرئيس المتنحي حسني مبارك بواسطة موقعي فيسبوك وتويتر بقيادة وائل غنيم المسؤول التنفيذي الإقليمي بجوجل[14]. ومن الأمثلة حجب الحكومة العراقية للفيسبوك في 2019 ؛ حجب الحكومة الإيرانية لموقعي فيسبوك وتويتر ووضع قائمة سوداء كبيرة من الروابط الممنوعة لتمنع المواطنين العاديين من الدخول عليها، وأكثر المواقع المُحرمة هي المواقع ذات المحتوي السياسي أو المحتوي الحكومي، وتختص بالرقابة في إيران هيئات خاصة هي المجلس الأعلى للفضاء المجازي، لجنة تحديد المواد غير اللائقة، شرطة الأنترنت، جيش الانترنت[15]. وقد تلجأ الحكومات بدل الحجب الكلي على استعمال تقنيات الفلترة لتضييق معطيات البحث لبلوغ ما بوسع المستخدم مشاهدته، ولسنا نعني هنا استخدام الفلترة لهذا الغرض ، أو لغرض حجب المواقع غير المشروعة كالمواقع الإباحية، إنما نعني استخدامها من الحكومات للتضييق على المعارضة والنشطاء في المجتمع المدني بالمخالفة لحق الوصول إلى المعلومة الذي تكرسه المادة 19 من الإعلان العالمي لحقوق الإنسان. وقد تتخذ الحكومات توقيف الفلترة مصيدة للمعارضين كما فعلت الحكومة السورية[16].

وهناك من الدول من يرفض مجتمعها المدني والقضاء تقييد المحتوى حتى إن كان لغرض مشروع ومتفق على مشروعيته، ومن ذلك ما قام به الكونغرس الأمريكي من وضع مشروع قانون متعلق بحماية الطفل على الأنترنت في 1997، هدفه حماية الأطفال من الوصول إلى المواقع الإباحية، لكن الاتحاد الأمريكي للحريات المدنية عارض المشروع بحجة أنه يمس حقوق الراشدين في التعبير، وإن الجهود الرامية إلى تقييد المحتوى من شأنها الإخلال بالتعديل الأول للدستور الأمريكي، لذلك؛ وبعد حوالي عشر سنوات من التقاضي أمام المحاكم الدنيا والمحكمة العليا الأمريكية رفض القانون نهائيا في 2009[17].

- **خفض تدفق الأنترنت** لمنع التعبئة لتنظيم المظاهرات السلمية ذات المطالب السياسية أو المطالب الاجتماعية، ففي الجزائر مثلا وتصديا للحراك الشعبي المعارض للعهدة الخامسة للرئيس بوتفليقة، لجأت الحكومة إلى خفض تدفق الأنترنت لإعاقة التواصل بين المواطنين، كما لجأت لاختراق حسابات المعارضين والناشطين في الحراك[18].

- **فرض قيود على التشفير والإلزام بكشف مفتاح التشفير:** قد تصدر الدولة قانونا يحد من استخدام أدوات التشفير التي تعزز الخصوصية على المواقع، وتعني تقنيات التشفير إخفاء هوية أطراف الاتصال ومحتواه، فقد اعتمدت دول عديدة قوانين تلزم الأفراد فك الشفرات عند أمرهم بذلك، مثل قانون جنوب أفريقيا لعام 2002 المتعلِّق بتنظيم اعتراض الاتصالات وتوفير المعلومات المتعلِّقة بها، الذي يقضي بتقديم المساعدة على فك التشفير من

أي شخص يملك مفتاح فك التشفير؛ وقانون فلندا المتعلق بالتدابير القسرية 540/1987 في المادة 4/4/أ؛ وقانون بلجيكا المتعلِّق بالجرائم الحاسوبية المؤرَّخ 28 نوفمبر 2000 في المادة 9 منه، ومثيله الأسترالي الصادر في 2001 في مادتيه 12 و28[19].

- التنصت واعتراض الاتصالات عبر مراقبة شبكات الاتصال وتتبع بيانات الاتصال عليها: تلزم شبكات الاتصالات، سواء الهاتفية أو عبر الأنترنت بالتستر على بيانات مستعمليها، ويسعى مناصرو الخصوصية إلى عدم الاحتفاظ ببيانات المستعملين إلا بقدر ما يسمح للشركة إعداد الفواتير وحاجاتها التجارية الأخرى[20]، إلا أن انتشار الجريمة الإليكترونية دفع بعض الدول لاتخاذ إجراءات تقييدية تلزم الاحتفاظ ببيانات الاتصال، كالتوجيه الأوروبي2006/24/CE في 15 مارس 2006 [21]والذي ألغته محكمة العدل الأوروبية بقرار صادر في 8 أفريل 2014[22]؛ و"قانون الاحتفاظ بالبيانات وقانون التحقيق" البريطاني سنة 2014؛ والقانون الأسترالي سنة 2015؛ والولايات المتحدة الأمريكية في "قانون حماية أمريكا" سنة 2007، ثم قانون مكافحة الإرهاب والأمن سنة 2015، القانون الجزائري 04/09 الذي تلزم المادة 11 منه مقدمي خدمات الاتصالات الاحتفاظ بجملة معطيات حددها النص لمدة سنة واحدة ابتداء من تاريخ التسجيل[23]. ذلك أنه قد يستدعي داعي الأمن الإفصاح عن البيانات، بحيث يسمح على سبيل الاستثناء لجهات إدارية أو قضائية الوصول للبيانات حسب ما يقتضيه التحقيق بناء على إذن قضائي أو دونه[24]؛ لكن قد تتعمم هذه الرقابة ليس على سبيل الاستثناء، بتركيب جهاز على شبكة الاتصالات المراد اعتراض اتصالات متعاملها، وذكر تقرير المقرر الخاص للأمم المتحدة حول الرقابة الرقمية 2019 أن الاتحاد الروسي يراقب شبكات الاتصال باستعمال تقنيات معدة لذلك[25].

- التصيد الاحتيالي لحسابات المستعملين (الهاكرز): هي تقنيات تستخدم لجمع البيانات عن مستخدمي الأنترنت، بحيث ينشئ المتصيد صفحات وهمية مستنسخة عن الصفحات المراد قرصنتها، وتستعمل هذه التقنيات للولوج للبريد الإليكتروني، حيث يمكن المتصيد الاطلاع على البيانات الشخصية وكلمة المرور ومعلومات سرية عن المستخدم[26].

- اختراق الأجهزة المحمولة باستعمال برامج التجسس، هي برامج مطورة ذات تقنية عالية هدفها التنصت على الاتصالات الرقمية، وتسببت في الكثير من الانتهاكات الواقعة على الصحفيين والنشطاء والمحامين، لعل أظهرهم مقتل الصحفي جمال خاشقجي، وتعقب المحامي الفلسطيني الفرنسي صلاح حموري والناشط الإماراتي أحمد منصور. ويعتبر بيغاسوس Pegasus الذي ينتجه مجمع NSO الإسرائيلي البرنامج النموذجي للتجسس، وهو

برنامج عالمي يتجسس على الهواتف الذكية للصحفيين والسياسيين والمحامين ونشطاء في مجال حقوق الإنسان وشخصيات رسمية في الأمم المتحدة ورؤساء دول وحكومات[27]، ويعمل هذا البرنامج بتوزيع رسائل نصية للبريد الإليكتروني أو روابط إليكترونية تحمل فيروس بيغاسوس، أو بتنزيل برامج خبيثة على الجهاز دون قصد، وذلك لأن الرابط أو الرسالة تنتحل جهة إرسال قانونية أو أنها واردة من جهات ذات علاقة بنشاط الشخص المراد التجسس على جهازه أو بمجاله الشخصي. ويتميز برنامج بيغاسوس بتقنية عالية جدا وقابلة للتكيف، تمكنها من اختراق الهواتف الذكية الأكثر تطورا في حماية الخصوصية[28].

وقد شهد شهر جويلية 2021 الإفصاح عن أكبر فضيحة تجسس بعد قضية Snowden[29] مست كل الدول، نشرتها منظمة Forbidden Stories بالمساعدة التقنية لمنظمة العفو الدولية، بعدها دعا فريق خبراء تابع للأمم المتحدة إلى حظر بيع تكنولوجيات الرقابة في انتظار وضع تنظيم صارم لها يراعي حقوق الإنسان[30]، وإلى هذا دعا تقرير المقرر الخاص للأمم المتحدة حول الحق في حرية الرأي والتعبير في ماي2019[31]، حيث جاء في التوصية "أ" أنه على الدول إقرار وقف اختياري فورا لتصدير وبيع ونقل واستعمال وخدمة أدوات المراقبة التي تطورها شركات خاصة إلى حين وضع نظام ضمانات يمتثل لحقوق الإنسان موضع التنفيذ.

- **تقنية التعرف على الوجوه والعواطف:** هي تقنية تعمل على التقاط سمات الوجه والتعرف على الشخص من خلاله، عن طريق تصنيف الأفراد على أساس الانتماء العرفي أو القومي. أما تفنية التعرف على العواطف فتسمح بالتعرف على انفعالات الشخص وردود فعله المحتملة من خلال تعابير وجهه. وقد أشار المقرر الخاص للأمم المتحدة حول الحق في حرية الرأي والتعبير في ماي2019 إلى أن الصين تستخدم تقنيات المراقبة هذه لتعقب ضد الإيغور وتحتفظ بسجلات تحركاتهم قصد الاستقصاء والفحص[32].

المحور الثاني

الإطار القانوني المفترض لرقابة رقمية [مقبولة]

تضع المواثيق الدولية قيودا على ممارسة بعض الحقوق والحريات، وهذه القيود تصلح أن تكون مسوغا للرقابة الرقمية، فما يسري على ممارسة الحق من قيود على الواقع يسري على ممارسته على الأنترنت، لتكون هذه القيود هي المجال المسموح للرقابة الرقمية، لكن مشكل هذه القيود أنها غير منضبطة (أولا)، لذلك، وحتى لا يبقى تقدير وجودها للسلطة

التقديرية لممارس الرقابة، وجب أن تؤطر الرقابة قانونا بشكل دقيق، سواء من حيث المدى ومن حيث الجهة المشرفة عليها (ثانيا).

أولا- التقيد بالدواعي الملجئة للرقابة الرقمية المحددة في قانون حقوق الإنسان

باعتبار أن إيجابيات الانترنت وسلبياتها تسير في شكل مواز لا يمكن فصلهما عن بعض، فالأنترنت التي تخول الأشخاص نقد الحكومات والتعبئة الشعبية للاحتجاج والتظاهر، هي نفسها الأنترنت التي تنشر الإباحية وتجند للعمل المسلح غير المشروع وتنتشر عبرها تجارة البشر والمخدرات، لذلك فإن حكومات الدول قد تتخذ محاربة هذه الظواهر حجة لممارسة الرقابة على الأنترنت، هذه الرقابة التي تتقيد بالقيود التي سطرها قانون حقوق الإنسان، وهذا ما عبرت عنه الجمعية العامة للأمم المتحدة في أن شواغل الأمن العام قد تبرر جمع وحماية بعض المعلومات الحساسة، ومع ذلك يجب على الدول أن تكفل التقيد التام بالالتزامات التي يلقيها عليها القانون الدولي في مجال حقوق الإنسان[33]، لكن المشكل أن قيود قانون حقوق الإنسان ذاته غير محددة ولا منضبطة وقابلة للتفسير اتساعا وضيقا، لهذا نجد التقارير الحديثة التي مست الرقابة الرقمية تحصرها في تحقيق أهداف ثلاثة.

وما دامت الورقة الحالّة تخص بشكل مباشر حرية الرأي وحرية التعبير والحق في الخصوصية، فإن مدار الدواعي المسوغة للرقابة الرقمية لا تخرج – أو لا يستساغ قانونا أن تخرج- عن تلك الواردة في المادتين 17 و19 من العهد الدولي للحقوق المدنية والسياسية، التي تفتح بغموضها انتهاك الحقوق التي كرستها، سواء بالنسبة لمفهوم التدخل التعسفي أو غير المشروع ، أو بالنسبة لمفهوم الأمن.

1- تقييد المساس بالخصوصية بالقيد العام المبهم "عدم التعسف والمشروعية".

لا تضع المادة 17 من العهد الدولي للحقوق المتعلقة بالحق في الخصوصية قيودا صريحة على هذا الحق، لكنها تجيز بمفهوم المخالفة التدخل والمساس بحرمة الحياة الخاصة إذا لم يكن التدخل تعسفيا أو غير مشروع، بمعنى أنها لا تحظر التدخل أو المساس بهذا الحق إلا ما كان منه تعسفيا أو غير مشروع. ولا تضع المادة 17 أي معيار يضبط القيود الجائزة خلافا للمادة 3/19 أدناه التي حددت الأهداف التي يجب أن تتوخاها القيود القانونية والضرورية على حريتي الرأي والتعبير. رغم ما ورد في التعليق العام رقم 16 بشأن المادة 17 من تعريف للتدخل التعسفي والتدخل غير المشروع، ف"غير المشروع" في مفهوم اللجنة المعنية بحقوق الإنسان كل تدخل لا يستند إلى قانون، فأي تدخل في الحياة الخاصة لا يكون إلا في الحالات التي

ينص عليها القانون، ولا يجوز أن يحدث التدخل الذي تأذن به الدول إلا على أساس القانون الذي يجب أن يكون متفقاً مع أحكام العهد وأهدافه[34].

أما التدخل التعسفي فإن التعليق رقم 16 لم يتضمن تحديدا له، إنما اكتفى بالنص أن التدخل الذي ينص عليه القانون قد يكون تعسفيا، وأن إدراج مفهوم التعسف هو ضمان أن يكون التدخل نفسه الذي يسمح به القانون موافقاً لأحكام العهد وأهدافه وأن يكون معقولاً بالنسبة للظروف المعينة التي يحدث فيها[35]. وقد فسرت اللجنة معنى المعقولية أن يتناسب التدخل في الخصوصية مع الغرض المقصود منه، ويجب أن يكون ضروريا في ظروف القضية[36].

إن التطور الكبير الذي شهده العالم في مجال الوسائل التي تمس الحياة الخاصة، أوجد وجوب تحيين مفهوم التدخل التعسفي الوارد في التعليق العام رقم 16 بالمعطيات الجديدة، حيث توسع مفهوم التدخل غير القانوني أو التعسفي، بحيث يعتبر تعسفيا وغير قانوني (وإن كان منصوصا عليه في القانون)، كل تقييد لحق الخصوصية لا تتوفر فيه معايير القانونية والتناسب والضرورة والارتباط بتحقيق هدف مشروع، مع إلقاء عبء إثبات الهدف المشروع على السلطات التي تتوخى تقييد الحق في الخصوصية، ووجوب ألا يجرد أي تقييد للحق في الخصوصية جوهر الحق من معناه ويجب أن يكون متسقاً مع حقوق الإنسان الأخر ى، بما فيها حظر التمييز[37]. وقد ذهب المقرر الخاص فرانك لارو في تقريره سنة 2013 إلى أن المادة 17، وإن لم تتضمن حكما تقييديا في صياغتها، فإنه يجب أن يخضع لنفس معيار القيود الجائزة المتعلق بالحق في حرية التنقل، على نحو ما أوضحه التعليق العام رقم 27[38].

أوكلت الفقرة الثانية من المادة 17 للدول الاختصاص بحماية الأفراد من التدخل غير القانوني والتعسفي، لذلك فإن تأطير عملية التدخل يكون بقانون دقيق وواضح ومتاح للعامة، ولعل أكثر القوانين تطورا اللائحة الأوروبية 2016/679 (UE) التي اتخذت في 27 أفريل 2016 ودخلت حيز النفاذ في ماي 2018[39]، والتي ألغت التوجيه 95/49/CE، حيث نصت في المادة 23 منها على القيود التي يمكن أن تسوغ تقييد الحقوق التي تضمنها اللائحة على بشرط ألا تمس بجوهر الحقوق والحريات الأساسية وان تكون إجراء ضروريا ومتناسبا في مجتمع ديمقراطي، وأن يكون هدفها ضمان:

أ- الأمن القومي؛

ب- الدفاع الوطني؛

ج- الأمن العمومي؛

د- الوقاية والكشف عن المخالفات الجزائية، وكذا التحقيقات والمتابعات الجزائرية وتنفيذ العقوبات الجزائية، بما فيها الحماية من التهديدات ضد الأمن العمومي والوقاية منها؛

هـ- أهداف أخرى ذات أهمية متعلقة بالصالح العام للاتحاد أو لدولة عضو، لاسيما مصلحة اقتصادية أو مالية هامة للاتحاد أو لدولة عضو، بما فيها المجالات النقدية والمالية والضريبية، الصحة العمومية والتأمينات الاجتماعية؛

و- حماية استقلال القضاء والإجراءات القضائية؛

ز- الوقاية والكشف عن مخالفات أخلاقيات المهن المنظمة، وكذا التحقيقات والمتابعات فيها؛

ح- مهمة رقابة أو تفتيش أو تنظيم مرتبطة، ولو بشكل ظرفي، بممارسة السلطة العامة، في الحالات المشار إليها في النقاط (أ) إلى (هـ) و (ز)؛

ط- حماية الشخص المعني أو حقوق وحريات الآخرين؛

ي- تنفيذ مقتضيات القانون المدني.

وتظهر الأهداف التي اعتبرتها المادة 23 أعلاه مشروعة لا تختلف كثيرا في عمومها عن الأهداف الثلاثة التي كثيرا ما تتردد في التقارير الأممية[40] وهي: **الأمن القومي، إنفاذ القانون والاستخبارات**، وهي اعتبارات غير منضبطة، فالأخيرة غالبا ما تشكل مدخلا للانتهاكات للطابع السري الذي يحوطها[41]؛ أما الأمن القومي، فهو لا يقل غموضا عن سابقه، أما إنفاذ القانون، فهو هدف واسع، تدخل ضمنه إجراءات التحقيق والتحري وإجراءات إنفاذ أي نص قانوني سواء كان مدنيا أو جزائيا، ومهما كانت المصلحة التي يحميها، عامة أو خاصة، ما يشكل مدخلا لفرضية التعسف باسم القانون في غياب ضمانات قوية، وأهمها استقلال القضاء واستقلال جهات التحري، وهذا ما يؤكد الحرص على توفير الشروط اللازمة في "القانون"[42] الذي يسوغ التدخل لحمايته، لأن وجود القانون وحده غير كاف لتسويغ التدخل، فقد يكون هذا القانون ذاته ظالما وغير مستجيب للمعايير التي تقتضيها حقوق الإنسان.

2 - تقييد الرقابة الرقمية بقيود حرية الرأي وحرية التعبير

للعلاقة الوطيدة بين الحق في الخصوصية وحرية الرأي والتعبير[43]، فإن القيد المفروض على الخصوصية يؤثر لا محالة على الحريتين، تأثير الوسيلة على المحتوى، إذ إن ممارسة حرية الرأي والتعبير يتأتى بتوفير الحق في الخصوصية باعتباره وسيلة وفي الوقت نفسه ضمانة لممارس الحريتين. كما تقترن حرية الرأي وحرية التعبير بالحق في المشاركة في الحياة

السياسية المكفول بالمادة 25 من العهد الدولي للحقوق المدنية والسياسية، كما بينته اللجة المعنية بحقوق الإنسان في تعليقها العام رقم 25[44]، لذلك فالمساس بحرية الرأي والتعبير مساس بالحق بالمشاركة في الحياة السياسية.

سبق أن المادة 17 لم تتضمن قيدا مباشرا على الحق في الخصوصية، بينما نجد المادة 3/19 رخصت تقييد حريتي الرأي والتعبير المنصوص عليهما تباعا في الفقرتين الأولى والثانية من المادة بمعيار ثلاثي: أن يكون ذلك ضروريا؛ وأن يكون بنص القانون؛ وأن يهدف لتحقيق إحدى الأهداف: - احترام حقوق الآخرين أو سمعتهم؛

- حماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة.

إن الأهداف المقيدة لحرية الرأي وحرية التعبير تنطبق على أي فضاء يمكن أن تمارس عليه، فيمكن للدولة أن تتحجج بهذه الأهداف لفرض رقابتها على الفضاء الرقمي، ولا يختلف اثنان في أن هذه القيود غير منضبطة، لذلك جاء في الفقرة 26 من التعليق العام رقم 34 على الفقرة الثالثة من المادة 19 إنه لا ينبغي للقانون أن يمنح سلطة تقديرية مطلقة للأشخاص المسؤولين عن تنفيذه في تقييد حرية التعبير، فيجب أن ينص القانون على توجيهات كافية للمكلفين بتنفيذه لتمكينهم من التحقق على النحو المناسب من أنواع التعبير التي تخضع للتقييد وتلك التي لا تخضع لهذا التقييد[45].

وتوضيحا للمعايير التي وضعتها المادة 3/19، ودفعا للسلطة التقديرية المطلقة للدولة، بينت اللجنة المعنية بحقوق الإنسان في التعليق العام رقم 34 بشأن السبب المشروع الأول لتقييد حرية التعبير وهو "احترام حقوق الآخرين وسمعتهم"، أن المقصود بتعبير الحقوق هي تلك المعترف بها في العهد وفي القانون الدولي لحقوق الإنسان عامة[46]. أما عن السبب الثاني المشروع وهو حماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة، فقد جاء في التعليق 34، فقد شددت اللجنة على اتخاذ قوانين الخيانة والأمن القومي وقوانين مكافحة إثارة الفتنة حجة "للقمع أو لحجب معلومات عن الجمهور تكون ذات مصلحة عامة مشروعة ولا تضر بالأمن القومي، أو لمقاضاة الصحفيين أو الباحثين أو الناشطين في مجال البيئة، أو المدافعين عن حقوق .الإنسان أو آخرين لأسباب تتعلق بنشرهم تلك المعلومات"[47]، فغموض معنى الأمن القومي –أو المعنى الضبابي للأمن القومي أو الوطني- يفتح المجال واسعا للقمع، لاسيما بالنسبة للصحفيين والنشطاء السياسيين والمدافعين عن حقوق الإنسان، وهذا ما رصده المقرر الخاص فرانك لا رو في تقريره 2013 [48] ، لذلك وجب التشدد في تطبيق المعايير التي تحكم الأحكام التقييدية التي تطبق في جميع حالات المراقبة محددة الأهداف،

لكنها تكتسي أهمية خاصة بالنسبة لتقييد حرية التعبير دفاعا عن مصلحة عامة[49]، لأن هؤلاء أكثر عرضة للتضييق والقمع.

ثانيا- نحو السعي لتأطير الرقابة الرقمية

حتي لا تُتخذ دواعي الأمن بمفهومه العام ذريعة للاعتداء على حقوق المواطن وحرياته، لا بد من إخضاع الرقابة المفروضة على النشاط الرقمي لإطار قانوني للوقاية من حدوث الآثار غير المرغوبة على حقوق الإنسان وحرياته (1)، وضمان وسائل ردعية وإصلاحية للمتضررين من آثار الرقابة وأهمها ضمان قضاء كفء ومستقل (2).

1- المبادئ الواجب مراعاتها عند تقنين الرقابة وقايةً من التعسف المؤدي إلى القمع:

تتفق التقارير الأممية على ضرورة التأطير القانوني لاستعمال تكنولوجيات الرقابة الرقمية، بوضع معايير قانونية ملزمة مناسبة لضمان خصوصية الاتصالات وأمنها وإغفال هوية أصحابها، ليتمكن الصحفيون والمدافعون عن حقوق الإنسان والمبلغون عن المخالفات، الاطمئنان لعدم تعرض اتصالاتهم للتتبع من الدول[50]، لكن مثل هذا التأطير في نظام دولي شامل لم يوجد بعد، وقد وضعت مجموعة مبادئ توصَى الدول بمراعاتها في تشريعاتها، تضمنتها التقارير الأممية، كما تضمنتها الوثيقة المسماة "ضرورية ومتناسبة. مبادئ دولية لتطبيق حقوق الإنسان فيما يتعلق بمراقبة الاتّصالات" والذي أعده بشكل تعاوني خبراء من جميع دول العالم في الخصوصية من منظمات حقوقية مختلفة ورائدة عالميا في مجال حماية الحقوق الرقمية، أطلقت رسميا النسخة الأولى من المبادئ المتضمنة ثلاثة عشر مبدأ من مجلس الأمم المتحدة لحقوق الإنسان في سبتمبر 2013، وخضعت للتعديل الصياغي في آخر نسخة لها مؤرخة في ماي 2014. وقد تضمنت الوثيقة الهدف من هذه المبادئ الإطار وهو بيان كيفيّة انطباق قوانين حقوق الإنسان الدّوليّة على البيئة الرقمية المعاصرة، خاصة تلك الحاصلة في تقنيات وأساليب مراقبة الاتصالات والتطوّر الحادث فيها، كما يمكن لهذه المبادئ أن تكون إطارًا لمجموعات المجتمع المدنيّ ولصناعة الاتصالات وللحكومات ولغيرها لتقييم مدى اتفاق تشريعات المراقبة الحاليّة أو المقترحة مع حقوق الإنسان[51]. ومن المبادئ الوقائية التي نجدها في هذه الوثيقة وفي تقارير الأمم المتحدة التي تعتبر إطارا عاما وقائيا يجب أن تضمنه التشريعات المقننة لعملية الرقابة التي تعتبر في ذاتها أول مطالب التأطير:

أ- الشرعية: يجب أن يكون أيُّ تطبيق أو إجراء من شأنه تقييد حقوق الإنسان منصوصًا عليه في القانون مع شرط ضمان علم الأفراد به، مع وجوب مراجعة هذه القوانين دوريا لتواكب سرعة التطور التقني، ووجوب أن تكون دقيقة بحيث تحدد الهدف المشروع الذي شرعت الرقابة لتحقيقه والجهات الكفيلة بممارسة الرقابة[52].

ب- الضرورة: أن تكون الرقابة ضرورية على نحو محدد وظاهر لتحقيق غرض شرعي[53]، وأن تقتصر على الحد الأدنى الممكن بيان ضرورته لتحقيق هدف مشروعٍ، ولا يُلجأُ للرقابة إلا عندما تكون هي الوسيلة الوحيدة لتحقيق هذا الهدف، وفي حال وجود أكثر من وسيلة، يجب أن تكون الرقابة هي أقلها انتهاكا لحقوق الإنسان[54].

ج- الملاءمة و التناسب: يجب أن تتناسب مراقبة الاتصالات التي يجيزها القانون على سبيل الاستثناء مع الغرض المشروع الذي تمارَس لأجله، بأن توجد إحدى الدواعي المشروعة المسوغة للرقابة الرقمية والتي يجب أن تحدد بدقة في القانون وتخضع للرقابة القبلية لقاض مستقل ومكون تكوينا كافيا في المجال الرقمي، كأن يوجد احتمال راجح لجريمة وقعت أو تهديدا مُعيّنا يوشك على الوقوع لقصد مشروع وتكون المعلومات المأخوذة من الرقابة ضرورية لجمع الأدلة حولها وألا توجد وسيلة أخرى غيرها للتحري والتحقيق، وأن يتعامل مع المعلومات المستقاة بالرقابة في حدود دنيا بحيث لا تمس بجوهر الحق في الخصوصية ولا بجوهر الحريات المنتهكة.

د- الشفافية ووجوب إبلاغ المعني بالرقابة الواقعة عليه: يلزم المبدأ الحكومات بالشفافية في تطبيق الرقابة الرقمية، فعليها أن تتيح لمقدمي الخدمات نشر كل الطلبات المقدمة إليها للرقابة على مستخدمي الخدمة التي تقدمها، والهدف من الرقابة. ومن قبيل الشفافية قيام الحكومة أو مقدم الخدمة بإبلاغ المعني بإذن الرقابة على اتصالاته ليتمكن من إجراء الطعون اللازمة إذا اقتضى الأمر، ولا يجوز تأخير الإبلاغ إلا في حال ما إذا كان الإخطار من شأنه إفشال الغرض الذي من أجله صُرِّح بالرقابة، أو يؤدي إلى خطر حال ووشيك على حياة إنسان وأصدرت جهة قضائيّة مستقلة وذات كفاءة بتأجيل الإخطار[55].

و- ضمانات التعاون الدولي: قد تحتاج الحكومات لطلب العون من مُقدِّمي خدمة أجانب أو من حكومات أجنبيّة، وحينذاك يجب أن تضمن اتفاقيات تعاون أمني وقانوني تتضمن أنه في حال تنازع قوانين أكثر من دولة واحدة، فإن قانون المراقبة الأكثر حماية لحقوق الإنسان هو المطبق، وعندما تطلب الحكومات مساعدة في إنفاذ القانون فإنّه يجب أن يكون الفعل المطلوب لأجله البيانات مجرما في قانون الدولتين، وليس للدولة أن تطلب

معلومات محميّة جهة أجنبيّة بغرض تجاوز القيود القانونية التي تفرضها القوانين المحلية، ويجب أن تُتاحَ اتفاقات التعاون الدولي للعموم تحقيقا للشفافية وإخضاعها لضمانات الصحة الإجرائية[56].

و- ضمانات ضد الرقابة غير المشروعة: يجب على الحكومات أن تتخذ تشريعات تجرم الرقابة الرقمية لغير الأهداف المبررة، وتفرض عقوبات جنائية ومدنيّة رادعة، ويجب أنْ تقضي القوانين بأنّ كُلَّ المعلومات المتحصل عليها بوسيلة تخالف هذه المبادئ لا يُعتّدّ بها وسيلة للإثبات أمام القضاء، ويجب على القوانين أن تقضي باستعمال المعلومات المحصل عليها في الهدف الذي جمعت لأجله، وأن تتلف بعد ذلك[57].

ز- إشراف هيئةٌ مستقلة ذات كفاءة، قد تكون محكمة أو آلية رقابة، على عملية رصد بيانات الاتصالات للدولة، فيشترط قبل تطبيق الرقابة الحصول على إذن من هذه الهيئة، ويحبذ ان تكون جهة قضائية لكن شرط أن تكون ذات كفاءة في المجال ومستقلة، لأنه لا معنى لإذن يشترط من الهيئة القضائية إذا كانت الهيئة ذاتها غير مستقلة عن الجهة الطالبة للإذن، ففقد ثبت في الواقع أن بعض الدول تنص تشريعاتها على الإذن القضائي المسبق، لكن ذلك لم يمنع من اتخاذ الرقابة الرقمية وسيلة لإسكات المعارضة والزج بها في السجون، فالقانون الجزائري 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ينص في المادة 4/4 أنه لا يجوز إجراء عمليات المراقبة المنصوص عليها في الفقرات السابقة إلا بإذن مكتوب من السلطة القضائية المختصة، لكن عدم استقلال السلطة القضائية سمح لفتح باب التضييق على المعارضة وتعقبها على مواقع التواصل، خاصة أن فقرات المادة الرابعة جاءت غير منضبطة وتفتح باب التفسير لما تخوله من سلطة تقديرية واسعة لطالب الإذن ولمانحه.

أما على الصعيد الدولي، ينبغي للدول أن تبرم معاهدات المساعدة القانونية المتبادلة لتنظيم الاطلاع على بيانات الاتصالات الموجودة لدى الجهات الأجنبية التابعة للشركات[58]، على غرار الاتفاقيات القضائية الثنائية.

2- إصلاح وردع التعسف الواقع بالرقابة الرقمية وإصلاح الضرر الناجم عنه:

من ضمانات الالتزام بالتأطير القانوني لعملية الرقابة الرقمية الذي عماده المبادئ المذكورة في البند 1، ضمان خضوع المخالفات للقانون المؤطِّر لرقابة قاض مستقل وذي كفاءة في موضوع الحقوق والحريات، لاسيما الحق في الخصوصية وحرية الرأي والتعبير، هذا علاوة على ملاءمة إيكال مهمة الإشراف على عملية الرقابة للقضاء بشرط أن يكون كفؤا من حيث

التكوين ومستقلا من حيث التبعية، إذ غالبا ما يكون مصدر الإخلال بالرقابة جهات من السلطة التنفيذية أو القطاع الأمني في الدولة، حتى إن كان منسوبا للقطاع الخاص أحيانا كالشركات العاملة في خدمة الاتصالات، فقد تعجز الحكومات عن تلبية متطلباتها في الرقابة سواء كانت الدواعي مشروعة أو تعسفية، فتعهد الأمر للشركات الخاصة التي تملك ما يلزم لتلبية هذه الاحتياجات[59].

إن كفاءة السلطة القضائية تتيح للأفراد الذين انتهك حقهم في الخصوصية نتيجة المراقبة التعسفية أو غير القانونية سبل انتصاف فعالة، انسجاما مع الالتزامات الدولية في مجال حقوق الإنسان؛ ويضمن محاكمة عادلة بتمكين الخاضع للرقابة الرقمية التعسفية من اللجوء إلى القضاء سواء طاعنا أمام القضاء في قرارات السلطة الوطنية لحماية المعطيات، أو أي جهاز إداري تابع للسلطة التنفيذية يتهم بالاعتداء على حقوقه الرقمية، أو ضد المسؤولين عن المواقع والمنصات، أو مطعونا ضده في قضايا جنائية حتى لا يكون القضاء عونا على قمع الحريات. لذلك تظهر أهمية استقلال القضاء عن أي جهاز آخر وضمان حياد القاضي بتخليصه من أي ضغط يمكن أن يخضع له في عملية رقابته على الرقابة الرقمية، سواء رقابة جنائية أو مدنية، أو رقابة إلغاء[60].

وقد ورد التأكيد على الاعتناء بالقضاء في الرقابة البعدية على عملية الرقابة التي تقوم بها الدولة أو تأمر بها القطاع الخاص في توصيات الجمعية العامة[61] وتقارير الأمم المتحدة باعتبارها إحدى وسائل الانتصاف[62]، فمادام مجال الرقابة مقيد بالقيود التي تجيزها اتفاقيات حقوق الإنسان، فإنها ملزمة بأن تتيح للمتضرر من ممارسات الدولة وسيلة إنصاف فعالة، سواء كانت قضائية، إدارية أو تشريعية، أو أي نظام آخر ينص عليه قانون الدولة، مع دعوة الدول الأطراف السعي لتنمية التظلم القضائي على النحو المنصوص عليه في المادة 3/2/ ب من العهد الدولي للحقوق المدنية والسياسية، لاسيما أن القضاء هو الجهاز الوحيد الكفيل بردع المخالفات الجسيمة التي تتخذ طابعا جزائيا[63].

إن فعالية وسائل الانتصاف (وأهمها القضاء) مرهون بقدرتها على وقف الرقابة التعسفية، ومن ذلك قدرتها على الأمر بحذف البيانات أو غير ذلك من أشكال الجبر، وتخويلها الوصول التام بلا عوائق إلى جميع المعلومات ذات الصلة والموارد والخبرات الضرورية لإجراء التحقيقات، والقدرة اللازمة لإصدار الأوامر[64].

لكن الواقع أن الحكومات لا توفر هذا المعطى المهم في أجهزتها القضائية خصوصا الدول ذات الحكومات التسلطية، وهذا ما سجله المقرر الخاص المعني بتعزيز وحماية الحق

في حرية الرأي والتعبير "فرانك لا رو" في تقريره سنة 2013، اعتبر في بنده السادس/ ألف انعدام الرقابة القضائية إحدى الشواغل المتعلقة بالمعايير القانونية الوطنية، حيث جاء في التقرير تخطي الدول الإذن القضائي المسبق بمباشرة الرقابة الرقمية [65]، كما سجل المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير في تقريره 2019 ضعف نتائج الرقابة القضائية البعدية للرقابة الرقمية، إما لأن الشكاوى لم تلق صدى لدى الجهات القضائية في حالات نموذجية أوردها التقرير[66]، أو لأن النظام القانوني للدولة لا يتيح مقاضاة الجهات الحكومية المتورطة في الرقابة غير المشروعة، ما جعل "تمكين الضحايا من أدوات الجبر القانونية على الصعيد المحلي" من الالتزامات التي أوصى التقرير فرضها على الدول[67]، لاسيما أن الرقابة الرقمية التعسفية محددة الهدف عادة ما يكون ضحيتها من الصحفيين والنشطاء والمعارضين السياسيين.

في المقابل قد نجد القضاء في بعض الدول كالولايات المتحدة الأمريكية يرفض كل قانون من شأنه

خاتمة

إن الانترنت ليست شبكة عالمية حرة لا حدود لها، إنما تلك صورة وهمية لمرتاديها، فهي تدفق لكمّ من المعلومات في مسارات تعترضها الحواجز التي تضعها الرقابة أي كان مصدرها، تترصد حرية التعبير وحرية الرأي على الفضاء الرقمي بداعي الأمن بمعناه الواسع، وذلك عبر انتهاك الخصوصية، ولا تكاد أي دولة تسلم منها، إلا أنّ مداها يتسع ويضيق حسب النظام السياسي في الدولة، وكثيرا ما تتخذها دول العالم الثالث ذات الحكومات التسلطية وسيلة لقمع المعارضة، أو قمع المطالب الاجتماعية وذلك لغياب التأطير القانوني الدقيق لعملية الرقابة، سواء في القانون الدولي أو القوانين الوطنية. وقد خرجت الورقة بجملة توصيات :

1- تعزيز الهيئات المنشأة في القوانين الوطنية لحماية الخصوصية والمعطيات الشخصية وضمان استقلالها الفعلي، وتنطبق التوصية في الجزائر على السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي المنشأة بالقانون 07/18.

2- إتاحة الولوج الحر لجميع التصاريح والتراخيص الصادرة عن السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي وذلك بنشرها على الموقع الإليكتروني (بعد إنشائه) لضمان الشفافية.

3- إلزام مقدمي الخدمات الإلكترونية بإعلام المستخدم تلقائيا دون طلب منه بكل الهيئات التي حُوِّلت بياناته الشخصية إليها.

4- الإلزام القانوني للمنصات الإلكترونية بالشفافية في استعمالها وسائل الرقابة الآلية للمحتوى، عبر الإفصاح الإلزامي بطريقة استخدامها الرقابة الآلية (سياستها في حجب المحتوى).

5- تأطير عملية الرقابة الرقمية بنصوص قانونية تستجيب لمعايير الأمم المتحدة المتجلية في المبادئ الثلاثة عشر تحت طائلة إلغائها.

6- السعي إلى إكمال جهود الاتحاد الإفريقي في مجال حماية البيانات الشخصية، لاسيما الاتفاقية الإفريقية حول الأمن السيبيرالي وحماية البيانات ذات الطابع الشخصي 2014، بالإسراع في المصادقة عليها لتدخل حيز النفاذ.

7- الانضمام إلى / والسعي لإنجاح المساعي الدولية الرامية إلى حظر بيع تكنولوجيات الرقابة، بما فيها برامج الجوسسة الإليكترونية على غرار برنامج بيغاسوس.

8- تدعيم جهود المجتمع المدني الناشط في مجال حماية الحقوق الرقمية، لاسيما تلك العاملة على التحسيس والتصدي الناعم لآثار الرقابة الرقمية التي تمارسها حكومات الدول ضد المعارضين والصحفيين، على غرار منظمة "حملة" الفلسطينية التي تسعى لتكريس وحماية الحقوق الرقمية الفلسطينية.

9- تخويل جمعيات المجتمع المدني، لاسيما تلك الناشطة في مجال حماية المستهلك وحماية البيانات الشخصية من اللجوء إلى القضاء بدعاوى جماعية في حال انتهاك التشريعات الخاصة بحماية البيانات الشخصية.

10- إخضاع عملية الرقابة الرقمية لرقابة قضاء مستقل عن السلطة التنفيذية وعن الضغوط التي قد يخضع لها القاضي لضمان رقابة حقيقية لا شكلية، حتى لا تتحول إلى وسيلة قمع للحريات يساهم القاضي في إضفاء الشرعية عليها.

---

[1]Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance, written by Privacy Organizations and Experts Worldwide 2014, p. 4. Avaible en line : https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf).

[2]Assemblée Nationale, Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique, Rapport n° 3119: Numérique et libertés, un nouvel âge démocratique, présenté par : M. Christian PAUL et Mme. Christiane FERAL- SCHUHL, p. 151.

[3] CDH/ CCPR/C/GC 34, observations générale 34 sur l'art. 19, Genève 11- 29 juillet 2011, p. 5.

[4]Conseil d'Etat, le numérique et les droits fondamentaux, étude annuelle du conseil d'Etat 2014, La documentation Française, 65, p. 97

[5] Ibid, p. 133

[6] مجلس حقوق الإنسان، الدورة 27 ، تقرير مفوضية الأمم المتحدة لحقوق الإنسان، الحق في الخصوصية في العالم الرقمي، 30 جوان 2014، ص 6. (A/HRC/27/37)

[7] مجلس حقوق الإنسان، الدورة 23، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، فرانك لا رو، 17 أفريل 2013، فقرة 24، ص 8. (A/HRC/23/40)

[8] المرجع نفسه، الفقرة 79، ص 27.

[9] A/70/290, 6 août 2015, Rapport du Secrétaire général des Nations unies de 2015, paras. 14 - 16

[10] A/ HRC/27/37, 30 juin 2014, p. 6

[11] بيان المفوضة السامية لحقوق الإنسان أمام قمة رايتسكون 2022. متاح على:
https://www.ohchr.org/ar/taxonomy/term/768

[12] Billel Aroufoune, Michel Durampart, Le Hirak algérien ou l'émergence d'une expression citoyenne en contexte autoritaire, p. 12. Disponible en ligne : https://hal.archives-ouvertes.fr/hal-02969779/document

[13] Félix TREGUER, Surveillance numérique, Contribution à l'ouvrage collectif « Le Nouveau Monde: Tableau de la France néolibérale », Popelard Allan, Anthony Burlaud et Grégory Rzepski (éds.), Paris, Éditions Amsterdam, 2021, p. 5

[14] بيتر بي سيل، تر: ضياء وراد، الكون الرقمي، مؤسسة هنداوي، ص 218.

[15] المرجع نفسه، ص 221؛ زينة عبد الله محمد مصطفى، الرقابة الإلكترونية وحرية الرأي والتعبير: دراسة مقارنة بين مصر وإيران، المركز العربي لأبحاث الفضاء الإلكتروني (ACCR)، يونيو 2016. متاح على:
https://accronline.com/article_detail.aspx?id=25895#_Toc451362622

[16] Billel Aroufoune, Michel Durampart, op. cit, p. 12

[17] بيتر بي سيل، المرجع السابق، ص 238- 239.

[18] Warda Baba Hamed, L'espace public numérique à l'aune des mutations sociopolitiques en Algérie, Synergies Algérie, n° 29 – 2021, p. 195.

[19] A/HRC/23/40, para. 71.

[20] بشبخ محمد حسين، أثر المراقبة الرقمية على الحريات العامة، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، 2016- 2017، ص111.

[21] Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE. Disponible en ligne: EUR-Lex - 32006L0024 - FR - EUR-Lex (europa.eu)

[22] C-293/12- Digital Rights Ireland et Seitlinger e.a. Arrêt de la Cour (grande chambre) du 8 avril 2014 Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a. Demandes de décision préjudicielle, introduites par la High Court (Irlande) et le Verfassungsgerichtshof.Disponible en ligne : CURIA - Recueil général – Cour de justice (europa.eu)

[23] قانون 04/09 مؤرخ في 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 47/ 2009.

[24] بشبخ محمد، المرجع السابق، ص 110.

[25] مجلس حقوق الإنسان، الدورة 41، المراقبة وحقوق الإنسان، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، 28 ماي 2019، ص 6 (A/ HRC/41/35)

[26] زينت ستار حبار كاظم اللامي، الحماية المدنية للبيانات الشخصية عبر الأنترنت (دراسة مقارنة)، مجلة ميسان للدراسات القانونية، مج 1، العدد 5، 2021، ص 144.

[27] Hugue HENRI, « Pegasus » - système mondial d'espionnage de téléphones. Disponible en ligne : https://www.academia.edu/50058594/_Pegasus_syste_me_mondial_d_espionnage_de_te_le_phones_par_Hugues_HENRI

[28] Ibid, p. 4.

[29] هي فضيحة تجسس أطلقها إدوارد سناودن عبر صحيفة الغارديان البريطانية في جوان 2013، مفادها استخدام حكومة الولايات المتحدة الأمريكية البرنامجPRISM الذي وضعته وكالة الأمن القومي NSA للتجسس على مستخدمي عمالقة الويب جوجل وفايسبوك وياهو بموافقة هؤلاء.

[30] Logiciels espions : des experts demandent un moratoire sur les technologies de surveillance, 12/8/2021. Disponible en ligne: https://news.un.org/fr/story/2021/08/1101612

[31] تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، 28 ماي 2019،(A/ HRC/41/35)، ص 3

[32] المرجع نفسه، ص 6

[33] A/C.3/71/L.39/Rev.1, Le droit à la vie privée à l'ère du numérique, 16 novembre 2016, p. 5

[34] اللجنة المعنية بحقوق الإنسان، التعليق العام رقم 16: المادة 17 (الحق في حرمة الحياة الخاصة)، الدورة 32، 8 أفريل 1988، الفقرة 3.

[35] المرجع نفسه، الفقرة 4.

[36] A/HRC/27/37, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, Le droit à la vie privée à l'ère du numérique, 30 juin 2014, para. 21.

[37] Ibid., para. 23

[38] A/HRC/23/40,17 avril 2013, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, paras. 28 et 29.

[39] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). Disponible en ligne: EUR-Lex - 32016R0679 - FR - EUR-Lex (europa.eu)

[40] A/HRC/27/37., para. 24

[41]Rapport n° 3119: Numérique et libertés, op. cit, pp. 154-135

[42] انظر شروط القانون الذي يتحقق به شرط قانونية التدخل في: A/HRC/27/37, pars. 29 et 29.

[43] A/HRC/23/40, paras. 24- 27.

[44] CCPR/C/21/Rev.1/Add.7,27 août 1996, observation générale No 25, paras. 8, 12 et 25.

[45] CCPR/C/GC/34, 12 septembre 2011, observation générale No 34, para. 25

[46] Ibid, para. 28

[47] Ibid., para. 29.

[48] A/HRC/23/40, paras. 58- 60.

[49] A/HRC/41/35, para. 26.

[50] A/HRC/41/35, para. 24/a et para. 22 ; A/HRC/23/40, para. 79

[51]Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance, op. cit, p. 2

[52] Ibid, p. 7 ; A/HRC/23/40, para. 83/a

[53] A/HRC/23/40, para. 83/b

[54] Necessary and Proportionate: International Principles on the Application of Human Rights to Communications Surveillance, op. cit, p. 7

[55] Ibid, p. 11 - 12

[56] Ibid, p. 11.

[57] Ibid, p. 12.

[58] A/HRC/23/40, para. 86

[59] A/HRC/41/35, para. 15.

[60] بشبخ محمد، المرجع السابق، ص 159 وما بعدها؛ زينت ستار حبار كاظم اللامي، المرجع السابق، ص 299.

[61] A/RES/68/167, adoptée le 18 décembre 2013, intitulée « Le droit à la vie privée à l'ère du numérique » clause 4/d ; A/RES/69/166, adoptée le 18 décembre 2014, clause 4/d

[62]A/HRC/41/35, para. 39.

[63] Ibid, para. 41.

[64] Ibid.

[65] A /HRC/23/40, paras. 54- 57

[66] A/HRC/41/35, paras 40- 45.

[67] A/HRC/41/35, paras. 54 -55.

الملتقى الوطني الإفتراضي حول "حقوق الإنسان في العصر الرقمي"
مداخلة بعنوان: حماية مُصدري بطاقات الإئتمان من الإساءة في إستعمالها
الأستاذة: فضيل نورة – أستاذة محاضرة (ب)

مقدمة

لقد أدى التقدم الحضاري والتكنولوجي وظهور التجارة الإلكترونية إلى إختراع العديد من الوسائل والأدوات المتطورة وابتكار العديد من الأجهزة الدقيقة تتعامل بها المصارف مع زبائنها، ويتعامل بها الأفراد في معاملاتهم وأنشطتهم المالية والمصرفية والتجارية سواء أكان ذلك على المستوى المحلي أو على المستوى الدولي، بحيث أصبح الصراف الآلي (البنك الإلكتروني) سِمة عصرنا الحالي، وعصب تعاملنا اليومي، فظهرت بطاقة الائتمان الإلكترونية أو بطاقة الوفاء، التي أخذت في الإنتشار بصورة متسارعة يوماً بعد يوم وبدأت تحل محل النقود الحقيقية، بل والشيكات في التداول اليومي بين أفراد المجتمع.[1]

ولا مناص من القول أنّ بطاقات الائتمان أصبحت من أنشطة الخدمات المصرفية التى تقدمها مئات الألوف من البنوك وتجنى من وراء ذلك أرباحًا طائلة، ويتعامل بها مئات الملايين من الأفراد لشراء احتياجاتهم من السلع والخدمات وسحب مبالغ نقدية بموجبها دون الحاجة إلى حمل نقود معهم، وتمثل وسيلة سهلة للحصول على ائتمان قصير الأجل لهم، كما أن الملايين من المؤسسات الاقتصادية حول العالم تقبل البيع وتأدية الخدمات بموجب هذه البطاقات مما يزيد من مبيعاتها وضمان حصولها على حقوقها من مصدر البطاقة.[2]

ولقد تعددت التعاريف لتوضيح حقيقة بطاقات الائتمان، لكن يمكن القول إنّ أقرب تعريف هو التعريف الذى أورده مجمع الفقه الإسلامي الدولى ونصه: « **بطاقات الائتمان مستند يعطيه مصدره لشخص طبيعى أو إعتبارى بناء على عقد بينهما يمكنه من شراء السلع والخدمات ممن يعتمد المستند دون دفع الثمن حالاً لتضمنه إلتزام المصدر بالدفع، ومنها ما يمكن من سحب النقود من المصارف**»[3].

وتجدر الإشارة إلى أنّ هذه البطاقات تتعدد أنواعها لعدة إعتبارات، فمن حيث المزايا توجد البِطاقات العادية أو الفضية أو الذهبية وتختلف فيما بينها فى حدود الإئتمان والمزايا الإضافية التى يتمتع بها حاملها، وبحسب الجهة المصدرة توجد البطاقات التى ترعاها منظمة عالمية ويشارك فى إصدارها جميع البنوك على مستوى العالم مثل **فيزا وماستر كارد**، وبطاقات ترعاها وتصدرها مؤسسة مالية واحدة مثل

1محي الدين إسماعيل علم الدين، **موسوعة أعمال البنوك من الناحيتين القانونية والعملية**، ج2، 1993، ص737.

2 محمد عبد الحليم عمر، **بطاقات الإئتمان: ماهيتها والعلاقات الناشئة عن استخدامها بين الشريعة والقانون**، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون – بجامعة الإمارات العربية المتحدة 4 – 6 مايو 2003، ص1.

3 قرارات وتوصيات المجمع الفقهي فى دورته السابعة المنعقدة بجدة 1412هـ – قرار رقم 7/1/65 فقرة: رابعاً.

بطاقة أمريكان أكسبريس، وبطاقات تصدرها مؤسسات تجارية لعملائها ليشتروا منها فقط دون وجود بنك وسيط، كما توجد بطاقة ضمان الشيك، أما من حيث النظم التكوينية لها فتوجد البطاقة الممغنطة، والبطاقة الرقائقية، والبطاقة الذكية[1]، ومن حيث نطاق التعامل بها توجد البطاقات المحلية والإقليمية والعالمية، وكذا بحسب طبيعة العلاقة وكيفية التعامل بالبطاقة.[2]

ولاشك في أنّ إستخدام بطاقات الإئتمان يؤدي إلى سرعة وسهولة تسوية المعاملات من خلال عملية الدفع، وفي نفس الوقت تمكن المتعامل من الإحتفاظ بالنقود السائلة، وهو ما يؤدي إلى توسيع رقعة التبادل التجاري بصفة عامة، خاصة إذا علمنا أنّه بإمكان حامل البطاقة أن يستعملها حتى خارج الإقليم الذي صدرت فيها هذه البطاقات، وهو ما جعلها أداة لإزالة الحواجز المكانية (بل حتى الزمانية).

هذا، وتجدر الإشارة هنا إلى أن البنك قبل تسليمه لبطاقات الإئتمان عمومًا، يعد مجموعة من الشروط يعرضها على طالب البطاقة الذي ليس بإمكانه مُناقشتها، كما تحدد الإتفاقيات بشكل خاص، الحقوق والالتزامات الناشئة عن هذا التّعاقد بالنسبة للطرفين وأهمها: إلتزام حامل البطاقة بالإمضاء عليها، وبالحفاظ على سرية الرقم الشفري المقدم إليه؛ للوقاية من حالات الإستخدام من قبل الغير المحتملة (السرقة أو الضياع)، كما يلتزم بالتأكد قبل إجراء أي عملية دفع أو سحب بالبطاقة من كفاية رصيد حسابه أو من فتح إئتمان له من قبل البنك، وعدم عدم تجاوز السّقف المتفق عليه، ومن أهم إلتزامات حامل البطاقة سداد ما ترتب عليه من مستحقات جراء استخدام البطاقة إلى البنك في التواريخ المُتفق عليها، ووفقا للشروط المحددة في العقد.[3]

وهذه البطاقة تخول حاملها الحق في الحصول على تسهيل إئتماني من مُصدر هذه البطاقة، حيث يُقدمها إلى التاجر ويحصل بموجبها على سلع وخدمات، تسدد قيمتها من الجهة مُصدرة البطاقة، ويجب على حامل البطاقة سداد القيمة للجهة المصدرة للبطاقة خلال أجل متفق عليه سلفًا، في المقابل تحصل الجهة مصدرة البطاقة على فوائد مقابل توفير إعتماد لحاملها، لهذا تعد هذه البطاقات أداة إئتمانية حقيقية، فضلاً عن كونها أداةً للوفاء.

ومن هنا تبرز الإشكالية التالية: **ماهي الطبيعة القانونية لبطاقات الإئتمان في التشريعين المقارن والجزائري؟ وهل توجد حماية قانونية كفيلة لهذه البطاقات في ظل غياب نصوص قانونية خاصة؟**

---

1 للتعرف أكثر على أنواع البطاقات أنظر: رياض فتح الله بصيله، **الجوانب الشرعية والمصرفية والمحاسبية لبطاقات الائتمان**، مؤسسة إيتراك للنشر والتوزيع، القاهرة ، 1997، ص ص 17- 26.

2محمد عبد الحليم عمر، **بطاقات الإئتمان: ماهيتها والعلاقات الناشئة عن استخدامها بين الشريعة والقانون**، ص5.

3جميل أحمد، كهينة رشام، **بطاقة الائتمان كوسيلة من وسائل الدفع في الجازئر**، مجلة الإقتصاد الجديد، عدد ديسمبر 2009، ص116.

للإجابة لهذه الإشكالية إرتأينا الإعتماد على المنهج التحليلي الوصفي، ولمعالجة هذه الخطة قسمنا هذه المداخلة إلى مبحثين إثنين: الطبيعة القانونية لبطاقات الإئتمان وطرق إساءة إستخدامها **(مبحث أول)**، الحماية القانونية لبطاقات الإئتمان **(مبحث ثان)**.

المبحث الأول: الطبيعة القانونية لبطاقات الإئتمان وطرق إساءة إستخدامها

لكي يكون في مقدورنا من بيان نطاق حماية مُصدري بطاقات الإئتمان الإلكترونية في ظل التشريعات المقارنة بصفة عامة وعلى ضوء التشريع الجزائري بصفة خاصة، علينا أن نحدد أولاً طبيعتها القانونية، وقد أثار عدم التنظيم القانوني للعقود التي تعد الأساس القانوني للوفاء ببطاقة الإئتمان خلافاً محتوماً حول طبيعتها القانونية لوجود مزج كبير لصور ومفاهيم قانونية لهذا العقد بسبب الصياغة المتبعة لها والتي تنفرد بها، بهدف ضمان استيفائها لحقوقها كاملة.

المطلب الأول: التكييف القانوني لبطاقات الإئتمان في القانون المقارن والتشريع الجزائري

اختلف الفقه حول الطبيعة القانونية لبطاقة الائتمان وخاصة أن أحكامها تختلف من بلد إلى آخر ومن بنك إلى آخر، وهذا ماسنتعرض اليه بالتفصيل في الفروع الآتية.

الفرع الأول : التكييف القانوني لبطاقات الإئتمان في القانون المقارن

أدى الإختلاف حول الطبيعة القانونية لبطاقات الائتمان بالمشرع المصري إلى عدم وضع تعريف أو تنظيم قانوني لها، بل اكتفى بإدراجها ضمن العمليات البنوك وفقا لما جاءت بها المادة 300 من القانوني التجاري المصري.[1]

أمّا المشرع الفرنسي أشار فقط إلى وظيفتها في قانون النقد و المالي حيث نصت المادة L311-3 على أنها: " **تعد وسائل دفع كل الوسائل التي تسمح لكل شخص بأن يحول أموال مهما كان السند أو الوسيلة التقنية المستعملة في ذلك.**"2

قدم القضاء الفرنسي تعريف لها في الحكم الصادر من محكمة النقض أنّها: "**بطاقة إلكترونية تمكن حاملها من سحب الأموال من أجهزة الصراف الآلية، كما تمكنه من الحصول على حاجيات دون أن يقوم بالدفع الفوري، فيقوم بتقديم البطاقة للتاجر محولا بذلك الالتزام بالدفع إلى البنك، والذي يقوم باقتطاع هذه المبالغ من حساب الحامل في وقت لاحق وفقًا لما تمّ الاتفاق عليه في العقد الذي يجمعهما** ".

1عاصم حنفي محمود موسى، "**الطبيعة القانونية لبطاقة الائتمان**"، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية من الشريعة والقانون، كلية الشريعة والقانون، جامعة الأزهر، د ت ن، ص.867 . عبد الرحمان صوفية، **النظام القانوني لبطاقة الائتمان**، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون الأعمال، كلية الحقوق و العلوم السياسية، جامعة محمد لمين دباغين، سطيف،2015، ص.17 .

2 Article L.311-3 du code monétaire et financier français .
https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006072026/

ويوجد هناك أكثر من رأي بصدد تحديد الوصف القانوني لبطاقة الائتمان الإلكترونية:

يرى إتجاه أن التعامل ببطاقة الائتمان الإلكترونية مع الغير سواء أكانوا تجاراً أو شركات يعتبر وكالة يتم بمقتضاها توكيل حامل البطاقة البنك الذي أصدر البطاقة في دفع ثمن السلعة أو الخدمة التي حصل عليها ثم يخصمها البنك من حسابه الموجود لديه، إذن هذا الرّأي يرى بوجود عقد وكالة، الموكل هو حامل البطاقة والوكيل هو البنك، وهذا هو رأي القضاء الإنكليزي في طبيعة الوفاء ببطاقة الإئتمان[1]، إلاّ أنّ هذا الرأي منتقد للأسباب التالية:

1- إن هذا الوصف يخالف ما هو معمول به في التداول ببطاقة الائتمان وتحديداً مع بعض القوانين التي خصصت نصوصاً قانونية لحماية بطاقة الائتمان من أي اعتداء.

2- إن بعض القوانين ومنها القانون الفرنسي لا يجيز الرجوع في أمر الدفع إلا في الحالات التي تفقد فيها البطاقة، أو تسرق، أو في حالة التصفية القضائية، بالإضافة إلى أن طبيعة الحوالة تمكن الآمر بالدفع أن يلغي الحوالة متى أراد، إلاّ أن هذه الميزة لا توجد عند استخدام بطاقة الائتمان، ومن ثم يعد الدفع عن طريق بطاقة الائتمان باعتبارها وكالة لا شك أن فيه مخالفة للواقع العملي والميداني والقانوني.[2]

ويذهب رأيٌ آخر إلى القول بأنّ بطاقة الائتمان الإلكترونية هي نقود إلكترونية تشبه العملات الأخرى، كالنقود الورقية والمعدنية المعترف بها في التداول قانوناً وتعاملاً[3] ، إلا أن هذا الرأي منتقد لأنه يتجاهل الصفة الذاتية للنقود باعتبارها أداة للوفاء والتعامل والقبول الإلزامي بين الأفراد وهي قابلة أيضاً لإعادة الاستعمال من عدة أشخاص، وهذا مالا يتلاءم وبطاقة الائتمان التي تعد من النقود المكتوبة ويتم تداولها بطريقة آلية عن طريق استعمالها بأدوات إلكترونية حديثة ومن ثم فهي غير قابلة للتداول.

في حين يذهب إلى القول بأنّ بطاقة الائتمان الإلكترونية هي أداة للوفاء بطبيعتها مستحقة الدفع بمجرد الإطلاع عليها ولا يجوز الرجوع فيها إلا وفقاً للحالات المحددة على سبيل الحصر في الاتفاق والمتمثلة في فقدانها أو سرقتها أو انتهاء العمل بها بين العميل والبنك، وهي بذلك تتشابه مع الشيك كأداة للوفاء بمجرد الإطلاع لا يجوز تحويله إلى أداة ائتمان فقط، ويمكن القول بعدم إمكانية إخضاع بطاقة الائتمان الإلكترونية لنفس أحكام الشيك لاختلاف كل منهما شكلاً وموضوعاً وحماية قانونية، مما يستدعي خضوع كل منهما لقواعد خاصة به من حيث التجريم والمسؤولية.

وأخيرًا هناك من يقول: إن بطاقة الائتمان لها طبيعة خاصة مميزة، فعقد بطاقة الائتمان هو مزيج من الوكالة والضمان والتعهد عن الغير والقرض، وان جانب الضمان أو الكفالة هو الأغلب، لأنّ ذمة العميل

---

1 Howard Johson, credit cards. International Banking Law, Nov. 1988, pp. 82-83.

2 جميل عبد الباقي الصغير، مصدر سابق، ص109؛ محمد صبحي نجم، **المسؤولية الجزائية عن الاستخدام غير المشروع لبطاقة الائتمان**، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون لكلية الشريعة والقانون وغرفة تجارة وصناعة دبي الذي عقد في دولة الإمارات العربية المتحدة للفترة من 10-2003/5/12، ص1163.

3 Tronche, **La monnaie électronique**, Revue de L'association nationale en Droit, No. 42, 1982, p03.

حامل البطاقة تبرأ أمام التاجر بثمن المشتريات بمجرد تقديم البطاقة بضمان وكفالة مصدر البطاقة الذي يقوم بالوفاء فيما بعد.[1]

الفرع الثاني: الطبيعة القانونية لبطاقات الإئتمان في التشريع الجزائري

إن وضع نظام الدفع بالبطاقة لن يكون ناجحًا إلاّ إذا كان نطاق قبولها واسعًا من قبل جميع البنوك، وفي هذا الإطار شعر النظام البنكي الجزائري بأهمية وضع نظام بنكي مُشترك لوسائل الدفع، يستجيب لرغبات الزبائن وفق أعلى شروط الأمن.[2]

فبالنسبة للمشرع الجزائري لم يضع تعريفًا خاصًا بالبطاقة الائتمان رغم انتشارها مؤخرًا في الجزائر، بل تعرض لتعريف بطاقة الدفع بصفة عامة، وهذا وفق **الأمر03-11** المتعلق بالنقد والقرض[3] تنص المادة 69 منه كالاتي:" **تعتبر وسائل دفع كل الأدوات التي تمكن كل شخص من تحويل الأموال مهما يكون السند أو الأسلوب التقني المستعمل**"، لتعريف المتعلق بوسائل الدفع ينطبق تمامًا على بطاقة الائتمان، كما أن المادة 66 من نفس الأمر تعرف العمليات المصرفية كما يلي :" **تتضمن العمليات المصرفية تلقي الأموال من الجمهور وعمليات القرض، وكذا وضع وسائل الدفع تحت تصرف الزبائن وإدارة هذه الوسائل**".

يفهم من خلال عبارة وسائل الدفع تحت تصرف الزبائن هي إشارة بصورة غير مباشرة لتعريف بطاقة الائتمان لوظيفتها الأساسية تحويل أو سحب الأموال، وهذا ما تضمنه القانون التجاري الجزائري المعدل بموجب الأمر 05-02 في الباب الرابع تحت عنوان "**وسائل وطرق الدفع**" وخصص الفصل الثالث منه لموضوع بطاقات الدفع و السحب.

قام المشرع الجزائري بالتنظيم أحكام الدفع الإلكتروني في المادتين 543 مكرر 23 و543 مكرر 24 .تنص المادة 543 مكرر في فقرتها الأولى من القانون التجاري الجزائري على مايلي:

"**تعتبر بطاقة دفع كل بطاقة صادرة عن البنوك والهيئات المالية المؤهلة قانونا تسمح لصاحبها بتحويل أو سحب الأموال**"، في الوقت الحالي لا يوجد أي نص قانوني صريح من طرف المشرع الجزائري يتضمن هذا النوع من العمليات المصرفية في الجزائر، ما عدا هذه الأحكام القانونية العامة.

---

1 د. ابو الوفا محمد ابو الوفا ابراهيم، مصدر سابق، ص2047

2جميل أحمد، كهينة رشام، **بطاقة الائتمان كوسيلة من وسائل الدفع في الجازئر**، المرجع السابق، ص133.

3**أمر رقم 03-11** مؤرخ في 26 أوت 2003 متعلق بالنقد والقرض، جريدة رسمية عدد52 ، صادر في 27 أوت 2003 معدل بالقانون رقم 17-10 مؤرخ في 20 محرم عام 1439 الموافق لـ 11 أكتوبر 2017 . الصادر في 21 محرم 1439 الموافق لـ 12 أكتوبر 2017 .

وضعت المصارف حيز تداول عقود نموذجية واتفاقيات من أجل نمو و تكريس طريقة الدفع الإلكترونية، وهذا لسد الفراغ التشريعي.[1]

المطلب الثاني: طرق وأساليب إساءة إستخدام بطاقات الإئتمان

تعد عملية الدفع عن طريق بطاقات الإئتمان عملية مصرفية، قد تكون داخل نفس الإقليم، كما قد تتعداه إلى خارجه لتصبح عملية دولية تتعدى فيها الأطراف أين تتم عبر فضاء معلوماتي مفتوح، هذا ما يدفع ببعض المحتالين على القانون الدخول إلى سوق هذه البطاقات، حيث يقومون باستعمال شتى الطرق لبلوغ قصدهم.

وإذا كانت صور هذا الإعتداء متعددة ومتنوعة، لكننا سنسلط الضوء على أهم الصور التي تقع من طرف حامل البطاقة، وكذا من الغير.

والجدير بالإشارة أن حامل البطاقة هو ذلك الشخص الذي حصل على البطاقة من البنك بمقتضى إتفاق بينهما، بمفهوم آخر هو ذلك الشخص الذي أبرم عقدًا مع البنك محله تسليم بطاقة إئتمان، علمًا أنّ هذا العقد يجب أن يكون مستوفيًا لجميع أركانه وشروطه المنصوص عليها عمومًا في القواعد العامة.

ويمكننا تصور إساءة استعمال الحامل لبطاقته الإئتمانية من خلال عدة طرق أو أساليب، لعل أبرزها وأهمها مايلي:

الفرع الأول: إستعمال بطاقة الإئتمان رغم إنتهاء صلاحيتها

لأسبابٍ أمنية، فإنّ الأصل أنّ لبطاقة الإئتمان مدة معينة ومحددة بدقة يعلمها حامل البطاقة، لأن هذه المدة مدونة على واجهة البطاقة.

فإذا انتهت صلاحية بطاقة الائتمان سواء لإلغائها أو لانتهاء مدتها وطلب البنك مصدر البطاقة من حاملها ردها، التزم حامل البطاقة بإعادتها إلى البنك لأنها سلمت إليه كعارية إستعمال فإذا رفض ردها يعتبر حامل البطاقة خائناً للأمانة، لأن البطاقة سلمت إليه على سبيل الأمانة لإستعمالها، وهذا ما أكد عليه القضاء الجنائي الفرنسي حيث قضت محكمة باريس بأحقية البنك في استرداد بطاقة الإئتمان، وفرضت غرامة تهديدية على الحامل بمقدار مبلغ مالي عن كل يوم تأخير في ردها.[2]

نخلص إلى القول بأنّ حامل بطاقة الإئتمان إذا امتنع عن رد بطاقة الائتمان إلى البنك، رغم ثبوت علمه بالاخطار المرسل إليه من البنك بالرد لانتهاء صلاحيتها، حيث تسلم هذه البطاقة إلى الحامل

---

1 أمحمدي بوزينة أمنة، "**النظام القانوني لتعامل ببطاقة الائتمان المتداولة في البنوك الجزائرية**"، مجلة القانون، كلية الحقوق والعلوم السياسية ، جامعة حسيبة بن بوعلي، العدد، 08 الشلف ، 2017، ص. 148.

2كيلاني محمود، **النظام القانوني لبطاقات الوفاء والضمان**، رسالة دكتوراه، جامعة عين شمس، 1996، ص818-819.

بموجب عقد الإضمام الذي يسمح له على سبيل عارية الاستعمال[1]، استخدامها وإعادتها بعد انتهاء العقد أو إلغائه وتظل البطاقة ملكاً للجهة المصدرة وليس للحامل، وبيان ذلك أن بطاقة الإئتمان تعد من قبيل الأشياء، وهي تعد منقولاً ذا طبيعة مادية وهو ما تقع عليه جريمة خيانة الأمانة، فضلاً عن أن الإمتناع عن رد البطاقة إلى البنك رغم طلبها – حتى ولو لم يستعملها بعد ذلك – يُعد اختلاساً ومن باب أولى لو إستخدمها فإن استخدامه هذا للبطاقة رغم إلغائها لا يجوز ويكشف عن تغيير نيته في نقل حيازته للبطاقة من حيازة ناقصة إلى حيازة كاملة.[2]

كما يمكننا أن نتصور هذا الأمر في الجزائر مثلاً حيث أن يمكن لحامل البطاقة المنتهية الصلاحية أن يستعملها في تعاملاته مع التجار يعني بغض النظر عن تكييف فعله قانونيًا، بحيث يكفي أن ما قام به العميل يعد عملاً غير مشروعًا، وهو ما دفع بالبنك إعتماد إجراء احترازي يتمثل في ابتلاع ماكنة الصراف الإلكتروني لكل بطاقة منتهية الصلاحية.

الفرع الثاني: إساءة استخدام بطاقة الائتمان الضائعة أو المسروقة

من المشاكل التي تواجه حامل بطاقة الإئتمان سرقتها أو ضياعها، ويزيد من صعوبة المشكلة، ما لوحظ في العمل من أن العملاء يخشون نسيان الرقم السري (PIN)، فيكتبونه على البطاقة أو في المفكرة الشخصية ومن ثم عندما تسرق البطاقة أو المفكرة يسهل على السارق معرفة الرقم السري، وللتقليل من مخاطر فقدان البطاقة أو سرقتها، فإنه ينص في عقد إنضمام الحامل لبطاقة الإئتمان على إلتزامه بالمحافظة عليها وإخبار البنك أو الجهة المصدر للبطاقة بفقدها أو سرقتها وذلك لتجنب استعمال الغير لها.

وعندما لا تحدد الجهة المصدرة للبطاقة طريقة معينة للإخبار، يكون الحامل الحق في اختيار الأسلوب المناسب للإخبار حتى وإن كان عن طريق الهاتف ولكن يجب إثبات الإخبار عندئذ، لأنّ المسؤولية بعد الاخطار تنتقل من عاتق الحامل إلى عاتق الجهة مصدرة البطاقة[3].

وقد يحدث أن يبلغ حامل بطاقة الإئتمان الجهة المصدرة لها بفقدانها أو سرقتها، ثم يستخدمها بعد ذلك في السحب أو الوفاء وقبل أن يقوم البنك ببرمجة الأجهزة الآلية لتوزيع النقود بعدم قبول البطاقة المبلغ عن فقدها أو سرقتها، حيث يقع التواطؤ بين حامل بطاقة الائتمان والتاجر، كأن يتفقان على

1أنظر نص المادة (341) من قانون العقوبات المصري والمادة (362) من قانون العقوبات القطري والمادة (404) من قانون العقوبات الإماراتي والمادة (314–1) من قانون العقوبات الفرنسي.

2 محمود أحمد طه، **شرح قانون العقوبات (القسم الخاص)**، ج3، دار النهضة العربية، القاهرة، 2001، ص405.

3محمد بلعرج، **ماستر كارد تستكمل خطة توسعها العالمية السريعة في الشرق الأوسط وشمال افريقيا**، مجلة اتحاد المصارف العربية، ع (257)، مايو 2002، بيروت، ص64.

إخطار البنك، بفواتير مبيعات بمبالغ نقدية كبيرة من التاجر إلى الحامل، ثم يدعي الحامل أن بطاقته مفقودة أو مسروقة وأنّه لم يشتر شيئاً من هذه البضائع كي تكون مسؤولية الوفاء بقيمة هذه البضائع على عاتق البنك، ثم يقتسم الحامل مع التاجر المبلغ النقدي بعد صرفه من البنك، وعندئذ يكون كل من الحامل والتاجر مرتكبين لجريمة الإحتيال باعتبارهم فاعلين أصليين لقيامهما بطرق إحتيالية تحمل البنك على الوفاء بثمن هذه البضائع للتاجر.[1]

وقد يرتكب الحامل وحده هذا الفعل غير المشروع، دون تواطؤ مع التاجر، وذلك بقيام الحامل بتنفيذ كل ما يجب عليه في حالة فقد البطاقة أو سرقتها من معارضه لدى البنك مصدر البطاقة مع إبلاغ السلطات المختصة، في حين أن البطاقة ما زالت في حوزته مستمراً في استخدامها في الوفاء لدى التجار المزودين بآلة الطباعة اليدوية خوفاً من اكتشاف أمره عن طريق الآلات الحديثة، بحيث لا يمكن اكتشاف الغش لدى هؤلاء التجار إلا في وقت لاحق عن طريق المواجهة بين التاجر والحامل، وقد يتحقق الغش بالاحتيال على التاجر لعدم مراجعة رقم البطاقة على أرقام البطاقات الملغاة نتيجة لفقدها أو سرقتها، وذلك بالإدعاء باستعجاله وأنه إذا لم يبع له التاجر فهناك غيره، أو أن مظهره يوحي بالثقة فيخجل التاجر من مراجعتها، ففي كل هذه الحالات يكون الحامل قد تحايل لحمل البنك على الوفاء بثمن مشترياته لدى التاجر، ممّا يعد طرقاً احتيالية بالإدعاءات الكاذبة وتقديم مستندات تؤيد هذه الإدعاءات وهذا يكفي لقيام الفعل غير المشروع، ذلك أن الحامل قد فقد صفته كحامل شرعي ابتداء من لحظة المعارضة أو الاخطار بفقد البطاقة أو سرقتها، وبالتالي يجب أن ينظر إليه على أنه من الغير ممّا يؤدي إلى حمل البنك على الاعتقاد بأن أي استخدام للبطاقة بعد تاريخ المعارضة يكون من عمل الغير.[2]

المبحث الثاني: الحماية القانونية لبطاقات الإئتمان

إن الاعتداء الذي قد يحصل على بطاقات الإئتمان إما أن يكون من قبل الحامل الشرعي للبطاقة أو من قبل الغي ، وعليه سوف نتعرض في هذا المبحث إلى الحماية المدنية لبطاقة الإئتمان **(مطلب أول)**، والحماية الجنائية لبطاقة الائتمان **(مطلب ثاني)**.

المطلب الأول: الحماية المدنية لبطاقة الإئتمان

إنّ الحماية المدنية لبطاقة الدفع تنشأ عن بطاقة الوفاء علاقات قانونية بين أطرافها الثلاث بمقتضى عقد يحكم العلاقة الناشئة بين مصدر البطاقة وحاملها، وعقد يحكم العلاقة بين المصدر والتاجر وآخر

1علي عدنان الفيل، **المسؤولية الجزائية عن إساءة استخدام بطاقة الائتمان الإلكترونية (دراسة مقارنة)**، المدونة الإلكترونية، أكتوبر 2015، بدون ترقيم.

2 جميل عبد الباقي الصغير، **الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة**، ط1، دار النهضة العربية، القاهرة، 1999، ص96. كيلاني محمود، مرجع سابق، ص876.

يحكم العلاقة بين الحامل والتاجر، وتعتبر هذه العقود من العقود الملزمة لجانبين وفي المقابل يترتب على الإخلال بأحد الالتزامات قيام المسؤولية المدنية، وبالتالي إعطاء الحق للطرف المتضرري فسخ العلاقة والمطالبة بالتعويض عن الضرر الذي نتج عن عدم تنفيذ أحد هذه الالتزامات، وهذه العقود تخضع للقواعد العامة في القانون المدني، ويكون أساس المطالبة بالتعويض هو المسؤولية العقدية متى توافرت أركانها من خطأ وضرر وعلاقة سببية.[1]

يترتب على العقد المبرم بين حامل البطاقة ومصدرها التزامات على عاتق الحامل ينبغي عليه احترامها والقيام بها، وكل إخلال بهذه الالتزامات يرتب مسؤولية عقدية وذلك في عدة حالات لعل أبرزها:

الفرع الأول: مسؤولية حامل البطاقة عن الإخلال بالالتزام باستعمالها في حدود المبلغ المتفق عليه

بحيث إذا تجاوز هذا المبلغ تقوم مسؤوليته العقدية وكان مسؤولا في مواجهة المصدر بمبلغ الزيادة وذلك في حالة الاتفاق بضمان الوفاء من دون تحديد للحد الأقصى لهذا الضمان، أما إذا وجد بند في العقد بين الحامل والمصدر يقضي بأن هذا الأخير لا يتضمن الوفاء إلا في حدود المبلغ المسموح به، فإن مسؤولية الحامل تكون تجاه التاجر وليس تجاه المصدر بمقتضى عقد البيع المبرم بينهما لأنّ المصدر هنا سوف يلتزم بالوفاء في حدود المبلغ الذي تضمنه العقد بينه وبين الحامل، ويبقى متمسكا به ، إذا تجاوز صاحب البطاقة المبلغ الذي يملكه في حسابه وهو سيء النية، أي يكون عالما بذلك، فإنه يتحمل المسؤولية المدنية بالتعويض عن الضرر الذي لحق البنك أو التاجر حسب الحالة.[2]

وهذا على أساس الإخلال بالالتزام التعاقدي، ويكون من حق الجهة المصدرة سحب البطاقة من الحامل لأنه أهدر الثقة الموجودة بينه وبين المصدر، إلا أنه وفي حالات خاصة تقتضيها ظروف التعامل في الوسط التجاري يمكنه (الحامل) أن يتجاوز الحد المسموح به في العقد إلى منحه البنك ترخيصًا بذلك، بمعنى أن البنك يمنح ائتمانا للحامل فيدفع المبلغ الزائد بدلاً عنه، ثم يعود عليه فيما بعد، بعد مرور المدة المتفق عليها بموجب اتفاق خاص بينهما، وهو اتفاق مستقل لا ينفي صفة الوفاء الفوري التي لا تمنح أي ائتمان طبيعتها إلا بموجب إتفاق مستقل حسب ارادة الأطراف، وهنا تقوم نسؤولية الحامل في حالة امتناعه عن رد مقدار التجاوز الذي نفذه البنك المُصدر.[3]

الفرع الثاني: مسؤولية حامل بطاقة الوفاء عن إخلاله بالتزام رد بطاقته

---

1 غنام محمد غنام، **الحماية الجنائية لبطاقات الإئتمان الممغنطة**، المنشور على موقع الدليل الإلكتروني للقانون العربي والمتاح على الرابط التالي: www.arablawinfo.com

2عبد الحليم بن مشري، **الحماية القانونية لبطاقات الدفع الإلكترونية**، مجلة الاجتهاد القضائي، المجلد 12، العدد01، مارس 2019، ص57.

3أبو الوفا محمد ابو الوفا إبراهيم، **المسؤولية الجنائية عن الإستخدام غير المشروع لبطاقة الإئتمان في القانون المقارن والفقه الإسلامي**، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون لكلية الشريعة والقانون وغرفة التجارة وصناعة دبي والذي عقد في الإمارات العربية المتحدة للفترة من 10-2003/05/12، ص 2044.

إذ يرتب العقد المبرم بين الجهة المصدرة للبطاقة وحاملها التزامًا على عاتق هذا الأخير برد البطاقة بمجرد انتهاء مدة صلاحيتها، أو بفسخ العقد بينهما، لذلك نتعقد مسؤولية حامل البطاقة في حالة الإمتناع عن ردها إلى المصدر لأحد السببين السابقين، فإذا إستعملها بعد ذلك التاريخ تنعقد مسؤوليته المدنية عن المبالغ التي استخدمها باستعمال البطاقة، ففسخ العقد يترتب عليه إعادة المتعاقدين إلى الحالة التي كانا عليها قبل التعاقد، فإذا استحال ذلك جاز الحكم بالتعويض.[1]

الفرع الثالث: مسؤولية حامل البطاقة عن إخلاله بالتزام إجراء المعارضة

يقع على الحامل التزام إبلاغ مُصدر البطاقة عن فقدان البطاقة أو سرقتها أو ضياعها وعلى كل الملابسات المتعلقة بذلك، وهو ملزم ببذل عناية الرجل العادي في الحفاظ عليها، لذلك فإذا ثبت أن ضياعها ناتج عن إهمال وتقصير من الحامل فإن مسؤوليته تنعقد عن المبالغ التي استخدمها من حصل على البطاقة بعده، وهو ما نصت عليه أغلب القوانين المقارنة[2] .

الفرع الرابع: مسؤولية حامل البطاقة عن إخلاله بالتزام تقديم بيانات صحيحة

يقع على عاتق الحامل التزام بأن يصرح بحسن نية عن كل ما يتعلق بشخصيته للبنك المصدر للبطاقة، فإذا خالف هذا الالتزام وقدم بيانات خاطئة باستعمال الطرق الاحتيالية، ذلك فمسؤوليته المدنية تكون قائمة، إلى جانب اعتبار تصرفه هذا جريمة نصب لتقديمه بيانات كاذبة وخاطئة عن شخصه، كما أنه إذا قام الحامل بإعارة البطاقة لشخص آخر لإستعمالها فإنه يعتبر قد خالف التزامًا تعاقديًا وهو شخصية بطاقة الدفع، ويعتبر مسؤولا مسؤولية عقدية يترتب عليها تحمل النفقات التي قام الغير بتنفيذها واسترداد البطاقة من البنك، إضافة إلى فسخ العقد.[3]

المطلب الثاني: الحماية الجنائية لبطاقة الإئتمان

الأصل أن الإخلال بالشروط العقدية الواردة في العقد المبرم بين البنك المُصدر والتاجر والعميل يثير المسؤولية المدنية لهذا الأخير في مواجهة كل من البنك والتاجر، وبالمقابل قد تشكل بعض التصرفات غير المشروعة للحامل سيء النية اعتداء على الذمة المالية للبنك والتاجر، مما يثير المسؤولية الجزائية لهذا الأخير، وتتجسد الحماية الجنائية لبطاقات الأئتمان في عدة مواضع وهي كالآتي:

الفرع الأول: الاعتداءات الواقعة على البطاقة الإلكترونية من قبل حاملها

من المعروف أن المسؤولية الجزائية شخصية فلا يسأل عنها إلا من ارتكب الجريمة أو شارك فيها4، ويتصور وقوع الاعتداءات التي يقوم بها العميل على بطاقات الإئتمان في عدة فروض منها :

استخدام بطاقة انتهت صلاحيتها، استخدام بطاقة ملغاة، إساءة استعمال بطاقات الوفاء.

1عبد الحليم بن مشري، **الحماية القانونية لبطاقات الدفع الإلكترونية**، المرجع السابق، ص58.

2فايز رضوان، **بطاقات الوفاء**، المطبعة العربية، القاهرة، 1990، ص71

3 CAVALDA CH, **Le droit pénal des cartes de paiement et de crédits**, Dalloz, 1994, p1.

4كيلاني محمود، مرجع سابق، ص 57

ونكتفي بعرض هذه الصور الثلاث نظرًا لكثرتها وتعددها:

أولاً: استخدام بطاقة إلكترونية منتهية الصلاحية

الأصل أن بطاقة الإئتمان محددة المدة، وقد تكون عام أو عامين، وعلى الحامل عند انتهاء مدتها أن يرجعها إلى البنك أو المؤسسة المالية المُصدرة لها، وان استمر في استعمالها بعد انقضاء هذه المدة فسوف يعاقب جنائيًا، وهو بهذا الفعل يعتبر مُرتكبا لجريمة خيانة الأمانة في مواجهة البنك، ومرتكبًا لجريمة النصب في مواجهة التاجر.

أما جريمة خيانة الأمانة فقد نصت المادة 376/01 قانون العقوبات الجزائري[1] على أنه "**كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقود أو بضائع أو أوراقًا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت التزاما أو إبراء لم تكن قد سلمت إليه إلا على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الاستعمال أو لأداء عمل باجر أو بغير اجر بشرط ردها أو تقديمها أو لاستعمالها أو لاستخدامها في عمل معين، وذلك إضراراً بمالكيها أو واضعي اليد عليها أو حائزيها يعد مرتكبا لجريمة خيانة الأمانة، ويعاقب بالحبس من ثلاثة أشهر إلى ثلاث سنوات وبغرامة من 500 إلى 20000 دينار.**" وجريمة خيانة الأمانة تنطبق على الحامل الذي يحتفظ بالبطاقة بعد انتهاء مدة صلاحيتها، ولذلك يتعرض الحامل لعقوبة جريمة خيانة الأمانة المعاقب عليها بالحبس من ثلاثة أشهر إلى ثلاث سنوات، وبغرامة مالية من 500 إلى 20.000 دج، بالإضافة إلى العقوبات التكميلية المنصوص عليها في المادة 09 مكرر من قانون عقوبات، وعلاوة على ذلك يجيز قانون العقوبات للجهات القضائية الحكم على الشخص المدان بالعقوبات التكميلية الاختيارية تصل إلى حد المنع من استعمال بطاقة الوفاء، بما في ذلك الشيك[2].

أما ارتكاب جريمة النصب في مواجهة التاجر، فقد نصت المادة 372 من قانون العقوبات الجزائري على أن: "**كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات أو الحصول على أي منها أو الشروع في ذلك، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث الأمل في الفوز بأي شيء أو ي وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء.**"

---

1 ابراهيم زكي، "بطاقة الائتمان والمثلث الخفي"، مجلة البنوك ، ص79. زين محمد الزماني، **التزوير والتزييف عن طريق بطاقات الائتمان**"، مجلة المحامي، عدد3، الرياض، 1421هـ .ص53.

2 HOWARD Johson, credit cards, International banking law, Nov1988, pp 82-83.

وبذلك فالحامل المرتكب لجريمة النصب يعاقب بالحبس من سنة على الأقل إلى 05 سنوات على الأكثر وبغرامة من 500 إلى 20.000 دج كما يجوز الحكم عليه بالحرمان من جميع الحقوق الواردة في المادة 14 أو من بعضها بالمنع من الإقامة وذلك لمدة سنة على الأقل و05 سنوات على الأكثر.

ثانيًا: استخدام الحامل للبطاقة الالكترونية الملغاة

قد يحدث أن يقوم البنك أو المؤسسة المالية المصدرة للبطاقة بإلغائها أثناء سريانها، وذلك لأن الحامل قد أساء استعمالها ولذلك يعاقب بسحب البطاقة منه، فيمتنع عن ردها ويقوم باستعمالها رغم تنبيهه بإعادتها إلى مصدرها، والحقيقة أنه يجب مؤاخذة حامل البطاقة عن هذا الفعل لأنه باستعماله لها رغم قرار السحب يكون قد فقد سنده الشرعي في استعمالها، ويتعين مساءلته جنائيًا حماية للثقة في هذه البطاقة وفي المعاملات التي تستخدم فيها ومنها التجارة الالكترونية خصوصًا.[1]

ويأخذ استخدام الحامل للبطاقة الملغاة نفس الحكم بالنسبة لاستخدام البطاقة المنتهية الصلاحية أي يشكل جريمة خيانة أمانة في مواجهة البنك، لأنه يتعين على الحامل إرجاع البطاقة الملغاة إلى البنك مصدرها، وجريمة النّصب في مواجهة التاجر حسن النية[2]، وعليه فإنّ استخدام البطاقة الملغاة يشكل جريمة يعاقب عليها قانون العقوبات الجزائري وفق الفقرات السابقة الخاصة باستخدام البطاقات المنتهية الصلاحية .

ثالثًا: إساءة استخدام بطاقة الإئتمان

تتحقق في فرضين اثنين : الأول: أن يقوم الجاني حامل البطاقة – بشراء سلع وخدمات تتجاوز قيمتها المبلغ الذي يضمنه البنك كحد أقصي لها، الثاني: أن يقوم حامل البطاقة بشراء سلع وخدمات لا تتجاوز قيمتها المبلغ الذي يضمنه البن لكن تتجاوز الرصيد الذي في حساب، وفي كلا الفرضين تتحقق أساءة استعمال البطاقة[3].

وقد اختلفت التكييفات القانونية لهذا الفعل بين من يرجعها إلى جريمة نصب وبين من يصفها سرقة وآخر يعتبرها خيانة أمانة واحتيال، إلا أنه وبالنظر إلى إساءة استعمال البطاقة لا يخضع لأي وصف من الأوصاف السابقة ويبقى خاضعا لقواعد المسؤولية المدنية المتعلقة بمخالفة الالتزامات

الفرع الثاني: الاعتداءات الواقعة على البطاقة الإئتمانية من قبل الغير

1عبد الحليم بن مشري، **الحماية القانونية لبطاقات الدفع الإلكترونية**، المرجع السابق، ص13.

2جميل عبد الباقي الصغير، المرجع السابق، ص67.

3 Tronche, **La monnaie électronique**, Revue de L'association nationale en Droit, No. 42, 1982, p03

تتعدد صور الأفعال التي يقترفها الغير على بطاقة الإئتمان، لعل أبرزها وأكثرها شيوعًا ما يلي:

أولاً: استعمال الغير للبطاقة الإلكترونية المسروقة أو المفقودة

فقد يعمد سارق البطاقة أو من عثر عليها إلى استعمالها في سحب النقود أو شراء السلع والخدمات، وذلك قبل قيام الحامل الشرعي لها بالإخطار عن السرقة أو السحب وقيام البنك بوضعها في قائمة المعارضات، وإعادة برمجة جهاز السحب النقدي الآلي حتى لا يقبل البطاقة عند استخدامها في سحب غير مشروع قبل المعارضة فيها، وتوجد صورة أخرى للسرقة وهي أن تكون البطاقة بحوزة حاملها ولم تسرق منه ويقوم باتخاذ الإجراءات اللازمة في حالة الفقد أو السرقة بإخطار البنك والمعارضة فيها ومع ذلك يستمر هو استعمالها في سحب النقود الأمر الذي يعكس إساءة لاستعمال هذه البطاقة كما ذكرنا سالفًا، تعتبر جريمة الاحتيال طبقًا لنص المادة 42 قانون العقوبات الجزائري التي تنص على: " **يعتبر شريكًا في الجريمة من لم يشترك اشتراكًا مباشرًا ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك، وعليه إذا علم التاجر أن البطاقة التي يستعملها الغير مزورة أو مسروقة ومع ذلك قبلها فإنه بعد شريكا في الجريمة ويسأل عنها، ونفس الشيء إذا كانت البطاقة ملغاة أو منتهية الصلاحية فتقوم مسؤوليته المدنية والجزائية عن استعمالها.**"

والسرقة كما عرفها قانون العقوبات الجزائري في المادة 350 منه هي: "**كل من اختلس شيئا غير مملوك له يعد سارقا**". وعرفها الفقه الجنائي بأنها اختلاس مال منقول مملوك للغير بنية تملكه، وعليه فمحل جريمة السرقة هو البطاقة نفسها لأنها تعد من قبيل المنقولات والسرقة لا ترد إلا على مال منقول مملوك للغير وهو الحامل.

أما فيما يخص الركن المعنوي لهذه الجريمة فهو يتمثل في القصد الجنائي العام بعنصريه العلم والإدارة أي العلم بأن المال المسروق مملوك للغير واتجاه الإرادة إلى اخذ ذلك المال وهو البطاقة وذلك بإرادة حرة وسليمة وخالية من العيوب، أما القصد الجنائي الخاص فيتمثل في نية تملك البطاقة من قبل الغير وحرمان الحامل منها والظهور بمظهر المالك الحقيقي لها أمام التاجر المعتمد لدى الجهة المصدرة لها بذلك يطبق بهذا الصدد عقوبة السرقة المنصوص عليها في المادة 350 ق.ع.ج وهي الحبس من سنة إلى 05 سنوات وغرامة مالية من 500 إلى 20.000 دج، أما إذا اقترنت السرقة بإحدى الظروف

المنصوص عليها في المادة 350 مكرر كاستعمال العنف أو التهديد فإن العقوبة تضاعف من سنتين إلى 10 سنوات، ويعاقب كذلك على الشروع فيها بنفس العقوبات المقررة للجريمة المرتكبة[1] .

وبالإضافة إلى مسؤولية الغير عن جريمة السرقة في البطاقة الضائعة يمكن مساءلته أيضا عن جريمة الاحتيال والنصب عند استعماله للبطاقة إذا ما استخدم اسما كاذبا لخداع التاجر، وإجباره على تسليم السلع والمشتريات، ويمكن أيضا مساءلته عن جريمة تزوير بتوقيعه علي فواتير الشراء[2].

ثانيًا: استعمال الخير لبطاقة الوفاء المزورة

ظهرت فكرة تزييف البطاقات الإتمانية كوسيلة يتحايل بها الجاني عن أجهزة التفتيش الآلي للمواصلات حتى يمكنه المرور منها دون سداد الأجرة وقد يستخدم الجاني البطاقة المزورة للسحب الآلي، ونذكر على سبيل المثال ما جاء في المواد من 01 إلى 57 من قانون حماية الشيكات وبطاقة الدفع الفرنسي[3]، والبطاقات المزورة تصدر في كل أنحاء العالم وهي تتميز بجودة فائقة بحيث أنها تبدوا في اغلب الأحوال أفضل من البطاقات التي تصدرها الجهة الأصلية ذاتها [4].

ويعرف التزوير بأنه تغيير للحقيقة بقصد الغش في محرر بإحدى الطرق التي نص عليها القانون تغييرا من شأنه أن يسبب ضررا، ورغم أن المشرع الجزائري قد نص على جريمة التزوير إلا أنه لم يتطرق إلى تعريفها، بل اكتفي بتحديد الطرق التي يتم التزوير بها ومحل التزوير والعقوبات المقررة لكل منها[5].

الخاتمة

تعد بطاقة الائتمان الإلكترونية وسيلة مستحدثة للوفاء، دون أن يتم الدفع نقداً للتجار، وبهذا يتفادى المواطن حامل البطاقة الأخطار التي يتعرض لها عند حمله النقود، كما تجعل البطاقة في مأمن من رفض التاجر قبول هذه الوسيلة في الوفاء، كما يحدث بالنسبة للشيك، إضافة إلى توفيرها الأمان للتجار، فهي تعد لهم وسيلة مضمونة للوفاء، وتحميهم من انخفاض القيمة الشرائية للنقود وتراكم الأموال لديهم، علاوة على تخليصهم من أخطار السرقة والضياع وزيادة عدد عملائهم.

ومنه نستنتج ما يلي:

1عبد الحليم بن مشري، **الحماية القانونية لبطاقات الدفع الإلكترونية**، المرجع السابق، ص69.

2 سميحة القيلولي، **الأوراق التجارية**، دار النهضة العربية، القاهرة ، 1992، ص309.

3انظر نص المادة (57–1) من قانون حماية الشيكات وبطاقة الدفع الفرنسي رقم (91–1382) لسنة 1991

4 . Martin, D, **Analyse Juridique du règlement par carte de payement**. Dalloz, 1987, p. 51.

5عبد الحليم بن مشري، **الحماية القانونية لبطاقات الدفع الإلكترونية**، المرجع السابق، ص69.

– يمكن لبطاقة الائتمان الإلكترونية أن تحل مقام النقود في الوفاء، فإذا كان الغرض من إيجاد طرق وفاء هو الحد من تداول النقود وانتقالها بما تتعرض له من أخطار السرقة والضياع، فقد أوجدت البيئة التجارية كثيراً من هذه الوسائل التي استعملت في الوفاء بأثمان السّلع الكبيرة مثل الأوراق التجارية، وبالرغم من شيوع هذه الوسائل التقليدية وقيامها بوظيفة الوفاء، إلاّ أنها ظلت غير مقبولة للوفاء بقيمة المشتريات الأساسية وخاصة قيمة السلع والخدمات التي يحتاجها العميل، فقد اعتاد التجار على قبول النقود في الوفاء دون سواها لهذه المشتريات، ولكن بطاقة الائتمان الإلكترونية أصبحت تغطي هذا النقص، بل أنها أصبحت تنافس وسائل الوفاء التقليدية في مجال تطبيقها نظراً لما تحققه من سبل حماية أكثر مما يتوافر للوسائل التقليدية في الوفاء.

- كما أن بطاقة الائتمان الإلكترونية تعد وسيلة ضمان، حيث تضمن للتاجر وفاءً كاملاً بقيمة المشتريات التي تعاقد عليها الحامل في حدود الرصيد المتفق عليه من قبل البنك.

- نظراً للتغيرات الاجتماعية والاقتصادية ابتدع العرف التجاري هذا النظام ثم أخذته البنوك، لتتوسع به لدرجة أنه أصبح عملية مصرفية تقدمها المصارف ضمن الخدمات المصرفية التي تضعها بين يدي الجمهور.

– لو أمعنا النظر في العلاقات التي ترتبط بالبطاقة لوجدنا نوعاً من التناغم والانسجام بينها، فالعقد المبرم بين التاجر والبنك للحصول على البطاقة كونها وسيلة وفاء، وارتباطها بمجموعها بالنظام الإلكتروني الموجود لدى التاجر والبنك، يجعل البطاقة تتآلف معه، لتنفيذ ما ترتب من العلاقات القانونية بطريقة تقنية حديثة، بحيث يصبح لدينا النظام القانوني ذا صبغة تقنية حديثة للوفاء والضمان.

– إن إساءة استخدام بطاقة الإئتمان الإلكترونية إمّا أن تكون من قبل مالكها أو من قبل الغير، فإن كان الاستخدام غير المشروع للبطاقة من قبل مالكها فإما أن يكون خلال فترة صلاحيتها أو بعد انتهاء مدة صلاحيتها أو بالحصول غير المشروع على بطاقة الائتمان الإلكترونية، وقد لاحظنا بأن المسؤولية الجزائية لا تقوم بحق الحامل إذا استعملها في السحب من حسابه بأزيد ممّا هو مقرر أو بأزيد مما تسمح له به حالة الرصيد بل تقوم بحقه المسؤولية المدنية مع اتخاذ إجراءات إدارية.

– أما بخصوص قيام الحامل بالوفاء بقيمة البضائع والخدمات لدى المحلات التجارية باستخدام بطاقته الائتمانية الإلكترونية رغم عدم وجود رصيد كافٍ، فيوجد هناك رأيين لدى الفقه الجنائي، فالرأي الأول يذهب إلى القول بمسؤولية الحامل عن جريمة احتيال، بينما يذهب الرأي الثاني إلى القول بعدم تحقق المسؤولية الجزائية والاقتصار فقط على تحقق المسؤولية المدنية.

- والملاحظ أن الفقهاء قد اختلفوا في تكييف واقعة استخدام الحامل لبطاقته الإئتمانية الإلكترونية الملغاة والمنتهية الصلاحية في الوفاء بقيمة السلع والخدمات وذهبوا في ذلك إلى رأيين، أحدهما يرى باعتبار الواقعة جريمة خيانة أمانة وثانيهما يرى بأن الواقعة جريمة احتيال.

- وختاماً، فإن بطاقة الائتمان الإلكترونية يمكن أن تكون محلاً لجريمة السرقة بغض النظر عمّا إذا كان الحساب به رصيد أو ليس به رصيد، لأنها تمثل قيمة في حد ذاتها، كما إنها تصلح لأن تكون محلاً لجريمة تزوير المحررات باعتبارها من المحررات الإلكترونية، وأخيراً فان استعمال بطاقات الائتمان الإلكترونية كوسيلة للدفع عن طريق شبكة الانترنت قد ارتبط به ظهور جرائم ممن يلتقط الأرقام السرية لتلك البطاقات ويقوم بالسحب من حسابات أصحابها.

التوصيات

- التدخل التشريعي لمواجهة القصور في التشريعات والقوانين الجزائية المقارنة بصفة عامة والتشريع الجزائري بثقة خاصة، أو تحديثها بالنص صراحة على تجريم إساءة استخدام بطاقة الائتمان الإلكترونية اعمالاً لمبدأ شرعية الجرائم والعقوبات حتى نصل إلى إقامة بنية قانونية للتصدي لمثل هذا النوع من الجرائم.

- تأهيل القائمين على أجهزة إنفاذ القانون لتطوير معلوماتهم في مجال تقنية المعلومات، وذلك من خلال تدريب وتأهيل القائمين بالضبط والخبراء وسلطات التحقيق والقضاة، وخاصة تدريب القضاة على التعامل وتفهم هذا النوع من القضايا التي تحتاج إلى خبرات فنية عالية لملائمة قبول هذا النوع من الأدلة في الإثبات وتقديرها، حتى يتمكن من الفصل في القضايا المتعلقة بهذا النوع من الجرائم الإلكترونية.

- ضرورة إهتمام المصارف بالشركات التجارية التي تتعامل ببطاقة الائتمان الإلكترونية بالوقوف على كل طرق وأساليب الاحتيال والخداع والتزوير في الاستخدام غير المشروع لبطاقة الائتمان الإلكترونية، مع ضرورة تدريب الموظفين والعاملين على كل ما يستجد في هذا المجال وذلك بإقامة برامج تدريبية مكثفة لموظفي المصارف.

- ضرورة إعداد برامج إلكترونية دقيقة يمكن من خلالها أن يشفر حامل البطاقة رقم بطاقته بنفسه ويرسله إلى التاجر المعتمد والذي بدوره يستطيع فك التشفير، للحد من إختراقات المعلومات المصاحبة لاستخدام بطاقة الائتمان عبر شبكة الانترنت.

قائمة المراجع:

أولا – المراجع العربية

- **الكتب**

1. رياض فتح الله بصيله، **الجوانب الشرعية والمصرفية والمحاسبية لبطاقات الائتمان**، مؤسسة إيتراك للنشر والتوزيع، القاهرة ، 1997
2. جميل عبد الباقي الصغير، **الحماية الجنائية والمدنية لبطاقات الائتمان الممغنطة**، دار النهضة العربية، القاهرة، 1999.

3. عبد الوهاب إبراهيم أبو سليمان، البطاقات البنكية الاقراضية والسحب المباشر من الرصيد (دراسة فقهية قانونية اقتصادية تحليلية)، دار القلم، دمشق، 1998 .
4. فايز رضوان، **بطاقات الوفاء**، المطبعة العربية، القاهرة، 1990 .
5. سميحة القليوبي، **الأوراق التجارية**، دار النهضة العربية، القاهرة، 1992.
6. محي الدين إسماعيل علم الدين، **موسوعة أعمال البنوك من الناحيتين القانونية والعملية**، ج2، 1993

- **الرسائل الجامعية**

1. كيلاني محمود، **النظام القانوني لبطاقات الوفاء والضمان**، رسالة دكتوراه، جامعة عين شمس، القاهرة، 1996.
2. عبد الرحمان صوفية، **النظام القانوني لبطاقة الائتمان**، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة محمد لمين دباغين، سطيف،2015

- **المقالات المنشورة**

1. إبراهيم زكي، "بطاقة الائتمان والمثلث الخفي"، مجلة البنوك.
2. زين محمد الزماني، "التزوير والتزييف عن طريق بطاقات الائتمان"، مجلة المحامي، عدد3، الرياض، 1421هـ .
3. خليل النجار، "**الخدمات المصرفية الجديدة**"، مجلة البنوك، المجلد التاسع عشر، 2001 .
4. جميل أحمد، كهينة رشام، **بطاقة الائتمان كوسيلة من وسائل الدفع في الجازئر**، مجلة الإقتصاد الجديد، عدد ديسمبر 2009.
5. محمد بلعرج، **ماستر كارد تستكمل خطة توسعها العالمية السريعة في الشرق الأوسط وشمال افريقيا**، مجلة اتحاد المصارف العربية، ع (257)، مايو 2002، بيروت.
6. أمحمدي بوزينة أمنة، "**النظام القانوني لتعامل ببطاقة الائتمان المتداولة في البنوك الجزائرية**"، مجلة القانون، كلية الحقوق والعلوم السياسية ، جامعة حسيبة بن بوعلي، العدد، 08 الشلف ، 2017، ص. 148.

- **الندوات العلمية والتقارير**

1. أبو الوفا محمد أبو الوفا إبراهيم، **المسؤولية الجنائية عن الاستخدام غير المشروع لبطاقة الائتمان في القانون المقارن والفقه الإسلامي**، بحث مقدم إلى مؤتمر الأعمال المصرفية

الإلكترونية بين الشريعة والقانون لكلية الشريعة والقانون وغرفة تجارة وصناعة دبي والذي عقد في دولة الإمارات العربية المتحدة للفترة من 10. -16 2003/5/12

2. محمد عبد الحليم عمر، **بطاقات الإئتمان: ماهيتها والعلاقات الناشئة عن استخدامها بين الشريعة والقانون**، بحث مقدم إلى مؤتمر الأعمال المصرفية الإلكترونية بين الشريعة والقانون، كلية الشريعة والقانون – بجامعة الإمارات العربية المتحدة 4 – 6 مايو 2003.

- **مواقع الانترنت**

1. Article L.311-3 du code monétaire et financier français . https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006072026/

ثانيًا: المراجع باللغة الأجنبية

1. CAVALDA CH, **Le droit pénal des cartes de paiement et de crédits**, Dalloz, 1994
2. Martin, D, **Analyse Juridique du règlement par carte de payement**. Dalloz, 1987
3. Tronche, **La monnaie électronique**, Revue de L'association nationale en Droit, No. 42, 1982
4. Howard Johson, credit cards. International Banking Law, Nov. 1988

التوصيات

1/-العمل على محاربة الأمية في مجال تقنيات المعلومات والإتصالات وتوفير مهارات إستخدام الأجهزة والتطبيقات.

2/-فرض أقل قدر ممكن من القيودعلى تدفق المعلومات عبر الأنترنت.

3/-ضرورة تحيين الأطر القانونية والتنظيمية للتجارة الإلكترونية والتوقيع الإلكتروني وحماية البيانات لتواكب التقنيات التكنولوجية.

4/-ضرورة اعتماد اتفاقية عالمية متعلقة بحماية المعطيات الشخصية.

5/-ضرورة وعي الدول بأن مسألة حماية المعطيات الشخصية هي حماية لسيادتها.

6/-إنشاء محكمة دولية مختصة بالملكية الفكرية لتنظر في مختلف النزاعات في هذا الشأن.

7/-توفير التمويل اللازم لتغطية التكاليف الخاصة بالتكنولوجية في جميع القطاعات.

8/-كفالة الإستعمال الآمن للأنترنت من خلال إنشاء هيئة وطنية تتولى مراقبة المواقع الإلكترونية على شبكة الأنترنت.

9/-تشديد العقوبات الجنائية على المعتدين على الحياة الخاصة للطفل في الفضاء الرقمي.

10/-ضرورة إدخال التأمين كتقنية جديدة في مجال الأمن السبيراني بالنسبة للأفراد والشركات.