جامعة مولود معمري – تيزي وزو –
كلية الحقوق والعلوم السياسية
قسم الحقوق

آليات الوقاية من جرائم تكنولوجيا الإعلام والاتصال

مذكرة لنيل شهادة الماستر في القانون
تخصص: قانون الأعمال

إعداد الطالبة:
- بلقاسم زكية

إشراف الأستاذة:
- د. سليماني حميدة

لجنة المناقشة:

- د/ اعراب كميلة، أستاذة محاضرة "أ"، جامعة مولود معمري، تيزي وزو، .....رئيسا.
- د/ سليماني حميدة، أستاذة محاضرة "أ"، جامعة مولود معمري، تيزي وزو،.....مشرفا ومقررا.
- د/ أيت يوسف صبرينة، أستاذة محاضرة "أ"، جامعة مولود معمري تيزي وزو،.....ممتحنا.

تاريخ المناقشة: 17/.06/2025

بسم الله الرحمن الرحيم

كلمة شكر

قال رسول الله صلى الله عليه وسلّم

"أفلا أكون عبدا شكورا؟"

الحمد لله الذي بنعمته تتم الصالحات،ونشكر الله على توفيقه قبل كل أحد،الفرد الصمد،الذي أمدنا بالقوة والعون لانجاز هذا العمل،وندعوه عزّ وجل أن يجعله خالصا لوجهه الكريم.

بعد شكر الله سبحانه وتعالى،أحمده بما وفقني وأعانني على إتمام هذه المذكرة،وسهل لي سبل البحث والعلم،أتقدم بجزيل الشكر لوالدي العزيزين الذين كانو لنا نورا في دربنا،وكانو لنا القدوة الحسنة لنا في الاستمرار لنجاحنا و اكمال دراستنا،كما أتوجه بالشكر الجزيل و عظيم الامتنان إلى أستاذتي المشرفة"سليماني حميدة"،التي منحتني من كل وقتها وجهدها وتوجيهاتها الثمينة،فكانت نعم الأساتذة والداعمة طوال مرحل هذا العمل التي لم تبخل عليّ بأية معلومة أو توضيح.إلى كل أساتذتنا بقسم الحقوق على المجهودات المبذولة لايصالنا إلى ما نحن عليه،وأشكر أيضا زملائي وأصدقائي الأعزاء الذين كانوا رفقاء الدّرب،وشاركوني هذه الرحلة بكل ما حملته من صعوبات وتحديات.

"لكم جميعا أسمى معاني الشكر والعرفان،وأسأل الله أن يوفقنا جميعا لما فيه الخير والنّجاح".

إهــداء

الحمد لله

حبا و شكرا و امتنا على البدء و الختام ها أنا اليوم أتوح لحظات الأخيرة في ذلك الطريق الذي كان يحمل في باطنة العثرات ورغما عنها ظلّت قدمي تخطو بكل صبر و طموح وعزيمة وتفاءل وحسنة ظن بالله.

أهدي بكل حب تخرجي

إلى ذلك الرّجل العظيم من كان لي العمود الفقري الذي ساندني بكل حبّ في ضعفي الذي أخرج أجمل ما بداخلي وشجعني دائما للوصول إلى طموحاتي أبي العزيز أدامك الله ظلاّ لنا.

إلى التي تعجز كل الكلمات عن وصفها إلى التي كانت النور في عتمتي التي كانت دعاؤها سر نجاحي

إلى التي ضحت من أجلي ورافقتني في كل أوقاتي و تعبت دون مقابل من أجلنا منحها الله الصحة والعافية أمي الحبيبة.

إلى إخوتي وأخواتي أدامكم الله إليّ سندا و الكتف الذي أستند إليه الحاضرين و البعيدين عن الأعين لكن هم في القلب .

إلى زملائي الذين شاركوني مقاعد الدراسة إلى كل من وقعت عليه عين من أهل الخير إلى كل من ساندني في انجاز هذا العمل

أساتذتنا الكرام إلى كل من كان له الفضل في وصولي إلى هذه المرحلة

أهدي لكم تخرجي.

مقدمة:

شهد العالم المعاصر في العقود الأخيرة تحوّلا جذريا في مختلف مجالات الحياة نتيجة للتطور الهائل الذي عرفته تكنولوجيا الإعلام و الإتصال، والذي شمل جميع أوجه النشاط البشري،سواء على الصعيد الفردي أو المؤسساتي أو الدولي.لقد أصبحت الشبكة العنكبوتية ومختلف الوسائط التكنولوجية أدوات أساسية في حياة الأفراد والمؤسسات،مما أدى إلى خلق وسائل الإعلام والاتصال أو الفضاء الرقمي،وهو فضاء متحرّر من القيود الجغرافية والزمنية، يتيح تواصلا فورياّ ونشرا واسعا للمعلومة، وتبادلا سريعا للبيانات والمعاملات.

باتت تختلف نظرة الناس نحو تكنولوجيا المعلومات الجديدة، ففي الوقت الذي تبعث فيه على الإعجاب في نفوس العديدين عند الاستفادة منها في علاج مشكلات عديدة،إلا أنها تبدو مروعة،لاسيما عندما يتعلق الأمر بتهديد أمن و حياة المجتمعات[1].

غير أن هذا التقدم الرقمي، الذي حمل معه الكثير من الإيجابيات، قد فتح الباب على مصراعيه أمام ظهور نوع جديد من الجرائم،تختلف عن الجرائم التقليدية في طبيعتها،ووسائل ارتكابها،وآثارها.وتعرف هذه الجرائم بجرائم تكنولوجيا الإعلام والإتصال، أو ما يصطلح عليه أحيانا بالجرائم الإلكترونية،وهي الأفعال غير مشروعة ترتكب بواسطة استخدام تكنولوجيا المعلومات والاتصالات،وتستهدف الأفراد،المؤسسات أو حتى الدول،مسببة أضرارا تمس الأمن الاقتصادي و الإجتماعي والحقوق الأساسية للأشخاص.

ومع تزايد الاعتماد على الوسائل الرقمية في جميع مناحي الحياة، خاصة بعد توجّه الدولة نحو الرقمنة و التحول الإلكتروني، بات من الضروري وضع آليات فعّالة للوقاية من جرائم تكنولوجيا الإعلام و الإتصال، وقد بادر المشرّع الجزائري إلى إصدار مجموعة من

1جاسم الطائي جعفرحسن ، جرائم تكنولوجيا المعلومات،رؤية جديدة للجريمة الحديثة،دار البداية نلشرون و موزعون،عمان ،2012

القوانين لمكافحة هذه الظواهر، من بينها القانون 09-04[1] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، إلى جانب إدماج أحكام تتعلق بالجريمة الإلكترونية في نصوص متفرقة،وهو ما يدل على إدراك متزايد لخطورة هذه الجرائم.

فعليه فإن الإشكالية المطروحة تتمثل في **ما مدى فعالية آليات *الوقاية من جرائم تكنولوجيا الإعلام و الاتصال، في ظل التطور السريع للتقنيات الرقمية وتزايد الاعتماد عليها في مختلف مجالات الحياة ؟*** ومن ثم ارتأينا من الأنسب للإحاطة بعناصر هذا الموضوع،وللإجابة على هذه الإشكالية المطروحة اعتمدنا على المنهج الإستقرائي الذي يدمج بين الوصفي لوصف هذه الجرائم وخصائصها و المنهج التحليلي لتحليل أساليب أو طرق التصدي لجرائم تكنولوجيا الإعلام والإتصال وذلك في كل من قانون رقم 04.09 وكذا الأمر رقم 11.21 المتعلق بقانون الإجراءات الجزائية[2].

ولمعالجة هذه الإشكالية تطرقنا إلى تبني خطة مقسمة إلى فصلين **(الفصل الأول)** تحت عنوان "الإطار المفاهيمي لجرائم تكنولوجيا الإعلام والإتصال ، أما **(الفصل الثاني)** يتناول "أساليب التصدي من جرائم تكنولوجيا الإعلام والإتصال".

1 قانون رقم 09-04 مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها،ج ر، عدد 47، صادر في16 أوت 2009.

2 قانون رقم 11.21 المؤرخ في 25 أوت 2021 يتمم الأمر رقم 155.66 المؤرخ في 08.06.1966 المتضمن قانون الإجراءات الجزائية،ج ر ،العدد65 ، صادر بتاريخ 26أوت 2021.

الفصل الأول

الإطار المفاهيمي لجرائم تكنولوجيا الإعلام و الاتصال

تعد جرائم تكنولوجيا الإعلام و الاتصال من التحديات الكبرى التي فرضها التقدم التكنولوجي، حيث أثارت هذه الظاهرة الإجرامية اهتماما واسعا في الأوساط الأكاديمية و القانونية، و قد نتج عن ذلك تعدد المصطلحات المستخدمة للإشارة إليها، مثل: جرائم الحاسوب، جرائم الانترنت ، الجرائم السيبرانية، و الجرائم الالكترونية و يشكل عدم وجود تعريف موحد لهذه الجرائم أحد التحديات الرئيسية التي تواجهها[1]**(المبحث الأول)**.

بالإضافة إلى ذلك ، تتميز هذه الجرائم بخصائص استثنائية ، سواء من حيث الأدوات التكنولوجية المستخدمة في ارتكابها، أو البيئة الافتراضية التي تحدث فيها ، أو حتى من حيث طبيعة المجرمين الالكترونيين الذين يتمتعون بمهارات تقنية عالية تجعلهم أكثر تعقيدا من المجرمين التقليديين ، هذه الخصائص جعلت مواجهة هذه الجرائم تحديا كبيرا،إذ تعتبر العقود الأخيرة تحولا جوهريا في تاريخ البشرية، حيث أطلق عليها اسم "عصر ثورة المعلومات" بسبب الانتشار الكبير للانترنت التي غيرت وجه العالم، و كما تم تسمية العصور السابقة بناءا على أهم الابتكارات التي شاهدتها، فإن العصر الحالي يستحق أن يسمى "عصر المعلومات" أو "عصر الثورة المعلوماتية ".

ومن أبرز سمات هذا العصر تطور الجريمة بشكل متلازم مع تطور التكنولوجيا **(المبحث الثاني)**.

1 بخوش هشام ،"الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في التشريع الجزائري"،**مجلة الحقوق والعلوم السياسية**،كلية الحقوق والعلوم السياسية،محمد الشريف مساعدية،جامعة سوق أهراس،العدد 07 ،2017 ،ص194.

المبحث الأول

مفهوم جرائم تكنولوجيا الإعلام و الاتصال

لقد أصبحت تكنولوجيا الإعلام و الاتصال اليوم ذات أثر كبير في المجتمع و في حياتنا اليومية، و لقد حققت تكنولوجيا المعلومات و الاتصالات فوائد عديدة تزايد الاعتماد عليها في مجال الحياة كافة،و يقدر ما أفرزته الوسائل التقنية الحديثة في مجال الرقي و التقدم الإنساني، بقدر ما مهدت إلى بروز أنماط جديدة من الجرائم بالغة الخطورة لارتباطها بنظم المعالجة الآلية للمعلومات و للتعرف أكثر على جرائم تكنولوجيا الإعلام و الاتصال سندرس المقصود بجرائم تكنولوجي، لم تعد مجرد وسيلة ،بل وحتى القلب النابض الذي يغذي كيان الإنسان العصري،رغم أن لها إيجابيات متعددة ،إلا أن لها في المقابل سلبيات لا يمكن تجاهلها[1]، المتمثلة في جرائم تكنولوجيا الإعلام و الاتصال**(المطلب الأول)** و من هنا إن التعامل مع هذه الجرائم تكنولوجيا الإعلام و الإتصال لا يكون بنفس الطريقة التي يتعامل بها القانون الجنائي مع الجرائم العادية، حيث أصبحت الحاجة إلى فهم طبيعتها القانونية بشكل دقيق**(المطلب الثاني)** .

1 – جاسم الطائي جعفرحسن ،مرجع سابق،ص107 .

المطلب الأول

المقصود بجرائم تكنولوجيا الإعلام و الاتصال

إن التطور الحاصل في تكنولوجيا الإعلام و الاتصال، وظهور شبكة الانترنت بكل ما حملته من تقدم و خدمات لم يمر على العالم بسلام، لأنه بقدر ما أحدث آثار إيجابية غير نمط حياة المجتمعات و ساهم في التطور في جميع المجالات و لاسيما المعاملات الإلكترونية ، بقدر ما كان له أثر سلبي على حياة الناس و مصالح الدول ، كل هذا تجلى في تطويع الانترنت و الوسائل الالكترونية لتكون عالما من عوالم الجريمة ، و هكذا ظهرت إلى الوجود الجريمة الالكترونية بشتى أنواعها**(الفرع الأول)**، مثلما للجرائم العادية خصائص ،فإن الأمر ينطبق كذلك على جرائم تكنولوجيا الإعلام و الإتصال أن لها خصائص خاصة بها**(الفرع الثاني)**.

الفرع الأول

تعريف جرائم تكنولوجيا الإعلام الاتصال

إن تكنولوجيا المعلومات بوصفها الأداة التي ترتكب عبرها أو من خلالها جرائم تكنولوجيا الإعلام و الاتصال ،لم تهتم معظم تشريعات دول العالم بوضع تعريفا محددا لجريمة تكنولوجيا الإعلام و الاتصال، إنما تركت الأمر لاجتهادات الفقهاء الذين انقسموا في ذلك إلى عدة جهات مختلفة ونجد الإتجاه الأول**(أولا)**،الإتجاه الثاني**(ثانيا)**والإتجاه الثالث**(ثالثا)**

أولا:الإتجاه الأول

فقد اعتمد الاتجاه الأول في تعريف هذه الجريمة على الجانب التقني المحيط لها أو وسيلة ارتكابها، فنجد الفقيه الألماني تاديمان Tièdement عرفها بأنها "كل أشكال السلوك

غير مشروع أو الضار بالمجتمع و الذي يرتكب باستخدام الحاسب الآلي "[1] في حين اعتبرها آخرون من نفس الاتجاه بأنها "نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود".

و منهم كذلك من عرفها بأنها "كل سلوك غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلي بقدر كبير لازما لارتكابه من ناحية ، و لملاحقته و تحقيقه من ناحية ثانية" أما البعض الآخر فاعتبرها كل نشاط أو سلوك إجرامي يؤدي فيه الحاسوب الآلي دور لإتمامه بشرط أن يكون هذا الدور على قدر من الأهمية"[2]

ثانيا:الإتجاه الثاني

في حين ركز الاتجاه الثاني من الفقه على الجانب الموضوعي لتعريف جريمة تكنولوجيا الإعلام و الاتصال ، إذ يرى بأنه لا يكفي لإطلاق هذا الوصف عليها بمجرد استخدام الحاسب الآلي أو أية وسيلة أخرى من وسائل الاتصال الحديثة ، بل يشترط كذلك أن يقع الفعل داخل نظام الحاسب الآلي لاحتسابها جريمة الكترونية .

و من هنا عرفها الفقيه الفرنسي ماس MASS بأنها " كل سلوك غير مشروع يتعلق بالمعلومات المعالجة و نقلها" وفي نفس السياق عرفت جريمة تكنولوجيا الإعلام و الاتصال كذلك بأنها "نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي ترسل عن طريقه"[3].

ثالثا:الإتجاه الثالث

أما الاتجاه الفقهي الثالث ، فقد ركز في تحديد لمقصود جريمة تكنولوجيا الإعلام والاتصال على الجانب المعرفي ، لا على الوسيلة أو الموضوع ، وذلك لكونها مرتبطة

1- نائلة عادل محمد فريد فودة، جرائم الحاسب الاقتصادية دراسة نظرية تطبيقية، دراسة النهضة العربية، لبنان، 2004،ص25.

2 نائلة عادل محمد فريد فودة ، مرجع سابق، ص26.

3 عبد الرحماني أمينة،مرابطين حفيظة، جرائم تكنولوجيا الإعلام و الإتصال،مذكرة لنيل الماستر في الحقوق،كلية الحقوق و العلوم السياسية،جامعة مولود معمري تيزي وزو، 2021،ص03.

بالجوانب المعرفية الفنية أو المعرفة باستخدام الحاسب الآلي و مختلف وسائل الاتصال الحديثة الأخرى ، فحسب أنصار هذا الاتجاه تعتبر جريمة تكنولوجيا الإعلام و الاتصال "أية جريمة يكون متطلبا لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب الآلي".

و من هذا المنطلق صرح الفقيه David Thimson بأن جريمة تكنولوجيا الإعلام و الاتصال هي تلك التي يتطلب لاقترافها توافر لدى فاعلها معرفة فنية بتقنية الحاسب. و السياق ذاته عرفها الأستاذ هشام فريد رستم بأنها "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه"[1]

مقابل ذلك نجد الفقه الجزائري قد تأثر كثيرا بمقاربة المؤتمر العاشر للأمم المتحدة لمنعجريمة الحاسب الآلي و شبكاته ، الذي عرف جريمة تكنولوجيا الإعلام و الاتصال بكل" جريمة يتم ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، و جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية"[2]. وهو ما انعكس على نية المشرع الجزائري في تبني معيار النظام لمعلوماتي لتحديد معالم هذه الجريمة ، و ذلك حينما نص المادة الثانية من قانون 04/09 بأن جرائم تكنولوجيا الإعلام و الاتصال هي "الجرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، و أي جريمة أخرى ترتكب أو يسهل ارتكابه عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية .

يلاحظ من هذا التعريف أن المشرع الجزائري لم يوضح بشكل محدد المقصود بجريمة تكنولوجيا الإعلام و الاتصال، بل اكتفى بالإشارة إلى بعض الجرائم الواردة في قانون العقوبات ضمن المواد من 394 مكرر إلى 394 مكرر 7. كما ترك المجال مفتوحا لتضمين أي جريمة أخرى ترتكب باستخدام أنظمة معلوماتية أو وسائل اتصالات إلكترونية.

1 بيومي حجازي عبد الفتاح ، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي، دار الفكر الجامعي الجزائر،2006،ص25.

2 زيدان زبيخة ، الجريمة المعلوماتية في التشريع الجزائري و الدولي ، دار الهدى ، الجزائر ،2011 ، ص17.

الفرع الثاني

خصائص جرائم تكنولوجيا الإعلام و الاتصال

تمثل جرائم تكنولوجيا الإعلام و الاتصال، أو ما يعرف بالجرائم الالكترونية تحديا كبيرا في العصر الرقمي الذي نعيش فيه، و تتسم هذه الجرائم بعدة خصائص تجعلها مختلفة عن الجرائم التقليدية ، فهي تعتبر جرائم عابرة للحدود**(أولا)**، كما أنها جرائم خفية و مستترة**(ثانيا)** ،جرائم صعبة الإثبات**(ثالثا)** و جرائم هادئة **(رابعا)**.

أولا: جرائم عابرة الحدود:

لقد وسعت شبكات المعلومات عملية الاتصال وتبادل المعلومات بين الدول و الأنظمة التي يفضّل بينها آلاف الأميال، و قد انعكست قدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون ، و هو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسري الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي لحصول الجريمة الالكترونية في مكان الجريمة و من ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل و بين المعلومات محل الاعتداء ، فقد يوجد الجاني في بلد ما و يستطيع الدخول إلى ذاكرة الكمبيوتر الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود في بلد ثالث.[1]

ثانيا: جرائم خفية ومستترة:

لا تترك هذه الجرائم أثر لها بعد ارتكابها ،مما يصعب الاحتفاظ الفني بآثارها إن وجدت ، فحتى الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة ، لأن الجاني

1 نائلة عادل محمد فريد ، مرجع سابق ، ص ص455- 456.

يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة ، كالتجسس و سرقة المكالمات و إتلاف البيانات و غيرها من الجرائم .[1]

هذا كله يصعب من مهمة المحقق العادي في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها و التضليل في التعرف على مرتكبيها، و في كل الأحوال تحتاج مواجهة هذه إلى خبرة فنية عالية متخصصة لإثباتها.

فغالبا ما يتم الكشف على هذا النوع من الجرائم بالصدفة و بعد مرور وقت طويل نسبيا. و من ثم فبالرغم من انتشار هذا النوع من الجرائم ، فإنه قليلا ما يبلغ عنها.

ثالثا: جرائم صعبة الإثبات:

تمتاز الجرائم المعلوماتية بصعوبة الاكتشاف و الإثبات و ذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز و الأرقام يصعب اكتشافها.

فالجريمة المعلوماتية لا تترك آثار ملموسة و بذلك لا تترك شهودا يمكن الاستدلال بأقوالهم و لا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات و تناولها بواسطة نبضات الكترونية غير مرئية.[2]

يصعب في الجرائم المعلوماتية العثور على دليل مادي للجريمة و ذلك راجع إلى استخدام الجاني وسائل فنية و تقنية معقدة في كثير من الأحيان، و هذا السلوك المادي في ارتكابها لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل و التلاعب به.

لجوء مرتكب الجرائم المعلوماتية إلى استخدام وسائل و أساليب مبتكرة تتميز بالطابع التقني و الفني المعقد،مما يجعل مهمة التصدي لهم تحديا كبيرا أمام الأجهزة الأمنية . و من

1 أعراب تاني نجية ، "الآليات الوقائية من جرائم تكنولوجيا الإعلام و الاتصال و مكافحتها في القانون الجزائري" ، **مجلة البحوث في الحقوق و العلوم السياسية** ، كلية الحقوق و العلوم السياسية جامعة أبو بكر بلقايد تلمسان ، المجلد08 ، العدد 01 ،2022ص456 .

2 سعيد نعيم ، آليات البحث و التحري المعلوماتي في القانون الجزائري ، مذكرة لنيل شهادة ماجستير ، كلية الحقوق والعلوم السياسية،جامعة الحاج لخضر باتنة ، 2013 ص 56.

أبرز تلك الأساليب قيام الجناة بزرع برامج خبيثة ضمن مجموعة من الحواسيب لتخضع لتحكم خارجي.

و يعرف هذا النوع من الجرائم بالاعتداء عن طريق "شبكة البوت نت " ، حيث يتمكن أحد القراصنة من التحكم بمجموعة ضخمة من الحواسيب المخترقة ، و التي قد تكون مرتبطة بإحدى شبكات البوت ، و تصل أعدادها أحيانا غلى الآلاف أو حتى الملايين من الأجهزة.[1]

رابعا: جرائم هادئة:

إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل و السرقة و غيرها من الجرائم، فالجرائم الإلكترونية لا تحتاج مجهود عضلي بل تعتمد على الدراسة الذهنية، و التفكير العلمي المدروس القائم على معرفة تقنية الكمبيوتر و ذلك يعود لكون هذا النوع من الجرائم عبارة عن معطيات و بيانات تتغير أو تعدل أو تمحي من السجلات المخزنة في ذاكرة الحاسوب ، إلا أن البعض يشبهها بجرائم العنف مثل ما ذهب إلي مكتب التحقيقات الفدرالي بالولايات المتحدة الأمريكية، نظرا لتماثل دوافع المعتمدين على نظم الحاسب الآلي مع مرتكبي العنف[2].

المطلب الثاني

الطبيعة القانونية لجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

للحديث عن الطبيعة القانونية للجريمة المعلوماتية و حول الوضع القانوني للبرامج والمعلومات، انقسم الفقه في اتجاهين لتحديد هذا الوضع القانوني، الاتجاه الأول يرى أن

1 دوباي سفيان ، يسعد صورية، الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ، مذكرة نيل شهادة ماستر، كلية الحقوق و العلوم السياسية، جامعة محمد البشير الابراهيمي ، برج بوعرريج ،2023 ،ص15.

2 رحموني محمد ، "خصائص الجريمة الالكترونية و مجالات استخدامها"، **مجلة الحقيقة** ،كلية الحقوق والعلوم السياسية،جامعة أحمد دراية،أدرار، العدد 41 ، 2018 ، ص 64.

جرائم المعلومات ذات طبيعة معينة **(الفرع الأول)** الاتجاه الثاني يرى أن جرائم المعلومات ما هي إلا مجموعة مستحدثة **(الفرع الثاني)**

الفرع الأول

جرائم المعلومات ذات طبيعة معينة

يفترض الاتجاه الأول أن جرائم المعلومات ذات طبيعية معينة ، بناءا على الحقيقة المقبولة و هي أن وصف القيمة يقدم أشياء ملموسة فقط أو أن الأشياء الموصوفة بالقيم هي الأشياء التي تمتلكها ، و بمفهوم المخالفة و نظرا لأن جرائم المعلومات تحمل طابعا معنويا ، فلا يمكن التعامل معها كقيمة مادية قابلة للاستحواذ ، إلا ضمن إطار حقوق الملكية الفكرية .

و مهما كان الحال ، فإن المسألة محسومة بعدم جواز الاستيلاء على معلومات الغير، و لهذا ، سعى هذا الاتجاه إلى حماية جرائم المعلومات من خلال دعوى المنافسة غير المشروعة ، بهدف صون حقوق الشخص الذي لا يستطيع أن يتمتع بأي حق استثنائي عليها[1].

الفرع الثاني

جرائم المعلومات مجموعة جرائم مستحدثة

يرى الاتجاه الثاني أن جرائم المعلومات تعد عن مجموعة من القيم المستخلصة، التي تتمتع بإمكانية الاستحواذ عليها بشكل مستقل عن دعامتها المادية . و يعتمد هذا الرأي على أساس مفاده أن لجرائم المعلومات قيمة اقتصادية قائمة بذاتها ، و هو ما يجعلها قابلة للحيازة رغم أن هذه الحيازة قد تتم بصورة غير مشروعة.

1 حوحو رمزي ،"مواجهة الجريمة المعلوماتية في الجزائر"،**مجلة الحقوق والحريات**، كلية الحقوق والعلوم السياسية،جامعة محمد خيضر ،بسكرة،العدد02 ،2014،ص45.

و تبنى هذه الفكرة على أساس العلاقة القانونية التي تربط بين الإنسان و الشيء الذي يملكه ، كما أوضح ذلك الفقيهان "كاتالا" (Catala) و "فيفان" (Vivante) ، حيث شبها العلاقة بين الفرد و المعلومة بعلاقة المالك بملكه. و بناء عليه ،يمكن اعتبار جرائم المعلومات مالا قابلا للتمليك أو الاستغلال ، ما يبرر إخضاعها للحماية القانونية أسوة بالأموال ذات الطبيعة المادية.[1]

المبحث الثاني

أنواع الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

مع التطور المتسارع لتكنولوجيا الإعلام والإتصال، برزت أنماط جديدة من الجرائم لم تكن معهودة من قبل،وهو ما دفع المشرع الجزائري إلى وضع نصوص قانونية خاصة لمواجهتها.و قد أولى المشرع أهمية بالغة لهذه الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال،فعرفها بموجب نص المادة 02 من القانون رقم 09-04 المتضمن القواعد الإجرائية للوقاية من جرائم تكنولوجيا الإعلام والإتصال بأن"**المقصود بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكبأو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.**"

كما توسّع قانون الإجراءات الجزائية ،بموجب أحكام نص المادة 211 مكرر22 فقرة 3 من الأمر رقم 11/21 معدل و المتمم للأمر 155/66 المتضمن قانون الإجراءات الجزائية[2] بأنها "**أي جريمة ترتكب أو يسهل ارتكابها باستعمال منظومة معلوماتية أو نظام للاتصالات الالكترونية أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيا الإعلام و الإتصال**".

1دوباي سفيان ، يسعد صورية ، مرجع سابق ، ص13.

2المادة 211 مكرر 22 من الأمر رقم 11.21،سالف الذكر.

فعليه ،يمكن تصنيف الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال إلى صنفين رئيسيين،الأول يشمل الجرائم التي تستهدف أنظمة المعالجة الآلية للمعطيات نظمها قانون العقوبات(**المطلب الأول**)، أما الثاني فيتعلق بالجرائم التي وردت في قوانين خاصة نظمت بعض الأفعال الإجرامية ذات الصلة بالتكنولوجيا الحديثة (**المطلب الثاني**).

المطلب الأول

جرائم تكنولوجيا الإعلام و الإتصال المنصوص عليها بموجب قانون العقوبات

جرم المشرع الجزائري الأفعال التي تهدد أنظمة معالجة البيانات الآلية من خلال تعديل قانون العقوبات بموجب القانون رقم 20-06[1] ، الذي خصص القسم السابع مكرر منه،التي تتعلق "المساس بأنظمة المعالجة الآلية للمعطيات، و تشمل على 08 مواد بدءا من المادة 394 مكرر وصولا إلى المادة 394 مكرر7 ، والمتمثلة في جريمة الدخول و البقاء الغير مصرح به في النظام المعالجة الآلية للمعطيات(**الفرع الأول**) جريمة إتلاف نظام المعالجة الآلية للمعطيات(**الفرع الثاني**) وجريمة إساءة إستخدام الأجهزة(**الفرع الثالث**).

الفرع الأول

جريمة الدخول و البقاء الغير مصرح له في النظام المعالجة الآلية للمعطيات

يشكل فعل الدخول بطريقة غير مشروعة إلى المنظومة المعلوماتية في حد ذاته جريمة ، إذ يستخلص من الوهلة الأولى أن مجرد اختراق جهاز الحاسوب سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد التسلية يعد انتهاكا للنظام ألمعلوماتي بطريقة غير مشروعة.

فعليه تقوم هذه الجريمة على ثلاثة أركان ركن شرعي(أولا) و ركن مادي(ثانيا)وركن معنوي(ثالثا)

1 القانون رقم 20-06 المؤرخ في 28 أفريل 2020 ،المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8جوان 1966،المتضمن قانون العقوبات،ج ر، عدد27 ،صادر بتاريخ 30 أفريل 2020 .

أولا:الركن الشرعي لجريمة الدخول والبقاء غير مصرح له في النظام المعالجة الآلية للمعطيات

و لقد تم النص على جريمة الدخول إلى النظام الآلي في قانون العقوبات الجزائري في المادة 394 مكرر: "**يعاقب بالحبس من ثلاثة(03) أشهر إلى سنة(01) و بغرامة من 50.000 دج إلى 100,000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.**[1]

ثانيا: الركن المادي لجريمة الدخول غير مصرح له في النظام المعالجة الآلية للمعطيات

يتمثل الركن المادي لجريمة الدخول و البقاء غير مصرح له في النظام المعالجة الآلية للمعطيات الذي يتجلى أولا في ارتكاب التعدي ، حيث يمكن أن يتخذ السلوك الإجرامي أشكالا إيجابية أو سلبية و يلزم الجاني بارتكاب فعل ايجابي ولا يمكن أن تتحقق الجريمة بنشاط سلبي . و الملاحظ على هذا النوع من الجرائم أنها ليست من الجرائم التي يطلق عليها جرائم ذوي الصفة ، مثل الرشوة، الاختلاس أو الزنا ، بل تقع و ترتكب عن كل شخص أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم لا، سواء كان يفهم أم لا يفهم بطريقة تشغيل النظام ، و سواء كان يستطيع أن يستفيد من الدخول أم لا.[2]

لا يعتبر تسجيل الدخول إلى نظام الكمبيوتر سلوكا غير قانوني في حد ذاته، و لكن هذا الوصف يستند إلى حقيقة أنه تم ارتكابه بشكل غير قانوني. هذا يعني أن الجاني يجب أن يكون مسجلا في البرنامج حتى يتم ارتكاب هذه الجريمة، و على هذا الأساس يستحسن استخدام لفظ الاتصال بالنظام الآلي، حيث أن الاتصال لا يثير الإشكال الذي يمكن أن يترتب على فعل الدخول. أما بخصوص طبيعة هذا النمط من الجرائم، فالأكيد أنها من

1 القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل و المتمم للأمر رقم 66-156 المؤرخ في 1966/06/08، المتضمن قانون العقوبات، ج ر، عدد 71،صادر بتاريخ 10 نوفمبر 2004.

2 مسعود أحمد ، "جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري" ، **مجلة الحقوق و العلوم الإنسانية**،كلية الحقوق والعلوم السياسية،جامعة زيان عاشور،الجلفة، المجلد10 ، العدد01 ، 2017 ، ص 484.

الجرائم الشكلية التي لا يتطلب لقيام ركنها المادي توافر نتيجة معينة، و هي كذلك من الجرائم المستمرة، لأن سلوك الجاني يمتد فيها طالما ظل يستغل النظام بطريقة غير مشروعة.

ثالثا: الركن المعنوي لجريمة الدخول و البقاء غير مصرح له في النظام المعالجة الآلية للمعطيات

هي جريمة عمدية يتدخل الركن المعنوي فيها بصورة القصد الجنائي،يتكون من علم و إرادة ،فيلزم لكي يتوافر هذا الركن أن تتجه إرادة الجاني إلى فعل الدخول أو إلى فعل البقاء داخل نظام المعالجة الآلية و أن يعلم الجاني أنه ليس له حق الدخول إلى النظام أو البقاء فيه.[1]

وتأسيسا على ذلك فإذا توافر القصد الجنائي بعنصره العلم والإرادة فإنه لا يتأثر بالباعث على الدخول أو البقاء فيظل القصد قائما حتى ولو كان الباعث هو الفضول،أو إثبات القدرة على المهارة أو الإنتصار على النظام[2].

الفرع الثاني

جريمة إتلاف نظام المعالجة الآلية للمعطيات

يعد إتلاف نظام المعالجة الآلية للمعطيات من أبرز صور الإعتداءات الإلكترونية التي تهدد أمن وسلامة المعلومات.فمع تنامي الاعتماد على التكنولوجيا في مختلف المجالات،أصبحت هذه الجريمة تمثل خطرا حقيقيا، و تختلف طرق و أساليب هذا الاعتداء بحسب الهدف الذي يسعى الجاني إلى تحقيقه**(أولا)** و أن لهذه الجريمة ثلاثة أركان ركن شرعي،مادي ومعنوي **(ثانيا)**.

1مناصرة يوسف،جرائم المساس بأنظمة المعالجة الآلية للمعطيات،منشورات دار الخلدونية، ،الجزائر،2018 ،ص133 .

مسعود أحمد ،مرجع سابق،ص484.[2]

أولا: أساليب إتلاف نظام المعالجة الآلية للمعطيات :

1- الفيروسات:

هي برامج حاسوبية سميت بهذا الاسم لتشابهها مع الفيروسات البيولوجية من حيث الانتقال و التكاثر ، و لها تأثيرات مدمرة على نظم المعلومات ، و تتميز الفيروسات بقدرتها على تعديل أو إتلاف البرامج و البيانات .

يصعب في الكثير من الأحيان التمييز بين البرامج السليمة و تلك المصابة بالفيروسات و يعد الانتشار السريع للفيروسات داخل نظم المعلومات من أبرز العوامل التي فاقت من خطورتها، خاصة مع تنوع الأنظمة و توافقها و انتشارها عبر الانترنت.

و رغم وجود برامج مضادة للفيروسات إلا أن الأخيرة مازالت قادرة على اختراق الأنظمة المعلوماتية و إلحاق الضرر بها، مهما كانت درجات الحماية.

2-القنبلة المعلوماتية :

تنقسم القنبلة المعلوماتية إلى قسمين[1]:

أ- القنبلة المنطقية: تهدف إلى تدمير المعلومات عند توافر شرط أو حدث معين مثل حذف اسم موظف من قاعدة بيانات الموارد البشرية يؤدي إلى تفعيل الفيروس .

ب- القنبلة الزمنية : ينطلق عملها في زمن أوتاريخ محدد أي موعد بذاته محدد مسبقا في برنامج القنبلة ،ومن أمثلها قضية حادثة شركة أوميغا أن قام موظف بدافع الانتقام بوضع برنامج لإتلاف بيانات الشركة التي طرد منها ليتم ذلك بعد 06 أشهر من مغادرته[2].

1 رامي حليم،"جرائم الإعتداء على أنظمة المعالجة الآلية للمعلومات"،**دراسات وأبحاث**،كلية الحقوق والعلوم السياسية،جامعة زيان بن عاشور ،الجلفة،المجلد01، العدد01 ،2009،ص ص349- 350.

2إدريس صاره ، زواقري أميرة،الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات،مذكرة نيل شهادة الماستر في الحقوق،كلية الحقوق والعلوم السياسية،جامعة مولود معمري تيزي وزو،2023 ،ص22 .

3- الدورة المعلوماتية:

تعد الدورة المعلوماتية نوعا من الفيروسات التي تتميز بقدرتها على الانتقال عبر شبكات نقل البيانات بهدف تعطيل عمل الأنظمة، أو إحداث خلل في إمكانية تبادل المعلومات،و من أبرز خصائصها أنها تنتشر عبر الشبكات بشكل ذاتي، دون حاجة إلى تدخل مباشر.

و قد أصبح مجرمو المعلوماتية يستخدمونها كوسيلة لاختراق الأنظمة ، و مثال ذلك ما وقع للإدارة الدفاع الأمريكية (DOD) ، حيث تعرضت لهجوم أجبر مسئولي القوات الجوية الأمريكية على إغلاق النظام لحمايته.[1]

أحيانا تضطر الجهات المسؤولة عن المواقف على إغلاقها نتيجة تعرضها لهجمات الكترونية متكررة ، كما حدث لإحدى المواقع التابعة لوزارة الدفاع الأمريكية ، و هو ما استدعى تطوير برامج وقاية أكثر فعالية .

ثانيا: أركان إتلاف نظام المعالجة الآلية للمعطيات:

لا يمكن اعتبار أي فعل جريمة إلا بتوفر الأركان الثلاثة: الركن الشرعي،الركن المعنوي و المادي .

1-الركن الشرعي لإتلاف نظام المعالجة الآلية للمعطيات

جرم المشرع الجزائري من خلال نص المادة 394 مكرر1 من قانون العقوبات و التي تنص على أنه"**يعاقب بالحبس من ستة (6)أشهر إلى ثلاث(3) سنوات و بغرامة مالية من 5000.00دج إلى 20.000.00 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو أزال أو عدّل بطريق الغش المعطيات التي يتضمنها".**

1 دوباي سفيان ، يسعد صورية ، مرجع سابق ، ص22.

2- الركن المادي لإتلاف نظام المعالجة الآلية للمعطيات

يشمل الركن كافة الأفعال التي ترتكب بهدف إتلاف المعلومات سواء عبر تدمير أنظمة الكمبيوتر أو تنفيذ أعمال تؤدي إلى تلف أو فقدان البيانات ، أو جعل البرامج غير قابلة للاستخدام.

وتتخذ هذه الأعمال عدة أشكال مثل الإتلاف ، التدمير ، التخريب ،المسح ،الحذف ، الإيقاف و كلها تؤدي إضعاف أو إزالة صلاحية المعلومة أو البرنامج .

بالتالي، فإن أي نشاط يؤدي إلى فقدان الشيء لصلاحيته أو تعديله بصورة تخرب جوهره ، يعد بمثابة إتلاف معلوماتي لأنه يعطل أداء المعلومة أو يعوق وظيفتها الأساسية.

فإن إتلاف المعطيات المعلوماتية يكون بإفساد الشيء حتى تفقد صلاحيته تبعا للغرض الذي أنشأت لأجله سواء بإدخال تعديلات جوهرية أو بإزالة معلومات أساسية أو بتعطيلها بحيث لا يمكن القيام بوظائفها.[1]

3- الركن المعنوي لإتلاف نظام المعالجة الآلية للمعطيات

يصنف إتلاف المعطيات ضمن الجرائم العمدية التي تستوجب توافر القصد الجنائي و يشترط فيها وجود نية إجرامية خاصة ، يهدف إلى تحقيق الأضرار المقصود بالمعلومات أو الأنظمة المستهدفة .

يتضح أن تحقق القصد الجنائي في جريمة إتلاف المعلومات يتطلب توافر عنصري العلم و الإرادة لدى الجاني ، ويقصد بالعلم أن يكون الفاعل مدركا أن أفعاله قد تؤدي إلى تخريب أو حذف أو تدمير البيانات و المعطيات داخل النظام المعلوماتي ، أما الإرادة اتجاه نية الجاني عمدا نحو تنفيذ هذا الفعل و إلحاق الضرر بتلك المعطيات .

يشترط هذا النوع من القصد توافر نية إجرامية محددة لدى الجاني حيث يجب أن تتجه

1 عون اسمهان ،"أركان جريمة الإتلاف المعلوماتي وعقوباتها، دراسة مقارنة،"،**مجلة الدراسات الإفريقية و حوض النيل** ،المركز الديمقراطي العربي ،الجزائر،المجلد04 ،العدد13 ،أكتوبر2021 ،ص363 .

إرادته نحو الإضرار بالمعلومات أو إفسادها أو التعديل فيها عمدا ، لما يؤدي إلى إتلافها أو التأثير على عمل النظام المعلوماتي أو البرامج المتصلة به[1].

الفرع الثالث

جريمة إساءة استخدام الأجهزة

مصطلح الأجهزة في هذه الجريمة يقصد به نوعان:الأول هو الأجهزة المادية مثل الأجهزة الإلكترونية التي تقوم بمعالجة البيانات بشكل آلي،أو أجهزة نقاط البيع،والثاني هو البرامج التي تستخدم لتسهيل ارتكاب الجرائم المعلوماتية المذكورة في هذا القسم.

ومن الملاحظ أن المشرّع الجزائري لم يشر بوضوح إلى النوع الأول،أي الأجهزة المادية،رغم أن استخدامها يتضمن حتما معالجة آلية للبيانات،ما يجعلها داخلة ضمن الإطار العام لهذه الجريمة[2].

أولا:الركن الشرعي لجريمة إساءة إستخدام الأجهزة

جرم المشرع الجزائري جريمة التعامل في معلومات غير مشروعة في نص المادة 394 مكرر2[3] فقرة1 من قانون العقوبات بنصها"**يعاقب بالحبس من شهرين(2) إلى ثلاث(3)سنوات و بغرامة من 1000.000دج إلى 5.000.000 دج كل من يقوم عمدا و عن طريق الغش بما يأتي:**

1-تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2-حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

---

1 بوطمين ماجدة ، "جريمة إتلاف المعطيات المعلوماتية " ، مذكرة لنيل شهادة الماستر في الحقوق ،كلية الحقوق والعلوم السياسية، جامعة العربي بن مهيدي، أم البواقي ،2018 ، ص ص39 -40.

2 مناصرة يوسف، ، مرجع سابق،ص157 .

3 المادة 394 مكرر2 من قانون العقوبات،سالف الذكر.

ثانيا:الركن المادي لجريمة إساءة استخدام الأجهزة

يتجلى الركن المادي في هذه الجريمة من خلال القيام بأفعال مثل تصميم أو البحث أو جمع أو توفير أو نشر أو المتاجرة في بيانات يتم تخزينها أو معالجتها أو إرسالها باستخدام نظام معلوماتي.كما ذلك إنتاج أو الحصول على جهاز يحتوي على برنامج معلوماتي تم تصميمه بهدف ارتكاب واحدة من الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للبيانات.

كما تشمل هذه الجريمة أيضا أي فعل يتعلق بتوفير رمز أو شفرة أو كلمة مرور أو بيانات تمكن من الدخول إلى نظام المعالجة الآلية للمعطيات،سواء كان الدخول إلى النظام كاملا أو إلى جزء منه.

وتعد هذه الجريمة مكتملة بمجرد القيام بتصميم أو البحث أو التجميع أو الاتجار ببيانات مخزنة أو معالجة أو مرسلة عبر منظومة معلوماتية،حتى لو لم تستخدم فعليا في ارتكاب جريمة،إذ يكفي وجود نية الإساءة.فعلى سبيل المثال،تصميم برنامج اختراق مثل الفيروس عمدا وبطريقة احتيالية يعد جريمة قائمة بذاتها تحت مسمى إساءة إستخدام الأجهزة[1].

ثالثا:الركن المعنوي لجريمة إساءة استخدام الأجهزة

الركن المعنوي في جريمة إساءة إستخدام الأجهزة يعتبر من نوع الجرائم العمدية، حيث يتجسد في القصد الجنائي الذي يتكون من عنصرين أساسيين:العلم و الإرادة.ويجب أن يكون الجاني على علم بأن فعله مخالف للقانون ،وأن تتجه إرادته إلى القيام بتصميم أو بحث أو توفير أو نشر أو معالجتها أو إرسالها عبر نظام معلوماتي.كما يشمل ذلك أيضا حيازة أو كشف أو نشر أو استخدام هذه البيانات لأي غرض،إذا كانت ناتجة عن إحدى الجرائم الواردة في هذا القسم من القانون.

1 مناصرة يوسف،مرجع سابق، ص ص157- 158.

يجب أيضا أن يكون الجاني على دراية بأن النشاط الذي يقوم به يمكن أن يؤدي إلى ارتكاب جرائم تمس بأنظمة المعالجة الآلية للمعطيات.لكن لا يكفي توافر القصد العام فقط،بل يجب أيضا أن تكون هناك نية خاصة، وهي نية الإضرار بالغير.ومع ذلك،فإن الجريمة تعد قائمة و مكتملة الأركان حتى في حالة مجرد حيازة برامج تم إنتاجها أو الحصول عليها بأي وسيلة ،طالما أنها تتيح إمكانية ارتكاب هذه الجرائم،دون الحاجة لاستخدامها فعليا[1].

المطلب الثاني

الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال المنصوص عليها في القوانين الخاصة

لم ينص المشرع الجزائري على جرائم تكنولوجيا الإعلام و الإتصال بموجب قانون العقوبات فقط بل نص على مجموعة من الجرائم التي يمكن تصنيفها على أنها جرائم تكنولوجيا الإعلام والإتصال في قوانين خاصة ،الجرائم الواردة في قانون 04.18 المتعلقة بالبريد و الاتصالات الإلكترونية[2] **(الفرع الأول)** و الجرائم الواقعة على التوقيع والتصديق الإلكتروني **(الفرع الثاني)** و جريمة تقليد المصنفات الإلكترونية **(الفرع الثالث)** و جريمة القذف المرتكبة عبر مواقع التواصل الإجتماعي التي نص عليها في قانون العقوبات المستحدث**(الفرع الرابع)**.

1 مناصرة يوسف،مرجع سابق،ص ص 162 -163. .

2 القانون رقم 18-04 المؤرخ في 10 ماي 2018،المتعلق بالبريد و المواصلات الإلكترونية ،ج ر،العدد 27 ،الصادر بتاريخ 13 ماي 2018 .

الفرع الأول

الجرائم الواردة في قانون 04.18 المتعلق بالبريد و الاتصالات الإلكترونية

يتضمن قانون رقم 04.18 المتعلق بالبريد و الإتصالات الإلكترونية السالف الذكر العديد من الأفعال التي تعد مخالفة لأحكامه ،والتي يمكن اعتبارها من الجرائم المرتبطة بتكتنولوجيا الإعلام والاتصال ، ومنها :

أولا: انتهاك خصوصية و سرية المراسلات المرسلة عبر البريد أو وسائل الاتصال الإلكترونية ، سواء من خلال افشاء محتواها أو نشره أو استخدامه دون إذن من المرسل أو المتلقي ، و تنص المادة 164من القانون رقم 04.18[1] على أن"**يعاقب بالحبس من سنة(01) إلى خمس (05) سنوات و بغرامة من 500.000دج إلى 1.000.000دج، كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو يخير وجودها**".

ثانيا: تحويل المراسلات الصادرة عن طريق البريد حسب المادة 165من القانون 04.18[2] التي تنص"**يعاقب بالحبس من سنة(1) إلى ثلاث(3)سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج أو بإحدى هاتين العقوبتين،كل متعامل للبريد يفتح أو يحول أو يخرّب البريد أو يساعد في ارتكاب هذه الأفعال.**

تسري نفس العقوبات على كل متعامل للاتصالات الإلكترونية يحوّل،بأي طريقة كانت،المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية، أو أمر أو ساعد في ارتكاب هذه الأفعال.

ويمكن الجهة القضائية أيضا النطق بواحدة أو أكثر من العقوبات التكميلية المنصوص عليها في المادة 9 من قانون العقوبات."

---

1 المادة 164 من القانون رقم 18-04 ،سالف الذكر.

2 المادة 165 من القانون رقم 18-04 ،سالف الذكر.

ثالثا: فتح أو تخريب البريد من قبل أي مستخدم أو طرف يتعامل مع خدمات البريد، كما ورد في المادة166 من القانون 04.18[1] "**يعاقب بالحبس من ستة(6) أشهر إلى سنتين (2) و بغرامة من 500.000 دج إلى 1.000.000 دج أو بإحدى هاتين العقوبتين، كل عون مستخدم من طرف متعامل للبريد يفتح أو يحوّل أو يخرّب البريد أو يساعد في ارتكاب هذه الأفعال في إطار ممارسة مهامه.**

يعاقب بنفس العقوبات كل شخص مستخدم لدى متعامل للاتصالات الإلكترونية،يحوّل،بأي طريقة كانت ستة(6) أشهر إلى سنتين(2)،و بغرامة من 500.000دج إلى 1.000.000دج،أو إحدى هاتين العقوبتين."

رابعا: إنشاء أو استخدام شبكة اتصالات إلكترونية متاحة للعامة دون الحصول على ترخيص، و تنص المادة 171من القانون 04.18[2] على أن"**يعاقب بالحبس من سنة(1) إلى ثلاث(3) سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج أو بإحدى هاتين العقوبتين،كل من ينشئ أو يستغل شبكة اتصالات إلكترونية مفتوحة للجمهور دون الرخصة المنصوص عليها في المادة 123 من هذا القانون أو مواصلة ممارسة النشاط خرقا لقرار التعليق أو سحب الرخصة**".

1 المادة 166 من القانون 18-04 ،سالف الذكر.

2 المادة 171 من القانون 18-04 ،سالف الذكر.

الفرع الثاني

الجرائم الواقعة على التوقيع و التصديق الالكتروني

استحدث المشرع و بموجب القانون رقم 04/15 المتعلق بالتوقيع و التصديق الإلكتروني[1] في الجزائر،ليؤطر هذا المجال و يوفر حماية قانونية لهذه الوسائل التقنية ،ويضع حدّا للفراغ التشريعي الذي كان قائما قبله، كما نص هذا القانون على تجريم بعض الأفعال التي تمس بأمن و سلامة التوقيع و التصديق الإلكتروني،إدراكا لخطورة هذه الجرائم على الثقة العامة و المعاملات الرقمية ، و من بين هذه الجرائم الواقعة على التوقيع و التصديق الإلكتروني نجد:

أولا: جنحة الإخلال بإخبار السلطة الاقتصادية عن التوقف عن النشاط :

نصت المادة 67 من القانون 04/15[2]سالف الذكر على أنه "**يعاقب بالحبس من شهرين إلى سنة واحدة و بغرامة من مائتي ألف دينار 20.000 دج إلى مليون دينار 1.000.000**" **أو بإحدى هاتين العقوبتين فقط ، كل مؤدي خدمات التصديق الإلكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58 و 59 من هذا القانون.**

ثانيا: جنحة إنشاء بيانات شهادة التصديق الالكتروني:

تطرق إليها المشرع الجزائري في المادة 70 من القانون 04/15[3] سالف الذكر و تنص على " **يعاقب بالحبس من ثلاثة (03) أشهر إلى سنتين (2) و بغرامة من مائتين ألف دينار(200.000) إلى مليون دينار(1.000.000دج) أو بإحدى هاتين**

1 القانون رقم 15-04 المؤرخ في 01 فيفري 2015،يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكتروني،ج ر ،العدد06، صادر بتاريخ 10 فيفري2015 .

2 المادة 67 من القانون 04.18،سالف الذكر.

3 المادة 70 من القانون رقم15-04 ،سالف الذكر.

العقوبتين فقط كل مؤدي خدمات التصديق الالكتروني أخل بأحكام المادة 42 من هذا القانون".

ثالثا: جنحة جمع البيانات الشخصية و استخدامها في غير الغرض المخصص لها

جاء في المادة 71 من القانون 04.15[1] سالف الذكر" **يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات و بغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار (1.000.000دج) أو بإحدى هاتين العقوبتين فقط ، كل مؤدي خدمات التصديق الالكتروني أخل بأحكام المادة 43 من هذا القانون".**

رابعا: جنحة إصدار شهادة التصديق الالكتروني دون ترخيص أو سحبه

المادة 72 من القانون 04.15[2]سالف الذكر تنص على: "**" يعاقب بالحبس من سنة (01) واحدة إلى ثلاث (03) سنوات و بغرامة من مائتين ألف دينار (200.000دج) إلى مليوني دينار (2.000.000دج) أو بإحدى هاتين العقوبتين فقط، كل من يؤدي خدمات التصديق الالكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه بالرغم من سحب ترخيصه".**

خامسا: جنحة الإدلاء بالإقرارات الكاذبة للحصول على شهادات التصديق :

جاء في المادة 66من القانون 04.15[3] على أنه " **يعاقب بالحبس من ثلاثة(03) سنوات و بغرامة من عشرين ألف دينار (20.000دج) إلى مائتي ألف دينار(200.000دج) أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة ".**

1 المادة 71 من القانون رقم 15-04 ،سالف الذكر

المادة 72 من القانون رقم04.15،سالف الذكر.[2]

3 المادة 66 من القانون 15-04 ،سالف الذكر.

سادسا: جنحة حيازة أو إنشاء أو استعمال بيانات توقيع مصونة خاصة بالغير

نصت المادة 68 من القانون 04.15[1] على أنه:" **يعاقب بالحبس من ثلاث (03) أشهر إلى ثلاث (03) سنوات و بغرامة من مليون دينار (1.000.000دج) إلى خمسة ملايين دينار (5.000.000دج) أو بإحدى هاتين العقوبتين فقط ، كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير**".

سابعا: جنحة استعمال شهادة التصديق الالكتروني الموصوفة لغير الغرض الذي منحت لأجله

جاء في المادة 74 من القانون 04.15[2]على أنه :" **يعاقب بغرامة من ألفي دينار (2.000دج) إلى مائتي ألف دينار (200.00دج) كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت لأجلها.**"

الفرع الثالث

جريمة تقليد المصنفات الإلكترونية

يعرف المصنف الرقمي على أنه: " مصنف إبداعي عقلي ينتمي إلى تقنية المعلومات و التي يتم التعامل معها بشكل رقمي.

أو هي مصنفات إبداعية ذهنية تنتمي إلى بيئة المعلومات الناتجة عن أدواتها التي جعلت منها مصنفات الكترونية أو رقمية، و هي تمثل التعبير عن النشاط الذهني الشخصي لمؤلفها، و يطلق عليها المصنفات المعلوماتية لتساير التقدم في الأداء لمصنفات الملكية الفكرية عبر الحواسيب و شبكة المعلومات لتتوافق مع الحاجات المشروعة لمستخدمي تلك الشبكة الدولية.[3]

1 المادة 68 من القانون 15-04 ،سالف الذكر.

المادة 74 من القانون 04.15،سالف الذكر.[2]

3 قيبوعة عبد الله ، خثير مسعود ، " الحماية الجزائية للمصنفات الرقمية في التشريع الجزائري "، **مجلة الدراسات القانونية المقارنة** ،كلية الحقوق و العلوم السياسية،جامعة حسيبة بن بوعلي، شلف،، المجلد06 ، العدد02 ، 2020 ، ص 137.

بالرجوع إلى المشرع الجزائري نجد أن كعادته لم يدرج تعريفا للمصنفات الرقمية، بل ذهب إلى تعدادها في المادة 04 من الأمر رقم 03-05[1] على سبيل المثال لا الحصر.

لقد جاء في الأمر 03-05 المتعلق بحقوق المؤلف و الحقوق المجاورة في المادة 151 على أنه :"يعتبر مرتكبا لجنحة التقليد كل من يقوم بالأعمال الآتية :

أولا:الجنح التي تمس بالحق المعنوي للمؤلف

و تشمل هذه الفئة الأفعال التي تنهك الحقوق المعنوية للمؤلف،و تتمثل في:

-الكشف غير المشروع عن المصنف الأدبي أو الأداء الفني،كما ورد في المادة 22 من الأمر رقم 05/03 المتعلق بحقوق المؤلف و الحقوق المجاورة بأن"**يتمتع المؤلف بحق الكشف عن المصنف الصادر باسمه الخاص أو تحت اسم مستعار.و يمكنه تحويل هذا الحق للغير.**

يعود الكشف عن المصنف بعد وفاة مؤلفه إلى ورثته ما لم تكن هناك وصية خاصة.

تفصل الجهة القضائية التي يختارها المبادر بكشف المصنف في حالة وقوع نزاع بين الورثة.

يمكن الوزير المكلف بالثقافة أو من يمثله أو يطلب من الغير إخطار الجهة القضائية للفصل في مسألة الكشف عن المصنف إذا رفض الورثة الكشف عنه و كان هذا المصنف يشكل أهمية بالنسبة للمجموعة الوطنية.

يمكن الوزير المكلف بالثقافة أو من يمثله أن يخطر الجهة القضائية المختصة للحصول على الإذن بالكشف عن المصنف إذ لم يكن للمؤلف ورثة".

1 الأمر رقم 03-05 المؤرخ في 19 جويلية 2003 ،المتعلق بحقوق المؤلف و الحقوق المجاورة،ج ر ،العدد43 ،صادر بتاريخ 20جويلية 2003.

-الإضرار بسلامة المصنف أو الأداء الفني،وهو ما نصت عليه المادة 25 [1]من الأمر رقم 05/03 على أن"**يحق للمؤلف احترام سلامة مصنفه و الاعتراض على أي تعديل يدخل عليه أو تشويهه أو إفساده إذا كان ذلك من شأنه المساس بسمعته كمؤلف أو بشرفه أو بمصالحه المشروعة**".

ثانيا:الجنح التي تمس بالحق المالي للمؤلف

تتعلق هذه الجنح بالاعتداءات على الحقوق المالية للمؤلف،وتشمل ما يلي:

-الاستنساخ غير مشروع للمصنف بأي وسيلة،لاسيما النسخ المقلدة في المجال المعلوماتي، مثل نسخ البرامج بشكل غير قانوني.

-إبلاغ الجمهور بالمصنف أو الأداء الفني من خلال التمثيل أو الأداء العلني أو البث السمعي أو البصري أو التوزيع أو أي وسيلة أخرى لنقل الإشارات الصوتية أو عبر أنظمة المعالجة الآلية.

ثالثا:الجنح المشابهة لجنحة التقليد

تشمل هذه الفئة الأفعال التي تتشابه في طبيعتها القانونية مع جرائم التقليد[2]،و تتمثل في:

-استيراد أو تصدير النسخ المقلدة ،سواء بالنقل المادي أو المعنوي،بما في ذلك عبر شبكات الانترنت.

-بيع النسخ المزورة من المصنفات مثل البرامج.

-تأجير أو عرض المصنفات المقلدة للتداول.

-المساعدة أو المشاركة في انتهاك حقوق المؤلف.

---

1 المادة 25 من الأمر رقم 03-05،سالف الذكر.

2 عيساني طه عبد الله فوزية ،"جريمة تقليد حقوق المؤلف في القانون الجزائري وتطبيقاتها في الببيئة الرقمية"،**مجلة الدراسات القانونية المقارنة** ،كلية الحقوق و العلوم السياسية ،جامعة حسيبة بن بوعلي ، شلف،المجلد 08 العدد 01 ،2022 ،ص361 .

-الامتناع عن دفع المكافأة المستحقة للمؤلف، كما ورد في المادة 154[1] من الأمر 05/03 أن"**يعد مرتكبا الجنحة المنصوص عليها في المادة 151 من هذا الأمر و يستوجب العقوبة المقررة في المادة 153 أعلاه،كل من يشارك بعمله أو بالوسائل التي يحوزها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة**".

إن المشرع الجزائري قد اعتبر برامج الحاسوب ضمن المصنفات الأدبية المحمية ،وأكد أن أي مساس بالحق المالي أو المعنوي للمؤلف في هذه البرامج يعدّ من أفعال التقليد[2].

الفرع الرابع

جريمة القذف

عرف المشرع الجزائري في المادة 296 من قانون العقوبات الجزائري جريمة القذف "**يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أوالهيئة الدعى عليها به أو إسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الادعاء أو ذلك الإسناد 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 تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة**".

تعد جريمة القذف من الجرائم الخطيرة التي جرّمتها معظم التشريعات في العالم و فرضت بشأنها عقوبات قانونية، نظرا لما تسببه من مساس بسمعة الأفراد وشرفهم.ومع التطور الكبير في وسائل التكنولوجيا، خاصة في مجالات الإعلام والإتصال وتكنولوجيا المعلومات،تغيّرت طرق ارتكاب هذه الجريمة من الأساليب التقليدية إلى أشكال حديثة،مثل القذف الإلكتروني أو المعلوماتي،وجريمة القذف عبر الانترنت أو مواقع التواصل الإجتماعي، والتي أصبحت من أكثر الجرائم شيوعا

1 المادة 154 من الأمر رقم 03-05 ،سالف الذكر.

2 عيساني طه ، عبد الله فوزية ،مرجع سابق،ص361 .

و انتشارا على الشبكة.وتقوم جريمة القذف على ثلاثة أركان: الركن الشرعي**(أولا)** و هو وجود نص قانوني يجرّم هذا الفعل،الركن المادي**(ثانيا)** و يشمل كل قول أو كتابة من شأنها المساس بكرامة و شرف الغير و أخيرا الركن االمعنوي**(ثالثا)** الذي يتمثل في توفر القصد الجاني لدى الفاعل، أي علمه بأن ما يصدر عنه يسيء للغير و رغبته في ذلك و هو وجود نص قانوني يجرّم هذا الفعل.

أولا:الركن الشرعي لجريمة القذف

الركن الشرعي هو وجود نص قانوني يجرّم الفعل و يمنعه، وهو ما تنص عليه المادة 1 من قانون العقوبات"**لاجريمة و لا عقوبة أو تدابير أمن بغير قانون"**[1].

وقد نص المشرّع الجزائري على جريمة القذف في قانون العقوبات ضمن الفصل المتعلق بالاعتداءات على شرف و اعتبار الأشخاص،وعلى حياتهم الخاصة وإفشاء الأسرار،وذلك في الباب الثاني من قانون العقوبات،خاصة في القسم الخامس، و قد ورد في المادة 296[2] من قانون العقوبات أن"**يعد قذفا كل ادعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعى عليها به أو إسنادها إليهم أو تلك الهيئة ويعاقب على نشر هذا الادعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى و لو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة".**

وتنص المادة 144[3] مكرر من قانون العقوبات الجزائري أن"**يعاقب بغرامة من مئة ألف 100.000دج إلى خمس مئة ألف 500.000دج،كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان ذلك عن طريق الكتابة**

1 المادة 1 من الأمر رقم 66-156 ،سالف الذكر.

2 المادة 296 من الأمر رقم 66-156 ،سالف الذكر.

3 المادة 144 من الأمر رقم 66-156 ،سالف الذكر.

أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية أخرى.

تباشر النيابة العامة إجراءات المتابعة الجزائية تلقائيا.

في حالة العود،تضاعف الغرامة".

ثانيا:الركن المادي لجريمة القذف

الركن المادي يتمثل في الفعل الخارجي الذي يأتيه الجاني،وهو إسناد واقعة معينة إلى شخص آخر تمس شرفه أو سمعته،ويتم ذلك بأي وسيلة علنية.ويتكوّن هذا الركن من ثلاثة عناصر رئيسية:

يقصد به نسبة واقعة معينة إلى المجني عليه على سبيل التأكيد،سواء كانت صحيحة أو كاذبة،مثل أن يقول شخص:"فلان سرق مال المؤسسة".

يشترط المشرع الجزائري في الواقعة المسندة أن[1]:

-تكون محددة ومعينة.

-تمس الشرف أو العرض أو تكون خادشة لسمعة الشخص أو عائلته.

-يمكن أن يكون المجني عليه شخصا طبيعيا أو معنويا،كما يمكن أن تكون جهة عمومية أو نظامية مثل البرلمان،أو جهة قضائية أو الجيش.

يجب أن تتعلق الواقعة المنسوبة بالمجني عليه وتمس شرفه أو اعتباره،و أن تكون واقعة محددة و ليست مجرد رأي أو وصف.

أن يتم القذف أمام الغير، سواء عن طريق الكتابة أو القول أو النشر في وسائل الإعلام أو مواقع التواصل الاجتماعي.فلا تقوم الجريمة إذا لم يكن هناك عنصر العلانية.

1عليلي عبد السلام ،"جريمة القذف عبر مواقع التواصل الإجتماعي دراسة تحليلية مقارنة بين التشريع الجزائري و التشريعات الأجنبية والعربية"،**مجلة الدراسات القانونية والاقتصادية**،المركز الجامعي بريكة،باتنة،المجلد05 ،العدد02، 2022،ص ص 578-579.

و يتحقق القذف سواء تم الإسناد بطريقة مباشرة أو غير مباشرة، و قد يكون عبر التصريح أو التلميح أو حتى باستخدام أساليب استفهامية أو غامضة، طالما أن المعنى يصل إلى الآخرين ويمسّ كرامة المجني عليه.

ثالثا:الركن المعنوي لجريمة القذف

الركن المعنوي لجريمة القذف هو الجانب النفسي أو القصد الجنائي الذي يجب أن يتوفر عند الجاني لقيام الجريمة.ويتكون هذا القصد من القصد العام فقط،أي لا يشترط القانون أن تكون لدى الجاني نية خاصة للإساءة،بل يكفي أن يكون مدركا لما يقوم به.

وبما أن جريمة القذف تعد من الجرائم العمدية، فالقصد العام فيها يتحقق إذا توافرت لدى الجاني العلم و الإرادة،أي أن يكون لديه إرادة واضحة لنشر هذه الأقوال على الملأ.و يتضح القصد الجاني من خلال أمرين:

1-قصد الإسناد:أن يكون الجاني قد تعمّد إسناد واقعة معينة إلى المجني عليه،وهو يعلم أن هذه الواقعة لو كانت صحيحة لأدت إلى معاقبته قانونا أو إلى احتقاره من قبل المجتمع.بمعنى آخر،يجب أن يفهم الجاني معنى العبارات التي قالها و مدى خطورتها على سمعة المجني عليه[1].

2-قصد العلانية:أن يكون الجاني قد تعمّد نشر و إعلان الواقعة التي أسندها للمجني عليه،سواء كان ذلك عبر وسائل التواصل الإجتماعي أو بالكلام أو بالكتابة أو غيرها من طرق العلانية.

ويشترط أيضا أن تكون إرادة الجاني سليمة،أي لا يكون قد أجبر أو هدد،حتى يحمّل المسؤولية الجنائية الكاملة.

1 عليلي عبد السلام ،مرجع نفسه،ص ص 579-580.

الفصل الثاني

أساليب التصدي لجرائم تكنولوجيا الإعلام والإتصال

شهد العالم في العقود الأخيرة تحولا رقميا شاملا لجميع القطاعات، ما جعل تكنولوجيا الإعلام والاتصال تحتل مكانة محورية في حياة الأفراد و المجتمعات.ورغم الإيجابيات لهذا التطور، إلا أنه ساهم في خلق بيئة خصبة لظهور أنماط جديدة من الجرائم، كالتجسس، الاحتيال المالي و الابتزاز الرقمي....إلخ

وقد فرضت هذه التحديات واقعا جديدا يستوجب تبني آليات وقاية شاملة و فعالة، قادرة على مواجهة التهديدات المتزايدة التي تطال الأفراد و المؤسسات و حتى الدول ،و من هذا المنطلق، برزت ضرورة اعتماد آليات فعالة للوقاية من هذه الجرائم، ،و يأتي تناول هذه الآليات كخطوة أساسية لفهم كيفية تحصين الفضاء الرقمي و ضمان استخدام آمن ومسؤول لتكنولوجيا الإعلام والإتصال، ومن بين هذه الآليات نجد أحكام الوقاية المنصوص عليها في قانون 04.09 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها **(المبحث الأول)** كذا أحكام الوقاية المنصوص عليها بموجب قانون الإجراءات الجزائية رقم 11.21 **(المبحث الثاني)**.

المبحث الأول

آليات الوقاية المنصوص عليها بموجب قانون رقم 09-04

قام المشرع الجزائري باتخاذ تدابير لحماية المجتمع من هذه الظاهرة الإجرامية المستجدة المتمثلة في جرائم تكنولوجيا الإعلام والإتصال، من خلال وضع قواعد قانونية جديدة تهدف إلى مكافحة هذا النوع من الجرائم ، تجسد ذلك من خلال إنشاء الهيئة الوطنية بموجب قانون رقم 04.09 للوقاية من جرائم تكنولوجيا الإعلام والإتصال **(المطلب الأول)** أين خولت لها مجموعة من المهام قصد تصدي لهذه الجرائم **(المطلب الثاني)**.

المطلب الأول

إنشاء الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الاتصال

تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال بموجب المادة 13 من القانون رقم 09-04 التي تنص"**تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال.**

تحدد تشكيلة الهيئة و تنظيمها و كيفيات سيرها عن طريق تجهدكم".

حيث هذه المادة نصت صراحة على إحداث هيئة وطنية تعنى بالوقاية من هذا النوع من الجرائم و مكافحتها، و ذلك في إطار تعزيز المنظومة الوطنية للأمن المعلوماتي والتصدي للتهديدات المرتبطة باستخدام تكنولوجيا الإعلام والإتصال ،التعرف على الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الاتصال(الفرع الأول)،كما حدد القانون رقم 04.09 سالف الذكر، تشكيلة هذه الهيئة **(الفرع الثاني)** كذا مهامها **(الفرع الثالث)**.

الفرع الأول

التعرف بالهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الاتصال

تعد الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والإتصال هي سلطة إدارية تتمتع بالشخصية المعنوية والاستقلال المالي تم إنشاؤها بموجب القانون 04/09 الذي أحالنا فيما يخص تنظيمها إلى التنظيم وفعلا صدر المرسوم الرئاسي رقم261/15[1] الصادر 2015/10/08 المتضمن تشكيلية وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والإتصال ومكافحتها، الذي تم تعديله بموجب المرسوم الرئاسي رقم 20-183[2] المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام و الإتصال ومكافحتها[3]، و تتمتع هذه الهيئة بالشخصية المعنوية**(أولا)**،الإستقلال المالي**(ثانيا)**،الأهلية**(ثالثا)**،الموطن**(رابعا)**،حق التقاضي**(خامسا)**وتحمل مسؤولية التعويض عن الأضرار التي تسببها الغير**(سادسا)**.

أولا:الشخصية المعنوية للهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الاتصال

يعد الاعتراف بالشخصية المعنوية للهيئة الوطنية للوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام و الاتصال خطوة بالغة الأهمية في تحديد مدى استقلاليتها. فلا يمكن

1المرسوم الرئاسي رقم 15-261 المؤرخ في 8أكتوبر2015،يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها،ج ر،العدد53،صادر في 11 أكتوبر2015،.

2المرسوم الرئاسي 20-183، المؤرخ في 2020/07/13، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام و الإتصال ومكافحتها، ج ر،العدد،40 صادر بتاريخ 18 جويلية2020.

3أجعود سعاد، الحماية الجزائية لتكنولوجيا الإعلام و الاتصال في التشريع الجزائري "دراسة على ضوء النصوص المستحدثة"، **مجلة الرسالة للدراسات و البحوث الإنسانية**، كلية الحقوق والعلوم السياسية،جامعة العربي التبسي،تبسة،المجلد 07، العدد 04، 2022،ص ص229- 230.

التقليل من أهمية الشخصية المعنوية لما لها من تبعات قانونية ، حيث يعتبر الشخص المعنوي كيانا قانونيا قائما بذاته.

ولقد نص القانون بشكل واضح على أن الهيئة الوطنية للوقاية من تكنولوجيا الإعلام و الاتصال و مكافحتها، تتمتع بالشخصية المعنوية و الاستقلال المالي، و يعد هذا الاعتراف وسيلة قانونية تؤدي إلى عدة نتائج، و من أبرز هذه النتائج، ما ورد في القانون المدني ،أن الشخصية المعنوية تمكن الهيئة من التمتع بالذمة المالية و الأهلية القانونية ضمن الحدود التي يحددها القانون ، و أن يكون لها موطن قانوني ، و حق التقاضي ، مع تحمل المسؤولية عن الأضرار التي قد تتسبب بها للغير[1].

ثانيا: ذمة مالية مستقلة

تتمتع الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الاتصال باعتبارها شخصا معنويا بذمة مالية مستقلة، مع ما يترتب على ذلك من نتائج قانونية باعتبار الذمة المالية مجموعة تترابط فيها العناصر الإيجابية والسلبية.

ثالثا: الأهلية

سواء كانت أهلية وجوب أو أهلية أداء، فإن الشخص المعنوي يتمتع بحقوق الملكية و له الحق في ممارسة السلطات المخولة له بموجب القوانين و الأنظمة ز وبناء على اعتماد الهيئة الوطنية للجهة المتخصصة في تكنولوجيا الإعلام و الاتصال كشخص معنوي ، فإن لها الأهلية ضمن الحدود التي يحددها نظامها الأساسي.وبالتالي تمنح هذه الجهة الحقوق والصلاحيات المنصوص عليها في القانون.

1 بوزيرة سهيلة ،"الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال،يبين سرية المعطيات الشخصية الإلكترونية و مكافحة الجرائم الإلكترونية، **المجلة النقدية للقانون و العلوم السياسية**، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو،المجلد 17، العدد02 ،2022 ،ص564.

رابعا : الموطن

يعد الموطن المكان الذي يوجد فيه مقر إقامتها، وقد حدد القانون موطن الهيئة الوطنية للوقاية من الفساد ومكافحته بمدينة الجزائر، و تتحدد أهمية الموطن القانونية في تحديد الاختصاص الإقليمي للجهات الفاصلة في منازعات الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الاتصال مع الغير.

خامسا: حق التقاضي

يعد حق التقاضي الممنوح للهيئات والوحدات الإدارية حقا مستقلا عن ذلك الممنوح للدولة ، إذ يمكن مقاضاة هذه الجهات من خلال ممثليها القانونيين وترفع الدعاوى ضد الهيئات والوحدات التي تتمتع بالشخصية المعنوية . وبناء عليه، فإن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، بصفتها شخصا معنويا [1]، تملك حق التقاضي سواء بصفتها مدعية أو مدعى عليها ، و يمثلها أمام القضاء رئيسها.

سادسا: تحمل مسؤولية التعويض عن الأضرار التي تسببها الغير

بما أن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال تعد شخصا معنويا ، فإنها تعتبر كيانا قانونيا مستقلا عن الأفراد المكونين لها.و بناء على ذلك ، تتحمل الهيئة المسؤولية الكاملة عن أي ضرر، ماديا كان أو معنويا ، قد تلحقه بالغير.

الفرع الثاني

تشكيلية الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال

حدد المرسوم الرئاسي رقم 15-261[2] سالف الذكر و وفقا للمادة الرابعة منه حدد تشكيلية الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال و مكافحتها و هي كالتالي:

1بوزيرة سهيلة ،مرجع سابق، ص565.

2المرسوم الرئاسي15-261 ،سالف الذكر.

-لجنة مديرية.

-مديرية عامة.

-مديرية المراقبة الوقائية و اليقظة الإلكترونية.

-مديرية التنسيق التقني.

-مركز العمليات لتقنية.

-ملحقات جهوية.

إلا أنه بصدور المرسوم الرئاسي 19-172[1] تم تقليص في تشكيلية لهيئة و أصبحت تتكون من:

-المديرة العامة و تضم: المديرية التقنية،و مديرية الإدارة و الوسائل.

-مجلس التوجيه.

أما المادة 05 من المرسوم 20-183[2] فقد تم وضع التشكيلة التالية:

-مجلس التوجيه.

-المديرية العامة: حسب المادة11 من المرسوم الرئاسي20-183[3] تضم :

-مديرية للمراقبة الوقاية و اليقظة الإلكترونية.

-مديرية الإدارة و الوسائل.

-مصلحة للدراسات و التلخيص.

-مصلحة التعاون و اليقظة التكنولوجية.

1المرسوم الرئاسي رقم19-172 مؤرخ في 2019/06/06 يحدد تشكيبة الهيئة الوطنية للوقاية من الجزائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها و تنظيمها و سيرها،ج.ر العدد 37 ،صادر بتاريخ 09 جوان 2019.

2 المادة 5 من المرسوم 20-183،سالف الذكر.

3المادة 11 من المرسوم 20-183 ،سالف الذكر.

أولا : مجلس التوجيه

حسب المادة 8 من المرسوم الرئاسي رقم 20-183[1] "**يجتمع المجلس 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 يطلب من أحد أعضائه أو من المدير العام للهيئة"

حسب المادة6 من المرسوم الرئاسي رقم 20-183[2] سالف الذكر، و برأسه رئيس و يمكن أن يفوض ممثليه ، و يتشكل من الأعضاء التالية:

-الوزير المكلف بالعدل.

-الوزير المكلف بالداخلية.

-الوزير المكلف بالمواصلات السلكية و اللاسلكية.

-المدير العام للأمن الداخلي.

-قائد الدرك الوطني.

-المدير العام للأمن الوطني.

لقد حددت المادة 07 من المرسوم الرئاسي20-183[3] مهام هذا المجلس حيث تنص **يكلف مجلس التوجيه لاسيما ب:**

-توجيه عمل الهيئة والإشراف عليه و مراقبته.

-دراسة كل مسألة تخضع لمجال اختصاص الهيئة ، لاسيما فيما يتعلق بتوفر شروط اللجوء للمراقبة الوقائية للاتصالات الإلكترونية المنصوص عليها في المادة 4 من القانون رقم 09-04 المؤرخ في 5 أوت 2000 المذكور أعلاه.

1المادة8 من المرسوم الرئاسي رقم20-183،سالف الذكر.

2المادة 6 من المرسوم الرئاسي رقم 20-183 ،سالف الذكر.

المادة 07 من المرسوم الرئاسي رقم 20-183 ،سالف الذكر.3

-المداولة حول الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

-المداولة حول مسائل التطوير و التعاون مع المؤسسات و الهيئات الوطنية و الأجنبية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام و الاتصال.

-القيم دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال للتمكن من تحديد مضامين العمليات الواجب القيام بها و الأهداف المنشودة بدقة.

-اقتراح كل نشاط يتصل بالبحث و تقييم الأعمال المباشرة في مجال الوقاية من جرائم تكنولوجيا الإعلام و الاتصال ومكافحتها.

-إعداد نظامها الداخلي و المصادقة عليه .

-دراسة التقرير السنوي لنشاطات الهيئة و المصادقة عليه

-الموافقة على برنامج الهيئة.

-دراسة مشروع و ميزانية الهيئة و الموافقة عليه.

-إبداء رأيه في كل مسألة تتصل بمهام الهيئة.

-تقديم كل اقتراح يتصل بمجال اختصاص الهيئة.

-المساهمة في ضبط المعايير القانونية في مجال اختصاصه.

ثانيا: المديرية العامة

تنص المادة 9 من المرسوم الرئاسي 20-183[1] سالف الذكر" **يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي و تنهى مهامه حسب الأشكال نفسه**"، لقد حددت

1 المادة 09 ، المرسوم الرئاسي 20-183 ،سالف الذكر.

المادة 10[1] من نفس المرسوم مهام المديرية العامة حيث تنص "**تتولى المديرية العامة على الخصوص الصلاحيات التالية:**

- السهر على السير الحسن للهيئة.

- إعداد مشروع ميزانية الهيئة و عرضه على مجلس التوجيه للموافقة.

- إعداد و تنفيذ برنامج عمل الهيئة بعد الموافقة عليه من قبل مجلس التوجيه.

-تنشيط وتنسيق ومتابعة ومراقبة أنشطة مكونات المديرية العامة.

- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

- تبادل المعلومات مع مثيلاتها في الخارج بهدف تجميع كل المعطيات المتعلقة بتحديد مكان و هوية مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والتعرف عليهم.

- تمثيل الهيئة لدى السلطات و المؤسسات الوطنية و الدولية.

- السهر على القيام بإجراءات التأهيل و آداء اليمين فيما يخص المستخدمين المعنيين في الهيئة.

-الإداري و المالي للهيئة.

- تحضير اجتماعات مجلس توجيه الهيئة.

- إعداد التقرير السنوي لنشاطات الهيئة ،ورفعه لمصادقة مجلس التوجيه.

ثالثا: كيفية سير عمل الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الإتصال

تنص المادة 07 من المرسوم الرئاسي رقم 19-172[2] سالف الذكر، على أن "**يجتمع مجلس التوجيه في دورة عادية مرتين في السنة،بناءا على استدعاء من رئيسه.**

1 المادة 10،المرسوم الرئاسي 20-183،سالف الذكر.

2 المادة 07 من المرسوم الرئاسي رقم 19-172 ،سالف الذكر.

ويمكنه أن يجتمع في دورة غير عادية كلما كان ذلك ضروريا،بناء على استدعاء من رئيسه أو بطلب من أحد أعضائه أو من المدير العام للهيئة".

كما تنص المادة 08[1] من المرسوم الرئاسي رقم 183.20 على أن "**تحدد قواعد وكيفيات سير مجلس التوجيه بموجب قرار من وزير الدفاع الوطني".**

ووفقا للفقرة الأولى من المادة 18 من المرسوم رقم 15-261[2]، تنص على أن تزويد الهيئة بقضاة و ضباط و أعوان من الشرطة القضائية ، بالإضافة إلى مساعدين من مصالح الاستخبارات العسكرية و الأمن و الدرك، و يحدد عددهم حسب الحاجة لإصدار قرارات مشتركة بين مختلف هذه المصالح ، كما يتم تزويد الهيئة بمستخدمين في مجالي الدعم التقني و الإداري ، و يتم استقدام هؤلاء من مصالح الاستعلام العسكري و الأمن و الدرك.

و من جهة أخرى يمكن للهيئة الاستعانة بأي خبير أو شخص يتمتع بالكفاءة لتعيينه في مهامها، كما يحق لها طلب أي وثيقة أو معلومة من أي جهاز أو مؤسسة ترى أنها ضرورية لتنفيذ المهام المسندة إليها.

الفرع الثالث

مهام الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والإتصال

قد خول المشرع الجزائري لهذه الهيئة مهمة المراقبة الوقائية في مجال الإتصالات، وذلك بهدف الوقاية من الجرائم التي تصنف ضمن الأعمال الإرهابية أو التي تهدد أمن الدولة،ويلاحظ أن المشرع منح الهيئة مهمة التحري في مختلف الجرائم التي تمس بأمن الدولة بشكل عام ،مثل التجسس ،الإرهاب،خاصة إذا تم ارتكابها باستخدام الوسائل الإلكترونية،مما يعني أن أي جريمة تمس بالأمن الوطني أو بمقومات الدولة الجزائرية تدخل

1 المادة 8 من المرسوم الرئاسي،19-172،سالف الذكر.

2 المادة 18 من المرسوم الرئاسي رقم 15-261 ،سالف الذكر.

ضمن اختصاص هذه الهيئة[1]،وحدد المرسوم الرئاسي رقم 21-439[2]المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والإتصال ومكافحتها، وانطلاقا من اسمها،يستنتج أن للهيئة دورين رئيسيين الوقاية من جرائم تكنولوجيا الإعلام والإتصال **(أولا)**،أما الدور الثاني يتمثل في مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال **(ثانيا)**.

أولا:الوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام و الاتصال

تتمثل مهمة الهيئة في الجانب الوقائي في توعية مستخدمي تكنولوجيا المعلومات بخطورة الجرائم التي قد يتعرضون لها أثناء استخدامهم لهذه الوسائل،وتعد هذه الخطوة من الإجراءات الوقائية المهمة،ومن بين أبرز هذه الجرائم:

-التجسس على الاتصالات و الرسائل الإلكترونية.

-التلاعب بالحسابات البنكية أو ببطاقات الائتمان.

-اختراق أجهزة المؤسسات الكبرى أو الهيئات الحكومية،وغيرها[3].

ثانيا:مكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال

بالرجوع إلى نص المادة 14 من القانون رقم 04/09[4] السالف الذكر، تستند إلى الهيئة مجموعة من المهام في مجال مكافحة هذا النوع من الجرائم، وهي كالتالي:

-تنشيط و تنسيق مختلف الجهود اللازمة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و العمل على مكافحتها.

---

1 بوزبرة سهيلة ،مرجع سابق،ص ص 562- 563 .

2المرسوم الرئاسي 21-439 المؤرخ في 7 نوفمبر 2021،يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها، ج ر،العدد86 ،صادر بتاريخ 11نوفمبر 2021 .

3أحمد مسعود مريم،آليات مكافحة جرائم تكنولوجيا الإعلام و الاتصال في ضوء القانون رقم 04/09 ،مذكرة لنيل شهادة الماجستير ،كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح، ورقلة،2013 ص45 .

4المادة 14 من القنون رقم 09-04 ،سالف الذكر.

-تبادل المعلومات مع الهيئات المماثلة في الخارج بهدف جمع كل ما يمكن أن يساعد في التعرف على مرتكبي هذه الجرائم.

كما أن المرسوم الرئاسي رقم 21-439 ، قد أضاف إلى المهام السابقة ما يلي حسب المادة 04 منهما يلي:

-الإسهام في تكوين محققين متخصصين في مجال التحقيقات التقنية المرتبطة بتكنولوجيا الإعلام و الاتصال.

-تطوير التعاون مع مختلف المؤسسات و الهيئات الوطنية.

-حفظ البيانات الرقمية المرتبطة بالأنظمة المعلوماتية، مع تحديد مصدرها ومسارها، لغرض استعمالها كأدلة في الإجراءات القضائية عند الحاجة.

من خلال أجهزتها التنظيمية تمتلك الهيئة صلاحيات واسعة على المستوى الإداري و المالي، من بينها:

-إعداد النظام الداخلي و المصادقة عليه، و هي مهمة تعود إلى اللجنة المديرة حسب المرسوم الرئاسي 15-261، وإلى مجلس التوجيه حسب المرسوم 19-172.

-ضمان التسيير الإداري والمالي للهيئة، ويتم ذلك إما من قبل المديرية العامة أو مديرية الإدارة و الوسائل، بحسب ما ينص عليه كل مرسوم.

من خلال دراسة المهام الموكلة للهيئة، يتضح أن المشرع منحها صلاحيات أغلبها استشارية و رقابية، إلى جانب بعض المهام الإدارية، لكنه في المقابل لم يمنحها صلاحيات قمعية ، أي أن دورها يظل وقائيا بالدرجة الأولى لا عقابيا.

حسب المادة 65 مكرر 07 من الأمر 66-155[1] المتضمن قانون الإجراءات الجزائية المعدل بالمادة 14 من القانون رقم 06-22، يمكن للهيئة أن تستعين بالشرطة القضائية في

1 المادة 65 مكرر 07 من الأمر رقم 66-155 المؤرخ في 1966/06/08، المتضمن قانون الإجراءات الجزائية، المعدل و المتمم بالأمر رقم 22-06 المؤرخ في 2022/03/21 ، ج ر، العدد20، صادر بتاريخ21 مارس2022 .

التحريات المرتبطة بالجرائم الالكترونية، لكنها لا تملك صلاحية تحريك الدعوى العمومية بنفسها،بل تحويل الملفات إلى وزير الدفاع، و هو ما يظهر أنها تفتقد إلى الاستقلال القضائي الكامل. و من جهة أخرى، ورغم أن القانون يقر بأن الهيئة مؤسسة ذات طابع إداري و تتمتع بالشخصية المعنوية، مما يفترض أن تكون مستقلة ماليا و إداريا، إلا أن الواقع يظهر عكس ذلك:

-**ماليا**:تخضع الهيئة لرقابة وزير الدفاع، الذي يعد الأمر بالصرف[1].

-**إداريا**:يتم إنشاء الهيئة تحت وصاية وزير الدفاع، والمدير العام و مستخدمي الهيئة يعينون وفق التنظيم المعمول به في وزارة الدفاع الوطني.

-**وظيفيا**:تلزم الهيئة بتقديم تقرير سنوي عن نشاطاتها إلى وزير الدفاع، مما يثبت تبعيتها الكاملة له، حسب ما ورد في القوانين التنظيمية الخاصة بها.

أما فيما يخص المادة 11 من الأمر رقم 66-155[2] فهي تؤكد أن مهام التحري و الضبط تعود أصلا للشرطة القضائية ، مما يبرز أن دور الهيئة يظل فقط مساندا في هذا المجال.

بالتالي، وعلى الرغم من أهمية الهيئة في الوقاية من جرائم تكنولوجيا الإعلام و الاتصال، إلا أن فعاليتها تبقى محدودة بسبب غياب الاستقلال الحقيقي، سواء في الجوانب الإدارية،المالية أو حتى القضائية،وهذا يجعلها خاضعة بشكل شبه كلي لسلطة وزير الدفاع.

1 بوزيرة سهيلة ، مرجع سابق،ص572.

2المادة 11 من الأمر رقم 66-155،سالف الذكر.

المطلب الثاني

القواعد الإجرائية المنصوص عليها في قانون رقم 09-04

في إطار سعي الدولة الجزائرية لتعزيز أمن الفضاء السيبراني و مواجهة التحديات الناجمة عن الاستخدام غير المشروع لتكنولوجيا الإعلام و الاتصال ، جاء القانون رقم 09-04 سالف الذكر، كخطوة تشريعية رائدة تهدف إلى وضع أساس قانوني واضح لمعالجة هذا النوع المستحدث من الإجرام، وقد تضمن هذا القانون أحكاما جزائية إجرائية تتناسب مع طبيعة الجريمة المعلوماتية، التي غالبا ما تتصف بالطابع الخفي و العابر للحدود، و تستوجب آليات خاصة للتحري و التحقيق وجمع الأدلة.

و من بين القواعد الإجرائية الخاصة التي تضمنها هذا القانون للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال نجد مراقبة الاتصالات الإلكترونية **(الفرع الأول)** ، تفتيش المنظومة المعلوماتية و حجز المعطيات **(الفرع الثاني)** و التزامات مقدمي خدمات الانترنت**(الفرع الثالث)**.

الفرع الأول

مراقبة الاتصالات الالكترونية

تعد مراقبة الإتصالات الإلكترونية من أبرز القضايا التي أثارت جدلا واسعا في السنوات الأخيرة،خاصة مع تطور وسائل الاتصال الحديثة وانتشارها الواسع فبينما تبرر هذه المراقبة بالحاجة إلى حماية الأمن ومكافحة الجريمة.

لقد عرف المشرع الجزائري الإتصالات الإلكتونية بموجب المادة 02 من القانون رقم 09-04[1] على أنها"**أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية**".

1المادة 2من القانون رقم 09-04 ،سالف الذكر.

نصت المادة 03 من القانون 09-04[1] على أنه "**مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات يمكن لمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية و في هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية و تجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية** "،نجد أن المشرع الجزائري حدد لنا حالات اللجوء إلى المراقبة الإلكترونية بموجب نص المادة 4 من قانون09.04 **(أولا)**،كما خول لها حماية مقررة للمراقبة الإلكترونية **(ثانيا)**،تكون اعراضه عن طريق اعتراض المراسلات السلكية أو اللاسلكيةأو عن طريق اعتراض البريد الإلكتروني**(ثالثا)**،ألاّ أن هذه المراقبة مقيدة بمدة زمنية لا يجوز مخالفتها**(رابعا)**.

أولا: حالات اللجوء إلى المراقبة الالكترونية حسب المادة 04 من القانون 09-04 فيما يلي:

1-الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة:

أجاز المشرع الجزائري اللجوء إلى مراقبة الاتصالات الإلكترونية و تفتيش المنظومة المعلوماتية في مرحلة تسبق ارتكاب الجريمة، أي لمجرد توفر معلومات لدى السلطة القضائية المختصة تشير إلى احتمال وقوع إحدى هذه الجرائم. و يعزى هذا الإجراء إلى خطورة هذه الأفعال و صعوبة الكشف عن مرتكبيها ، إضافة إلى أنها غالبا ما ترتكب عبر وسائل الاتصال أو التحكم عن بعد ، مما يستوجب اتخاذ تدابير وقائية استباقية[2].

1المادة 3 من القانون 09-04 ،سالف الذكر.

2 ثابت دينازاد ، "مراقبة الاتصالات الإلكتزونية و الحق في حرمة الحياة الخاصة في القانون الجزائري"،**مجلة العلوم الاجتماعية و الإنسانية** ،كلية الحقوق والعلوم السياسية،جامعة العربي التبسي،تبسة،المجلد،العدد01، 2012، ص ص 210-211.

2- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني:

في هذه الحالة ، يمكن اتخاذ إجراءات المراقبة أو التفتيش قبل وقوع الجريمة ، بمجرد تلقي السلطة القضائية معلومات تشير إلى تهديد جدي. و يهدف هذا الإجراء إلى الحيلولة دون وقوع جرائم قد تضر بشكل مباشر بأمن الدولة و مؤسساتها.

3-لمقتضيات التحريات و التحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية:

تتخذ إجراءات المراقبة الالكترونية أو تفتيش المنظومات المعلوماتية خلال مراحل ما بعد ارتكاب الجريمة ، خصوصا عندما تعجز الوسائل التقليدية عن الوصول إلى الأدلة أو معرفة هوية الجناة. و يلاحظ هنا أن نص البند (ج) من الفقرة الأولى في المادة 4 لم يحدد نوع الجرائم المعنية، مما يفهم منه أن هذه الإجراءات قد تطبق على جميع الجرائم المرتبطة بتكنولوجيا الإعلام و الاتصال ، لا سيما الجرائم المنظمة أو العابرة للحدود.

4- تنفيذ طلبات المساعدة القضائية الدولة المتبادلة:

في حالة ارتكاب جرائم تتعلق بتكنولوجيا الإعلام و الاتصال خارج الإقليم الوطني ، يجوز للسلطات الجزائية تنفيذ مراقبة الاتصالات أو تفتيش المنظومات المعلوماتية داخل الإقليم إذا كان ذلك من شأنه المساهمة في كشف الجريمة و مرتكبيها، شريطة أن يتم ذلك في إطار التعاون القضائي الدولي ، وفقا للاتفاقيات الدولية و مبدأ المعاملة بالمثل[1].

ثانيا: الحماية المقررة للمراقبة الإلكترونية

تعمل عدة قوانين عن حماية سرية و خصوصية الاتصالات الإلكترونية من بينها:

---

1 ثابت دينازاد ،مرجع سابق، ص211 .

1- قانون البريد و الاتصالات الإلكترونية:

تنص المادة 119 من قانون البريد و الاتصالات الإلكترونية18-04[1]سالف الذكر، على "**يلزم متعامل و الاتصالات الإلكترونية باتخاذ التدابير التي من شأنها أن تضمن سرّية المكالمات والمعلومات التي يحوزونها عن مشتركيهم. وألا يسمح بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية و الوصلات والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية وفقا للتشريع المعمول به.و يجب عليهم أن يطلعوا أعوانهم على الالتزامات التي يخضعون لها و على العقوبات التي يتعرضون لها في حالة عدم احترامهم لهذه الأحكام**".

تضمنت المادة 164 من القانون الأحكام المتعلقة بجريمة التنصت على الاتصالات السلكية و اللاسلكية، بينما عالجت المادتان 165 و 166 جريمة تحويل مضمون هذه الاتصالات، سواء من خلال إفشاءها أو نشرها أو استخدامها بشكل غير مشروع[2] . ووفقا للمادة 187 من قانون البريد و الاتصالات الإلكترونية18-04[3] سالف الذكر، "**يعد الشخص المعنوي مسؤولا جزائيا عن الجرائم المذكورة في هذا القانون، طبقا للقواعد المنصوص عليها في قانون العقوبات**".

2- قانون العقوبات:

يكفل المشرع حماية قانونية خاصة لسرية و خصوصية الاتصالات الالكترونية ، حيث يعد اعتراض هذه المراسلات أو الاطلاع عليها أو تحويلها دون إذن، جريمة تمس بحرمة

1 المادة 119 من القانون رقم 18-04 ،سالف الذكر .

2 روابح فريد ،"ضمانات حرمة الحياة الخاصة أثناء إجراء مراقبة الاتصالات الإلكترونية"، **مجلة الأبحاث القانونية و السياسية**،كلية الحقوق والعلوم السياسية،جامعة محمد الصديق بن يحي جيجل،المجلد02 ، العدد02، 2020،ص9 .

3 المادة 187 من القنون 18-04 ،سالف الذكر.

الحياة الخاصة ، و ذلك وفقا لأحكام المواد303 مكرر و 303 مكرر 3 من القانون رقم 06-23[1] المعدل و المتمم للأمر 66-156 المتضمن قانون العقوبات.

كما يعد تقصير مقدمي خدمات الانترنت في الالتزام بالتداخل لسحب أو تخزين أو حجب المحتويات التي تشكل جرائم ، أو عدم وضع الترتيبات التقنية اللازمة لذلك ، مخالفة صريحة لنص المادة 394 مكرر 8من قانون العقوبات[2].

3- قانون الوقاية من جرائم تكنولوجيا الإعلام و الاتصال:

يتضمن قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها عدة أحكام تهدف إلى حماية سرية الاتصالات و خصوصية الأفراد، حيث تنص المادة 3 من هذا القانون على ضرورة احترام الأحكام القانونية التي تضمن سرية المراسلات و الاتصالات عند وضع الترتيبات التقنية المتعلقة بمراقبة الاتصالات الإلكترونية و تسجيلها و تجميعها، وذلك في الحالات التي تقتضيها متطلبات التحريات أو التحقيقات القضائية الجارية ، أو للحفاظ على النظام العام.

كما تؤكد المادة 4 على أن هذه الترتيبات التقنية يجب أن تنفذ في إطار احترام الحياة الخاصة للغير، و تحت طائلة العقوبات في حال الإخلال بذلك.

تنص المادة 27 من المرسوم الرئاسي رقم 15-261 [3] سالف الذكر، المتعلق بتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ، على إلزام مستخدمي الهيئة بالتقيد بالسر المهني و واجب التحفظ ، و يشترط عليهم أداء اليمين القانونية للحفاظ على سرية المعلومات التي يطلعون عليها أثناء عمليات مراقبة الاتصالات الالكترونية.

1قانون رقم 06-23 المؤرخ في 20ديسمبر2006 ،يعدل و يتمم الأمر رقم 66-156 المتعلق و المتضمن قانون العقوبات،ج ر ،عدد84 ،صادر بتاريخ24 ديسمبر2006 .

2 روابح فريد ،مرجع سابق ،ص06.

3المادة 127 من المرسوم الرئاسي رقم 15-261، سالف الذكر.

ثالثا: أشكال مراقبة الاتصالات الالكترونية

من صور مراقبة التصالات الالكترونية نجد:

1- اعتراض المراسلات السلكية و اللاسلكية:

يمكن تعريف اعتراض المراسلات على أنه إجراء تحقيقي ينفذ بشكل سري و يمس بسرية الأحاديث الخاصة ، و يصدر بأمر من الجهة القضائية المختصة و وفقا للإجراءات التي يحددها القانون بهدف الحصول على دليل غير مادي حول الجريمة. و يتضمن هذا الإجراء ، الاستماع سرا إلى الأحاديث الخاصة ، و يعد من الوسائل الحديثة الفعالة التي تعتمدها الجهات الأمنية و القضائية لمكافحة الجرائم الخطيرة ، و يتم عبر وسائل الاتصال السلكية و اللاسلكية[1].

منح المشرع الجزائري للسلطات القضائية صلاحية اعتراض المراسلات السلكية و اللاسلكية و ذلك بموجب المادة 65 مكرر 05 من قانون الإجراءات الجزائية، التي أضيفت بموجب القانون رقم 06- 22[2] و مع ذلك لم يقدم المشرع الجزائري تعريفا دقيقا لهذا الإجراء ، المعروف أيضا بالتنصت.

2- اعتراض البريد الالكتروني:

يعد اعتراض البريد الالكتروني أحد أشكال مراقبة الاتصالات الالكترونية، و نظرا لاعتماده على شبكة الانترنت كوسيلة للتواصل، فإن الطرق التقليدية للمراقبة لا تعد فعالة في هذا السياق. لهذا السبب، ظهرت برامج و تقنيات متطورة قادرة على مراقبة البريد

1ياسير الأمير فارق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية دراسة تأصيلية تحليلية و مقارنة للتنصت على المحادثات التلفزيونية و التي تجري عبر الانترنت و الأحاديث الشخصية نظريا و عمليا ، دار المطبوعات الجامعية، الإسكندرية ،2009 ،ص150.

2القانون رقم 06-22 ،المؤرخ في 20ديسمبر 2006 ،المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها،ج ر،العدد 84 ،صادر بتاريخ 24ديسمبر 2006.

الإلكتروني، من أبرزها نظام Carnivore، الذي تستخدمه وكالة التحقيقات الفيدرالية الأمريكية (FBI) في عمليات التجسس[1].

رابعا: مدة مراقبة الاتصالات الإلكترونية

حددت المادة 65 مكرر من قانون الإجراءات الجزائية مدة المراقبة الإلكترونية بأربعة أشهر قابلة للتجديد. في حين لم يحدد القانون رقم 09-04 مدة المراقبة إلا في حالات الجرائم الإرهابية والتخريبية و تلك التي تمس بأمن الدولة ، حيث تطبق نفس المدة التي تنص في المادة 65 مكرر7 من القانون رقم 06-22[2] من قانون الإجراءات الجزائية بأن"**يجب أن يتضمن الإذن المذكور في المادة 65 مكرر5 أعلاه،كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.**

يسلم الإذن مكتوبا لمدة أقصاها أربعة(4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية".

غير أنه إذا تعلقت المراقبة بجرائم الإرهاب أو التخريب أو المساس بأمن الدولة ، فإن المادة 4 الفقرة 5 من القانون 09-04[3] تنص **"لا يجو اجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتبوب من السلطة القضائية المختصة"**

تنص على أن الإذن الذي يمنحه النائب العام لدى مجلس قضاء الجزائر العاصمة للهيئة الوطنية للوقاية من الجرائم الإلكترونية تكون مدة ستة أشهر قابلة للتجديد ، و ذلك بناءا على تقرير يوضح طبيعة الترتيبات التقنية المستخدمة و الأهداف المرجوة منها.

---

1 بن يحي إسماعيل ،"التعريف بمراقبة الإتصالات الإلكترونية كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية"،**مجلة صوت القانون**،،كلية الحقوق والعلوم السياسية،جامعة الجيلالي بونعامة خميس مليانة،العدد2 ،2022 ص ص1072- 1073 .

2المادة 65 مكرر7 من القانون رقم 06-22 ،سالف الذكر.

3المادة 4الفقرة5 من القانون 09-04 ،سالف الذكر.

الفرع الثاني

تفتيش المنظومة المعلوماتية وحجز المعطيات

يعد التفتيش من الإجراءات الأساسية في مرحلة التحقيق، حيث يتمثل هدفه في البحث عن أدلة تثبت وقوع الجريمة، وهو بحد ذاته لا يعتبر دليلا، بل وسيلة تهدف إلى الوصول إلى أدلة مادية يمكن الاعتماد عليها قانونيا،و يظل الهدف الأساسي لعملية تفتيش المنظومة المعلوماتية **(أولا)**هو وضع اليد على الأدلة المادية التي تساعد على كشف المجرم،ومما يتطلب ذلك من تدابير حجز معينة[1]**(ثانيا)**.

أولا: التفتيش

يمكن تعريف التفتيش بأنه إجراء من إجراءات التحقيق يباشره شخص مخول قانونا، و يهدف إلى البحث عن أدلة مادية تتعلق بجناية أو جنحة، داخل مكان يتمتع بحرمة قانونية، و ذلك بغض النظر عن موافقة صاحبه.

أو أنه عملية بحث دقيقة في مكنون أسرار الأفراد، سعيا للكشف عن أدلة جريمة ارتكبت فعلا. و هو إجراء يتم ضمن التحقيق الابتدائي، و يمارسه في الأصل قاضي التحقيق، و قد يخول لضباط الشرطة القضائية كاستثناء[2].

يتضح أن التفتيش يتمحور حول فكرة جوهرية مفادها البحث و التحري داخل المجال الخاص بالأفراد للكشف عن الحقيقة، مع ضمان التوازن بين متطلبات التحقيق و احترام حرمة الحياة الخاصة.

---

1 بوحليط يزيد ، تفتيش المنظومة المعلوماتية وحجز المعطيات في التشريع الجزائري،**التواصل في الإقتصاد والإدارة والقانون** ،كلية الحقوق والعلوم السياسية،جامعة باجي مختار ،عنابة،عدد48، 2016،ص90.

2 هميسي رضا ،"تفتيش المنظومات المعلوماتية في القانون الجزائري"،**مجلة العلوم القانونية و السياسية**،كلية الحقوق والعلوم السياسية،جامعة قاصدي مرباح،ورقلة،العدد05،جوان 2012، ص160 .

1-شروط التفتيش

أ الشروط الشكلية:

أ. 1-توقيت التفتيش: عندما يتعلق الأمر بالجرائم المرتبطة بأنظمة المعالجة الآلية للمعطيات، يسمح بإجراء التفتيش و المعاينة و الحجز سواء في الأماكن السكنية أو غير السكنية ، و في أي وقت من ساعات النهار أو الليل ، شريطة الحصول على إذن مسبق من وكيل الجمهورية المختص.

أ.2-حضور الأطراف أثناء التفتيش: ألزم المشرع الجزائري أن يتم التفتيش داخل المنزل بحضور المتهم، و إذا تعذر ذلك لأي سبب يطلب من المتهم تعيين ممثل عنه لحضور إجراءات التفتيش. أما إذا امتنع عن تعيين ممثل أو كان في حالة فرار، وجب أن يجري التفتيش بحضور شاهدين من غير الموظفين التابعين لضباط الشرطة القضائية.

أ.3-محضر التفتيش:في الجرائم المتعلقة بالمعطيات الرقمية ، تعد محاضر الشرطة القضائية محاضر بحث ابتدائي، و تكتسي أهمية بالغة سواء كوسيلة إثبات توثق وقوع الجريمة و نسبتها إلى مرتكبها، أو بسبب السلطات الواسعة المخولة لضباط الشرطة القضائية في هذا السياق[1].

ب-الشروط الموضوعية:

ب.1-سبب التفتيش: يستند إجراء التفتيش إلى الاشتباه في ارتكاب جريمة معلوماتية بوجه عام، وهو ما يبرر التدخل للبحث عن الأدلة الرقمية.

ب.2-محل التفتيش: يتمثل محل التفتيش في هذه الجرائم بالحاسب الآلي، الذي يعد الوسيلة الرئيسية التي ترتكب من خلالها الجريمة، و النافذة التي تربط المستخدم بالعالم الرقمي.

1 دوباي سفيان،يسعد صورية ،مرجع سابق، ص55.

ب.3-السلطة الخاصة بالقيام بالتفتيش:تتمثل الجهة القضائية المخولة قانونا للقيام بعمليات التفتيش في كل من قاضي التحقيق والنيابة العامة، و يختلف هذا الإسناد بحسب التشريعات،حيث يعد قاضي التحقيق أو النيابة العامة السلطة الأصلية،في حين يمكن أن تمنح هذه الصلاحية استثناءا لأعوان الضبط القضائي. و في حال وقوع جريمة من صنف الجنايات أو الجنح، و تعذر وجود قاضي التحقيق المختص، يجوز للمسؤول عن التحقيق إذا استدعت الضرورة اتخاذ إجراء عاجل أن يعرض المسألة على أي قاض موجود ضمن دائرة اختصاص قاضي التحقيق أو في منطقة قريبة، لاتخاذ ما يلزم من قرارات مؤقتة، على أن تحال الأوراق لاحقا إلى قاضي التحقيق المختص بأقرب فرصة ممكنة[1].

ثانيا: حجز المعطيات المعلوماتية

لم تعد القواعد التقليدية للتفتيش كافية للتعامل مع الجرائم المرتبطة بتكنولوجيا المعلومات و الاتصال، نظرا لطبيعتها التقنية و البيئة الرقمية التي ترتكب فيها. لذلك، أقر المشرع الجزائري في المادة 6 من القانون 04/09[2] أن"**عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11أدناه،تحت تصرف السلطات المذكورة.**

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزوها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

1 عثمانين عز الدين ،"إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصالات المعلوماتية"، **مجلة دائرة البحوث و الدراسات القانونية و السياسية**،كلية الحقوق والعلوم السياسية،المركز الجامعي تيبازة،،العدد 04، جانفي 2018 ، ص ص57 -58.

2 المادة 06 من القانون رقم 09-04،سالف الذكر.

إمكانية حجز المعطيات المخزنة ضمن النظم المعلوماتية، إذا كانت تسهم في كشف الجريمة و التعرف على مرتكبيها.

1-الحفاظ على سلامة المعطيات بعد الحجز

و يتم هذا الحجز من خلال نسخ البيانات المستهدفة، بالإضافة إلى المعلومات الضرورية لفهمها، على وسائط تخزين إلكترونية قابلة للحجز، توضع في إحراز وفقا لأحكام قانون الإجراءات الجزائية.وتعتمد هذه الطريقة عندما لا يكون من الضروري حجز النظام المعلوماتي بالكامل، خاصة إذا كانت المعطيات موجودة على القرص الصلب لجهاز تابع لمزود الخدمة .و تشمل عملية النسخ أيضا البيانات التكميلية التي تسمح بقراءة و فهم البيانات الأصلية، خصوصا إذا كانت الأخيرة تحتاج إلى برامج أو أدوات تقنية معينة لعرضها بشكل مفهوم.

تلتزم الجهة المختصة باتخاذ الإجراءات اللازمة للحفاظ على سلامة المعطيات داخل المنظومة المعلوماتية محل التفتيش.ويتطلب ذلك إستخدام الوسائل التقنية المناسبة لضمان بقاء البيانات قابلة للاستغلال لاحقا، بما في ذلك إمكانية تشكيلها أو إعادة تشكيلها إذا تطلب الأمر ذلك.

2الحجز عن طريق منع الوصول إلى المعطيات: في بعض الحالات، قد يكون من غير الممكن نسخ المعطيات لأسباب تقنية[1]، كأن تكون مخزنة داخل أنظمة تشغيل يصعب التعامل معها.وفي هذه الحالة، تلزم المادة 7 من القانون 04/09 [2] أن " **إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6أعلاه ،لأسباب تقنية،يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي**

1فلاح عبد القادر،"حجز وحفظ المعطيات في الجريمة الالكترونية"،**مجلة صوت القانون**،كلية الحقوق والعلوم السياسية،جامعة الجيلالي بونعامة الخميس مليانة، المجلد 08 ،العدد01 ،2021،ص181.

2 المادة 07 من القانون رقم 09-04 ،سالف الذكر.

تحتويها المنظومة المعلوماتية ،أو إلى نسخها،الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".

السلطة المنفذة باستخدام تقنيات تمنع الوصول إلى تلك المعطيات، خاصة من قبل الأشخاص المخولين باستخدام النظام المعلوماتي. ويعد هذا الإجراء وسيلة احترازية مهمة تهدف إلى حماية الأدلة من أي تلاعب أو محاولة لإخفائها ضمن بيئتها الرقمية الأصلية[1].

الفرع الثالث

التزامات مقدمي خدمات الانترنت

أوجب القانون رقم 09-04 على مقدمي خدمات الانترنت مجموعة من الالتزامات الأساسية، وذلك بهدف دعم جهود مكافحة الجريمة الإلكترونية، وتمكين السلطات المختصة من الوصول إلى المعلومات الضرورية أثناء التحقيق نجد:

أولا:الالتزام بمساعدة الضبط القضائي: يلتزم مقدمو خدمات الانترنت، مثل متعهدي الوصول و مزودي الإيواء و المعلومات، بتقديم كل المعطيات المتوفرة لديهم إلى سلطات الضبط القضائي عند الحاجة.ويتطلب ذلك منهم الاحتفاظ بالبيانات الخاصة بمستخدمي خدماتهم،حتى تكون جاهزة عند طلبها فالخدمات عبر الانترنت تمر عبر جهات،كل منها يؤدي دورا معينا، مثل ربط المستخدم بالشبكة أو تخزين المعلومات أو نقلها،ما يجعل تعاونهم ضروريا لكشف الجرائم الإلكترونية.

ثانيا:الالتزام بحفظ المعطيات المتعلقة بحركة السير: ألزم القانون المذكور أعلاه مقدمي الخدمة بالاحتفاظ بمعطيات تقنية مهمة، ومن هذه المعطيات ما نصت عليه المادة 11 من القانون 04-09[2] "**مع مراعاة طبيعة ونوعية الخدماتيلتزم مقدمو الخدمات بحفظ:**

أ-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

---

1 أجعود سعاد ، مرجع سابق،ص ص 228 -229.

2 المادة 11 من القانون04-09،سالف الذكر.

ب-المعطيات المتعلقة بالتجهيزات الظرفية المستعملة للاتصال.

ج-الخصائص التقنية و كذا تاريخ ووقت و مدة كل اتصال.

د-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.

هـ-المعطيات التي تسمح بالتعرف على المرسل أو المرسل إليهم الاتصال و كذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف ،يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه".

-سحب المحتوى الغير مشروع.

-وضع الترتيبات التقنية لحصر إمكانية الدخول للمعلومات غير المشروعة[1].

المبحث الثاني

القواعد الإجرائية المنصوص عليها في قانون العقوبات

فرض التطور السريع لتكنولوجيا الإعلام و الاتصال على المشرع ضرورة مواكبة هذا الواقع بترسانة قانونية تتلاءم مع خصوصيات جرائم تكنولوجيا الإعلام والإتصال. و من هذا المنطق، عمل المشرع الجزائري على وضع قواعد إجرائية خاصة تهدف إلى الوقاية هذه من الجرائم،نظرا لتعقيدها التقني.من خلال الأمر رقم11.21 المعدل و المتمم لقانون الإجراءات الجزائية مجموعة من الإجراءات المستحدثة التي تستهدف تعزيز فعالية التحريات و التحقيقات، منها إنشاء القطب الجزائي المتخصص لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال **(المطلب الأول)** ولردع هذه الأخيرة يستوجب وضع مجموعة من العقوبات**(المطلب الثاني)**.

1أجعود سعاد، مرجع سابق،ص229.

المطلب الأول

إنشاء القطب الجزائي المتخصص

جاء الأمر 11/21 ليحدث تعديلا مهما على قانون الإجراءات الجزائية،حيث أضاف من خلال الباب السادس من الكتاب الأول جهازا قضائيا جديدا يعرف باسم "القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال".

و قد تم تحديد الاختصاص الإقليمي و النوعي لهذا القطب ضمن المواد من 211 مكرر22 إلى 211 مكرر29، ليكون هذا الجهاز مختصا بالتحقيق و المتابعة القضائية في الجرائم الإلكترونية وكل ما يتعلق بها، بهدف تعزيز فعالية العدالة في هذا المجال المستحدث و المعقد و ذلك من خلال تحديد، الإختصاص النوعي(**الفرع الأول**) و الإختصاص الإقليمي للقطب (**الفرع الثاني**).

الفرع الأول

الاختصاص النوعي للقطب الجزائي المتخصص

بدأت فكرة الأقطاب القضائية المتخصصة من خلال توسيع الاختصاص الإقليمي في المجال الجزائي،وظهر ذلك بشكل رسمي عند صدور القانون 14/04 ، الذي عدل و أتم الأمر 155/66 المتعلق بقانون الإجراءات الجزائية[1].

قد نصت المادة40 مكرر من القانون 04-14[2] أن"**تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية و التحقيق و المحاكمة أمام الجهات القضائية التي تم توسيع إختصاصها المحلي طبقا للمواد 37و40 و329من هذا القانون،مع مراعاة أحكام المواد من 40 مكرر1 إلى40 مكرر5أدناه**".على إمكانية توسيع اختصاص كل من وكيل الجمهورية،قاضي التحقيق،والمحكمة في حالات معينة تتعلق بجرائم محددة،وذلك من أجل

1 القانون رقم 04-14 المؤرخ في 2004/11/10، يعدل و يتمم الأمر رقم 66-155 المؤرخ في 8جوان 1966 ، المتضمن قانون الإجراءات الجزائية، ج ر ،العدد 71، صادر بتاريخ 10 نوفمبر2004.

2 المادة40 مكرر من القانون 04-14 ،سالف الذكر.

تسهيل التحقيق و التحري.وتم دعم هذا التوجه بصدور المرسوم التنفيذي رقم 06-348[1] بتاريخ 5 أكتوبر 2006،و الذي نص على تمديد الاختصاص المحلي لبعض المحاكم، مما سمح بإنشاء أقطاب جزائية متخصصة. وقد بدأت هذه الأقطاب عملها فعليا في عام 2008.

و من بين هذه الأقطاب، تم إنشاء القطب الجزائي الوطني المتخصص في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على مستوى محكمة مقر مجلس قضاء الجزائر.ويتمتع هذا القطب باختصاص وطني،حيث يمارس وكيل الجمهورية وقاضي التحقيق ورئيس القطب صلاحيتهم على كامل التراب الوطني[2]، كما هو منصوص عليه في المادة 211 مكرر23 من الأم11/21[3] أن"**يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال،وكذا قاضي التحقيق ورئيس ذات القطب صلاحياتهم في كامل الإقليم الوطني**".

الفرع الثاني

الاختصاص الإقليمي للقطب الجزائي

يختص القطب الجزائي الوطني المتخصص بالتحقيق و المتابعة في مجموعة من الجرائم، من أبرزها:

-الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال،خاصة تلك المعقدة أوالعابرة للحدود.

-الجرائم التي تمس بأمن الدولة أو الدفاع الوطني.

-جرائم نشر و ترويج أخبار كاذبة تؤثر على الأمن أو السكينة العامة.

---

1 المرسوم التنفيذي رقم06-348 المؤرخ في 2006/10/5 ، يحدد كيفيات تنفيذ بعض أحكام القانون رقم 04-15 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها،ج ر، العدد 62 ، صادر بتاريخ 8 أكتوبر 2006.

2 أجعود سعاد ،مرجع سابق، ص ص 230-231 .

3 المادة 211 مكرر23 من القانون21-11 ،سالف الذكر.

-جرائم المساس بأنظمة المعالجة الآلية للمعطيات في الإدارات و المؤسسات العمومية.

- جرائم الاتجار بالأشخاص أو الأعضاء البشرية و تهريب المهاجرين.

- جرائم التمييز وخطاب الكراهية

كما يختص القطب بالجرائم المنصوص عليها في الباب السادس من قانون الإجراءات الجزائية إذا كانت تشكل جنحا. و يتم تحديد اختصاص القطب بناء على طبيعة الجريمة و تعقيدها، خاصة إذا كانت تتطلب وسائل تحري خاصة أو خبرة فنية متخصصة أو تعاونا قضائيا دوليا.

تظهر هذه الإجراءات التزام المشرع الجزائري بتطوير المنظومة القضائية لمواجهة التحديات التي تفرضها الجرائم الحديثة و المعقدة، خاصة في ظل التطور التكنولوجي المتسارع[1].

المطلب الثاني

العقوبات المقررة لجرائم تكنولوجيا الإعلام و الاتصال

أدى الانتشار الواسع لتكنولوجيا الإعلام والاتصال إلى ظهور أشكال جديدة من الإجرام، استدعت تدخل المشرع بوضع نصوص قانونية خاصة لمواجهتها، وقد تم تخصيص عقوبات تأخذ بعين الاعتبار طبيعة هذه الجرائم الحديثة، و أهميتها في تحقيق الردع و حماية النظام المعلوماتي، فقررتلها مجموعة من العقوبات الأصلية **(الفرع الأول)** و كذا العقوبات التكميلية **(الفرع الثاني)**.

الفرع الأول

العقوبات الأصلية

العقوبات الأصلية هي عقوبات يفرضها القانون على جرائم تكنولوجيا الإعلام

1 أجعود سعاد، مرجع سابق،ص231 .

و الإتصال و التي نجد فيها عقوبات بسيطة(**أولا**) و عقوبات مشددو(**ثانيا**).

أولا:العقوبات البسيطة

في العقوبات البسيطة نجد الغرامات أو الحبس لفترة قصيرة

1-جريمة التلاعب غير المصرح به بالمعلومات:

لقد قام المشرع الجزائري بتبيان عقوبة مرتكب جريمة الدخول غير المصرح به إلى أنظمة المعالجة الآلية للمعطيات إلا أنه فرق بين الشخص الطبيعي و الشخص المعنوي.

أ/- الجزاءات المقررة للشخص الطبيعي:

لقد نصت المادة 394 مكرر/1 على أن العقوبة في هذه الحالة تكون من ثلاثة أشهر إلى سنة و الغرامة من 50.000دج إلى 200.000دج إذا كان الدخول مجرد أو غير مرتب لنتيجة إجرامية . أما إذا كان الدخول مرتب لنتيجة إجرامية فنميز بين نتيجتين إذا ترتب على الدخول حذف أو تغيير للمعطيات هنا تضاعف العقوبة فتصبح الحبس، فنميز بين نتيجتين[1]:

من ستة أشهر إلى سنتين و الغرامة 100.000دج إلى 400.000دج و هذا ما نصت عليه المادة 2/394.

إذا ترتب على هذا الدخول تخريب لنظام اشتغال المنظومة هذا يكون الحد الأدنى لعقوبة الحبس ستة أشهر وحدها الأقصى سنتين أما الغرامة من 50.000دج إلى 300.000دج و هذا ما نصت عليه المادة 2/394.

بالإضافة إلى العقوبات الأصلية هناك عقوبات تكميلية و تتمثل في المصادرة و الغلق و يقصد بالمصادرة الأجهزة و البرامج و الوسائل المستخدمة في تنفيذ الجريمة. و لقد نصت المادة 394 مكرر6 من القانون04-15[2] على ما يلي: " **مع الاحتفاظ بحقوق الغير حسن**

1 دوباي سفيان،يسعد صورية،مرجع سابق،ص20.

2 المادة 394 مكرر6 من القانون رقم04-15 ،سالف الذكر.

نية ، بحكم بمصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

ب/ الجزاءات المقررة للشخص المعنوي :

تنص المادة 394 مكرر 4 من القانون 04-15[1] على أن "**يعاقب الشخص المعنوي الذي يرتكب إجدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس(5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".**

ويلاحظ أن المشرع الجزائري اعتبرو أن الضحية جهة معينة (مثل الدفاع الوطني أو الهيئات، المؤسسات العامة) ظرفا مشددا تضاعف من العقوبة، فقد نصت المادة 394مكرر3[2] و التي جاء فيها :"**يعاقب بالحبس من سنتين (2) إلى عشر (10) سنوات وبغرامة من 700.000دج إلى 2.000.000دج إذا استهدفت الجرائم المنصوص عليها في القسم الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق العقوبات الأشد"..**

2-جريمة تعامل في معلومات غير مشروعة:

نصت المادة 394 مكرر2، الفقرة1، على أن العقوبة تكون الحبس من شهرين إلى ثلاث سنوات، وغرامة مالية تتراوح ما بين 1.000.000دج إلى 10.000.000دينارجزائري[3].

3- جريمة تقليد المصنفات الالكترونية:

أقر المشرع الجزائري نوعين من العقوبات لجنحة التقليد، أصلية وتبعية:

1 المادة 394 مكرر من القانون رقم 04-15 ،سالف الذكر.

2 المادة 394مكرر3 من القانون04-15 ،سالف الذكر.

القانون رقم 66-156 ،سالف الذكر.

-**العقوبات الأصلية:** بالرجوع إلى نص المادة 153 من الأمر 03-05 فإن العقوبتان المقررتان لجنحة التقليد ، و الأفعال الأخرى التي تشكل في مجموعها جنح مماثلة لجنحة التقليد تتمثل في الحبس و الغرامة .

أ- الحبس: و هي عقوبة سالبة للحرية توقع على مرتكب هذه الجنحة و قد حصرها المشرع الجزائري من ستة (06) أشهر إلى ثلاث (03) سنوات و الملاحظ أن المشرع الجزائري أجبر القاضي الفاصل في المنازعة بالحكم بكلي العقوبتين و ذلك لاستعماله حرف الربط (واو).

ب- الغرامة: لقد حدد المشرع الجزائري في المادة 153 من الأمر رقم 03- 05 العقوبة المالية لهذه الجنحة من خمسمائة ألف دينار جزائري (500.000دج) كحد أدنى و مليون دينار جزائري (1.000.000دج) كحد أقصى .

ثانيا:العقوبات المشددة

1-حسب صفة المجني عليه:

المشرع شدَّد العقوبة إذا كانت المعلومات المعتدى عليها تخص الدفاع الوطني أو المؤسسات العامة، لما لهذا النوع من المعلومات من أهمية وحساسية كبيرة[1].

2-حسب النتيجة المترتبة عن الجريمة:

نص القانون الجزائري، فنصت المادة 394 مكرر، الفقرتان2و3، على مضاعفة العقوبة إذا ترتب عن الفعل حذف أو تغيير في البيانات، وتصل العقوبة إلى الحبس من ستة(06) أشهر إلى سنتين، وغرامة من 50.000 دج إلى 300.000 دينار جزائري[2].

1 قبايلي سمية، الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال في التشريع الجزائري،مذكرة لنيل شهادة الماستر في الحقوق ،كلية الحقوقوالعلوم السياسية،جامعة العربي بن مهيدي، أم البواقي 2017،ص25 .

2 سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير،كلية الحقوق و العلوم السياسية ، جامعة أبو بكر بلقايد ،تلمسان،2011،ص ص96-98 .

الفرع الثاني

العقوبات التكميلية

بالإضافة إلى العقوبات الأصلية، أضاف القانون الجزائري عقوبات تكميلية حسب المادة394 مكرر6 من قانون العقوبات "**مع الاحتفاظ بحقوق الغير حسن النية،يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية،يعاقب بالعقوبات المقررة للجريمة ذاتها**".،وتشمل هذه العقوبات إجراءات إضافية تفرض على الجاني إلى جانب الحبس أو الغرامة و تتمثل:

1-المصادرة:

تعتبر المصادرة عقوبة إضافية تطبق على الأدوات مثل الأجهزة و البرامج التي استخدمت في ارتكاب جريمة تتعلق بالأنظمة المعالجة الإلكترونية للبيانات، مع ضرورة احترام حقوق الأشخاص الذين امتلكوها بحسن النية[1].

2-العقوبات التكميلية لجريمة تقليد المصنفات

بالإضافة إلى العقوبات الأصلية، نص المشرع الجزائري على مجموعة من العقوبات التكميلية لجريمة تقيد المصنفات التي يجب على المحكمة المختصة الحكم بها في حال إدانة المتهم بإحدى الجرائم المذكورة سابقا، وتشمل هذه العقوبات ما يلي :[1]

أ- **المصادرة:** حيث تنص المادة 157 من الأمر رقم 03- 05 على ما يلي :" **تقرر الجهة القضائية المختصة :**

-مصادرة المبالغ التي تساوي مبلغ الإيرادات أو أقساط الإيرادات الناتجة عن الاستغلال غير الشرعي لمصنف أو أداء محمي.

1 قبايلي سمية ، مرجع سابق، ص25.

-مصادرة و إتلاف كل عتاد أنشئ خصيصا لمباشرة النشاط غير المشروع و كل النسخ المقلدة".

ب- نشر حكم الإدانة : تنص المادة 158 من الأمر رقم 03- 05 على أنه : " **يمكن الجهة القضائية المختصة ، بطلب من الطرف المدني، أن تأمر بنشر أحكام الإدانة كاملة أو مجزأة في الصحف التي تعينها ، و تعليق هذه الأحكام في الأماكن التي تحددها ، و من ضمن ذلك على باب مسكن المحكوم عليه و كل مؤسسة أو قاعة حفلات يملكها ، على أن يكون ذلك على نفقة هذا الأخير شريطة ألا تتعدى ستة (06) أشهر للمؤسسة التي يستغلها المقلد أو شريكه أو أن تقرر الغلق النهائي عند الاقتضاء"**[1].

ج- غلق المؤسسة: نصت الفقرة الثانية من المادة 156 من الأم 03 - 05 على أنه:"**....كما يمكن الجهة القضائية المختصة أن تقرر الغلق المؤقت مدة لا تتعدى ستة (06) أشهر للمؤسسة التي يستغلها المقلد أو شريكه أو أن تقرر الغلق النهائي عند الاقتضاء**".

و مما لا شك فيه أن الموقع الالكتروني يعد جزءا من مفهوم المؤسسة، باعتباره الوعاء الذي يضم مختلف المصنفات، لاسيما أن هذه المواقع تتيح لنا الوصول إلى المصنفات المنشورة إلكترونيا عبر الشبكة[2].

1 المادة 158 من الأمر رقم 03-05 ،سالف الذكر.

2 المادة 156 من الأمر رقم03-05،سالف الذكر.

الخاتمة

من خلال دراستنا لموضوع آليات الوقاية من جرائم تكنولوجيا الإعلام والاتصال،نرى أن مواجهة هذه الجرائم ليست خيارا،بل ضرورية للحفاظ على الأمن الرقمي للمجتمعات،إن التعامل مع هذه الجرائم يتطلب نهجا متعدد الركائز يجمع بين الصرامة القانونية والذكاء التقني والوعي المجتمعي.

وقد وضع المشرع الجزائري آليات للوقاية والتحدي على هذه الجرائم التي غزت كل العالم وليس فقط المجتمعات،وهذه الأخيرة نعتبرها حجز الزاوية في التصدي الفعال لهذه الجرائم، في ظل صعوبة الكشف عنها ومعالجتها بعد وقوعها.

هنا قد توصلنا أثناء هذه الدراسة إلى مجموعة من النتائج الهامة التي نذكر منها :

-بادر المشرع الجزائري بإصدار قانون 09-04 كخطوة أولى في مواكبة تطور الجرائم الإلكترونية.

-الجرائم المعلوماتية تتميز بطبيعتها الخاصة والمعقدة التي لا تستوعبها القوانين التقليدية.

-الوقاية الفعالة من هذه الجرائم لا تقتصر فقط على الجانب القانوني ،بل تتطلب تكوينا مستمرا واستثمارا في الوسائل التقنية ونشر الوعي المجتمعي.

-التحقيق في الجرائم في الجرائم المعلوماتية يتطلب خبرات تقنية عالية وهو ما يشكل تحديا أمام الجهات القضائية والأمنية.

-الردع القانوني يبقى ضروريا لمواجهة الجرائم التي وقعت بالفعل.

-الإعتماد على الأدلة الرقمية في الإجراءات القضائية ما يزال يواجه تحديات تقنية وقانونية،تتعلق بسلامة البيانات وسهولة التلاعب بها.

-توفير الإمكانيات الحديثة كضمان الوقاية من جرائم تكنولوجيا الإعلام والاتصال.

-المقاربة الجزائرية في مكافحة الجرائم الإلكترونية تبقى غالبا فردية،في حين أن التعاون الدولي في هذا المجال ضروري لمواجهة هذه الجرائم العابرة للحدود.

-تحتاج الجزائر إلى تعزيز انضمامها إلى الاتفاقيات الدولية ذات الصلة مثل اتفاقية بوداست المتعلقة بالجرائم الإلكترونية.

-ضعف التوعية القانونية لدى الأفراد حول حقوقهم الرقمية وسبل الحماية من التهديدات،يزيد من انتشار الظواهر مثل الخداع الإلكتروني.

-البيئة الرقمية في الجزائر تعاني من غياب سياسة أمن معلومات واضحة،وهو ما يزيد هشاشتها أمام الهجمات السيبرانية.

-القيام بالتفتيش والمراقبة للوقاية من جرائم تكنولوجيا الإعلام والاتصال،خاصة عند الأطفال غير البالغين.

-إنشاء هيئة وطنية للوقاية من جرائم تكنولوجيا الإعلام و الاتصال.

-مقدمو خدمات الأنترنت في الجزائر لا يتمتعون بالشفافية الكافية في التعاون مع السلطات،ما قد يعطل الوصول إلى الأدلة أو مرتكبي الجرائم.

-استحداث القطب الجزائي المتخصص في تعزيز فعالية المتابعة القضائية لهذا النوع من الجرائم.

-تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

-إعداد خطط ،وتحضير الوسائل المادية الكافية،لدراسة كل الصعوبات المحتملة والحوادث الطارئة وكيفية مواجهتها عمليا.

-زرع ثقافة التنديد بالجرائم الالكترونية ،والعمل على تهذيب المستخدمين للانترنت والفضاءات الرقمية،مع تبيان الطرق الصحيحة لاستخدامها.

قائمة المراجع والمصادر

أولا: الكتب

1- **بيومي حجازي عبد الفتاح** ، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الجزائر ،2006.

2-**حاسم الطائي جعفر حسن** ، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، دار البداية ناشرون وموزعون،عمان، ،2012.

3-**زيدان زليخة**، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للنشر والتوزيع،الجزائر ،2011.

4-**فارق ياسير الأمير** ، مراقبة الأحاديث الخاصة في الإجراءات الجنائية دراسة تأصيلية تحليلية ومقارنة لتنصت على المحادثات التلفزيونية والتي تجري عبر الإنترنت والأحاديث الشخصية نظريا وعمليا، دار المطبوعات الجامعية، الجزائر ،2009.

5-**مناصرة يوسف**، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، منشورات دار الخلدونية ،الجزائر ،2018.

6- **نائلة عادل محمد فريد فدوة**، جرائم الحاسب الآلي الإقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، ،لبنان،2005.

ثانيا: المذكرات الجامعية

أ-مذكرات الماجستر:

1-أحمد مسعود مريم ،آليات مكافحة جرائم تكنولوجيا الإعلام والإتصال في ضوء القانون رقم09-04،مذكرة نيل شهادة الماجستر، كلية الحقوق والعلوم السياسية،جامعة قاصدي مرباح ورقلة، 2013.

2-سعيد نعيم،آليات البحث والتحري المعلوماتي في القانون الجزائري ،مذكرة نيل شهادة الماجستير ،كلية الحقوق والعلوم السياسية،جامعة الحاج لخضر ،باتنة،2013.

3-سفيان سوير، جرائم المعلوماتية، مذكرة لنيل الماجستير، كلية الحقوق والعلوم السياسية،جامعة أبو بكر بلقايد، تلمسان،2011 .

ب-مذكرات الماستر:

1-إدريس صاره،زواقري أميرة،الإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات،مذكرة نيل شهادة الماستر في الحقوق،كلية الحقوق والعلوم السياسية،جامعة مولود معمري تيزي وزو،2023.

2- بوطمين ماجدة ،جريمة إتلاف المعطيات المعلوماتية،مذكرة لنيل شهادة الماسترفي الحقوق، كلية الحقوق والعلوم السياسية،جامعة العربي بن مهيدي أم البواقي 2018.

3-دوباي سفيان،يسعد صورية،الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، مذكرة نيل شهادة الماستر،كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعرريج، 2023.

4-عبد الرحماني أمينة ،مرابطين حفيظة،جرائم تكنولوجيا الإعلام والإتصال، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية،جامعة مولود معمري، تيزي وزو،2021 .

4-قبايلي سمية،الجرائم المتصلة بتكنولوجيا الإعلام والإتصال في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق و العلوم السياسية،جامعة العربي بن مهيدي،أم البواقي،2017..

ثالثا:المقالات

1-أجعود سعاد ،"الحماية الجزائية لتكنولوجيا الإعلام و الاتصال في التشريع الجزائري دراسة على ضوء النصوص المستحدثة"،**مجلة الرسالة للدراسات والبحوث الإنسانية**،جامعة العربي التبسي،الجزائر،المجلد07،العدد04 ،2022،ص ص214-234.

2-أعراب تاني نجية ،"الآليات الوقائية من جرائم تكنولوجيا الإعلام والإتصال ومكافحتها في القانون الجزائري"،**مجلة البحوث في الحقوق والعلوم السياسية** ،كلية الحقوق والعلوم السياسية،جامعة أبو بكر بلقايد تلمسان،الجزائر،المجلد 08،العدد01 ،2022،ص ص451-473.

3-بخوش هشام ،"الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في التشريع الجزائر"،**مجلة الحقوق والعلوم السياسية**،كلية الحقوق والعلوم السياسية، جامعة سوق أهراس،العدد 07 ،2017 ،ص ص194-206.

4-بن يحي اسماعيل ،"التعريف بمراقبة الاتصالات الالكترونية كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية"،**مجلة صوت القانون**،كلية الحقوق

والعلوم السياسية،جامعة الجيلالي بونعامة الخميس مليانة،العدد2022،02،ص ص1066-1086.

5-بوحليط يزيد ،"تفتيش المنظومة المعلوماتية و حجز المعطيات في التشريع الجزائري"،**مجلة التواصل في الاقتصاد و الإدارة والقانون**، كلية العلوم القانونية والسياسية، جامعة باجي مختار،عنابة،عدد48 ،2016،ص ص82-94 .

6-بوزيرة سهيلة ،"الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية"،**المجلة النقدية للقانون والعلوم السياسية**،الكلية الحقوق والعلوم السياسية،جامعة تيزي وزو،المجلد 17،العدد02 ،2022،ص ص560-575.

7-تابت دينازاد ،"مراقبة الاتصالات الالكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري"،**مجلة العلوم الاجتماعية والانسانية**،كلية الحقوق والعلوم السياسية،جامعة العربي التبسي،تبسة، المجلد05،العدد01، 2012 ،ص ص205-231.

8-جبار فطيمة ،"مراقبة الإتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري،**مجلة الدراسات القانونية المقارنة**،كلية الحقوق والعلوم السياسية،جامعة حسيبة بن بوعلي ،شلف ،العدد03، 2016 ،ص ص9-22.

9- حوحو رمزي ،"مواجهة الجريمة المعلوماتية في الجزائر"،**مجلة الحقوق والحريات**،كلية الحقوق والعلوم السياسية،جامعة محمد خيضر، بسكرة، العدد02 ،2014،ص ص37-56.

10-رامي حليم،"جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات"،**مجلة دراسات وأبحاث**،كلية الحقوق والعلوم السياسية،جامعة زيان عاشور الجلفة ،المجلد 01،العدد01، 2009،ص ص339-353.

11-رحموني محمد ،"خصائص الجريمة الإلكترونية و مجالات استخدامها"،**مجلة الحقيقة**، جامعة أحمد دراية،أدرار ،العدد41،2018،ص ص432-451 .

12- روابح فريد "ضمانات حرمة الحياة الخاصة أثناء مراقبة الاتصالات الإلكترونية،**مجلة الأبحاث القانونية والسياسية**،كلية الحقوق والعلوم السياسية،جامعة محمد الصديق بن يحي ،جيجل،المجلد02،العدد02،2020،ص ص1-30.

13-عبد الله قيبوعة مسعود خثير،"الحماية الجزائية للمصنفات الرقمية في التشريع الجزائري"،**مجلة الدراسات القانونية المقارنة**،كلية الحقوق والعلوم السياسية، جامعة حسيبة بن بوعلي،شلف،المجلد،06 ،العدد02،2020،ص ص1134-1155.

14-عثماني عز الدين ،"إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصالات المعلوماتية"،**مجلة دائرة البحوث والدراسات القانونية و السياسية** كلية الحقوق والعلوم السياسية،المركز الجامعي تيبازة،العدد،04 ،2018،ص ص48-66 .

15-**عليلي عبد السلام** ،"جريمة القذف عبر مواقع التواصل الإجتماعي دراسة تحليلية مقارنة بين التشريع الجزائري والتشريعات الأجنبية العربية"،**مجلة الدراسات القانونية والاقتصادية**، المركز الجامعي بريكة، الجزائر، المجلد05، العدد 02 ،2022،ص ص571-597.

16-**عون اسمهان** ،"أركان جريمة الإتلاف المعلوماتي وعقوبتها دراسة مقارنة"،**مجلة الدراسات الإفريقية وحوض النيل**،المجلد 04 ،العدد13 ،2021،ص ص361-370.

17-**عيساني طه ، عبد الله فوزية** ،"جريمة تقليد حقوق المؤلف في القانون الجزائري وتطبيقاتها في البيئة الرقمية"،**مجلة الدراسات القانونية المقارنة**،كلية الحقوق والعلوم السياسية،جامعة قاصدي مرباح، ورقلة، المجلد 08،العدد،01 ،2022،ص ص357-375.

18-**فلاح عبد القادر**،"حجز وحفظ المعطيات في الجريمة الالكترونية"،**مجلة صوت القانون**،كلية الحقوق والعلوم السياسية، جامعة الجيلالي بونعامة الخميس مليانة، المجلد 08 ،العدد01 ،2021،ص ص177-194.

19- **مسعود أحمد** ،"جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري"، ، **مجلة الحقوق والعلوم السياسية**،كلية الحقوق والعلوم السياسية،جامعة زيان عاشور الجلفة، المجلد10، العدد2017،01، ص ص482-491.

20- **هميسي رضا** ،"تفتيش المنظومات المعلوماتية في القانون الجزائري"،**مجلة العلوم القانونية والسياسية**، كلية الحقوق والعلوم السياسية،جامعة الوادي، الجزائر ،المجلد3، العدد2012،2 ص ص157-182.

رابعا:النصوص القانونية

أ-النصوص التشريعية:

1-الأمر رقم 03-05 مؤرخ 2003/07/19 ،المتعلق بحقوق المؤلف و الحقوق المجاورة،ج ر،العدد43 ،الصادر بتاريخ 2003/07/20.

2-قانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 66-156 المؤرخ في 1966/06/08،المتضمن قانون العقوبات،ج ر،العدد71،الصادر بتاريخ2004/11/10.

3-قانون رقم 04-14 المؤرخ 2004/11/10،يعدل و يتمم اللأمر 66-155 مؤرخ في 1966/06/08،المتضمن قانون الإجراءات الجزائية،ج ر ،العدد71 ،صادر 2004/11/10 .

4-قانون رقم 06-23 المؤرخ في 20ديسمبر2006 المعدل والمتمم الأمر رقم 66-156 المتعلق و المتضمن قانون العقوبات،ج ر ،العدد84،الصادر 2006/12/24.

5-قانون رقم 06-22،المؤرخ في 20ديسمبر2006 ،المعدل والمتمم للأمر رقم 66-156 المتعلق و المتضمن قانون الإجراءات الجزائية ،ج ر،العدد84،الصادر24 ديسمبر2006 .

6-القانون رقم 09-04 المؤرخ في 05أوت2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها،ج ر،العدد47 ،الصادر في 16 أوت 2009 .

7-القانون رقم 15-04 المؤرخ في 2015/02/01 ،يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكتروني ،ج ر ،العدد06 ،الصادر 2015/02/10.

8-القانون رقم 18-04 المؤرخ في 2018/05/10 ،المتعلق بالبريد والمواصلات الإلكترونية ،ج ر،العدد27 ،الصادر 2018/05/13.

9-القانون رقم 20-06المؤرخ في 2020/04/28 ،المعدل والمتمم للأمر رقم 66-156 ،المتضمن قانون العقوبات،ج ر ،العدد27،الصادر بتاريخ 2020/04/30.

10-الأمر 21-11 المؤرخ 2021/08/25 ،معدل و متمم للأمر66-156،متضمن قانون العقوبات،ج ر،العدد44،الصادر بتاريخ2021/08/26 .

ب-النصوص التنظيمية:

1-مرسوم تنفيذي رقم 66-348 المؤرخ 2006/10/05،يحدد كيفيات تنفيذ بعض أحكام القانون رقم 04-15 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال و مكافحتها،ج ر ،العدد62 ،الصادر في 2006/10/08 .

2-مرسوم رئاسي 15-261المؤرخ في 2015/10/08،يحدد تشكيلية وتنظيم كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها،ج ر ،العدد53،الصادر في 2015/10/08.

3-مرسوم رئاسي رقم 19-172 مؤرخ في 2019/06/06،يحدد تشكيلية الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها وتنظيمها وسيرها،ج ر، العدد37 ،الصادر في 2019/06/09.

4-مرسوم رئاسي 20-183 مؤرخ في 2020/07/13 ،يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال ومكافحتها،ج ر، ،العدد40،الصادر في 2020/07/18.

5-المرسوم الرئاسي 21-439 المؤرخ في 2021/11/07،يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها،ج ر،العدد 86، الصادر في 2021/11/11.

فهرس الموضوعات

مقدمة:	01
الفصل الأول: **الإطار المفاهيمي لجرائم تكنولوجيا الإعلام و الاتصال**	03
المبحث الأول: مفهوم جرائم تكنولوجيا الإعلام و الاتصال	04
المطلب الأول: المقصود بجرائم تكنولوجيا الإعلام و الاتصال	05
الفرع الأول: التعريف بجرائم الإعلام و الاتصال	05
أولا:الإتجاه الأول	05
ثانيا:الإتجاه الثاني	06
ثالثا:الإتجاه الثالث	06
الفرع الثاني: خصائص جرائم تكنولوجيا الإعلام والاتصال	08
أولا:جرائم عابرة للحدود	08
ثانيا:جرائم خفية ومستترة	08
ثالثا:جرائم صعبة الإثبات	09
رابعا:جرائم هادئة	10
المطلب الثاني:الطبيعة القانونية لجرائم تكنولوجيا الإعلام والاتصال	10
الفرع الأول:جرائم المعلومات ذات طبيعة معينة	11
الفرع الثاني: جرائم المعلومات مجموعة جرائم مستحدثة	11

المبحث الثاني: أنواع الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال	12
المطلب الأول: جرائم تكنولوجيا الإعلام والإتصال المنصوص عليها بموجب قانون العقوبات	13
الفرع الأول: جريمة الدخول أو البقاء الغير مصرح له في النظام المعالجة الآلية للمعطيات	13
أولا:الركن الشرعي لجريمة الدخول أو البقاء الغير مصرح في	14
ثانيا:الركن المادي لجريمة الدخول أو البقاء الغير مصرح في النظام المعالجة الآلية للمعطيات	14
ثالثا:الركن المعنوي لجريمة الدخول أو البقاء الغير مصرح في النظام المعالجة الآلية للمعطيات	15
الفرع الثاني: جريمة إتلاف نظام المعالجة الآلية للمعطيات	15
أولا:أساليب اتلاف نظام المعالجة الآلية للمعطيات	16
ثانيا: أركان جريمة اتلاف نظام المعالجة الآلية للمعطيات	17
الفرع الثالث: جريمة إساءة استخدام الأجهزة	19
أولا:الركن الشرعي لجريمة إساءة إستخدام الأجهزة	19
ثانيا:الركن المادي لجريمة إساءة استخدام الأجهزة	20
ثالثا:الركن المعنوي لجريمة إساءة استخدام الأجهزة	20
المطلب الثاني: الجرائم متصلة بتكنولوجيا الإعلام و الاتصال في المنصوص عليها في القوانين الخاصة	21

الفرع الأول: الجرائم الواردة في قانون18-04 المتعلق بالبريد والاتصالات الالكترونية	22
أولا: انتهاك خصوصية و سرية المراسلات المرسلة عبر البريد أو وسائل الاتصال الإلكترونية سواء من خلال افشاء محتواها أو نشره أو استخدامه دون إذن من المرسل أو المتلقي	22
ثانيا: تحويل المراسلات الصادرة عن طريق البريد	22
ثالثا: فتح أو تخريب البريد من قبل أي مستخدم أو طرف يتعامل مع خدمات البريد	23
رابعا: إنشاء أو استخدام شبكة اتصالات إلكترونية متاحة للعامة دون الحصول على ترخيص	23
الفرع الثاني: الجرائم الواقعة على التوقيع و التصديق الالكتروني	24
أولا: جنحة الإخلال بإخبار السلطة الاقتصادية عن التوقف عن النشاط :	24
ثانيا: جنحة إنشاء بيانات شهادة التصديق الالكتروني:	24
ثالثا: جنحة جمع البيانات الشخصية و استخدامها في غير الغرض المخصص لها	25
رابعا: جنحة إصدار شهادة التصديق الالكتروني دون ترخيص أو سحبه	25
خامسا: جنحة الإدلاء بالإقرارات الكاذبة للحصول على شهادات التصديق :	25
سادسا: جنحة حيازة أو إنشاء أو استعمال بيانات توقيع مصونة خاصة بالغير	26
سابعا: جنحة استعمال شهادة التصديق الالكتروني الموصوفة لغير الغرض الذي منحت لأجله	26

الفرع الثالث: جريمة تقليد المصنفات الالكترونية	26
أولا:الجنح التي تمس بالحق المعنوي للمؤلف	27
ثانيا:الجنح التي تمس بالحق المالي للمؤلف	28
ثالثا:الجنح المشابهة لجنحة التقليد	28
الفرع الرابع:جريمة القذف	29
أولا:الركن الشرعي لجريمة القذف	30
ثانيا:الركن المادي لجريمة القذف	31
ثالثا:الركن المعنوي لجريمة القذف	32
الفصل الثاني: **أساليب التصدي لجرائم تكنولوجيا الإعلام والإتصال**	33
المبحث الأول: آليات الوقاية المنصوص عليها بموجب قانون رقم 04.09.	34
المطلب الأول: إنشاء الهيئة الوطنية لوقاية جرائم تكنولوجيا الإعلام و الاتصال	34
الفرع الأول: التعرف بالهيئة الوطنية لوقاية جرائم الإعلام و الاتصال	35
أولا:الشخصية المعنوية للهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والإتصال	35
ثانيا:ذمة مالية مستقلة	36
ثالثا:الأهلية	37
رابعا:الموطن	37
خامسا:حق التقاضي	37

سادسا: تحمل مسؤولية التعويض عن الأضرار التي تسببها الغير	37
الفرع الثاني: تشكيلية الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والاتصال	37
أولا:مجلس التوجيه	39
ثانيا:المديرية العامة	40
ثالثا:كيفية سير عمل الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام والإتصال	41
الفرع الثالث: مهام الهيئة الوطنية للوقاية من جرائم تكنولوجيا الإعلام و الإتصال	42
أولا:الوقاية من الجرائم المرتبطة بتكنولوجيا الإعلام و الاتصال	43
ثانيا:مكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال	43
المطلب الثاني: القواعد الإجرائية المنصوص عليها في قانون رقم 04.09.	45
الفرع الأول: مراقبة الإتصالات الإلكترونية	46
أولا:حالات اللجوء إلى المراقبة الالكترونية بموجب نص المادة 04 من القانون 04-09	47
ثانيا: الحماية المقررة للمراقبة الإلكترونية	48
ثالثا: أشكال مراقبة الاتصالات الالكترونية	51
رابعا: مدة مراقبة الاتصالات الإلكترونية	52
الفرع الثاني: تفتيش المنظومة و حجز المعطيات	53
أولا: التفتيش	53

ثانيا:حجز المعطيات	55
الفرع الثالث: التزامات مقدمي الخدمات	57
أولا:الالتزام بمساعدة الضبط القضائي	57
ثانيا:الالتزام بحفظ المعطيات المتعلقة بحركة السير	57
المبحث الثاني: القواعد الإجرائية المنصوص عليها في قانون العقوبات	58
المطلب الأول: انشاء القطب الجزائي المتخصص	59
الفرع الأول: الإختصاص النوعي للقطب المتخصص	59
الفرع الثاني: الإختصاص الإقليمي للقطب	60
المطلب الثاني: العقوبات المقررة لجرائم تكنولوجيا الإعلام و الاتصال	61
الفرع الأول: العقوبات الأصلية	61
أولا:العقوبات البسيطة	62
ثانيا:العقوبات المشددة	64
الفرع الثاني: العقوبات التكميلية	65
خاتمة:	67
قائمة المراجع والمصادر	69
الفهرس:	78

ملخص:

تعد جرائم تكنولوجيا الإعلام والإتصال من أبرز التحديات التي تواجه المجتمعات الحديثة،نظرا لارتباطها المباشر بالتطور السريع في الوسائل الرقمية،و تشملهذه الجرائم العديد من الأفعال غير القانونية مثل جريمة الدخول والبقاء الغير مصرح في النظام المعالجة الآلية للمعطيات،جريمة اتلاف نظام المعالجة الآلية للمعطيات،جريمة القذف،وقد أصبحت هذه الجرائم أكثر تعقيدا بسبب طبيعتها غير الملموسة وسهولة ارتكابها عبر الحدود،تسلط المذكرة على أهمية الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال من خلال وضع آليات متعددة،أبرزها وضع قوانين صارمة تجرم هذا النوع من الأفعال،القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصالو مكافحتها،والقانون رقم 21-11 المتضمن قانون الإجراءات الجزائية،وهذه القوانين تعزز التعاون بين الدول وتطوير وسائل الحماية التقنية،كما تؤكد على ضرورة التوعية المجتمعية والتوعية الإعلامية لتعزيز الإستخدام الآمن والمسؤول للتكنولوجيا الإعلام والإتصال.

الكلمات الإفتتاحية:

تكنولوجيا الإعلام والإتصال،جرائم تكنولوجيا الإعلام و الإتصال،الجرائم الإلكترونية وأليات الوقاية من جرائم تكنولوجيا الإعلام و الاتصال.