وزارة التعليم العالي والبحث العلمي

جامعة محمد البشير الإبراهيمي برج بوعريريج

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مكملة لمقتضيات نيل شهادة مهني أكاديمي

في الحقوق

تخصص: قانون الإعلام الآلي والأنترنت

الموضوع:

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إعداد الطالبين:

– دوبابي سفيان

– يسعد صورية

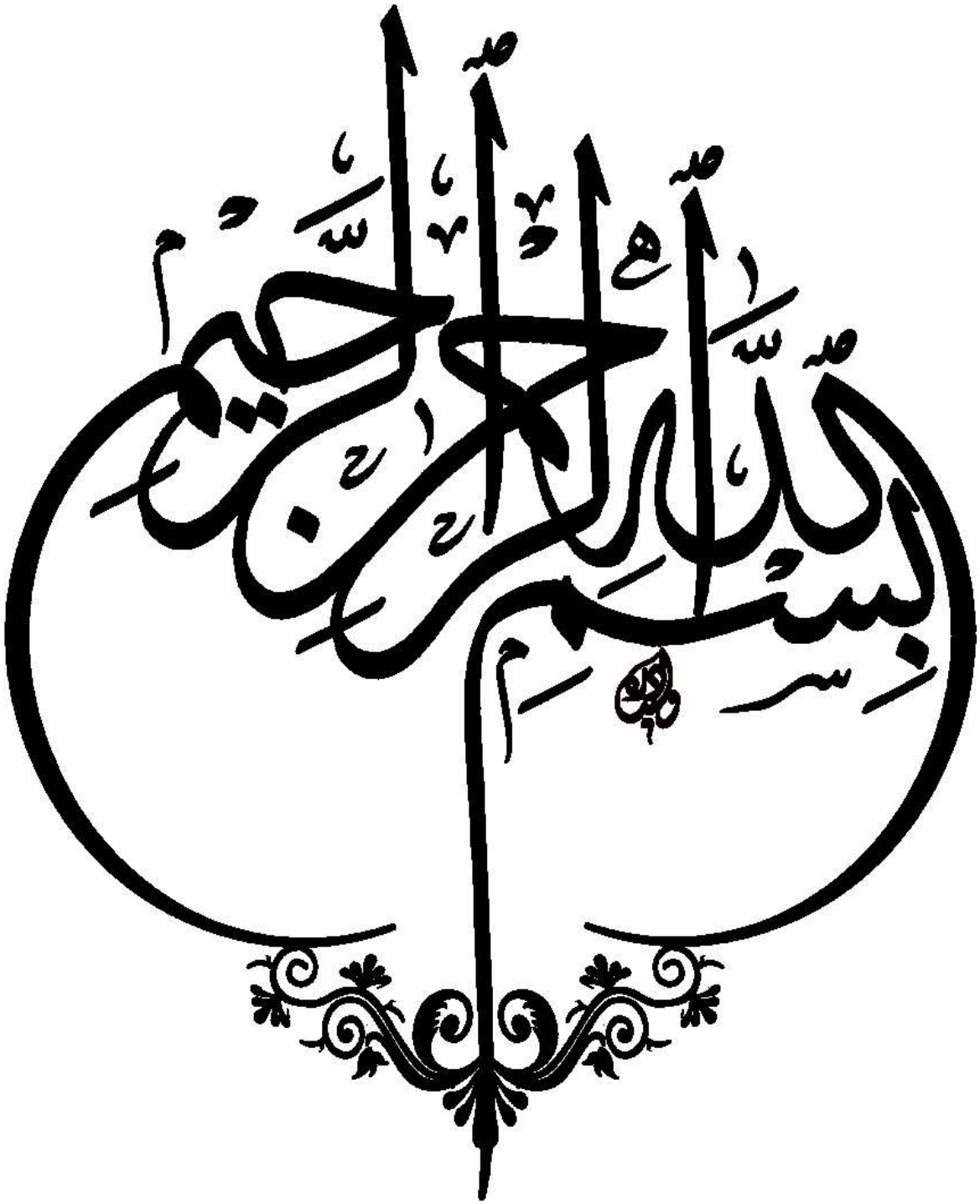
تحت إشراف:

الدكتور خوضري محمد

لجنة المناقشة

(اللقب والاسم)	(الرتبة)	(الصفة)
دكدوك هودة	أستاذ محاضر – أ–	رئيسا
خوضري محمد	أستاذ محاضر — أ–	مشرفا
نزيهة مكاري	أستاذ محاضر — أ–	ممتحنا

السنة الجامعية : 2022/ 2023


بسم الله الرحمن الرحيم

شكر وتقدير

بعد أن من الله علينا بانجاز هذا العمل ، فإننا نتوجه إليه الله سبحانه وتعالى أولا وأخرا بجميع ألوان الحمد والشكر على فضله وكرمه الذي غمرنا به فوفقنا إلى ما نحن فيه راجين منه دوام نعمه وكرمه ، وانطلاقا من قوله صلى الله عليه وسلم :"من لا يشكر الناس لا يشكر الله "،فإننا نتقدم بالشكر والتقدير والعرفان إلى الأستاذة المشرفة " ....."

،على إشرافها على هذه المذكرة وعلى الجهد الكبير الذي بذلته معنا ، وعلى نصائحها القيمة التي مهدت لنا الطريق لإتمام هذه الدراسة، فلها منا فائق التقدير والاحترام ، كما نتوجه في هذا المقام بالشكر الخاص لأساتذتنا الذين رافقونا طيلة المشوار الدراسي ولم يبخلوا في تقديم يد العون لنا وخاصة الأستاذ .

وندين بالشكر أيضا إلى كل عمال مؤسسة، الذين ساعدونا من خلال تقديم جميع التسهيلات ومختلف التوضيحات والمعلومات المقدمة من طرفهم لانجاز هذا البحث .

وفي الختام نشكر كل من ساعدنا وساهم في هذا العمل سواء من قريب أو بعيد حتى ولو بكلمة طيبة أو ابتسامة عطرة

إهداء

الحمد لله الذي أعاننا بالعلم وزيننا بالحلم وأكرمنا بالتقوى وأجملنا بالعافية

أتقدم بإهداء عملي المتواضع إلى

الذرع الواقي والكنز الباقي، إلى من جعل العلم منبع اشتياقي، لك أقدم وسام

الاستحقاق إلى ..... أطال الله عمرك .

رمز العطاء وصدق الإيباء ، إلى ذروة العطف والوفاء ، لك أجمل حواء ،أنت أمي الغالية أطال الله عمرك .

وإلى رمز الصداقة وحسن العلاقة زملاء الدراسة دفعة ..... .

إلى من هم انطلاقة الماضي وعون الحاضر سند المستقبل اللواتي لا عيش بدونهن ولا متعة إلا برفقتهن إخوتي الأعزاء

إلى الزملاء

وفي الأخير يا رب ..

يا رب لا تدعني أصاب بالغرور إذا نجحت ولا أصاب باليأس إذا فشلت بل ذكرني دائما بأن الفشل هو التجربة الذي تسبق النجاح أمين يا رب العالمين

.....

إهـــــــــــداء

أهدي هذا العمل إلى من قال فيهما

"واخفض لهما جناح الذل من الرحمة وقل رب ارحمهما كما ربياني صغيرا "سورة الإسراء الآية 24.

إلى الوالدين الكريمين حفظهما الله وأطال في عمرهما ،

إلى الإخوة والأخوات ، إلى كل الأهل والأقارب ،

إلى جميع الأصدقاء،

إلى كل من عرفته من قريب أو بعيد،

إلى من رفعوا رايات العلم والتعليم

أساتذتي الأفاضل،

إلى كل من سقط سهوا من قلمي ولم يسقط من قلبي.

مقدمة

شهد العالم في العقود الأخيرة ثورة في تكنولوجيا المعلومات ، والتي أصبحت طريقًا مثاليًا للتقدم الثقافي والاقتصادي، ويعد الوصول إلى المعلومات رهانا كبيرا للإنسان نظرا لارتباطها بمختلف مجالات النشاط الإنساني وجوانب الحياة المعاصرة، ذلك أن توفير المعلومات وحسن استغلالها من المقومات الضرورية لدفع عجلة تقدم الأمم وازدهارها وصار وجودها دعامة أساسية لجهود التنمية والرقي المعرفي.

على الرغم من الفوائد الهائلة التي تم تحقيقها والتي يتم تحقيقها في مجال تكنولوجيا المعلومات على جميع المستويات وفي مختلف مجالات الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية رافقتها في المقابل جملة من الانعكاسات السلبية الخطيرة جراء سوء استخدام هذه التقنية المتطورة والانحراف عن الأغراض المتوخاة منها، تجلت في تفشي طائفة من الظواهر الإجرامية المستحدثة، ألا ظاهرة الجرائم المعلوماتية، التي لم تعد تقتصر على وهي إقليم دولة واحدة، بل تجاوزت حدود الدول، وهي جرائم مبتكرة ومستحدثة تمثل إحدى صور الذكاء الإجرامي مما صعب من مهمة إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية، كما كشفت عن عدم قدرة قواعد الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أو على صعيد الملاحقة الجنائية الدولية.

وبما أن الجريمة الإلكترونية ظاهرة جديدة بسبب ارتباطها بتقنيات المعلومات والاتصالات، فقد كافح المهتمون بدراسة هذا النوع الجديد من الإجرام لإيجاد تعريف مناسب يناسب طبيعتها ، ولكن دون جدوى، لذا اختلفت التعاريف التي تتناول هذه الظاهرة الإجرامية غير أنه ومع ذلك فإن كافة المحاولات لإيجاد تعريف جامع جاءت قاصرة على الإحاطة بكافة أوجه هذه الظاهرة، وفي المسعى ذاته تبنى مؤتمر الأمم المتحدة العاشرة لمنع الجريمة ومعاقبة المجرمين تعريفا جامعا للجريمة المعلوماتية بأنها كجريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية.

تتطلب معالجة هذه القضية تطوير إطار قانون جنائي وطني برؤى تشريعية متشابهة ، تعكس الصحة القانونية وجميع جوانب وأبعاد هذه التقنيات الجديدة، بما يضمن في الأحوال كافة احترام مبدأ قانونية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وتتكامل فيه مع الأهداف التي تقرها المعاهدات الدولية في هذا الشأن.

والواقع أن المشرع الجزائري على غرار باقي التشريعات العربية والغربية وضع عديد القواعد الخاصة بالوقاية من الجرائم المتصلة بالجرائم المعلوماتية ومكافحتها وتجلى ذلك من خلال ما احتواه التشريع العقابي وكذا القواعد الإجرائية التي تتبع في مجال الكشف عنها هذا فضلا عن إصدار المشرع الجزائري للقانون 09-04 المؤرخ في 05/ 09/ 2009 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذا استحداثه بموجب المرسوم الرئاسي 15- 261 المؤرخ في 08/ 10/ 2015 للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. والمرسوم 20- 183 الذي أعاد تنظيم هاته الهيئة.

ومما دفعنا لاختيار الموضوع قيد الدراسة هو تنامي ظاهرة الإجرام المعلوماتي والاعتداءات الواقعة على الأشخاص والمؤسسات في الجزائر بالآونة شكّل دافعا وحافزا قويا للبحث ودراسة الموضوع، كما شكّل لدينا مستوى من الوعي بالأهمية الأكاديمية للموضوع، ناهيك عن الرغبة في معرفة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتخوفات التي تختلجنا، وكذا الوسائل والآليات المعدة لمكافحة هذا النوع من الجرائم الخاصة.

أما من الناحية الموضوعية فهذه الدراسة محاولة جادة منا لفهم كيفية مجابهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي أوجدها المشرع الجزائي الجزائري.

وعليه تهدف هاته الدراسة إلى جملة من الأهداف العلمية والعملية، حيث تبرز الأهداف العلمية من هذه الدراسة التي تندرج ضمن الدراسات القانونية، والتي تهتم بدراسة

الإجرام المعلوماتي، ومدى مساهمة هذه الدراسة في معرفة سبل الوقاية من هذه الجرائم الحديثة، أما عن الأهداف العملية فدراسة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من الموضوعات التي تم تناولها بشكل مجحف ومقتضب، إلا أن الملاحظ هو أن هناك اهتمام متنامي من قبل الباحثين القانونيين بهذا الموضوع بعد انتشار هذه الظاهرة على مختلف أنحاء العالم عامة وعلى المستوى الوطني بشكل خاص . وعليه فإن الدراسة تسعى إلى:

- إعطاء مفهوم للجرائم المتصلة بتكنولوجيات الإعلام والاتصال وأهم الخصائص التي تتمتع بها؛
- معرفة أصناف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في التشريع الجزائري؛
- معرفة الإجراءات المتبعة بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

انطلاقا من مما سبق ارتأينا طرح الإشكالية التالة:

- **كيف عالج المشرع الجزائري الجرائم المتصلة بتكنولوجيات الإعلام والاتصال؟**

للإجابة على الإشكالية تم الاعتماد على المنهج الوصفي وكذا المنهج التحليلي وهذا من خلال استقراء النصوص القانونية المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ولمعالجة هاته الإشكالية المذكورة أعلاه ارتأينا تبني خطة ثنائية مقسمة إلى فصلين، حيث تناولنا في **الفصل الأول:** وتم عنونته بـ"الإطار المفاهيمي والتشريعي للجرائم المتصلة بتكنولوجيات الإعلام والاتصال"؛ وهو بدوره تم تقسيمه إلى مبحثين حيث تم تخصيص المبحث الأول الإطار الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أما المبحث الثاني فهو مخصص لأصناف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أما **الفصل الثاني:**

والموسوم بعنوان "آليات مجابهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وهو مقسم إلى مبحثين، المبحث الأول: وتم التطرق فيه إلى الهيئة الوطنية للوقاية من هذه الجرائم، أما المبحث الثاني فتم التطرق إلى القواعد الإجرائية المتبعة بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

الفصل الأول

الإطار المفاهيمي والتشريعي للجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تمهيد:

أدى التقدم التكنولوجي في تكنولوجيا المعلومات وشبكات الاتصالات إلى تغييرات جذرية انعكست في أنواع مختلفة من النشاط الاقتصادي حيث أن معظم الخدمات في مختلف القطاعات كانت إلكترونية، وهنا أصبح من السهولة غزو خصوصية الإنسان والمؤسسات سواء داخل الوطن أو خارجه من خلال وسائل الاتصال الحديثة والمتطورة.

إن التطور التكنولوجي في وسائل الاتصال والإعلام أفرز تهديدات جديدة وجرائم متطورة ترتبط بتكنولوجيا الإعلام والاتصال.

المبحث الأول: الإطار المفاهيمي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

يشار إلى العقود القليلة الماضية باسم عصر ثورة المعلومات، وهو الوقت الذي انتشرت فيه الإنترنت وأجهزة الكمبيوتر وفتحت الإمكانيات للعقل البشري. وبما أن العصور السابقة سميت على اسم أهم الابتكارات ، فهناك العصر البرونزي ، وعصر البخار ، وعصر الثورة الصناعية، فالعصر الذي نعيشه يستحق بامتياز أن يطلق عليه عصر المعلومات والثورة المعلوماتية. والملاحظ في هذا العصر تطور الجريمة بتطور تكنولوجيا الإعلام وظهر نوع جديد من الجرائم يطلق عليها الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

ومن خلال هذا المبحث سنتطرق إلى مفهوم الجرائم المتصلة بتكنولوجيا لإعلام والاتصال (المطلب الأول) وخصائصها (المطلب الثاني).

المطلب الأول: مفهوم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

قبل الخوض في إعطاء مفهوم للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وجب التطرق أو إلى نظام المعلومات باعتباره العنصر المشترك بين جميع الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

الفرع الأول: مفهوم وتطور نظام المعلوماتية في الجزائر

أولا: تعريف نظام المعلوماتية

هناك من يعرف نظام المعلوماتية بأنه "النظام الذي يستخدم تكنولوجيا المعلومات في بعدها المادي Hardware والذهني Software[1].

[1] سعد غالب ياسين، مبادئ نظم المعلومات، دار اليازوري العلمية للنشر والتوزيع، عمان، 2018، ص26.

في حين عرفه آخرون بأنه: "مجموعة برامج وأجهزة تستخدم لإنشاء أو استخراج المعلومات أو إرسالها أو استلامها أو عرضها أو معالجتها أو تخزينها"[1].

وبالرجوع غلى التشريع الجزائري فلقد عرف للنظام المعلوماتي في المدة 2 من القانون رقم 09-04 بأنه أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين[2].

تعتبر عملية الحماية من الأخطار التي تهدد أنظمة المعلومات من المهام المعقدة والصعبة والتي تتطلب من إدارة نظم المعلومات الكثير من الوقت والجهد والموارد المالية وذلك للأسباب التالية[3]:

1. التقدم التقني السريع يجعل الكثير من وسائل الحماية متقادمة من بعد فترة وجيزة من استخدامها.
2. التأخر في اكتشاف الجرائم الرقمية مما لا يتيح للمنظمة إمكانية التعلم من التجربة والخبرة لمتاحة.
3. العدد الكبير من الأخطار التي تهدد عمل نظم المعلومات.
4. توزع الوسائط الإلكترونية على العديد من المواقع التي يمكن أن تكون أيضا متباعدة.
5. وجود التجهيزات الرقمية في عهدة أفراد عديدين في المنظمة وأحيانا خارجها.
6. صعوبة الحماية من الأخطار الناتجة عن ارتباط المنظمة بالشبكات الخارجية.

[1] إبراهيم محمد بن حمود الزنداني، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وأثرها على حجية أدلة الإثبات وأحكامها في القانون اليمني والكويتي والقطري: دراسة شرعية وقانونية مقارنة، جامعة قطاني، 2019، ض247.

[2] القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق5غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[3] عبد الصبور عبد القوي علي مصري، منال عبد الله عبد الرحمن، المحكمة الرقمية والجريمة المعلوماتية دراسة مقارنة، مكتبة القانون والاقتصاد، الرياض، ط1، 2012، ص46.

7. تكاليف الحماية يمكن أن تكون عالية بحيث لا تستطيع العديد من المنظمات تحملها.

ثانيا: كرونولوجيا نظام المعلوماتية في الجزائر

لقد عرفت الجزائر ثلاث مراحل كبرى في سياستها الموجهة إلى تكنولوجيات الإعلام والاتصال فيما فيها مجال المعلوماتية وهي كالتالي:

أولا: مرحلة السبعينات (1970): لقد اعترفت الجزائر في سنة 1968 بأهمية مجال المعلوماتية، وقامت بإنشاء المعهد الوطني للإعلام الآلي (INI) ومركز التكوين والبحث في الإعلام الآلي (CERIST)، بهذا بدأت الجزائر تأخذ مكانها في مجال تكنولوجيا المعلومات. لذلك ، مكنت هذه السياسة من إنشاء نظام المعلومات الإدارية في المصانع والخدمات ، وكذلك إنشاء شبكات إدارة المعلومات الأولى: الحساب الجاري، سونطراك، الخطوط الجوية الجزائرية، وتكوين مئات المهندسين والتقنيين في الإعلام الآلي[1].

ثانيا: مرحلة الثمانينات والتسعينات: في هذه الفترة قامت الجزائر بعصرنة قطاع الاتصالات وفق التكنولوجيا الحديثة حيث تم إيصال 3788 مشترك بالهاتف الثابت بكثافة تقدر ب4.5%. وفي سنة 1994 عرفت الجزائر أول ارتباط لها بالإنترنت وذلك عبر مركز البحث والإعلام العلمي والتقني. وكانت الجزائر آنذاك مرتبطة بالإنترنت عبر إيطاليا، وكان هذا الارتباط نتيجة مشروع تعاون مع منظمة اليونسكو بغية تأسيس شبكة معلومات في إفريقيا تدعى (RINAF) وتكون فيها الجزائر النقطة المركزية (المحورية) للشبكة في شمال إفريقيا. أما في سنة 1996 فقد وصلت سرعة الخط إلى 64 ألف حرف في الثانية يمر من خلال باريس بينما في 1998 تم ربطها بواشنطن ع طريق القمر الصناعي بقدرة 1 ميغابايت/ ثانية. أما في سنة 199 أصبحت قدرة الإنترنت في الجزائر بقوة 2 ميغابايت/ثانية

[1] أحمد عمراني، "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في التشريع الجزائري والمقارن"، مجلة الحضارة الإسلامية، العدد16، ماي2012، ص598.

إلى جانب تأسيس 30 خطا هاتفيا جديد من خلال نقاط الوصول التابعة للمركز والمتوفرة عبر ربوع الوطن. أما الهاتف النقال فقد عرف أول دخول له في الجزائر سنة 1994، وفي سنة 1999 وضعت الجزائر إصلاحات وقامت بتشريع قانون جديد سنة 2000 والذي وضع حد لاحتكار الدولة لنشاطات الاتصالات[1].

ثالثا: بعد الألفين إلى يومنا هذا: نفذت الحكومة الجزائرية إصلاحات بعيدة المدى في مجال تكنولوجيا المعلومات والاتصالات ، والتي تعكس التوجهات الاستراتيجية الواردة في برنامج رئيس الجمهورية. ونصت هذه الإصلاحات على ما يلي[2]:

- ✓ تحديث البنية التحتية للاتصالات وتجهيز البلاد كلها، وحتى المناطق الريفية.
- ✓ توسيع نطاق الخدمات وتحسين جودتها.
- ✓ تعزيز تكنولوجيا المعلومات والاتصالات كعنصر هيكلة من أجل التنمية الرقمية وعاملا رئيسيا من عوامل القدرة التنافسية للاقتصاد الوطني.

الفرع الثاني: تعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

ليس هناك تعريف واحد وشامل للجرائم المتصلة بتكنولوجيا الإعلام والاتصال، فلقد اختلف الفقهاء والباحثين في تعريفهم لهذا النوع من الجرائم وعليه سنسعى في هذا الفرع تقديم بعض التعريفات للجرائم المتصلة بتكنولوجيا الإعلام والاتصال عند بعض الفقهاء (أولا) والتعريف القانوني الجزائري لها (ثانيا).

[1] نوال مغزيلي، "تكنولوجيا الإعلام والاتصال في الجزائر: دراسة للمؤشرات وتشخيص للمعيقات"، المجلة الجزائرية للأمن ولتنمية، العدد12، 2018، ص197.

[2] الصديق بن بوزة، إيمان بن زيان، "واقع تكنولوجيا المعلومات والاتصال في الجزائر خلال الفترة 2000-2016"، مجلة العلوم الاجتماعية والإنسانية، باتنة01، العدد34، جوان 2016، ص88.

أولا: التعريف الفقهي للجرائم المتصلة بتكنولوجيات الإعلام والاتصال

لقد عرف خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OESD بأن الجريمة المعلوماتية هي: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو لمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[1].

وهناك من يعرفها بأنها:" تلك الأفعال التي تمثل الاعتداء على مصلحة محمية بموجب الشرع أو النظام أو القانون، عن طريق التعدي على النظام المعلوماتي، أو استخدامه في ارتكاب الجرائم، أو إيصالها إلى المتلقي، بهدف تحقيق مصلحة معينة أو الإضرار بالغير، ويقوم بهذه الأفعال أشخاص لهم دراية باستخدام النظام المعلوماتي"[2].

ولقد عرفها MERW بأنها:" الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"[3].

أما ROSB فيعرفها بأنها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلوماتية المخزنة داخل الحاسب الآلي والتي تحول طريقه"[4].

ويعرفها مندورة بأنها: "ذلك النوع من الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها"[1].

---

[1] أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، ط1، 2014، ص100.

[2] خالد بن مرزوق بن سراج العتيبي، الجوانب الإجرائية في الشروع في جرائم المعلوماتية دراسة مقارنة، مكتبة القانون والاقتصاد، الرياض، 2014، ص32.

[3] محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، كتاب الجمهورية، (د.ب)، 2010، ص36.

[4] محمد علي سكيكر، مرجع سابق، ص36.

ويعرف الفقيهان (mechel &credo) إلى أنها تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحساب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته[2].

ومن خلال التعريفات السابقة يمكن تعريف الجريمة المعلوماتية بأنها كل فعل أو امتناع عن فعل غير مشروع مخالف لأحكام القانون، يرتكبه شخص أو أكثر وهذا باستخدام جهاز الحاسب الآلي.

ثانيا: موقف المشرف الجزائري من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

لقد قام المشرع لجزائري بتعريف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة2 الفقر أ من القانون رقم 09-04 بأنها: " جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[3].

[1] مبروك بن مرزوق الروقي، القصد الجنائي في الجرائم المعلوماتية دراسة تأصيلية مقارنة، مكتبة القانون والاقتصاد، الرياض، 2013، ص26.

[2] عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة، المركز القومي للإصدارات القانونية، ط1، 2012، ص41.

[3] القانون رقم 09-04، مرجع سابق.

المطلب الثاني: الإطار التشريعي للجرائم المتصلة بتكنولوجيا الإعلام والاتصال

للحديث عن الطبيعة القانونية للجريمة المعلوماتية وحول الوضع القانوني للبرامج والمعلومات، إضافة إلى خصائصها، سنتناول في هذا المطل من خلال فرعين.

الفرع الأول: الطبيعة القانونية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال

انقسم الفقه في اتجاهين لتحديد الوضع القانوني للمعلومات. يفترض الاتجاه الأول أن المعلومات ذات طبيعة معينة ، بناءً على الحقيقة المقبولة وهي أن وصف القيمة يقدم أشياء ملموسة فقط ، أو أن الأشياء الموصوفة بالقيم هي الأشياء التي تمتلكها، وبمفهوم المخالفة وباعتبار أن المعلومة لها طبيعة معنوية فلا يمكن اعتبارها من قبيل القيم القابلة للاستحواذ عليها إلا في ضوء الحقوق والملكية الفكرية. وأيا كان الأمر فإن الأمر مستقر بصدد وجود خطأ عند الاستيلاء على معلومات الغير ولذلك فقد حاول هذا الاتجاه أن يحمي هذه المعلومات بدعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استثنائي[1].

أما الاتجاه الثاني يرى أن المعلومات ما هي إلا مجموعة مستحدثة من القيم قابلة للاستحواذ مستقلة عن دعامتها المادية، على سند من القول أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة، وأنها ترتبط كما يقول الأستاذان " vivant &catala" بمؤلفهما عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه، بمعنى أن المعلومات مال قابل للتملك أو الاستغلال

[1] رمزي حوحو، منيرة بلورغي، "مواجهة الجريمة المعلوماتية في الجزائر"، مجلة الحقوق والحريات، العدد02، 2014، ص45.

على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال[1].

الفرع الثاني: خصوصية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

إن جرائم المتصلة بتكنولوجيات الإعلام والاتصال تتميز بالعديد من السمات تتمثل في:

1. **من حيث الدافع إلى ارتكابها:** فإنها تستهدف رفع عناصر الذمة المالية؛ بسبب طمع المجرم ورغبته في الاستيلاء على المال، أو بسبب قهر نظام الحاسب وتخطي الحواجز المضروبة حوله أو بدافع الانتقام من الغير كرب العمل أو أحد الزملاء.
2. **من حيث تشكيل نظام المعالجة الآلية للبيانات:** إن جرائم المعلوماتية يمكن أن ترتكب أثناء أي مرحلة من مراحل التشغيل الأساسية وهي مراحل الإدخال أو الإخراج.

–ففي مرحلة المدخلات يمكن ترجمة المعلومات إلى لغة مفهومة من قبل الحساب، وبهذا يسهل إدخال معلومات غير صحيحة وعدم إدخال وثائق أساسية، وبذلك يمكن في مرحلة المدخلات ارتكاب الجانب الأكبر من الجرائم المعلوماتية.

–وفي مرحلة المعالجة يمكن إدخال أي تعديلات لتحقيق هدف إجرامي عن طريق التلاعب في برامج الحاسب، كتشغيل برامج جديدة أو دس تعليمات غير مصرح بها أو عمل برامج أصلية.

ويتطلب التشغيل في مرحلة المعالجة توافر معرفة فنية عميقة لدى الفاعل، والجرائم التي ترتكب في هذه المرحلة نادرا ما تكتشف، وقد يكون عامل المصادفة هو سبب اكتشافها.

[1] مخلد إبراهيم الزعبي، "فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية" "دراسة قانونية""، المجلة العربية للنشر العلمي، العدد73، تشرين الثاني 2021، ص281.

-أما في مرحلة الإخراج فإن التلاعب يقع في النتائج التي يخرجها الحاسب عن طريق إدخال بيانات صحيحة، وتعالج فيه بطريقة صحيحة[1].

3. **صعوبة الإثبات:** أهم ميزة لهذا النوع من الجرائم يصعب اكتشافها وإثباتها، حيث يصنفها البعض بأنها إجرام خفي يأتي الجاني جريمته في الخفاء، وبالتالي يصعب ضبطه، وإنما جريمة معقدة يتسم مرتكبها بالذكاء والاحتراف، لذا فالجريمة تكون أكثر تعقيدا الأمر الذي قد يصعب معرفة أو اكتشاف مرتكبها وهذا بسبب مجموعة من العناصر وتتمثل في:

- ✓ إن جزءا كبيرا من الأدلة غير ملموس ويول بسرعة، ويرجع ذلك إلى أن أنواع العناوين الإلكترونية والبيانات تخزن في ذاكرة النظام الحاسوبي لمدة قصيرة ولا تخزن بشكل دائم.
- ✓ أنه إذا تم العثور تلك الأدلة فنه من السهولة إتلافها من قبل الجناة، فضلا ن أن غياب الاعتراف القانوني بطبيعة تلك الأدلة يعد من أهم عوائق الإثبات.
- ✓ لجوء مرتكبي الجرائم المعلوماتية إلى استخدام وسائل وأساليب متجددة تتميز بالطابع التقني والفني المعقد، والتي يصب على أفراد الأجهزة الأمنية التعامل معها مثل جرائم بواسطة مجموعة حواسيب يزرع فيها برنامج يخضع لتحكم خارجي، ويطلق عليها جرائم الاعتداء بواسطة شبكة البوت نت، حيث يمكن لأحد القراصنة التحكم في مجموعة من الحواسيب المخترقة الموجودة على إحدى شبكات البوت نت قد تصل إلى آلاف أو ملايين الأجهزة.
- ✓ صعوبة الوصول للدليل بفحص كميات هائلة من المعلومات.

[1] محمد علي سكيكر، مرجع سابق، ص40.

- ✓ إحجام المحني عليه في بعض الحالات عن الإبلاغ عن وقوع تلك الجرائم خشية من زعزعة ثقة عملائهم (مثل الجرائم التي تستهدف البنوك أو الشركات)، إذ قد تكون الخسائر الكاملة أكبر من الخسائر الناجمة عن الهجوم الإلكتروني الذي تعرض له[1].

4.**جرائم معقدة:** يصعب اكتشاف هذه الجرائم لكونها تقنية بحتة تتميز بالتعقيد يمكن تدمير بياناتها والتخلص من معلوماتها بسرعة البرق. كما تمتاز هذه الجرائم بغياب الدليل المادي، الذي يمكن من إدانة الفاعل، مثل الدم والشعر والبصمة لكونها تتم في فضاء افتراضي يصب إثبات الدليل الافتراضي الذي يسهل محوه والتلاعب به وفيه. هذا بالإضافة إلى قلة خبرة رجال الضبطية القضائية من الناحية الفنية لتتبع هذا النوع من الجرائم.

5. جرائم مستترة: يبدو أن المجني عليه الذي يتعرض إلى هذا النوع من الجرائم قيلا ما يلجأ إلى التبليغ خشية من التشهير. فغالبا ما يتم اكتشاف هذا النوع من الجرائم بالصدفة وبعد مرور وقت طويل نسبيا. ومن ثم فبالرغم من انتشار هذا النوع من الجرائم، فإنه قليلا ما يبلغ عنها.

6.جرائم ناعمة: لا يتطلب القيام بهذه الجرائم بذل جهد علي أو جسدي سوى تحريك اليدين والأصابع مع قدرة ذهنية وإلمام بتقنيات الحاسوب وتكنولوجيا المعلومات عكس الجرائم التقليدية التي تتطلب جهد كبير لإتمامها.[2]

[1] اسمهان بن مالك، "خصائص الجريمة المعلوماتية وأسباب ارتكابها"، مجلة البيبان للدراسات القانونية والسياسية، المجلد04، العدد01، 2019، ص114.

[2] سليم عليوة، "الجريمة المعلوماتية"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد06، العدد01، جوان 2021، ص1216.

المبحث الثاني: أصناف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

من خلال هذا المبحث سيتم التعرف على الجرائم لماسة بأنظمة المعالجة الآلية للمعطيات في ظل قانون العقوبات (المطلب الأول) الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في ظل النصوص القانونية (المطلب الثاني).

المطلب الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في ظل قانون العقوبات الجزائري

تتمثل جرائم المساس بأنظمة المعالجة الآلية يكون فيها نظام المعالجة الآلية محل الاعتداء وهدفه.

الفرع الأول: جريمة الدخول أو البقاء غير المصرح له في النظام المعلوماتي

لقد تم النص على جريمة الدخول إلى النظام الآي في قانون العقوبات الجزائري في المادة 394 مكرر: "يعاقب بالحبس من ثلاثة (03) أشهر إلى سنة (01) وبغرامة من 50.000دج إلى 100.000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.[1]

وجريمة الدخول غلى النظام الآلي تقوم على ركنين ركن مادي وركن معنوي كالتالي:

أولا: الركن المادي

الفعل الإجرامي لهذه الجريمة هو عمل إجرامي يتجلى أولاً في ارتكاب التعدي ، حيث يمكن أن يتخذ السلوك الإجرامي أشكالًا إيجابية أو سلبية ويلزم الجاني بارتكاب فعل إيجابي، ولا يمكن أن تتحقق الجريمة بنشاط سلبي. والملاحظ على هذا النوع من الجرائم أنها ليست

[1] القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 1966/06/08، المتضمن قانون العقوبات، الجريدة الرسمية الجزائرية، العدد71 بتاريخ 2004/11/10.

من الجرائم التي يطلق عليها جرائم ذوي الصفة، مثل الرشوة أو الاختلاس أو الزنا، بل تقع وترتكب عن كل شخص أيا كانت صفته سواء كان يعمل في مجال الأنظمة أم لا، سواء كان يفهم أم لا يفهم طريقة تشغيل النظام، وسواء كان يستطيع أن يستفيد من الدخول أم لا.[1]

لا يعتبر تسجيل الدخول إلى نظام الكمبيوتر سلوكًا غير قانوني في حد ذاته، ولكن 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، وعلى 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 الجرائم الشكلية التي لا يتطلب لقيام ركنها المادي توافر نتيجة معينة، وهي كذلك من الجرائم المستمرة، لأن سلوك الجاني يمتد فيها طالما ظل يستغل النظام بطريقة غير مشروعة.[2]

ثانيا: الركن المعنوي

يُزعم أن جريمة الدخول إلى النظام أو البقاء فيه جريمة خبيثة، مما يعني أن إرادة الجاني يجب أن تكون للدخول إلى النظام أو معرفة أنه محظور بموجب القانون، أي بمفهوم المخالفة يستبعد من نطاق التجريم الدخول العرضي إلى النظام. وقد أكدت محكمة استئناف باريس ذلك حينما نفت مسؤولية الجاني على فعل الدخول الذي تم بطريق الخطأ.

إلا أن الفقه اختلف حول طبيعة القصد الجنائي العام يكف لقيام الركن المعنوي، في حين ذهب آخرون إلى أن الجريمة تقوم على القصد الجنائي العام وكذا الخاص. ويرجع هذا الاختلاف إلى التباين في تفسير مصطلح "عن طريق الغش" الذي استعمله المشرع

[1] أحمد مسعود، "جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري"، مجلة الحقوق والعلوم السياسية، المجلد10، العدد01، 2017، ص484

[2] أحمد مسعود، المرجع نفسه، ص484.

الجزائري، هذه العبارة التي تقابلها كلمة (frauduleuement) في نص المادة 1/323 من قانون العقوبات الفرنسي.[1]

فيما يتعلق بنوع سوء النية الذي يشترطه المشرع لإدراج هذه العبارة ، يمكن القول إن كلمة "احتيال" يمكن تفسيرها على أنها تعني أن المشرع الجزائري أشار إلى الحاجة إلى نية جنائية محددة بالإضافة إلى سوء النية العام. ، بحد ذاته إذا كانت نيته كافية لنية إجرامية عامة، لكان قد استعمل عبارة عمدا مثلما ذهبت إليه تشريعات كثيرة.

عادةً ما يُطرح السؤال عن سبب ارتكاب الجريمة عندما يتعلق الأمر بمجرمي الإنترنت الصغار (أو المجرمين الهواة) الذين يرتكبون الجريمة من أجل المتعة والتسلية، فيمكن أن القصد الجنائي يتحقق بشأنهم لأن ذلك يعني معرفتهم بأنهم يقدمون على الاختراق دون وجه حق وأن الباعث هنا _الذي يتمثل في اللعب_ لا يغير من الأمر شيئا، حيث لا ينفي ذلك علمهم لأنه لا يحق لهم الدخول.[2]

ثالثا: العقوبة المقررة للجريمة

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

[1] نسمة بطيحي، "جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي"، مجلة الفقه القانوني والسياسي، المجلد01، العدد01، ص81.

[2] نسمة بطيحي، مرجع سابق، ص81.

أ/- الجزاءات المقررة للشخص الطبيعي

لقد نصت المادة 394 مكرر/1 على أن العقوبة في هذه الحالة تكون من ثلاثة أشهر إلى سنة والغرامة 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:[1]

1. إذا ترتب على الدخول حذف أو تغيير للمعطيات هنا تضاعف العقوبة فتصبح الحبس من ستة أشهر إلى سنتين والغرامة من 100.000دج إلى 400.000دج وهذا ما نصت عليه المادة 394 /2.
2. إذا ترتب على هذا الدخول تخريب لنظام اشتغال المنظومة هنا يكون الحد الأدنى لعقوبة الحبس ستة أشهر وحدها الأقصى سنتين أما الغرامة من 50.000دج إلى 300.000دج وهذا ما نصت عليه المادة 394 /2.

بالإضافة إلى العقوبات الأصلية هناك عقوبات تكميلية وتتمثل في المصادرة والغلق، ويقصد بالمصادرة الأجهزة والبرامج والوسائل المستخدمة في تنفيذ الجريمة. ولقد نصت المادة 394 مكرر6 على ما يلي: " مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل 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"[2].

[1] حفيظ بن غربة، "جريمة الدخول غير المصرح به إلى منظومة معلوماتية في التشريع الجزائري"، مجلة القانون والعلوم السياسية، المجلد03، العدد02، ص209.

[2] القانون رقم 04-15 ، مرجع سابق.

ب/- الجزاءات المقررة للشخص المعنوي

لقد نصت المادة 394 مكرر4 على عقوبة للشخص المعنوي في حالة قيامه بالجريمة الدخول غير المصرح به إلى أنظمة المعالجة الآلية للمعطيات وحددتها بخمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

ومما ينبغي الإشارة إليه أن المشرع الجزائري جعل من صفة المجني عليه ظرفا مشددا تضاعف فيه عقوبة جريمة الدخول غير المصرح به إلى أنظمة لمعالجة لآلية للمعطيات وذلك ما نصت عليه المادة 394 مكرر3 والتي جاء في محتواها: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، ودون الإخلال بتطبيق عقوبات أشد"[1].

الفرع الثاني: جريمة إتلاف نظام المعالجة الآلية

ويقصد هنا الإتلاف المنطقي أي إتلاف معلومات الحاسوب وبياناته باستخدام الطرق المنطقية والمعلوماتية وتنوع أساليب الاعتداء على المعلومات بحسب الهدف الذي يرمي الجاني إلى تحقيقه[2]

أولا: أساليب إتلاف نظام المعالجة الآلية

1/- الفيروسات

هو برنامج حاسوبي أطلق عليه اسم فيروس لتشابهه الوثيق مع فيروس بيولوجي من حيث انتقاله وتكاثره ووظائفه التدميرية في نظم المعلومات وقدرته على تعديل البرامج الأخرى

[1] حفيظ بن عربة، مرجع سابق.

[2] رامي حليم، "جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات"، دراسات وأبحاث، المجلد01، العدد01، 2009، ص349

المرتبطة به، كما يستطيع الفيروسات التمييز بين البرامج السليمة ولبرامج التي سبق وأن أصبحت بالفيروس. ومن أهم العوامل التي ساعدت على انتشار السريع للفيروسات داخل الأنظمة المعلوماتية هي القرصنة المعلوماتية وتوافق الأجهزة وكذلك الانتشار الواسع لشبكة الإنترنت. وعلى الرغم من إنتاج العديد من البرامج المضادة للفيروسات تبقى هذه الفيروسات لها القدرة على اختراق النظم المعلوماتية وتدعيم البيانات مهما كانت الموانع والحصون.

2/- القنبلة المعلوماتية

وتنقسم إلى قسمين:[1]

-**القنبلة المنطقية:** ويهدف هذا الفيروس إلى تدمير المعلومات عند حدوث ظرف معين مثل تدمير نظام تسيير الموارد البشرية لمؤسسة معينة عند شطب اسم أحد الموظفين من القائمة.

-**القنبلة الزمنية:** يعمل هذا الفيروس في ساعة محددة من يوم معني ومن أبرز الأمثلة عن ذلك فيروس Micheal anglo وفيروس Macmag وفيروس shernobel ويتميز هذا الأخير بأنه فيروس الأول الذي يصيب المكونات المادية بالخراب والتف إلى جانب المكونات المعنوية (المعلومات) واكتشف هذا فيروس سنة 1998.

3/- الدودة المعلوماتية

وهي أنظمة معلومات تتميز بقدرتها على التنقل عبر شبكات نقل المعلومات من أجل عرقلة عملها وتعطيلها ، وتعطيل إمكانية التبادل ، إلخ. وأهم ما يميز هذه الفيروسات، الانتشار عبر الشبكات عن طريق توليد نفسها. ولقد أصبح مجرموا المعلوماتية يتفاخرون باستخدامها كوسيلة لاختراق الأنظمة ومن الأمثلة الواقعية على ذلك ما حدث في صفحة إدارة الدفاع الأمريكية DOD الخاصة بالقوات الجوية الأمريكية التي تعرضت واجهتها

[1] رامي حليم، مرجع سابق، ص350.

المرحبة بزوار الموقع إلى اعتداء أجبر المسؤولين على إغلاق المواقع التي تملكها إدارة الدفاع الأمريكية، ليتم تريب برنامج وقاية أشد منها.[1]

ثانيا: الأركان العامة لجريمة الإتلاف المعلوماتي

لا تقوم الجريمة بدون توافر الركنين المادي والمعنوي علاوة على الركن الشرعي.

1.الركن المادي في جريمة الإتلاف المعلوماتي

تشمل الأعمال الإجرامية التي تشكل جريمة إتلاف المعلومات جميع الأعمال التي تنطوي على تدمير أنظمة الكمبيوتر وجميع الأعمال التي تؤدي إلى استبعاد قاعدة المعلومات، كما يتحقق بأي نشاط يؤدي إلى إعدام صلاحية المحل المعلوماتي، وقد جاءت التشريعات بتعبيرات مختلفة للدلالة على هذا السلوك ومنها تعبير "الإتلاف" و"التدمير" و"التخريب" و"مسح البرامج والبيانات" و"إيقاف" أو "حذف" أو أي سلوك آخر يجعل البيانات أو البرامج والمحررات المعلوماتية غير صالحة للاستعمال كليا أو جزئيا.

وعليه 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.[2]

2/-الركن المعنوي في جريمة الإتلاف المعلوماتي

إن إتلاف المعطيات تعتبر من الجرائم العمدية المقترنة وجوبا بالقصد الجنائي مع ضرورة توافر القصد الجنائي الخاص.

[1] رامي حليم، مرجع سابق، ص350.

[2] إسمهان عون، "أركان جريمة الإتلاف المعلوماتي وعقوباتها _دراسة مقارنة_"، مجلة الدراسات الإفريقية وحوض النيل، المجلد04، العدد13، اكتوبر 2021، ص363.

أ-**القصد الجرمي العام:** بالرجوع إلى نص المادة 394 مكرر1 من قانون العقوبات الجزائري يتضح له أن القصد الجنائي في جريمة إتلاف المعلومات يتطلب توافر عنصر العلم والإرادة لدى الجاني، ويقصد بعنصر العلم هو أن يكون الجاني عالما أن ما يقوم به من شأنه تخريب وتدمير ومحو وإتلاف المعطيات الموجودة داخل النظام المعلوماتي. أما عنصر الإرادة فيفسر على أن تتجه إرادة الجاني إلى إتلاف المعطيات الموجودة داخل النظام المعلوماتي.

ب-القصد الجرمي الخاص: يجب أن تتوفر النية الإجرامية لدى الجاني للقيام بهذه الجريمة، أي أنه يجب أن تتجه إرادة لفاعل لتخريب وإفساد أو تغيير في حالة المعطيات والمعلومات والبرامج الموجودة في النظام المعلوماتي.[1]

الفرع الثالث: القواعد المشتركة بين كل جرائم أنظمة المعالجة الآلية للمعطيات

تشترك الجرائم المشار إليها أعلاه في مجموعة من القواعد تتمثل فيما يلي[2]:

1. **مضاعفة العقوبة:** في نص المادة 394 مكرر3 أن العقوبات المقررة لهذه الجرائم تضاعف وذلك متى كان من شأنها أن تمس الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.
2. **المشاركة في جمعية أشرار:** تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر5، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية والملاحظ أنه يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية الأشرار، حيث تنص المادة 394 مكرر5 من قانون العقوبات: "كل من شارك في

[1] ماجدة بوطمين، "جريمة إتلاف المعطيات المعلوماتية"، مذكرة لنيل شهادة الماستر في الحقوق، تخصص جنائي للأعمال، جامعة العربي بن مهيدي أم البواقي، 2018/2017، ص39-40

[2] عائشة شيخي، بوزيان عياشي، "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وأشكالها الاقتصادية وآليات مكافحتها"، مجلة الدراسات الحقوقية، المجلد02، العدد02، 2015، ص160.

مجموعة أو في اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو بعدة أفعال مادية، يعاقب بالعقوبات المقررة بالجريمة ذاتها".

3. **المصادرة:** ورد في أحكام المادة 394 مكرر6 على أنه مع الاحتفاظ بحقوق الغير حسن النية فإنه يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من جرائم الغش المعلوماتي علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها.
4. **جزاء الشخص المعنوي:** لقد نصت المادة 18 مكرر من القانون 15/04 المتضمن قانون لعقوبات أن: "العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح هي الغرامة التي تساوي خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي.
5. **الشروع:** لقد نصت المادة 394 مكرر 7 من قانون العقوبات على أنه: "يعاقب الشروع في ارتكاب جنح المنصوص عليها في هذا القانون هي ذاتها المقررة للجنحة". ويفهم من النص أن إرادة المشرع هي توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية.

المطلب الثاني: الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ظل النصوص القانونية

سيتم التعرف على بعض الجرائم المنصوص عليها في النصوص القانونية مثل جريمة تقليد المصنفات الإلكترونية (الفرع الأول) والجرائم الواقعة على التوقيع والتصديق الإلكترونيين (الفرع الثاني) والجرائم المنصوص عليها في قانون التأمينات (الفرع الثالث).

الفرع الأول: جريمة تقليد المصنفات الإلكترونية

أولا: التعريف بجريمة تقليد المصنفات الإلكترونية

تعتبر المصنفات لإلكترونية بأنها: "مصنفات إبداعية ذهنية تنتمي إلى بيئة المعلومات الناتجة عن أدواتها التي جعلت منها مصنفات إلكترونية أو رقمية وهي تمثل التعبير عن النشاط الذهني الشخصي لمؤلفها ويطلق عليها المصنفات المعلوماتية لتساير التقدم في الأداء لمصنفات الملكية الفكرية عبر الحواسيب وشبكة المعلومات لتتوافق مع الحاجيات المشروعة لمستخدمي تلك الشبكة الدولية"[1].

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

-الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء الفنان مؤد أو عازف،

-استنساخ أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة،

-استيراد أو تصدير نسخ مقلدة من مصنف أو أداء،

-بيع نسخ مقلدة لمصنف أو أداء،

-تأجير أو وضع رهن التداول لنسخ مقلدة مصنف أو أداء".[2]

ثانيا: صور الاعتداءات الماسة بحقوق الملكية الفكرية

[1] عبد الله قيبوعة، مسعود خثير، "الحماية الجزائية للمصنفات الرقمية في التشريع الجزائري"، مجلة الدراسات القانونية المقارنة، المجلد06، العدد02، 2020، ص1137.

[2] الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة.

إن الاعتداءات الواقعة على حقوق الملكية الفكرية الإلكترونية ليست على صورة واحدة، بل تتخذ صورا متعددة وهي كالآتي[1]:

1.القرصنة الفكرية الإلكترونية: التي تتمثل في سرقة الملكية الفكرية وتهديد الإبداع الثقافي الاقتصادي، حيث بلغت نسبة المبيعات المقرصنة إلى حجم المبيعات الثقافية حوالي 65% للكتاب، و90% للبرامج الإلكترونية.

2.**إتلاف مصنفات قواعد الحاسب وقواعد البيانات:** تتمثل في تخريب الشيء موضوع الجريمة بإتلافه أو التقليل من قيمته بجعله غير صالح للاستعمال أو تعطيله أو إدخال نوع من الجرثومة في نظام الكمبيوتر لها أشكال عديدة قادرة على التسبب بإلحاق أضرار وخسائر مالية فادحة بمالك البرنامج، أو الإدخال أو المحو أو أي فعل آخر بقصد تعطيل وظيفة من وظائف الكمبيوتر أو نظام الاتصالات (الشبكات).

3.**الاختراق أو الدخول غير المصرح به إلى أجهزة شبكات الحاسب:** للوصول إلى المصنفات الإلكترونية بغية العدوان عليها، وتتم من خلال برامج متوفرة على الإنترنت يمكن لمن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير.

4.**التجسس الإلكتروني:** كانت أغراضها مختلفة في مجالات مختلفة ، على سبيل المثال ، في مجال الاقتصاد ، والنشاط الاقتصادي، وفي مجال الأسرار، وخصوصية الأفراد، وكذلك في المجالات العسكرية والسياسية، ولعل المجال الاقتصادي الذي يحتوي على كم هائل من المعلومات السرية شكل مجالا خصبا لاستفحال التجسس المعلوماتي، كالتجسس التجاري والتجسس الصناعي المراد منه كشف سر الصفة.

[1] عبد الكريم محمد ظلام، مروة أحمد بادنجكي، "حماية المصنفات الإلكترونية في الفضاء الرقمي"، مجلة المستقبل للدراسات القانونية والسياسية، المجلد06، العدد02، 2022، ص7-8.

ثالثا: العقوبة المقررة لجريمة تقليد المصنفات الإلكترونية

يتمتع المصنف الإلكتروني بالحماية بموجب القانون الجنائي من وقت إنشائه أو من وقت نشره أو توزيعه لأول مرة، ولق قام المشرع الجزائري بتحديد العقوبات المقررة للاعتداءات على حقوق الملكية الأدبية والفنية من خلال الأمر 03-05 والمتمثلة في:

1.عقوبات أصلية: الحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500.000 دج إلى 1.000.000 دج سواء تمت عملية النشر داخل الجزائر أو خارجها.

2.عقوبات تكميلية: بالإضافة إلى ذلك ، أعطى التشريع القاضي حرية فرض عقوبات أخرى تتمثل في مصادرة مبالغ مساوية للدخل من الاستغلال غير المصرح به للعمل، مصادرة وإتلاف كل عتاد أنشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة.[1]

الفرع الثاني: الجرائم الواقعة على التوقيع والتصديق الإلكتروني

استجاب المشرعون الجزائريون للتغييرات في وسائل الاتصال والإعلام واستخدامها في مختلف المعاملات، حيث سار على نهج تشريعات العالم في الاعتراف بالكتابة الإلكترونية التي دعت الأمم المتحدة غليها من خلال لجنة أونيسترال التابعة لها. وفي هذا الصدد نص المشرع الجزائري في المادة 323 مكرر 1 من القانون المدني المعدل والمتمم بالقانون رقم 05-10 الصادر في 20-07-2005 على انه:

"يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".[1]

[1] سمية قبايلي، "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في التشريع الجزائري"، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أم البواقي، 2017/2016، ص25.

أولا: مفهوم التوقيع والتصديق الإلكترونيين

1/- مفهوم التوقيع الإلكتروني: إفادة مكتوبة بصيغة إلكترونية تتكون من حرف خاص ومميز أو رقم أو رمز أو إشارة أو صوت أو شفرة خاصة ومميزة ، ينتج عن إتباع وسيلة آمنة، وهذا البيان يلحق أو يرتبط منطقيا ببيانات المحرر الإلكتروني (رسالة البيانات) للدلالة على هوية الموقع على المحرر والرضا بمضمونه.

ويقصد بالتوقيع الإلكتروني وفق المشرع الجزائري بأنه بيانات في شكل إلكتروني، مرفقة منطقيا ببيانات إلكترونية أخرى تستعمل كوسيلة توثيق.

2/- مفهوم التصديق الإلكتروني: عملية قانونية فنية تُستخدم لإثبات أن الرسائل والتوقيعات الإلكترونية صادرة عن الشخص المنسوب إليه دون تشويه أو تزوير أو تزييف، تتم بواسطة طرف محايد مستقل، يقوم بإصدار شهادة إلكترونية تحقق الغرض المطلوب.[2]

ثانيا: الجرائم الواقعة على التوقيع والتصديق الإلكتروني

تتمثل في:[3]

- **جنحة الإخلال بإخبار السلطة الاقتصادية عن التوقف عن النشاط:** نصت على هذه الجريمة المادة 67 من القانون 04/15 على أنه "يعاقب بالحبس من شهرين إلى سنة واحدة وبغرامة من مائتي ألف دينار 20.000دج إلى مليون دينار 1.000.000دج

[1] فاطمة الزهراء تبوب، "التوقيع والتصديق الإلكترونين في ظل القانون رقم 15-04 المؤرخ في أول فبراير 2015"، حوليات جامعة الجزائر، المجلد29، العدد02، 2016، ص312.

[2] أمينة قهواجي، ليلى مطالي، "الإطار المفاهيمي والقانوني للتوقيع والتصديق الإلكترونيين في الجزائر، المشكاة في الاقتصاد التنمية والقانون، المجلد02، العدد02، 2019، ص20-21.

[3] عزيزة لرقط، "الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي تمنغست، الجزائر، المجلد06، العدد01، 2017، ص119-124.

أو بإحدى هاتين العقوبتين فقط كل مؤدي خدمات التصديق الإلكتروني أخل بالتزام إعلام السلطة الاقتصادية بالتوقف عن نشاطه في الآجال المحددة في المادتين 58-59 من هذا القانون.

- **جنحة إنشاء بيانات شهادة التصديق الإلكتروني:** تناولها المشرع الجزائري في المادة 70 من القانون 04/15 وتنص على "يعاقب بالحبس من ثلاثة أشهر إلى سنتين وبغرامة من مائتين ألف دينار إلى مليون دينار أو بإحدى هاتين العقوبتين فقط كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 42 من هذا القانون".
- **جنحة جمع البيانات الشخصية للموقع واستخدامها في غير الغرض المخصص لها:** ونص عليها المشرع الجزائري في المادة 71 "يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03)سنوات وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار (1.000.000دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون".
- **جنحة إصدار شهادة التصديق الإلكتروني دون ترخيص أو سحبه:** وهذا ما تم النص عليه في المادة 72 على أنه "يعاقب بالحبس من سنة (01) واحدة إلى ثلاث سنوات وبغرامة من مائتين ألف دينار (200.000دج) إلى مليوني دينار (2.000.000دج) أو بإحدى هاتين العقوبتين فقط كل ما يؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الإلكتروني للجمهور دون ترخيص أو كل مؤدي خدمات التصديق الإلكتروني يستأنف أو يواصل نشاطه بالرغم من سحب نشاطه.
- **جنحة الإدلاء بالإقرارات الكاذبة للحصول على شهادات التصديق:** نص عليها المشرع الجزائري في المادة 66 على أنه "يعاقب بالحبس من ثلاث (3) أشهر إلى (3) سنوات وبغرامة من عشرين ألف دينار (20.000دج) إلى مائتي ألف دينار

(200.000دج) أو بإحدى هاتين العقوبتين فقط، كل ما أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكتروني موصوفة.

- **جنحة حيازة أو إنشاء أو استعمال بيانات توقيع مصونة خاصة بالغير:** وهذا ما جاء في المادة 68 على أنه "يعاقب بالحبس من ثلاثة (03) أشهر إلى ثلاث (03) سنوات وبغرامة من مليون دينار (1000.000دج) إلى خمسة ملايين دينار أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع إلكتروني موصوف خاصة بالغير.
- **جنحة استعمال شهادة التصديق الإلكتروني الموصوفة لغير الغرض الذي منحت لأجله:** نصت المادة 74 على أنه "يعاقب بغرامة من ألفي (2.000دج) دينار إلى مائتي ألف دينار (200.000دج) كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها".[1]

الفرع الثالث: الجرائم المنصوص عليها في قانون التأمينات

تضمن أحكام البطاقة الإلكترونية الصادرة عن هيئة الضمان الاجتماعي القانون رقم 83-11 إثر تتميمه رقم 08-01 حيث جاء في المادة6 مكرر وك6 مكرر منه أنه تثبت صفة المؤمن له اجتماعيا ببطاقة إلكترونية صالحة في كل التراب الوطني وتمت الإحالة بشأن تسميتها وأحكامها إلى التنظيم. ثم جاء المرسوم التنفيذي رقم 10-116 لينص على أنه تسمى البطاقة الإلكترونية للمؤمن له اجتماعيا بطاقة الشفاء، وتتضمن معلومات شخصية تتعلق بالمؤمن له اجتماعيا.[2]

[1] عزيزة لرقط، مرجع سابق، ص124.

[2] نجاة عباوي، "الحماية الجزائية لبطاقة الشفاء الإلكترونية"، مجلة الحقيقة، المجلد16، العدد03، 2017، ص293.

لقد نصت المادة 93 مكرر 2 من القانون 08-01 على أنه: "يعاقب كل من يسلم أو يستلم البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج بغرض استعمالها بطريقة غير مشروعة، بالحبس من سنتين إلى خمس سنوات وبغرامة من 100.000دج إلى 200.000دج[1].

أي شخص يقوم عن طريق الاحتيال بتغيير أو حذف البيانات الفنية أو الإدارية الواردة في البطاقة الصحية الإلكترونية أو في المفتاح الإلكتروني للمهنيين الصحيين ، كليًا أو جزئيًا ، يكون عرضة للملاحقة القضائية، وهي نفس العقوبة التي تطبق كذلك على كل من قام بتعديل أو نسخ وبطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا، أو المفتاح الإلكتروني لهيكل العلاج أو مهني الصحة[2].

الفرع الرابع: الجرائم المرتبطة بتكنولوجيات الاتصال والإعلام

جاء القانون 04/09 بهدف الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ويقدم آليات مراقبة الاتصالات الإلكترونية وتجميعها وتسجيلها من أجل القيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

لقد سمح القانون بإجراء مراقبة للاتصالات الإلكترونية وفقط وليس غيرها من الأنظمة التي جاءت بها الاتفاقية العربية لمكافحة جرائم تقنيات المعلومات، لذلك فهناك فرق بين الرقابة والمراقبة، فالرقابة هب المتابعة عن بعد والمحافظة على تطبيق القانون في مجال معين، أما المراقبة فتفيد الاستمرار والتتبع غير المنقطع لمعرفة ما يجري داخل ميدان معين.

[1] القانون رقم 08-01، المؤرخ في 23 يناير 2008، المتمم للأمر رقم 83-11، المؤرخ في 02 يوليو 1983، المتعلق بالتأمينات الاجتماعية، الجريدة الجزائرية، العدد04، الصادرة في 27 يناير 2008.

[2] سمية قبايلي، مرجع سابق، ص27.

ومن ثم فإن المشرع الجزائري لم يترك المراقبة على إطلاقها بل حدد عمليات المراقبة لتشمل ثلاث حالات[1]:

- ✓ المراقبة من أجل الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- ✓ في حالة توفير معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- ✓ لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية، وذلك في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

[1] نوال مجدوب وآخرون، الجريمة المعلوماتية وأثرها على التنمية الاقتصادية، ج1، المركز الديمقراطي العربي، برلين، ألمانيا، ط1، 2020، ص105-106.

خلاصة الفصل:

إن التشريع الجزائري قد عرّف الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات على أنها جرائم انتهاك أنظمة معالجة البيانات الآلية المحددة في قانون العقوبات ، وكذلك أي جريمة أخرى تم ارتكابها أو تسهيلها من خلال أصبح نظام تكنولوجيا المعلومات أو الاتصال. ويتسم هذا النوع من الجرائم بالتعقيد والتشابك، بالإضافة إلى صعوبة تحديد الجاني واكتشافه، كما أنها جرائم تتسم بالمرونة.

تم تصنيف جرائم الحاسوب ، كما حددها المشرع الجزائري في القانون الجنائي ، إلى جرائم تتعلق بأنظمة معالجة البيانات الآلية ، على سبيل المثال. بجريمة الدخول أو التواجد غير المصرح به في نظام الحاسب وجريمة العبث بنظام الحاسب، جريمة إتلاف النظام المعلوماتي ولد نص عليها المشرع الجزائري في قانون العقوبات. بالإضافة غلى جرائم أخرى والمنصوص عليها في القوانين الأخرى وتتمثل في جريمة تقليد المصنفات الإلكترونية، الجرائم الواقعة التوقيع والتصديق الإلكترونيين، والجرائم المنصوص عليها في قانون التأمينات.

الفصل الثاني

آليات مجابهة الجرائم

المتصلة بتكنولوجيات الإعلام والاتصال

تمهيـــد:

أدت التطورات التكنولوجية في مجال تقنيات وشبكات الاتصال الحديثة إلى ظهور العديد من الجرائم الحديثة المتعلقة بتكنولوجيا المعلومات والاتصالات. رافق هذا التطور الكبير في جرائم تكنولوجيا المعلومات والاتصالات قوانين مختلفة ، بما في ذلك في الجزائر. وهذا بإنشاء هيئات مختصة في هذا النوع من الجرائم، بالإضافة إلى تبني إجراءات معينة للكشف والحد من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ومن خلال هذا سيتم تقسيم الفصل غلى مبحثين أساسيين:

المبحث الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المبحث الثاني: القواعد الإجرائية المتبعة بالنسبة للجرائم لمتصلة بتكنولوجيات الإعلام والاتصال.

المبحث الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

حرص المشرع الجزائري على معرفة المزيد عن الأحداث العالمية في مجال مكافحة الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات ، أنشأ المكتب الوطني لمنع الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات؛ و من خلال هذا المبحث سيتم التطرق في المطب الأول إلى تشكيلة الهيئة وتنظيمها أما المطلب الثاني فهو مخصص لمهام الهيئة.

المطلب الأول: تشكيلة الهيئة وتنظيمها

قبل الخوض في تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وجب التطرق إلى الشخصية المعنوية لهذه الهيئة.

الفرع الأول: الشخصية المعنوية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

لقد نص القانون صراحة على أن الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته تتمتع بالشخصية المعنوية والاستقلال المالي، وأهم النتائج التي ترتبت عن الاعتراف بالخصية المعنوية تتمثل فيما يلي[1]:

أولا: ذمة مالية مستقلة: تتحمل الوكالة الوطنية للوقاية من الجرائم الإلكترونية ، بصفتها كيانًا قانونيًا ، مسؤوليتها المالية ، مع ما يترتب على ذلك من نتائج قانونية باعتبار الذمة المالية مجموعة تترابط فيها العناصر الإيجابية والسلبية.

[1] سهيلة بوزبرة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية"، المجلة النقدية للقانون والعلوم السياسية، المجلد17، العدد02، 2022، ص564-565.

ثانيا: الأهلية: يحق للكيان القانوني التملك، والحق في إبرام العقود والصلاحيات الأخرى الممنوحة له بموجب القوانين واللوائح ودستوره وأسس إنشائه، مع مراعاة المكتب الوطني لمنع الجرائم الإلكترونية والاتصالات. التقنيات ككيان قانوني، فتكون لها الأهلية في الحدود التي يقررها لها القانون، لذلك يكون لها الحق في التعاقد، والحق في قبول الهبات وغيرها من الحقوق والسلطات المخولة لها قانونا.

ثالثا: الموطن: وهو مقر الهيئة، ولقد حدد موقع الهيئة القانون الجزائري بالجزائر العاصمة، وتتحدد أهمية الموطن القانونية في تحديد الاختصاص الإقليمي للجهات الفاصلة في منازعات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع الغير.

رابعا: حق التقاضي: قانون الإجراءات الذي تم إنشاؤه للأجهزة والوحدات الإدارية مستقل عن قانون الإجراءات المطبق على الدولة ، حيث يمكن مقاضاته من قبل ممثليها، حيث ترفع الدعاوي ضد الهيئات والوحدات التي تتمتع بالشخصية المعنوية، ومنه فالهيئة يمكن لديها حق التقاضي سواء كمدعي أو مدعى عليها ويمثلها رئيسها أمام القضاء[1].

الفرع الثاني: تشكيلة الهيئة وتنظيمها

لقد تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها بموجب المادة 13 من القانون رقم 09-04.

[1] سهيلة بوزبرة، مرجع سابق، ص565.

إن المرسوم الرئاسي 15-261 ووفقا للمادة الرابعة حدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وهي كالتالي[1]:

-لجنة مديرة.

-مديرية عامة.

-مديرية المراقبة الوقائية واليقظة الإلكترونية.

-مديرية التنسيق التقني.

-مركز العمليات لتقنية.

-ملحقات جهوية.

إلا أنه وبصدور المرسوم الرئاسي 19-172 تم تقليص في تشكيلة لهيئة وأصبحت تتكون من:

-المديرية العامة وتضم: المديرية التقنية، ومديرية الإدارة والوسائل.

-مجلس التوجيه.

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

-مجلس التوجيه

-المديرية العامة: وتنقسم إلى:

[1] المرسوم الرئاسي رقم 15-261، المؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة لوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الجزائرية، العدد53، الصادر في تاريخ 08 أكتوبر 2015.

- ✓ مديرية للمراقبة الوقائية واليقظة الإلكترونية.
- ✓ مديرية الإدارة والوسائل.
- ✓ مصلحة للدراسات والتلخيص.
- ✓ مصلحة التعاون واليقظة التكنولوجية.[1]

أولا: مجلس التوجيه: بحسب المادة8 من المرسوم الرئاسي رقم 20-183 يجتمع المجلس في دورة عادية مرتين السنة، بناء على استدعاء من رئيسه، كما يمكن 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. ويرأسه رئيس الجمهورية ويمكن أن يفوض ممثليه، ويتشكل من الأعضاء التالية:

-الوزير المكلف بالعدل.

-الوزير المكلف بالداخلية.

-الوزير المكلف بالمواصلات السلكية واللاسلكية.

-المدير العام للأمن الداخلي.

-قائد الدرك الوطني.

-المدير العام للأمن الوطني.[2]

ولقد حددت المادة 07 مهام مجلس التوجيه بأنه يكلف بـ:

[1] المرسوم 20-183، المؤرخ في 13 يوليو2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام ولاتصال ومكافحتها، الجريدة الرسمية الجزائرية، العدد40، الصادر بتاريخ 26 ذو القعدة 1441 الموافق18 يوليو2020.

[2] لمادة06، المرسوم 20-183، مرجع سابق.

-توجيه عمل الهيئة والإشراف عليه ومراقبته.

-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 14 شعبان عام 1430 الموافق 5غشت سنة 2000 والمكور أعلاه.

-المداولة حول الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

-المداولة حول مسائل التطوير والتعاون مع المؤسسات والهيئات الوطنية والأجنبية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

-القيم دوريا بتقييم حالة التهديد في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال للتمكن من تحديد مضامين العمليات الواجب القيام بها والأهداف المنشودة بدقة.

-اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

-إعداد نظامها الداخلي والمصادقة عليه.

-دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليه.

-دراسة مشروع وميزانية الهيئة والموافقة ليه.

-إبداء رأيه في كل مسألة تتصل بمهام الهيئة.

-تقديم كل اقتراح يتصل بمجال اختصاص الهيئة.

-المساهمة في ضبط المعايير القانونية في مجال اختصاصه.[1]

ثانيا: المديرية العامة

باستقراء المادة 9 من المرسوم الرئاسي 20-183 فإنه يدير الهيئة العامة مدير عام يعين بموجب مرسوم رئاسي وكذلك بالنسبة إلى انتهاء مهامه. ولقد حددت المادة 10 من نفس المرسوم فتتمثل صلاحياتها فيما يلي[2]:

-السهر على السير الحسن للهيئة.

-إعداد مشروع ميزانية الهيئة وعرضه على مجلس التوجيه للموافقة.

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

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

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

-تمثيل الهيئة لدى السلطات والمؤسسات الوطنية والدولية.

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

-ضمان التسيير الإداري والمالي للهيئة.

[1] المرسوم 20-183، مرجع سابق.

[2] المرسوم الرئاسي 20-183، مرجع سابق.

-تحضير اجتماعات مجلس توجيه الهيئة.

-إعداد التقرير السنوي لنشاطات الهيئة ورفعه لمصادقة مجلس التوجيه.

الفرع الثالث: كيفية سير عملها

تنص المادة 07 من المرسوم الرئاسي 19-172 أن يجتمع مجلس التوجيه في دورة عادية بناء على استدعاء من رئيسه أو بطلب من أحد أعضاءه أو من المدير العام للهيئة. وتضيف المادة 08 من المرسوم أن تحدد قواعد وكيفية سير مجلس التوجيه بموجب قرار من وزير الدفاع، وكانت الفقرة الأولى من المادة 18 من المرسوم رقم 15-261، تنص أن الهيئة تزود بقضاة وضباط وأعوان للشرطة القضائية كما تزود أيضا بأعوان من مصالح الاستعلامات العسكرية والأمن والدرك، يحدد عددهم بصدور قرارات مشتركة بين مختلف هذه المصالح، كما تزود أيضا الهيئة بمستخدمي الدعم التقني والإداري ويجلب هؤلاء من مستخدمي المصالح العسكرية للاستعلام والأمن والدرك.

ومن جهة أخرى كان يمكن للهيئة أن تستعين بأي خبير أو أي شخص يمكن أن يعينها في أعمالها كما يمكن لها أن تطلب من أي جهة أو جهاز أو أي مؤسسة تسليم كل وثيقة أو معلومة ضرورية لإنجاز المهم المسندة إليها[1].

المطلب الثاني: مهام الهيئة وحدود استقلاليتها

وجب أولا التعرف على صلاحيات ومهام الهيئة (الفرع الأول) وحدود استقلاليتها الوظيفية (الفرع الثاني).

[1] عبد النبي مصطفى، "قراءة في النصوص القانونية المنظمة للهيئة الوطنية لوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها"، دفاتر السياسة والقانون، المجلد13، العدد03، 2021، ص403.

الفرع الأول: مهام الهيئة

من خلال اسمها فإن للهيئة دوران أساسيان يمكن أن تلعبهما في حالة تأسيسها:

أولا: الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تهدف التدابير الوقائية إلى توعية مستخدمي تكنولوجيا المعلومات والاتصالات بخطورة الجرائم التي قد يقعون ضحية لها أثناء تصفح أو استخدام هذه التقنيات، ومن أهم هذه الجرائم نذكر:

-التجسس على الاتصالات والرسائل الإلكترونية.

-التلاعب بحسابات العملاء أو ببطاقات ائتمانهم.

-اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية...الخ.[1]

ثانيا: مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

بالرجوع إلى المادة 14 من القانون 04/09 نجد أن مهام هذه الهيئة تتمثل في[2]:

1.تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

2.مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

[1] أحمد مسعود مريم، "آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09"، مذكرة لنيل شهادة الماجستير، تخصص: قانون جنائي، كلية الحقوق واللوم السياسية، جامعة قاصدي مرباح ورقلة، 2013/2012، ص45.

[2] القانون04/09، مرجع سابق.

3.تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف عل مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

أما من خلال أحكام المرسوم الرئاسي 21-439 المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فإضافة إلى المهام المسندة لها بموجب أحكام القانون 04/09 المشار إليه سابقا تكلف الهيئة على الخصوص ووفقا لنص المادة 04 منه بما يأتي:

1.تحديد الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ووضعها حيز التنفيذ.

2.المساهمة في تكوين المحققين المتخصصين في مجال لتحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال.

3.تطوير التعاون مع المؤسسات والهيئات الوطنية في مجال الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

4.تجميع وتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية[1].

وتملك الهيئة صلاحيات أخرى في المجال الإداري والمالي بواسطة أجهزتها الداخلية:

-المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام والاتصال وذلك بالنظر للخبرة التي تملكها؛

[1] سعاد أجعود، "الحماية الجزائية لتكنولوجيات الإعلام والاتصال في التشريع الجزائري دراسة على ضوء النصوص المستحدثة"، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد07، العدد04، جوان 2022، ص230.

-إعداد النظام لداخلي ولمصادقة عليه ويكون للجنة المديرة في ظل المرسوم الرئاسي رقم 15-261 ولمجلس التوجيه في ظل المرسوم الرئاسي رقم 19-172.

-دراسة أو إعداد التقرير السنوي لنشاطات الهيئة والمصادقة عليه ويكون للجنة المديرة في ظل المرسوم الرئاسي رقم 15-261 وللمديرية العامة في ظل المرسوم الرئاسي رقم 19-172؛

-السهر على حسن سير الهيئة (للمديرية العامة في ظل المرسومين الرئاسيين)؛

-إعداد وتنفيذ برنامج عمل الهيئة؛

-دراسة مشروع ميزانية الهيئة ولموافقة عليها (للجنة المديرة في ظل المرسوم الرئاسي رقم 15-261 ولمجلس التوجيه في ظل المرسوم الرئاسي رقم 19-172)؛

-تنشيط أنشطة هياكل الهيئة وتنسيقها ومراقبتها (للمديرية العامة في ظل لمرسومين الرئاسيين)؛

-ضمان التسيير الإداري والمالي للهيئة (المديرية العامة في ظل المرسوم الرئاسي رقم 15-261 ومديرية الإدارة والوسائل في ظل المرسوم الرئاسي رقم 19-172).[1]

الفرع الثاني: حدود الاستقلالية الوظيفية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

إن مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تخضع لنوعين من الرقابة[1]:

[1] إلهام خرشي، "النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، مجلة الأبحاث القانونية والسياسية، المجلد04، العدد01، 2022، ص68.

أولا: رقابة السلطة التنفيذية على مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

تنص المادة 32 من المرسوم الرئاسي رقم 15-261 على أنه يرفع رئيس اللجنة المديرة للهيئة إلى رئيس الجمهورية تقارير فصلية عن نشاطات الهيئة، أي أن المظهر الشائع لدى المشرع الجزائري بشأن السلطات الإدارية المستقلة هو إدراج عنصر القرابة على نشاطاتها، وفي ذلك تناقض مع الطبيعة القانونية المصرح بها في المادة 2.

ثانيا: رقابة السلطة القضائية على مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها

لقد نصت المادة 4 من المرسوم الرئاسي رقم 15-261 على رقابة السلطة القضائية "تمارس الهيئة المهام المنصوص عليها في المادة 14 من القانون رقم 09-04 تحت رقابة السلطة القضائية". وجاء هذا شارحا في المادة 41 إذ نصت على ما يلي: "تمارس الهيئة اختصاصها كصاحبة اختصاص أصيل وحصري في مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص"، إلا أن النص لم يحدد الجهة القضائية المختصة بالرقابة وهذا ما أدى إلى التحكم إلى القواعد العامة الخاصة بالطعون ضد قرارات السلطات لإدارية المستقلة إذ تنص المادة 09 من القانون العضوي رقم 98-01 على ما يلي: "يختص مجلس الدولة كدرجة أولى وأخيرة، بالفصل في دعاوي الإلغاء والتفسير، وتقدير المشروعية في القرارات الإدارية الصادرة عن السلطات الإدارية المركزية، والهيئات العمومية والمنظمات المهنية الوطنية".[2]

[1] بدرة إبراهيم لعور، "الأمن الإلكتروني وفقا للتشريع الجزائري: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال نموذجا"، المجلة العربية للدراسات الأمنية، المجلد32، العدد72، 2018، ص255.

[2] بدرة إبراهيم لعور، مرجع سابق، ص255.

المبحث الثاني: القواعد الإجرائية المتبعة بالنسبة للإجراءات المتصلة بتكنولوجيات الإعلام والاتصال

لقد قام المشرع الجزائري بسن قواعد إجرائية تتلاءم مع الطبيعة التقنية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومن بين الإجراءات الحديثة في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نجد مراقبة الاتصالات الإلكترونية (المطلب الأول) وتفتيش المنظومات المعلوماتية (المطلب الثاني) ودور مقدمي الخدمات في التحريات والتحقيقات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال (المطلب الثالث).

المطلب الأول: مراقبة الاتصالات الإلكترونية

إن مراقبة الاتصالات الإلكترونية من بين الأساليب الحديثة لمكافحة الجرائم المستحدثة ومن خلال هذا المطلب سيتم التطرق إلى مفهوم مراقبة الاتصالات الإلكترونية (الفرع الأول)

الفرع الأول: مفهوم مراقبة الاتصالات الإلكترونية

إن مفهوم مراقبة الاتصالات الإلكترونية مصطلح مركب سنحاول تعريف كل مصطلح على حدى.

أولا: تعريف المراقبة

1.لغة: المراقبة تعني الملاحظة، فراقب الشيء حرصه أو رصده، والرقيب هو الحارس أو الحافظ، والمرقب آلة لرصد الفلك.

2.اصطلاحا: وهي وضع شخص، أو وسائل نقل، أو أماكن أو مواد بصورة سرية تحت رقابة سرية أو دورية، بهدف الحصول على معلومات خاصة بالنشاط، أو كشف شخصية

الأفراد، وهي تفيد في منع إتمام الجريمة، وجمع الأدلة عنها والتأكد من صحة المعلومات، ثم الحصول عليها بالفعل[1].

ثانيا: تعريف الاتصالات الإلكترونية

حسب القانون 09-04 تم تعريف الاتصالات الإلكترونية بأنها: "أي تراسل أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"[2].

ثالثا: مراقبة الاتصالات الإلكترونية

لقد نصت المادة 03 من القانون 09-04 على أنه "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".[3]

وتتمثل حالات اللجوء إلى المراقبة الإلكترونية حسب المادة 04 من القانون 09-04 فيما يلي:

-الوقاية من الأفعال الموصوف بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

[1] فطيمة جبار، "مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري"، مجلة الدراسات القانونية المقارنة، العدد03، ديسمبر2016، ص14.

[2] القانون09-04، مرجع سابق.

[3] القانون 09-04، المرجع نفسه.

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

-لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية

-في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة[1].

الفرع الثاني: الحماية القانونية للاتصالات الإلكترونية

هناك عدة قوانين سعت إلى حماية الاتصالات الإلكترونية نذكر أهمها:

أولا: قانون البريد والاتصالات الإلكترونية

لقد ألزمت المادة 119 متعاملي الاتصالات الإلكترونية باتخاذ التدابير التي من شأنها أن تضمن سرية المكالمات والمعلومات التي يحوزنها عن مشتركيهم، وألا يسمحوا بوضع أي ترتيبات بغرض اعتراض الاتصالات أو مراقبة المكالمات الهاتفية والوصلات والمحادثات والمبادلات الإلكترونية دون إذن مسبق من السلطة القضائية. ويجب عليهم أن يطلعوا أعوانهم على التزاماتهم والعقوبات التي يتعرضون لها عند عدم احترامهم لهذه الأحكام.

أما المادة 164 فقد نظمت أحكام جريمة التنصت على الاتصالات السلكية واللاسلكية. في حين نجد المادة 165 و166 تنصان على جريمة تحويل مضمون الاتصالات السلكية واللاسلكية بإفشائها أو نشرها واستعمالها[2].

[1] القانون 09-04، المرجع نفسه.

[2] فريد روابح، "ضمانات حرمة الحياة الخاصة أثناء إجراء مراقبة الاتصالات الإلكترونية"، مجلة الأبحاث القانونية والسياسية، المجلد02، العدد02، 2020، ص9.

ثانيا: في قانون الوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها

لقد جاء في المادة 3 من القانون على أنه يجب مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات عند وضع الترتيبات التقنية لمراقبة الاتصالات الإلكترونية وتسجيلها وتجميعها عندما يقتضيها ضرورات التحريات والتحقيقات القضائية الجارية، أو يقتضيها الحفاظ على النظام العام.

أما المادة 04 فقد أوجبت أن تكون الترتيبات التقنية الموضوعة للأغراض المنصوص عليها في الفقرة (أ) في إطار احترام الحياة الخاصة للغير تحت طائلة العقوبات[1].

الفرع الثالث: أشكال مراقبة الاتصالات الإلكترونية

تتمثل صور مراقبة الاتصالات الإلكترونية:

أولا: اعتراض المراسلات السلكية واللاسلكية

لقد خول المشرع الجزائري للجهات القضائية اعتراض المراسلات السلكية واللاسلكية وهذا بنص المادة 65 مكرر05 من قانون الإجراءات الجزائية والتي أضيفت بموجب القانون06-22.

وتعرف اعتراض المراسلات السلكية واللاسلكية على أنها إجراء تحقيق يباشر خلسة، وينتهك سرية الأحاديث الخاصة تأمر به السلطة القضائية في الشكل المحدد قانون بهدف

[1] فريد روابح، مرجع سابق، ص10.

الحصول على دليل غير مادي لجريمة تحقق وقوعها ويتضمن من ناحية استراق السمع إلى الحديث ومن ناحية أخرى حفظه على الأشرطة عن طريق أجهزة مخصصة لهذا الغرض[1].

ثانيا: اعتراض البريد الإلكتروني

اعتراض البريد الإلكتروني هو شكل من أشكال مراقبة الاتصالات الإلكترونية ولأنه يتم وضعه عمداً على الإنترنت كوسيلة للاتصال، فإن الطرق التقليدية ليست مناسبة لمراقبة البريد الإلكتروني، لهذا ظهرت برامج متطورة قادرة على مراقبة البريد الإلكتروني من بينها نظام كارنيفور CARNIVORE والذي تستخدمه وكالة المباحث الفيدرالية الأمريكية للتجسس[2].

الفرع الرابع: الحالات المسموح بها في إجراء مراقبة الاتصالات الإلكترونية

تتمثل هذه الحالات حسب القانون 09-04 في:[3]

أولا: الوقاية من ارتكاب الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة

تعد مراقبة الاتصالات الإلكترونية خطوة في الفترة التي تسبق الجرائم التي تنطوي على تكنولوجيا المعلومات والاتصالات، وتبدأ من بمجرد وصول العلم إلى السلطة القضائية المختصة باحتمال ارتكاب جريمة من جرائم الإرهاب أو لتخريب أو جريمة من الجرائم

[1] ياسر الأمير فارق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية دراسة تأصيلية تحليلية ومقارنة للتصنت على المحادثات التلفونية والتي تجري عبر الإنترنت والأحاديث الشخصية نظريا وعمليا، دار المطبوعات الجامعية، الإسكندرية، ط1، 2009، ص150.

[2] إسماعيل بن يحي، "التعريف بمراقبة الاتصالات الإلكترونية كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية"، مجلة صوت القانون، المجلد08، العدد02، 2022، ص1073.

[3] دنيازاد ثابت ، "مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري"، مجلة العلوم الاجتماعية والإنسانية، المجلد05، العدد01، 2012، ص210-211.

الماسة بأمن الدولة. والسبب في ذلك صعوبة التوصل إل معرفة مرتكبي مثل هذه الجرائم وخطورة هذه الأفعال على الدولة وعلى حياة الأفراد وممتلكاتهم، ذلك أن هذه الأفعال في كثير من الأحيان تؤدي إلى نتائج جرمية وخيمة يصعب تلافيها.

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

في هذه الحالة أيضًا ، يجب تطبيق المراقبة الجنائية للاتصالات الإلكترونية بمجرد وصول المعلومات إلى السلطة القضائية ، إذا كانت هذه المعلومات تشكل خطرًا على النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ثالثا: مقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية

وتكون في حالة عدم جدوى الإجراءات التقليدية في معرفة مرتكبي الجرائم، ويتم اللجوء إليها في جميع الجرائم بتكنولوجيات الإعلام والاتصال.

رابعا: في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة

يتعلق ذلك بالجرائم المرتكبة خارج البلاد، وستؤدي عملية مراقبة الاتصالات الإلكترونية في الجزائر إلى نتائج للبلد المعني في التحقيق في هذه الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات ومقاضاة مرتكبيها، بشرط أن يتم ذلك في إطار تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة أي أن يكون ذلك في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل.[1]

[1] دنيازاد ثابت ، مرجع سابق، 211.

المطلب الثاني: تفتيش المنظومات المعلوماتية

يعتبر التفتيش عن الجريمة المعلوماتية من أصعب أنواع التفتيش، وهذا راجع إلى التطور التكنولوجي في وسائل الاتصال.

الفرع الأول: مفهوم التفتيش

يعرف التفتيش بأنه إجراء من إجراءات التحقيق، تقم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها في محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه[1].

وهناك من يعرّف الرقابة بأنها من أنشطة التحقيق التي يقوم بها الموظف المختص وفق الإجراءات التي يحددها القانون، في محل يتمتع بحرمته، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقق وقوعها، لإثبات ارتكابها ونسبها إلى المتهم، وقد أحاط إجراء التفتيش _نظرا لمساسه بالحريات الخاصة للأفراد بضمانات عديدة[2].

وهناك من يعرفه بأنه وسيلة من وسائل التحري عن مختلف الأدلة المعنوية والمادية للجريمة، يهدف إلى جمع الأدلة التي تؤدي إلى كشف الحقيقة وضبطها والوصول غلى دليل حاسم، لأنه لا إدانة ولا جزاء دون دليل[3].

الفرع الثاني: شروط التفتيش في المنظومات المعلوماتية

وتنقسم إلى شروط شكلين وشروط موضوعية تتمثل في الآتي:

أولا: الشروط الشكلية وهي كالآتي:[1]

---

[1] سامي حسني الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة، 1972، ص36.

[2] عوض محمد عوض، قانون الإجراءات الجنائية، ج1، مؤسسة الثقافة الجامعية، 1989، ص475.

[3] رضا هميسي، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، العدد05، جوان 2012، ص162.

1. **وقت إجراء التفتيش:** عندما يتعلق الأمر بأنظمة المعالجة الآلية للمعطيات فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل من ساعة من ساعات النهار أو الليل وهذا بناء على إذن مسبق من وكيل الجمهورية المختص.
2. **حضور الأشخاص المعنيين أثناء التفتيش:** واشترط المشرع الجزائري أن يتم تفتيش المنزل بحضور المتهم وفي حالة منعه من ذلك أثناء الإجراءات، كان على ضابط الشرطة القضائية أن يكلفه بتعيين ممثل له وإذا امتنع عن ذلك أو كان هاربا كان من الواجب أن ينوبه عنه شاهدين غير الموظفين الخاضعين له.
3. **محضر التفتيش:** في الجرائم الماسة بالمعطيات الآلية: تسمى محاضر الشرطة القضائية محاضر البحث الابتدائي وتكمن أهميتها في قيمتها الممنوحة لها كوسيلة إثبات على وقوع الجريمة ونسبتها إلى فاعلها من جهة، ومن خطورة الصلاحيات الواسعة الممنوحة بموجبها لضابط الشرطة القضائية.

ثانيا: الشروط الموضوعية: وتتمثل في[2]:

1. **سبب التفتيش:** ارتكاب الجريمة المعلوماتية بشكل عام.
2. **محل التفتيش:** محل التفتيش بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها على العالم.
3. **السلطة الخاصة بالقيام بالتفتيش:** تتمثل الجهة القضائية التي تم إسنادها مهمة التفتيش في قاضي التحقيق أو النيابة العامة باختلاف التشريعات كسلطة أصلية، أو استثناء في رجال الضبط القضائي. وفي حالة وقوع جريمة من نوع الجنايات أو

[1] عز الدين عثماني، "إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية"، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد04، جانفي 2018، ص57-58.

[2] عز الدين عثماني، مرجع سابق، ص58-59.

الجنح ولم يكن قاضي التحقيق المختص موجودا فإن على المسؤول عن التحقيق عندما تقتضي الضرورة إصدار قرار أو إجراء فوري في التحقيق عرض الأمر على أي قاضي في منطقة اختصاص قاضي التحقيق أو أي منطقة قريبة لاتخاذ ما يلزم على أن تعرض الأوراق على قاضي التحقيق المختص في أقرب وقت.

المطلب الثالث: دور مقدمي الخدمات في التحريات والتحقيقات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال

الفرع الأول: مفهوم مقدمي الخدمات

تتنوع تقنيات المعلومات والاتصالات، خاصة فيما يتعلق بخدمات الاتصالات السلكية واللاسلكية مثل الهواتف المحمولة والشبكات الرقمية للإنترنت، وهو ما يجعل عملية توصيل الخدمات المتنوعة لهذه التكنولوجيا إلى مستعمليها يتطلب توافر مجموعة من الفاعلين على رأسهم مقدمي الخدمات، المنصوص عليهم في القانون 09-04 الذي يعرفهم على أنهم[1]:

1. أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.
2. وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

الفرع الثاني: التزامات مقدمي الخدمات

تتمثل التزامات مقدمي الخدمات في مساعدة السلطات طبقا للمادة 10 من قانون الإجراءات الوقائية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في حفظ المعطيات المتعلقة بحركة السير وفقا للمادة11، ولقد أضاف المشرع في المادة 12 التزامات خاصة

[1] عز الدين عثماني، مرجع سابق، ص53.

بمقدمي الإنترنت، والسبب في هذه الالتزامات على سبيل المثال ، أن المراسلات الإلكترونية التي يتلقاها مقدم خدمة المتلقي ولم يطلع عليها بعد قد تحولت إلى حالة الأرشفة الإلكترونية. في هذه المرحلة ، توجد النسخة المؤرشفة من الاتصال فقط في شكل إجراء انتظار أولي أو مؤقت. تم استلام مستلمًا من مزود الخدمة ، وبمجرد استلام المرسل إليه المراسلة بالبريد الإلكتروني فإن موقف مزود الخدمة يتراوح بين أمرين: إما أن يقوم بمسح تلك الرسالة، أو أن يقوم بتخزينها في حال طلب السلطات لتلك الرسالة، وعليه فيقوم بالتجميع والتسجيل والحفظ وتقديمها لهذه السلطات لتساعدها في كشف الحقيقة. كالتالي[1]:

أولا: مساعدة السلطات

وفقا للمادة 10 من قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها فإن مزود الخدمات يلتزم بما يلي:

– مساعدة السلطات في إجراء الإجراءات التحضيرية لجمع وتسجيل بيانات محتوى الرسالة في الوقت المناسب، بحيث أنه لمّا كان مزود الخدمة بإمكانه مراقبة ومعرفة جميع الخطوات التي يتبعها المستخدم إذ يتاح له معرفة المواقع التي زارها والمعلومات التي خزنها وكل الاتصالات التي أجراها، ومن ثم فإنه ملزم بتمكين جهات التحقيق من كل المعلومات التي تبحث عنها، وذلك بتجميعها أو تسجيلها.

–وضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من ذات القانون تحت تصرف السلطات المكلفة بالتحريات القضائية.

[1] إلهام بن خليفة، "القواعد الإجرائية الحديثة لمواجهة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، كلية الحقوق والعلوم السياسية، جامعة حمه لخضر الوادي، ص11.

-الحفاظ على السرية، إذ يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها[1].

ثانيا: حفظ المعطيات المتعلقة بحركة السير

لقد نصت المادة 11 من القانون 09-04 على أن يلتزم مقدمو الخدمات بحفظ:

أ-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ب-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ج-الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

د-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

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

بالنسبة لنشطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه[2].

ويترتب على ذلك أن إجراء المصادرة يتم بعد أن يقوم مقدمو الخدمة بجمع وتسجيل وتخزين لاحق للوصول بشكل نهائي إلى أيدي الجهات المسؤولة عن التحقيق القضائي، وتكتسي هذه الإجراءات أهمية بالغة من حيث كونها أداة تنقيب وتحري مفيدة من أجل تحديد مصدر الاتصال ومآله عن طريق أرقام الهاتف، كما توفر بيانات مرتبطة بالساعة والتاريخ والمدة المتعلقة بأنواع الاتصالات غير المشروعة.

وتحدد مدة حفظ المعطيات بسنة واحدة ابتداء من تاريخ التسجيل.

[1] إلهام بن خليفة، مرجع سابق، ص12.

[2] القانون 09-04، مرجع سابق.

ثالثا: التزامات خاصة بمقدمي خدمة الإنترنت

حسب المادة 12 من نفس القانون يتعين على مقدمي خدمات الإنترنت على:

أ- التدخل الفوري لسحب المحتويات التي يتيحون الاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو جعل الدخول إليها غير ممكن.

ب-وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام أو الآداب العامة وإخبار المشتركين لديهم بوجودها.[1]

رابعا: مسؤولية مقدمي الخدمات عن إخلالهم بالالتزامات القانونية المفروضة عليهم

يتعرض مقدمو الخدمات للملاحقة القضائية ويتحملون العقوبات المنصوص عليها في قانون العقوبات إذا لم يلتزموا بالسرية ، ولكن على العكس من ذلك أفشوا جميع أسرار التحري والتحقيق، كما يتحملون المسؤولية الجنائية عن إخلالهم بالتزام الحفظ، حيث تطبق على الشخص الطبيعي وفقا للفقرة الرابعة من المادة 11 من القانون 09-04 عقوبة الحبس من 06 أشهر إلى 05 سنوات وغرامة من 50.000 دج إلى 500.000 دج، وهذا مع عدم الإخلال بالعقوبات الإدارية، إذ أن مقدمي الخدمات يتعاملون مع هيئات وتفرض عليهم هذه الأخيرة عدة التزامات تقيد في دفتر الشروط، وفي حال إخلالهم بها تطبق عليهم جزاءات كسحب الرخصة إضافة إلى عقوبات إدارية أخرى، وتطبق على الشخص المعنوي طبقا للفقرة الأخيرة من نفس المادة وفقا للقواعد المقررة في قانون العقوبات[2].

[1] القانون 09-04، مرجع سابق.
[2] إلهام بن خليفة، مرجع سابق، ص12.

خلاصة الفصل:

من خلال ما تمت مناقشته في هذا الفصل ، يبدو واضحًا لنا أن المشرع الجزائري قد أنشأ وكالة وطنية لمنع الجرائم المتعلقة بتكنولوجيا المعلومات والاتصالات، وأسند إليها عدة مهام من أجل مكافحة الجرائم المتعلقة بتكنولوجيات الإعلام والاتصال.

لقد قام المشرع الجزائري بوضع الإجراءات المتبعة في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وهذا من خلال القانون 09-04. فلقد أعطى أهمية للمراقبة الإلكترونية وتفتيش المنظومات المعلوماتية وكذا دور مقدمي الخدمات لما لها من أهمية في الوصول إلى مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

خاتمة

تعرف جرائم الكمبيوتر هي الجرائم الجنائية لتزوير أنظمة معالجة البيانات الآلية بالمعنى المقصود في القانون الجنائي ، وكذلك جميع الجرائم الجنائية الأخرى التي يتم ارتكابها أو جعلها ممكنة بواسطة نظام كمبيوتر أو نظام اتصال إلكتروني. بناءً على هذا التعريف ، يمكن تصنيفها إلىجريمة تتعلق بالمعلومات فقط يكون هدف الجريمة فيها هو نظام الكمبيوتر، وجرائم تقليدية يتدخل العنصر المعلوماتي كوسيلة لإرتكابها وتؤثر الطبيعة الخاصة لهذه الجرائم على إجراءات كشفها ومتابعتها، نظرا لقلة الاثار المادية التي تخلفها وكثرة الأشخاص الذين يترددون على مسرح الجريمة ويثير البحث والتحري عنها الكثير من الإشكالات القانونية ما جعل المشرع الجزائري يتدخل لتقييد هذه الإجراءات على نحو يعزز الحريات الشخصية للأفراد هذه الخصوصية لا تقتصر على المستوى الوطني فقط بل تسارع مختلف دول العالم لمجابهة هذا النوع المستحدث من الجرائم من خلال إنشاء هيئات دولية وإبرام معاهدات تسمح بتجسيد التعاون الدولي في هذا المجال.

وقد أدى هذا الوضع إلى ظهور عدد من الاستئنافات على المستوى الإجرائي ، والتي تتناول بشكل أساسي بعض القضايا القانونية المتعلقة بأخذ الأدلة على هذه الجرائم ، لأنها لا تترك أي عواقب مادية ملموسة، كما هو الحال في الجرائم التقليدية مما يقتضي الاهتمام بوضع تشريعات تتلاءم وطبيعة هذا النوع من الجرائم.

وعليه نخلص إلى جملة من النتائج:

- تنوع طرق الجريمة الالكترونية وتعدد أساليبها مع تقدم الزمن وتطور التقنية الحديثة.
- عدم حرص المستخدم على وضع برامج حماية ضد الفيروسات والتجسس.
- عدم تحديث أنظمة الحماية المستخدمة.

– وجود نقص وضعف في التشريعات والقوانين الخاصة بهذا النوع من الجرائم مما أسهم في تمادي المجرمين .

– وكذلك الأحكام المتعلقة بالاختصاص الإقليمي للقانون الجنائي الجزائري ، حيث تم توسيع الاختصاص الإقليمي للسلطات القضائية لمقاضاة الجرائم ضد مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني ، مع مراعاة هذه التقنيات الحديثة يمكن أن يفعلوا عندما يتعارضون مع مصالح الدولة ، حتى على أراضي البلدان الأخرى ، من قبل الجزائريين أو الأجانب، أيضا فإن عالمية استغلال تكنولوجيات الإعلام والاتصال وخاصة الانترنت أدت إلى حذف الحدود الإقليمية وأصبحت الجرائم تمتد عبر عدة أقاليم وتكون من اختصاص القانون الجزائي لأكثر من دولة مما قد ينجر عنه تنازع في الاختصاص أو رفض له، مما قد ينشأ للمجرمين أماكن لا قانون فيها فكان التعاون الدولي في هذا النوع من الجرائم مفيدا وفعال جدا ولا يتأتى ذلك إلا باستعمال الطرق الحديثة للتواصل ما بين السلطات القضائية دون المرور بالطرق الدبلوماسية المعقدة وهو ما تم تشريعه فعلا ضمن هذا القانون.

– مقدمو الخدمات الذين تتماشى تقنياتهم مع تطور تقنيات المعلومات والاتصالات الحديثة ، يلعبون أيضًا دورًا مهمًا في مكافحة هذا النوع من الجرائم وفي تقديم الدعم الفني للجهات المعنية بالتحقيق والتحقيق في الجرائم المرتكبة من قبلهم أو ضدهم، وأيضا الالتزام بما قرره المشرع بحفظ للمعطيات المعلوماتية يسمح للمتحرين تتبع الجريمة وحركة المجرمين.

لذلك يمكن القول إن المشرع الجزائري يعمل باستمرار على مكافحة هذا النوع من الجرائم من خلال التشريعات وتحديثها وإنشاء هيئات مع مراعاة ما يميز جرائم تكنولوجيا المعلومات والاتصالات عن الجرائم الأخرى، ناهيك عن الأثر الذي تتركه، سواء تعلق الأمر

بدول كالجوسسة والجرائم المتعلقة بالأمن القومي ، أو تلك المتعلقة بسرقة والتعدي على بيانات الأفراد الشخصية.

كما يمكن تقديم جملة من الاقتراحات، ألا وهي:

- يتعين في ذات الوقت التأهيل المناسب لكوادر الأجهزة القضائية بما يجعلها قادرة على التعامل مع هذه الجرائم بكفاءة واقتدار.
- استحداث ضبطية قضائية متخصصة في مجال الجرائم المعلوماتية أسوة بالدول المتقدمة ، ذلك أن أخطارها البالغة من شأنها تحديد الكيان الاقتصادي للدول.

ضرورة إبرام إتفاقيات دولية في مجال مكافحة جرائم تكنولوجيات الإعلام و الإتصال، من أجل تعزيز التعاون الدولي لكشف و إثبات الجريمة.

قائمة المصادر

والمراجع

النصوص الرسمية:

- **النصوص التشريعية:**

أولا: الأوامر

1. الأمر رقم 03-05 المؤرخ في 19 جمادى الأولى عام 1424 الموافق 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة.

ثانيا: القوانين

1. القانون رقم 09-04 مؤرخ في 14 شعبان 1430 الموافق5غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
2. القانون رقم 04-15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر رقم 66-156 المؤرخ في 1966/06/08، المتضمن قانون العقوبات، الجريدة الرسمية الجزائرية، العدد71 بتاريخ 2004/11/10.

3. القانون رقم 08-01، المؤرخ في 23 يناير2008، المتمم للأمر رقم 83-11، المؤرخ في 02 يوليو 1983، المتعلق بالتأمينات الاجتماعية، الجريدة الجزائرية، العدد04، الصادرة في 27 يناير 2008.

- **النصوص التنظيمية:**

1. المرسوم الرئاسي رقم 15-261، المؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة لوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الجزائرية، العدد53، الصادر في تاريخ 08 أكتوبر2015.

2. المرسوم التنفيذي 20-183، المؤرخ في 13 يوليو2020، يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام ولاتصال ومكافحتها، الجريدة الرسمية الجزائرية، العدد40، الصادر بتاريخ 26 ذو القعدة 1441 الموافق18 يوليو2020.

المؤلفات:

أولا: الكتب

1. إبراهيم محمد بن حمود الزنداني، إجراءات الاستدلال والتحقيق الابتدائي في الجرائم الإلكترونية وأثرها على حجية أدلة الإثبات وأحكامها في القانون اليمني والكويتي والقطري: دراسة شرعية وقانونية مقارنة، جامعة قطاني، 2019.
2. أيمن عبد الله فكري، الجرائم المعلوماتية دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، ط1، 2014.
3. خالد بن مرزوق بن سراج العتيبي، الجوانب الإجرائية في الشروع في جرائم المعلوماتية دراسة مقارنة، مكتبة القانون والاقتصاد، الرياض، 2014.
4. سامي حسني الحسيني، النظرية العامة للتفتيش، دار النهضة العربية، القاهرة، 1972.
5. سعد غالب ياسين، مبادئ نظم المعلومات، دار اليازوري العلمية للنشر والتوزيع، عمان، 2018.
6. عبد الصبور عبد القوي علي مصري، منال عبد الله عبد الرحمن، المحكمة الرقمية والجريمة المعلوماتية دراسة مقارنة، مكتبة القانون والاقتصاد، الرياض، ط1، 2012.
7. عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية دراسة قانونية قضائية مقارنة، المركز القومي للإصدارات القانونية، ط1، 2012.
8. عوض محمد عوض، قانون الإجراءات الجنائية، ج1، مؤسسة الثقافة الجامعية، 1989.

9. مبروك بن مرزوق الروقي، القصد الجنائي في الجرائم المعلوماتية دراسة تأصيلية مقارنة، مكتبة القانون والاقتصاد، الرياض، 2013.
10. محمد علي سكيكر، الجريمة المعلوماتية وكيفية التصدي لها، كتاب الجمهورية، (د.ب)، 2010.
11. نوال مجدوب وآخرون، الجريمة المعلوماتية وأثرها على التنمية الاقتصادية، ج1، المركز الديمقراطي العربي، برلين، ألمانيا، ط1، 2020.
12. ياسر الأمير فارق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية دراسة تأصيلية تحليلية ومقارنة للتصنت على المحادثات التلفونية والتي تجري عبر الإنترنت والأحاديث الشخصية نظريا وعمليا، دار المطبوعات الجامعية، الإسكندرية، ط1، 2009.

ثانيا: المقالات

1. أحمد عمراني، "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في التشريع الجزائري والمقارن"، مجلة الحضارة الإسلامية، العدد16، ماي2012.
2. أحمد مسعود، "جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري"، مجلة الحقوق والعلوم السياسية، المجلد10، العدد01، 2017.
3. إسماعيل بن يحي، "التعريف بمراقبة الاتصالات الإلكترونية كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية"، مجلة صوت القانون، المجلد08، العدد02، 2022.
4. اسمهان بن مالك، "خصائص الجريمة المعلوماتية وأسباب ارتكابها"، مجلة البيبان للدراسات القانونية والسياسية، المجلد04، العدد01، 2019.
5. إسمهان عون، "أركان جريمة الإتلاف المعلوماتي وعقوباتها _دراسة مقارنة_"، مجلة الدراسات الإفريقية وحوض النيل، المجلد04، العدد13، اكتوبر 2021.

6. إلهام خرشي، "النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال"، مجلة الأبحاث القانونية والسياسية، المجلد04، العدد01، 2022.
7. أمينة قهواجي، ليلى مطالي، "الإطار المفاهيمي والقانوني للتوقيع والتصديق الإلكترونيين في الجزائر، المشكاة في الاقتصاد التنمية والقانون، المجلد02، العدد02، 2019.
8. بدرة إبراهيم لعور، "الأمن الإلكتروني وفقا للتشريع الجزائري: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال نموذجا"، المجلة العربية للدراسات الأمنية، المجلد32، العدد72، 2018.
9. حفيظ بن غربة، "جريمة الدخول غير المصرح به إلى منظومة معلوماتية في التشريع الجزائري"، مجلة القانون والعلوم السياسية، المجلد03، العدد02.
10. دنيازاد ثابت ، "مراقبة الاتصالات الإلكترونية والحق في حرمة الحياة الخاصة في القانون الجزائري"، مجلة العلوم الاجتماعية والإنسانية، المجلد05، العدد01، 2012.
11. رامي حليم، "جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات"، دراسات وأبحاث، المجلد01، العدد01، 2009.
12. رضا هميسي، "تفتيش المنظومات المعلوماتية في القانون الجزائري"، مجلة العلوم القانونية والسياسية، العدد05، جوان 2012.
13. رمزي حوحو، منيرة بلورغي، "مواجهة الجريمة المعلوماتية في الجزائر"، مجلة الحقوق والحريات، العدد02، 2014.
14. سعاد أجعود، "الحماية الجزائية لتكنولوجيات الإعلام والاتصال في التشريع الجزائري دراسة على ضوء النصوص المستحدثة"، مجلة الرسالة للدراسات والبحوث الإنسانية، المجلد07، العدد04، جوان 2022.

15. سليم عليوة، "الجريمة المعلوماتية"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد06، العدد01، جوان 2021.
16. سهيلة بوزبرة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بين سرية المعطيات الشخصية الإلكترونية ومكافحة الجرائم الإلكترونية"، المجلة النقدية للقانون والعلوم السياسية، المجلد17، العدد02، 2022.
17. الصديق بن بوزة، إيمان بن زيان، "واقع تكنولوجيا المعلومات والاتصال في الجزائر خلال الفترة 2000-2016"، مجلة العلوم الاجتماعية والإنسانية، باتنة01، العدد34، جوان 2016.
18. عائشة شيخي، بوزيان عياشي، "الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وأشكالها الاقتصادية وآليات مكافحتها"، مجلة الدراسات الحقوقية، المجلد02، العدد02، 2015.
19. عبد الكريم محمد ظلام، مروة أحمد بادنجكي، "حماية المصنفات الإلكترونية في الفضاء الرقمي"، مجلة المستقبل للدراسات القانونية والسياسية، المجلد06، العدد02، 2022.
20. عبد الله قيبوعة، مسعود خثير، "الحماية الجزائية للمصنفات الرقمية في التشريع الجزائري"، مجلة الدراسات القانونية المقارنة، المجلد06، العدد02، 2020.
21. عبد النبي مصطفى، "قراءة في النصوص القانونية المنظمة للهيئة الوطنية لوقاية من جرائم تكنولوجيات الإعلام والاتصال ومكافحتها"، دفاتر السياسة والقانون، المجلد13، العدد03، 2021.
22. عز الدين عثماني، "إجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال المعلوماتية"، مجلة دائرة البحوث والدراسات القانونية والسياسية، العدد04، جانفي 2018.

23. عزيزة لرقط، "الحماية الجنائية للتوقيع والتصديق الإلكترونيين في التشريع الجزائري"، مجلة الاجتهاد للدراسات القانونية والاقتصادية، المركز الجامعي تمنغست، الجزائر، المجلد06، العدد01، 2017.

24. فاطمة الزهراء تبوب، "التوقيع والتصديق الإلكترونين في ظل القانون رقم 15-04 المؤرخ في أول فبراير 2015"، حوليات جامعة الجزائر، المجلد29، العدد02، 2016.

25. فريد روابح، "ضمانات حرمة الحياة الخاصة أثناء إجراء مراقبة الاتصالات الإلكترونية"، مجلة الأبحاث القانونية والسياسية، المجلد02، العدد02، 2020.

26. فطيمة جبار، "مراقبة الاتصالات الإلكترونية بين الحظر والإباحة في التشريع الجزائري"، مجلة الدراسات القانونية المقارنة، العدد03، ديسمبر2016.

27. مخلد إبراهيم الزعبي، "فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية" "دراسة قانونية""، المجلة العربية للنشر العلمي، العدد73، تشرين الثاني 2021.

28. نجاة عباوي، "الحماية الجزائية لبطاقة الشفاء الإلكترونية"، مجلة الحقيقة، المجلد16، العدد03، 2017.

29. نسمة بطيحي، "جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي"، مجلة الفقه القانوني والسياسي، المجلد01، العدد01.

30. نوال مغزيلي، "تكنولوجيا الإعلام والاتصال في الجزائر: دراسة للمؤشرات وتشخيص للمعيقات"، المجلة الجزائرية للأمن ولتنمية، العدد12، 2018.

الرسائل الجامعية:

رسائل الماجيستير:

1. أحمد مسعود مريم، "آليات مكافحة جرائم تكنولوجيات الإعلام والاتصال في ضوء القانون رقم 04/09"، مذكرة لنيل شهادة الماجستير، تخصص: قانون جنائي، كلية الحقوق واللوم السياسية، جامعة قاصدي مرباح ورقلة، 2013/2012.

مذكرات الماستر:

1. سمية قبايلي، "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في التشريع الجزائري"، مذكرة مكملة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي للأعمال، جامعة العربي بن مهيدي، أم البواقي، 2017/2016.
2. ماجدة بوطمين، "جريمة إتلاف المعطيات المعلوماتية"، مذكرة لنيل شهادة الماستر في الحقوق، تخصص جنائي للأعمال، جامعة العربي بن مهيدي أم البواقي، 2018/2017.

فهرس

المحتويات

مقدمـــة: 1

تمهيد:..... 6

المبحث الأول: الإطار المفاهيمي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال..... 7

المطلب الأول: مفهوم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال..... 7

الفرع الأول: مفهوم وتطور نظام المعلوماتية في الجزائر 7

الفرع الثاني: تعريف الجرائم المتصلة بتكنولوجيا الإعلام والاتصال 10

المطلب الثاني: الإطار التشريعي للجرائم المتصلة بتكنولوجيا الإعلام والاتصال 13

الفرع الأول: الطبيعة القانونية للجرائم المتصلة بتكنولوجيات الإعلام والاتصال 13

الفرع الثاني: خصوصية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 14

المبحث الثاني: أصناف الجرائم المتصلة بتكنولوجيات الإعلام والاتصال..... 17

المطلب الأول: الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في ظل قانون العقوبات الجزائري..... 17

الفرع الأول: جريمة الدخول أو البقاء غير المصرح له في النظام المعلوماتي 17

الفرع الثاني: جريمة إتلاف نظام المعالجة الآلية..... 21

الفرع الثالث: القواعد المشتركة بين كل جرائم أنظمة المعالجة الآلية للمعطيات 24

المطلب الثاني: الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ظل النصوص القانونية 25

الفرع الأول: جريمة تقليد المصنفات الإلكترونية 26

الفرع الثاني: الجرائم الواقعة على التوقيع والتصديق الإلكتروني 28

الفرع الثالث: الجرائم المنصوص عليها في قانون التأمينات 31

الفرع الرابع: الجرائم المرتبطة بتكنولوجيات الاتصال والإعلام 32

خلاصة الفصل: 34

الفصل الثاني 2

آليات مجابهة الجرائم 2

المتصلة بتكنولوجيات الإعلام والاتصال 2

تمهيـد:..... 36

المبحث الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال. 37

المطلب الأول: تشكيلة الهيئة وتنظيمها 37

الفرع الأول: الشخصية المعنوية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال 37

الفرع الثاني: تشكيلة الهيئة وتنظيمها 38

الفرع الثالث: كيفية سير عملها 43

المطلب الثاني: مهام الهيئة وحدود استقلاليتها..... 43

الفرع الأول: مهام الهيئة 44

الفرع الثاني: حدود الاستقلالية الوظيفية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها 46

المبحث الثاني: القواعد الإجرائية المتبعة بالنسبة للإجراءات المتصلة بتكنولوجيات الإعلام والاتصال 48

المطلب الأول: مراقبة الاتصالات الإلكترونية 48
الفرع الأول: مفهوم مراقبة الاتصالات الإلكترونية 48
الفرع الثاني: الحماية القانونية للاتصالات الإلكترونية..... 50
الفرع الثالث: أشكال مراقبة الاتصالات الإلكترونية 51
الفرع الرابع: الحالات المسموح بها في إجراء مراقبة الاتصالات الإلكترونية..... 52
المطلب الثاني: تفتيش المنظومات المعلوماتية 54
الفرع الأول: مفهوم التفتيش 54
الفرع الثاني: شروط التفتيش في المنظومات المعلوماتية 54
المطلب الثالث: دور مقدمي الخدمات في التحريات والتحقيقات المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال..... 56
الفرع الأول: مفهوم مقدمي الخدمات..... 56
الفرع الثاني: التزامات مقدمي الخدمات 56
خلاصة الفصل: 60
خاتمـــــة 62
قائمة المصادر والمراجع..... 66
فهرس المحتويات 74

ملخص:

إن الثورة التكنولوجية التي يعيشها الإنسان اليوم أفرزت جرائم حديثة تتعلق بتكنولوجيات الإعلام والاتصال، وتتسم هذه الجرائم بالتعقيد والتشابك، وصعوبة معرفة مرتكبيها وبمرونتها. هذا ما أدى إلى المسارعة بسن قوانين وتشريعات تتلاءم مع هذا النوع من الجرائم باعتبار أن القوانين الجزائية القديمة لا تتماشى مع هذه الجرائم نظرا لخصوصيتها.

ولقد قام المشرع الجزائري بإحداث ترسانة من القوانين للوقاية من هذه الجرائم، بحيث تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالإضافة إلى تحديد قواعد إجرائية تخص هذه الجرائم من مراقبة الاتصالات الإلكترونية، تفتيش المنظومة المعلوماتية.

الكلمات المفتاحية: الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، الهيئة الوطنية، القواعد الإجرائية.

Abstract:

The technological revolution in which man is living today has resulted in modern crimes related to information and communication technologies. This is what led to the rush to enact laws and legislation that are in line with this type of crime, given that the old penal laws are not in line with these crimes due to their specificity.

The Algerian legislator created an arsenal of laws to prevent these crimes, so that the National Authority for the Prevention of Crimes Related to Information and Communication Technologies was established, in addition to defining procedural rules related to these crimes from monitoring electronic communications to inspecting the information system.

***Keywords**: crimes related to information and communication technologies, national authority, procedural rules.*