جامعة بلحاج بوشعيب عين تموشنت
كلية الحقوق والعلوم السياسية

القسم: الحقوق
تخصص: قانون عام

مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر في الحقوق تخصص: قانون عام

الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري

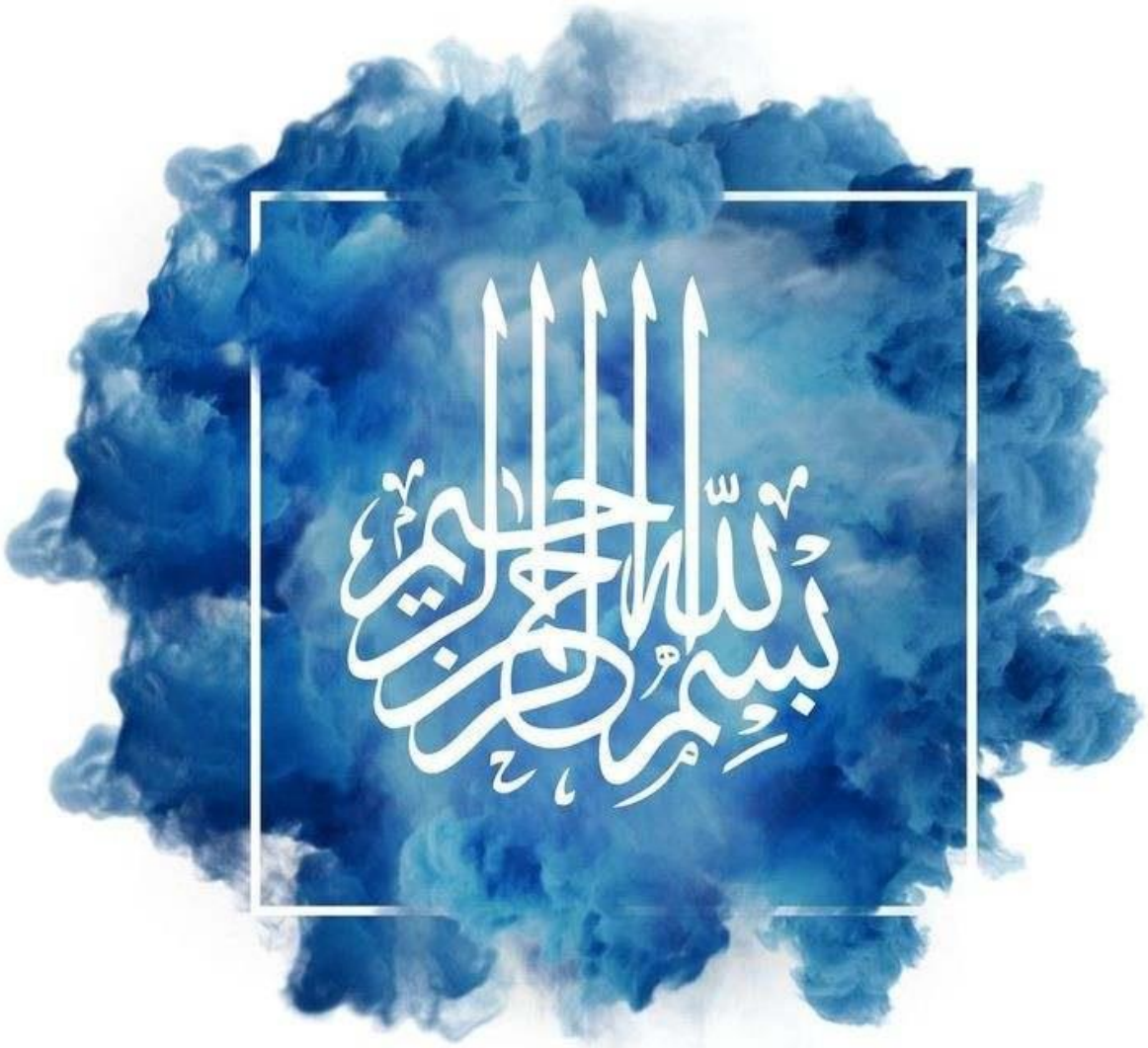
من إعداد الطالبتين:
بخدة خيرة
مولاقان فضيلة

تحت إشراف:
د.روان حسن كمال

لجنة المناقشة:

الرئيس	بن عدة عبد الرحمان	أستاذ مساعد أ	جامعة بلحاج بوشعيب ع-ت
المشرف	روان حسن كمال	أستاذ محاضر ب	جامعة بلحاج بوشعيب ع-ت
مناقشا	قدودو جميلة	أستاذة التعليم العالي	جامعة بلحاج بوشعيب ع-ت

السنة الجامعية: 2023-2024


بسم الله الرحمن الرحيم

بسم الله الرحمن الرحيم

﴿إِنَّ الَّذِينَ كَذَّبُوا بِآيَاتِنَا وَاسْتَكْبَرُوا عَنْهَا لَا تُفَتَّحُ لَهُمْ أَبْوَابُ السَّمَاءِ وَلَا يَدْخُلُونَ الْجَنَّةَ حَتَّى يَلِجَ الْجَمَلُ فِي سَمِّ الْخِيَاطِ وَكَذَلِكَ نَجْزِي الْمُجْرِمِينَ﴾

سورة الأعراف الآية 40

الشكر والتقدير

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ ﴿رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ﴾ سورة النمل الآية 19 .

الشكر لله عز وجل على نعمه ونسأل الله التوفيق والنجاح في الدنيا والآخرة.

اعترافا بالفضل والجميل نتقدم بخالص الشكر وعميق التقدير والامتنان إلى الأستاذ المشرف الدكتور "**روان حسن كمال**" على نصائحه وتوجيهاته التي أنارت دربي، والذي لم يبخل على بمراجعه ومعلوماته القيمة.

كما أخص بالشكر للأستاذة الأفاضل أعضاء لجنة المناقشة كل من الأستاذ "**بن عدة عبد الرحمان**" الأستاذة "**قدودو جميلة**" الذين تحملوا عبء قراءة هذا البحث وقبلوا المشاركة في المناقشة جزآهم الله جميعا أوفر جزاء.

وكل الشكر إلى كل من ساهم معنا في انجاز هذا العمل المتواضع سواء بمعلومة او نصيحة او كلمة طيبة.

الإهداء

إلى من قال فيهما الله عز و جل ﴿وَقَضَىٰ رَبُّكَ أَلَّا تَعْبُدُوا إِلَّا إِيَّاهُ وَبِالْوَالِدَيْنِ إِحْسَانًا ۚ إِمَّا يَبْلُغَنَّ عِندَكَ الْكِبَرَ أَحَدُهُمَا أَوْ كِلَاهُمَا فَلَا تَقُل لَّهُمَا أُفٍّ وَلَا تَنْهَرْهُمَا وَقُل لَّهُمَا قَوْلًا كَرِيمًا﴾

سورة الإسراء الآية 23.

إلى كل من لا يمكن للكلمات أن توفي حقهما الوالدين الكريمين

إلى من استلهمت منه معنى الثبات رفيق دربي زوجي العزيز

إلى نور الحياة و دقات الفؤاد صغاري أنفال ، ريتاج ، زكريا

إلى من كانوا سندي و عضدي في الحياة إخوتي و عائلاتهم

والى كل الأهل و جميع الأصدقاء والزملاء

خيرة

الإهداء

إلى من علمني العطاء بدون انتظار، إلى من احمل باسمه بكل فخر، ارجوا من الله أن يمدد في عمرك وان يرزقك الصحة والعافية

..... أبي العزيز .....

إلى ملاكي وقدوتي في الحياة، إلى معنى الحب والحنان إلى بسمة الحياة وسر الوجود، إلى من كان دعائها سر نجاحي، وحنانها بلسم جراحي، إلى كل من في الوجود بعد الله والرسول ﷺ

.... أمي الغالية .....

إلى سندي وقوتي وملاذي بعد الله، إلى من اظهر لي أجمل ما في الحياة وساعدني في مشواري الدراسي.

..... زوجي الغالي.....

إلى أملى المتجدد في الحياة ابنتي الغالية "**لجين تسنيم**"

إلى أختي وأخي حفظهم الله ورعاهم، إلى جميع أهلي وأقاربي الذين تمنوا لي الخير.

إلى الأخوات التي لم تلدهم أمي .....صديقاتي .....

فضيلة

قائمة أهم المختصرات

ج.ر: جريدة الرسمية

ج: الجزء

د.س.ن: دون سنة نشر

ص: صفحة

ط: الطبعة

ع: العدد

ف: فقرة

ق.الإ.ج .ج. م .م : قانون الإجراءات الجزائية الجزائري المعدل والمتمم

ق.ع.ج.م.م : قانون العقوبات الجزائري المعدل والمتمم

م: مجلد

Art :Article

Éd: Édition .

N: Numéro

O.p.cit : ouvrage précédemment

P: Page

مـــــقدمـــــة

مقدمة

عرف العالم خلال النصف الثاني من القرن العشرين ثورة جديدة اصطلح على تسميتها بالثورة المعلوماتية، ثورة هائلة في مجال تقنية المعلومات، بلغت ذروتها باختراع الحاسب الآلي الذي غزى المؤسسات والمرافق وحتى البيوت، وتوجت بظهور شبكة المعلومات الدولية "الانترنت"، هذا التطور المتلاحق الذي زاوج بين قطاعي تكنولوجيا المعلومات والاتصالات خلق بيئة افتراضية تتدفق فيها المعلومات والاتصالات دون أي اعتبار للحدود أو السيادة.[1]

حيث أن التقنيات العالية التي تقوم عليها الثورة المعلوماتية من استخدام للحواسيب والشبكات المعلوماتية شكلت قفزة نوعية حضارية،[2] وجعلت من المعلومات قوة لا يستهان بها في أيدي الدول والأفراد على حد سواء، وأضحت بذلك القطاعات المختلفة تعتمد وبشكل أساسي في تسيير عملها على الأنظمة والشبكات المعلوماتية لما تتميز به من دقة وسرعة في تجميع المعلومات وتخزينها ومعالجتها ،ومن تم نقلها وتبادلها بين الأفراد والمؤسسات المختلفة داخل الدولة الواحدة وخارجها، وهكذا صارت الأنظمة مستودعا لأسرار الأشخاص سواءا المتعلقة بحياتهم الشخصية أو بنشاطاتهم وأعمالهم المالية والاقتصادية وبالمقابل أيضا مستودعا لأسرار الدول العسكرية الاقتصادية والسياسية وغيرها من الأسرار التي تكتسي القدر الكبير من الأهمية والسرية.

وعلى الرغم من هذا الجانب المشرق والايجابي لعصر المعلوماتية، إلا انه قد أحدث من الجانب الأخر انعكاسات سلبية نجمت عن إساءة استخدام الأنظمة واستغلالها على نحو غير شرعي ولأغراض إجرامية تهدف إلى إلحاق الضرر بمصالح الأشخاص والمؤسسات وتصل إلى تهديد الدولة بحد ذاتها، هذه الانتهاكات غير المشروعة عرفت بالجريمة المعلوماتية، التي غيرت الجريمة من صورتها التقليدية المادية إلى أخرى معنوية يسهل إخفاء معالمها ويصعب تتبع مرتكبها وإقامة الدليل عليه ويقف فيها المحقق التقليدي عاجزا عن التعامل معها.

ذلك أن الإجرام المعلوماتي يقوم على الاحتيال والمساس بالبيانات والمعطيات، ويرتكب باستخدام وسائل مختلفة وبواسطة أساليب حديثة ومبتكرة مخالفة للقانون وهو يأخذ عديد الأشكال ولا ريب أن جرائم المساس بالأنظمة المعالجة آليا من ابرز صوره، ولا جدل يثار في اعتبار هذا النوع من الجرائم من أخطر وأعقد الجرائم على الإطلاق والتي تأتي في مقدمة الأشكال الجديدة للجريمة المنظمة، وكل هذا نابع من

[1]– نبيلة بن عائشة، ***الجريمة الالكترونية***، مداخلة في إطار ندوة وطنية منظمة بكلية الحقوق جامعة الجزائر 1، بتاريخ 2019/11/19، تحت رئاسة كوثر مازوني، منشورة بمجلة الندوة الوطنية، ط 1، دار الخلدونية للنشر والتوزيع، الجزائر 2022، ص 360.

[2]– نهلا عبد القادر المومني، ***الجرائم المعلوماتية***، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص 13.

طبيعتها المتميزة والمعقدة من حيث ذاتية أركانها وحداثة أساليب ارتكابها والبيئة التي تجري فيها وخصوصية مرتكبيها ووسائل كشفها.

واتساقا مع ما سبق ذكره فان المساس بأنظمة المعالجة الآلية للمعطيات هي جريمة معلوماتية، تنشأ في الخفاء في عالم افتراضي، كما أنها سهلة الارتكاب لا تخلف أي أثار محسوسة، ويقترفها مجرمون أذكياء يمتلكون المعرفة التقنية للتعامل في مجال المعالجة الآلية للمعطيات ويتمتعون بمهارات وخبرات عالية فضلا على أنها جرائم عابرة للحدود تتم عبر شبكة اتصال لا متناهية غير مرئية بإمكان أي شخص الولوج إليها حول العالم.[1]

إذ أن الخصائص التي تتميز بها جرائم المساس بأنظمة المعالجة الآلية للمعطيات خلق صعوبة في التعامل مع النشاطات الإجرامية المترتبة عنها وتكييفها على أساس النصوص القانونية التقليدية، ذلك أنها تمثل ضربا من ضروب الذكاء الإجرامي الذي أوجب على مختلف الأنظمة التشريعية الجزائية تطوير وتحديث تشريعاتها التقليدية بذكاء يضاهي الذكاء الإجرامي،[2] فكان لابد من وضع أطر قانونية ملائمة جديدة وإدخال تعديلات على القوانين السارية المفعول بما يتلاءم مع الوضع الجديد، بصياغة نصوص قانونية تكسر الصعوبات التي يطرحها هذا النمط الجديد من الإجرام، وتحمي الأنظمة المعلوماتية، وتردع إساءة استعمالها، ذلك أن التقدم العلمي والتكنولوجي لا يمكن أن يسير وحده بمعزل عن أي تقدم قانوني يواكبه ويحافظ عليه ويكفل حمايته، كما أن التفاعل الرهيب مع تكنولوجيا الإعلام والاتصال وبوجود ثغرات في الحماية التقنية عزز دور الحماية الجزائية ودفع بأغلب التشريعات لسد النقص وبسط قوانين ردعية في شقيها الموضوعي والإجرائي.

وبالنسبة للوضع في الجزائر باعتبارها واحدة من الدول التي سايرت التطور التكنولوجي بإيجابياته وسلبياته فهي بذلك معنية بالتصدي للإجرام المعلوماتي ومكافحته، فكان لابد على المشرع الجزائري من أحدث إطار قانوني لسد كل الفراغات في الشقين التجريمي والعقابي دون إغفال الشق الإجرائي، وذلك برصد إجراءات جزائية تحظى بالخصوصية وتتلاءم مع الطبيعة التقنية للجريمة المستحدثة مع الاحتفاظ بالإجراءات الكلاسيكية التي تبقى قاسما مشتركا مع الجرائم التقليدية.

هذا وان الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات تحظى بأهمية بالغة ذلك أنها ظاهرة من ظواهر الإجرام التقني المستحدث والذي لا يزال في حاجه ماسة إلى مزيد من البحث والدراسة خاصة وأن هذه

---

[1]– يوسف مناصرة، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات –ماهيتها، صورها، الجهود الدولية لمكافحتها**،– دراسة مقارنة–، ط1 ، دار الخلدونية، الجزائر، 2018، ص 11.

[2]– عثمان خرشي، **إجراءات سير الدعوى العمومية في الجرائم المعلوماتية**، أطروحة دكتوراه ، قانون جنائي وعلوم جنائية كلية الحقوق والعلوم السياسية جامعة مولاي طاهر سعيدة، السنة الجامعية 2020–2021، ص 04.

الجرائم تشكل خطر كبيرا يهدد مختلف المعاملات الالكترونية التي يقوم بها الأفراد والمؤسسات والهيئات على حد سواء، كما أن آثارها لم تتوقف على المستوى الداخلي، بل امتدت لتشمل المستوى الدولي.

يضاف إلى ذلك أن الحماية الجزائية أضحت مطلب أساسي ينشده جميع مستخدمي نظام المعالجة الآلية للمعطيات من اجل ضمان حماية خاصة لأمن النظم المعلوماتية ولكافة المعلومات التي تحتويها، في الوقت الذي يتنامى فيه الاعتماد على هذه النظم وظهور ما يعرف ببنوك المعلومات، بحيث أصبحت المعلومات المخزنة في تلك النظم عرضة لمخاطر إساءة الاستخدام والوصول إليها بطرق غير مشروعة أكثر من أي وقت مضى إذا ما تم مقارنتها بالوضع التقليدي الذي تكون فيه المعلومات والبيانات في سجلات ورقية تحفظ في خزائن خلف أبواب مغلقة.[1]

وما يبرز أهمية هذه الدراسة الأسباب التي دفعت بنا إلى اختيار هذا الموضوع، هي كونه من المواضيع المستحدثة، ذات الطابع القانوني الممزوج بالطابع التقني المرتبط ارتباطا واضحا مع التطور التكنولوجي المعلوماتي، ونضيف للأسباب السابقة، الاهتمام بمعالجة الجرائم المرتبطة بالعالم الافتراضي الرقمي وذلك بغية الكشف عن الملامح والجوانب المختلفة لهاته الظاهرة الإجرامية، والإحاطة بكافة الأحكام القانونية المتعلقة بردعها ومكافحتها، ذلك أن التطورات التكنولوجية الحديثة، وكذا ظهور المعاملات الالكترونية وانتشارها على نطاق واسع وغير محدود، وضع الدول أمام عقبت قانونية متعددة، خصوصا فيما يتعلق بالاعتداءات الواقعة على الأنظمة المعلوماتية، فأصبحت مواجهة هذه الجرائم واقعا مفروضا من خلال تجريم الاعتداءات الواقعة على المعلومات، خصوصا ما تعلق منها بأنظمة المعالجة الآلية للمعطيات وعليه فإن موضوع الدراسة يقتضي البحث في مختلف الأحكام الموضوعية المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، على ضوء ما تضمنه قانون العقوبات، الدراسة أيضا تتطلب التوقف عند وجوبية تبيان مختلف الإجراءات والجهود المبذولة للوقاية ومكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

أما عن الصعوبات التي واجهتنا في دراسة الموضوع، فتكمن أساسا في ما يتميز به الموضوع من مصطلحات تقنية خارج التخصص إضافة إلى شح المادة العلمية فيما يخص المعالجة الآلية للمعطيات إذ أن جل الدراسات السابقة التي خاضت في الموضوع عالجته كجزئية باعتباره جريمة من جرائم المعلوماتية كما أهملت في غالب الأحيان تسليط الضوء على الشق الإجرائي، وكذلك واجهنا صعوبة في تحديد خطة البحث المناسبة ذلك أن الموضوع يحتوي على محاور كثير ولا يمكن إدراجها جميعها ضمن دراسات مذكرة ماستر المقيدة بعدد معين من الصفحات.

[1]– البركه الطيبي، **الحماية الجنائية لأنظمة المعالجة الإلية للمعطيات دراسة مقارنة**، أطروحة دكتوراه ، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة احمد دارية ،أدرار، الجزائر،السنة الجامعية 2020–2021، ص 10.

لكل ما سبق عرضه وباعتبار الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات أضحت مطلبا وغاية تسعى جل التشريعات لضمانها من ذلك التشريع الجزائري الذي سعى جاهدا لمواكبة جميع المستجدات الراهنة بتكييف القوانين وفقا لذلك، هذا ما يقودنا إلى التساؤل عن **مدى فعالية ونجاعة النصوص القانونية التي رصدها المشرع الجزائري للتصدي للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؟**

هذا وتتفرع عن هذه إشكالية إشكاليات فرعية تتمحور أساسا حول:

- ما مدى قدرة القواعد الموضوعية التي سنها المشرع الجزائري في مكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات؟
- ما مدى كفاية الأحكام الإجرائية في مواجهة هذا النوع من الإجرام؟

وبغية الإجابة على الإشكالية الرئيسية المثارة وما تمخض عنها من إشكاليات فرعية تم الاعتماد على المنهج التحليلي الذي يتماشى مع طبيعة الموضوع المطروح كون الدراسة ستعتمد على تحليل أهم النصوص الآلية للمعطيات المنظمة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات في مختلف التشريعات وكذا رصد هاته الجرائم وفقا لما نص عليه التشريع الجزائري، يضاف إلى ذلك الاستعانة بالمنهج المقارن على سبيل الاستئناس ، و ذلك عند التعرض لبعض الصكوك الدولية ذات الصلة بموضوع الدراسة.

أما من الناحية الهيكلية وتماشيا مع إشكالية البحث المثارة فقد قسمت الدراسة إلى فصلين، حيث خصص الفصل الأول لتناول مختلف القواعد الموضوعية المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ، أما الفصل الثاني من هذه الدارسة فيتضمن الإطار الإجرائي لمكافحة هذا النوع من الجرائم.

الفصل الأول:

الأحكام الموضوعية لمواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات

كان للتقدم التكنولوجي الهائل في مجال تكنولوجيا الإعلام والاتصال الأثر البالغ في اعتماد التقنية المعلوماتية في كافة جوانب الحياة، حتى أصبح لا غنى للإنسان عنها، لكن بالمقابل نتج عن سوء استخدامها طائفة جديدة من الجرائم تستهدف المعلومات وبرامج الحاسوب، وهو الجانب المظلم للمعلوماتية[1] هذا الأمر الذي أعطى مفهوم جديد للجريمة والمجرم على حد سواء لارتكابها داخل بيئة افتراضية متاحة للجميع تتعدد فيها الوسائل وتختلف فيها الأهداف، وفي خضم هذا النشاط الإجرامي غير المسبوق، أصبح لزاما على رجال القانون أن يكونوا بالمرصاد لهذه الظاهرة الإجرامية المستحدثة التي تختلف في مفهومها وأركانها وتقنيات ارتكابها، ويتميز الجناة فيها عن الجرائم التقليدية المعروفة.[2]

إن تطور أنواع وأساليب الإجرام المعلوماتي الذي رافق التطور التكنولوجي عزز الحاجة الماسة إلى إرساء قواعد حماية قانونية في مواجهة هذا النوع المستحدث من الجرائم لاسيما تلك التي تمس بالمعطيات المعالجة آليا بالنظر لتوجه غالبية الدول لرقمنه كافة قطاعاتها، حيث سارعت مختلف التشريعات إلى حماية أنظمتها المعلوماتية على غرار المشرع الجزائري سواء بتبني المعاهدات والاتفاقيات الدولية من جهة وسن قوانين داخلية من جهة ثانية تصب كلها في إطار مكافحة الإجرام المعلوماتي.

المشرع الجزائري تدخل بوضع حماية جزائية موضوعية لأنظمة المعالجة الآلية للمعطيات من خلال عدة نصوص لاسيما قانون العقوبات المعدل والمتمم3، بداية باستحداثه القسم السابع مكرر بعنوان المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات المعدل و المتمم بموجب القانون 04/15 المؤرخ في 10 نوفمبر 2004 [4]، بمقتضى المواد 394 مكرر إلى 394 مكرر 8 حيث جرم من خلالها الاعتداءات الواردة على نظام المعالجة الآلية للمعطيات وحدد لكل فعل منها ما يقابله من الجزاء، مع إضفاء بعض التعديلات على المواد السالفة الذكر بموجب القانون 16-02 المؤرخ في 19 جوان 2016[5] ،و القانون 06/24 المؤرخ في 28افريل2024 [6]، بالإضافة إلى ذلك قام بوضع إطار قانوني أكثر ملائمة وانسجاما مع

---

[1]– لحسن ناني ، **التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية**، النشر الجامعي الجديد، تلمسان، الجزائر، 2018، ص 10.

[2]–يزيد بوحليط، **الجرائم الالكترونية والوقاية منها في القانون الجزائري**، ، دار الجامعة الجديدة، الإسكندرية، مصر،2019 ، ص 11.

[3]- الأمر رقم 66-156 المؤرخ في 08جوان 1966 المتضمن قانون العقوبات ، ج ر 49 المؤرخة في 11 جوان 1966 .

[4]- القانون رقم 15-04 ، المؤرخ في 10 نوفمبر 2004 ،ج ر 71 المؤرخة في 10 نوفمبر 2004 ، يعدل و يتمم الأمر رقم 66-156 المؤرخ في 08جوان 1966 المتضمن قانون العقوبات.

[5]- القانون 16-02 ، المؤرخ في 19جوان 2019 ، ج ر 37 المؤرخة في 22 جوان 2016 ج ر 37 المؤرخة في 22 جوان 2016 ، يعدل و يتمم الأمر رقم 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات.

[6]- القانون 24-06 ، المؤرخ في 28افريل 2024 ج ر 30 المؤرخة في 30افريل.2024 يعدل و يتمم الأمر رقم 66-156 المؤرخ في 08جوان 1966 المتضمن قانون العقوبات .

خصوصية الجريمة الافتراضية بسنه القانون 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،[1] كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية الجزائري [2]وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة بتحديد مصدرها والتعرف على مرتكبها،[3] إضافة إلى عديد القوانين المكلمة ذات الصلة، وبناءا على ما سبق، فإننا سنقوم بتقسيم الدراسة في هذا الفصل إلى مبحثين تناول خلال المبحث الأول خصوصية مفاهيم المساس بأنظمة المعالجة الآلية للمعطيات وإرساء قواعد التجريم، أما المبحث الثاني فقد خصصناه لدراسة أوجه الاعتداء على أنظمة المعالجة الآلية للمعطيات و جزاءات المساس بها من خلال إبراز صور هذه الجرائم والجزاءات المترتبة على المساس بأنظمة المعالجة الآلية لها.

[1]- القانون 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر47، المؤرخة في 16 أوت 2009.

[2]- الأمر رقم 66-155 المؤرخ في 08جوان 1966 المتضمن قانون الإجراءات الجزائية ، المنشور بالجريدة الرسمية، العدد 48 ، المؤرخة في 10 جوان 1966 المعدل و المتمم.

[3]- البركه الطيبي، **المرجع السابق** ، ص 16.

المبحث الأول: المساس بأنظمة المعالجة الآلية للمعطيات خصوصية المفاهيم وتأصيل قواعد التجريم

أدى التقدم الهائل الذي أضحى واضحا في المجال التكنولوجي، والزيادة في عدد مستخدمي التكنولوجيا والأجهزة الحديثة من أشخاص طبيعية أو هيئات وأشخاص معنوية، إلى ظهور فئة جديدة من الإجرام المرتبطة بالتكنولوجيا، وأصبحت بذلك الجريمة في مجال المعطيات الرقمية بأبعادها ومظاهرها الحديثة تشكل تهديدا مباشرا لا تقتصر عواقبه على الأفراد والمجتمعات فحسب بل امتدت أثارها لتهدد دول برمتها بالنظر لتزايد نسب ارتكاب هذه الجريمة في الآونة الأخيرة وعدم ثباتها مقارنة بالتطورات التكنولوجية المستمرة، الأمر الذي انعكس على مضامين القوانين والأنظمة، حتى تتماشى مع طبيعة الجريمة المستحدثة ومعطياتها وآثاره،[1] وبناء عليه كانت الحاجة ملحة لتحديد وضبط المفاهيم لما لهذه الجرائم من خصوصية تميزها عن باقي الجرائم التقليدية وبالمقابل تحديد أسس قيام المسؤولية الجزائية لمرتكبيها، فكان لابد من وجود تطور قانوني لاسيما على المستوى الجزائي لإحداث توازن بين تطور مستوى الجرائم الماسة بالمعطيات الرقمية وبين تطور أساليب مكافحتها، كل ذلك جعل المشرع الجزائري على غرار نظرائها من المشرعين يبحث في مدى نجاعة الأنظمة والقوانين السائدة ومعرفة مكان النقص والقصور من اجل صياغة تشريعات تضمن تحقيق أقصى فعالية ممكنة لمكافحة هذه الجريمة وافرد جرائم المساس بأنظمة المعالجة الآلية للمعطيات بجملة من الأحكام الموضوعية، ضمن القسم السابع مكرر من قانون العقوبات المعدل والمتمم بعنوان **"المساس بأنظمة المعالجة الآلية للمعطيات"**، من المواد 394 مكرر الى 394 مكرر07، متأثرا بجملة من الاتفاقيات المبرمة في هذا الشأن والتي من أهمها "اتفاقية بودابست لمكافحة الإجرام المعلوماتي كما سن في فترات متعاقبة جملة من القوانين المكملة ذات الصلة، وعموما هذا ما سنخصه بالدراسة والتحليل ضمن هذا المبحث المقسم إلى مطلبين، المطلب الأول بعنوان "الإطار المفاهيمي لجرائم المساس بأنظمة المعالجة الآلية للمعطيات" والمطلب الثاني بعنوان "إرساء قواعد تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات".

المطلب الأول: الإطار المفاهيمي لجرائم المساس بأنظمة المعالجة الآلية للمعطيات

أولى فقهاء العصر الحديث عناية خاصة ونوعية بالجرائم المعلوماتية بما في ذلك الجرائم التي تمس الأنظمة المعلوماتية المعالجة آليا، حيث أفرد لها علما خاصا أطلق عليه **"علم الإجرام المعلوماتي"**، هذا الأخير أصبح يتردد ويتبلور على ألسنة الكثير من الفقهاء لدرجة الإلحاح على مزيد من البحث والتقصي والدراسة حوله وذلك بغية الإحاطة بكافة جوانب هذا النوع من الإجرام الذي يختلف اختلافا شاسعا عن

[1]– بسمة مامن، "***جرائم المساس بأنظمة المعالجة الالية للمعطيات في التشريع الجزائري***"، مجلة الحقوق والعلوم السياسية، جامعة خنشلة ، الجزائر، م09 ،ع01، 2022، ص 487.

الجرائم التقليدية[1]،وهو ما يحتم التطرق بالدراسة لخصوصية المفاهيم المتعلقة بهذا النوع من الإجرام، باعتبارها إحدى الجرائم المستحدثة التي تتمتع بخصائص تميزها عن غيرها من الجرائم التقليدية ، كما أنّ المجرم فيها يتمتع بمهارات متفردة كما يلجأ إلى استخدام تقنيات وأساليب خاصة في اعتدائه على عناصر ومعطيات مثيرا جدلا فقهيا في مدى وجوبيه الحماية التقنية السابقة لقيام المسؤولية الجزائية، هذا ما سيتم التطرق إليه ضمن هذا المطلب المقسم إلى أربع فروع.

الفرع الأول: تعريف نظام المعالجة الآلية للمعطيات وتحديد طبيعته القانونية.

إن التقدم التكنولوجي المتزايد في مجال المعلوماتية وما يتطلبه من ضرورة القيام بتوفير وجمع ومعالجة وتبادل المعلومات في وقت واحد أدى إلى ابتكار أنظمة المعالجة الآلية للبيانات، والتي تقوم على مجموعة من العناصر أو المكونات المترابطة التي تعمل معا لتحقق هدف معين، وهو معالجة المعطيات، هذا ونلمس أن غالبية التشريعات تجنبوا الخوض في مسألة وضع تعريف تشريعي محدد لنظام المعالجة الآلية للمعطيات تاركين ذلك إلى الفقه والقضاء، وأتجه معظمهم إلى تعريف النظام المعلوماتي في حد ذاته، نظرا لكون التعريف التقني للنظام المعلوماتي يتفق مع تعريف نظام المعالجة الآلية للمعطيات.[2]

البند الأول: التعريف الفقهي والقانوني لأنظمة المعالجة الآلية للمعطيات

عرف الفقيه خالد ممدوح إبراهيم نظام المعالجة الآلية للمعطيات بأنه" مجموعة العناصر المتداخلة والمتفاعلة مع بعضها البعض والتي تعمل على البيانات والمعلومات ومعالجتها وتخزينها وبثها وتوزيعها بغرض دعم صناعة القرارات والتنسيق وتأمين السيطرة على المنظومة إضافة لتحليل المشكلات للموضوعات المعقدة".[3]

في حين ذهب جانب من الفقه الفرنسي الى تعريفه بانه: "كل وحدة أو مجموعة من الوحدات القادرة على معالجة أو تخزين البرامج والمعلومات أو أجزاء الدخول أو الخروج أو الارتباط والتي تهدف الى نتيجة محددة في هذه المجموعة وتكون موضوعا للحماية بنظام الأمن".[4]

---

[1]– عثمان خرشي، **المرجع السابق** ، ص 21.

[2]– البركه الطيبي، **المرجع السابق** ، ص 20.

[3]– نسيمة جدي ، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات**، رسالة الماجستير في القانون الجنائي، كلية الحقوق جامعة وهران،الجزائر ،السنة الجامعية 2013– 2014، ص 17 ،نقلا عن خالد ممدوح إبراهيم، "**التقاضي الإلكتروني**" (دط)، دار الفكر الجامعي، الإسكندرية ،2009 ص298 .

[4]– بوبرقيق عبد الرحيم،" ***مفهوم أنظمة المعالجة الآلية للمعطيات في الجرائم المحددة في المواد 394 مكرر إلى 394 مكرر 2من قانون العقوبات الجزائري"*** ، مجلة الدراسات والبحوث القانونية، جامعة المسيلة،الجزائر، م4، ع1، جوان 2019، ص 357.

من جهة أخرى عرف مجلس الشيوخ الفرنسي نظام المعالجة الآلية للمعطيات على أنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تكون كل منها الذاكرة، المعطيات، أجهزة الإدخال والإخراج و أجهزة الربط التي تربط بينها مجموعة من العلاقات التي عن طريقها تم تحقيق نتيجة معينة، وهي معالجة المعطيات، على أن يكون هذا المركب خاضعا لنظام المعالجة الفنية".[1]

على المستوى الدولي عرفت الاتفاقية الدولية لمكافحة إجرام تقنية المعلومات (إتفاقية بودابست) نظام المعالجة الآلية للمعطيات بموجب الفقرة (أ) من المادة الأولى من الفصل الأول على أنه: "كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة والتي يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى تنفيذا لبرنامج معين بأداء معالجة آلية للبيانات".[2]

وفي القانون العربي الموحد لمكافحة سوء استخدام تكنولوجيات المعلومات والاتصالات في صيغته المعدلة نجد في مادته الأولى تعريفا لنظام المعالجة الآلية للمعطيات على أنه: "كل مجموعة مركبة من وحدة أو عدة وحدات للمعالجة سواء كانت متمثلة في ذاكرة الحاسوب وبرامجه أو وحدات الإدخال والإخراج والاتصال التي تساهم في الحصول على نتيجة معينة".[3]

وعرف النظام المعلوماتي من طرف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بأنه "مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات".[4]

أما على المستوى الداخلي فان المشرع الجزائري تجنب في بداية الأمر أن يضع أي تعريف لنظام المعالجة الآلية للمعطيات ضمن قانون العقوبات باعتبار العناصر التي يتكون منها النظام من معطيات وبرامج تخضع لتطور تكنولوجي مستمر ومتلاحق وتنشأ في بيئة افتراضية، غير أنه استدرك الامر اثر صدور القانون رقم 09-04 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم

---

[1]- محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الالي**، دار الجامعة الجديدة، الإسكندرية، مصر،2007، ص 26.

[2] Art 1er de la convention sur la cybercriminalité adoptée par la Comité des ministres du Conseil de l'Europe le 8 novembre 2001 prévoit que : « **L'expression 'système informatique' désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données** ».

اتفاقية على الرابط الالكتروني الاتي: https://www.coe.int/fr/web/cybercrime/the-budapestconvention

تاريخ الاطلاع 29-03-2024 ، 21:30 سا .

[3]- نعيم سعيداني،**آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة ماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر،السنة الجامعية 2016-2017، ص 45.

[4]- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، الأمانة العامة لجامعة الدول العربية، إدارة الشؤون القانونية العربية، لشبكة القانونية، www.arablegalnet.org ، تاريخ الاطلاع 29-01-2024 ، 23:00 سا .

المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،[1] حيث تضمنت أحكام المادة الثانية، تحت عنوان المصطلحات ما يلي: يقصد في مفهوم هذا القانون بما يأتي:

الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.[2]

جاء هذا التعريف واسعا وشاملا لجميع الجرائم المعلوماتية البحثة الممثلة في جرائم المساس بأنظمة المعالجة الآلية للمعطيات وكل الجرائم المرتكبة بوسيلة معلوماتية أو اتصال إلكتروني، وهو عبارة أيضا عن تعريف ينصب على وصف للسلوك المجرم المرتبط بالمنظومة المعلوماتية وربطها بوسيلة ارتكابها المنحصرة في المنظومة المعلوماتية أو نظام للاتصالات الإلكترونية، بل أكثر من ذلك أن هذا التعريف حاول أن يحيط بجميع الجرائم التي من الممكن أن تقع في هذه البيئة، بهدف تجنب حصر هذه الجريمة في مجال ضيق يسمح بإفلات العديد من صورها من دائرة التجريم.[3]

البند الثاني: الطبيعة القانونية الخاصة لأنظمة المعالجة الآلية للمعطيات .

تختلف الجريمة الواقعة على النظام المعلوماتي باختلاف الزاوية التي يقع عليها الاعتداء، فمن ناحية قد يكون هذا الأخير نفسه هو وسيلة للجريمة وأداة لتنفيذها، ومن ناحية أخرى قد يكون هو موضوعا للجريمة أو محلا لها، فنكون في الحالة الأولى بصدد جرائم تقليدية بحثة يكون فيها النظام المعلوماتي هو أداة ارتكاب الجريمة المعلوماتية ووسيلة تنفيذها، حيث يمكن للجاني استخدام الحاسوب لارتكاب جرائم السرقة أو النصب أو تزوير المحررات المعلوماتية عن طريق التلاعب في معطيات الحاسوب، أما الحالة الثانية فالجرائم المعلوماتية تتفق والجرائم التقليدية البحثة من ناحية وجود اعتداء على المكونات المادية للنظام المعلوماتي فإذا كان الاعتداء يقع على البرامج والمعطيات، أي الجانب المعنوي عن طريق السرقة أو التقليد أو محو أو تغيير أو إضافة في المعطيات أو إفشاء لمحتوياتها فهذا ما يشكل جرائم المساس بأنظمة المعالجة الآلية للمعطيات،[4] وعليه فإنه إذا كان النظام المعلوماتي هو المستهدف في الجريمة المرتكبة نكون أمام جرائم نظام المعالجة الآلية للمعطيات.

---

[1]– البركه الطيبي، **المرجع السابق** ، ص 27.

[2]– المادة 02 من القانون 09–04 – السالف الذكر– .

[3]– رشيدة بوكر، **جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن**، ط1، منشورات الحلبي الحقوقية لبنان، 2012، ص 44.

[4]– يوسف مناصرة، **المرجع السابق** ، ص 19– 20.

هذا وتعتبر جرائم المساس بأنظمة المعالجة الآلية باعتبارها صورة من صور الجرائم المعلوماتية من أخطر الجرائم المستحدثة التي ظهرت نتيجة التطور الهائل في مجال التقنية العالية وبالتالي فإن أمر تحديد طبيعة هذا النمط من الإجرام يعتريه صعوبات ترجع إلى خصوصية هذا النوع من الجرائم التي تطال المعلومات.

وعليه وفي إطار محاولة تحديد الطبيعة الخاصة لهذا النوع من الجرائم اتجه بعض الفقهاء إلى القول أنها ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي لان معظم حالات ارتكابها يرتبط بـمجال المعالجة الإلكترونية للبيانات، كما يشير أيضا إلى أنّ تحديد هذه الطبيعة تستلزم إضافة مجال معالجة الكلمات أو معالجة النصوص، والتعامل أيضا مع مفردات جديدة مثل البرنامج والبيانات مما يجعل القانون الجنائي عاجز عن مواجهة هذا التطور المعلوماتي لعجز نصوصه، وللتطور السريع المتلاحق في حقل المعلوماتية.

مع الإشارة في ذات الاتجاه ان الجاني في هذا النمط من الإجرام يتجه للاعتداء على المعلومات بما تمثله من أسرار وبيانات وأموال مما يجعل أمر تحديد المال المعلوماتي أيضا من الأمور التي تتطلب تحليلا وتأهيلا قانونيا خاصا وفقا للتطور التقني المتسارع، بحيث تصبح البيانات باعتبارها جزء من معطيات الحاسب الآلي لها صفة المال الذي تغير وصفه وأصبح يرد على أي شيء له قيمة اقتصادية.[1]

ومن تم فان مصطلح نظام المعالجة الآلية للمعطيات مصطلح ينطبق على أي نظام مهما كان مسماه يحتوي على مجموعة من العناصر المرتبطة مع بعضها البعض تهدف إلى تحقيق نتيجة معينة، وهي معالجة المعطيات، ويترتب على المساس بالمكونات المادية أو المعنوية مساسا بالنظام، ولا تشكل جريمة إلا إذا كانت هذه المكونات المادية أو المعنوية تشارك في تطبيقات فعلية داخل نظام كامل أو لها القدرة على ذلك ويكون لها دور في تحقيق الغاية الأساسية وهي معالجة المعطيات ويدخل في ذلك شبكة الانترنت، البريد الالكتروني، موقع الانترنت، البطاقات الكترونية، بطاقة الائتمان البنكية، القرص النقال والمرن والمضغوط، الأشرطة الممنغطة ....وهي كلها تعد أنظمة معلوماتية[2].

الفرع الثاني: خصوصية جرائم المساس بأنظمة المعالجة الآلية للمعطيات

تعتبر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من الجرائم المعلوماتية وهي بذلك تتميز عن الجرائم التقليدية التي ترتكب في العالم المادي، حيث تتسم بطابع خاص يجعل منها ظاهرة إجرامية حديثة لم يعرفها العالم من قبل، ويتجلى ذلك من حيث خصائص الجريمة ذلك انها جريمة صامتة وسريعة عابرة

[1]– محمود محمد عبابنة، **جرائم الحاسب وأبعادها الدولية**، ط 1، دار الثقافة للنشر والتوزيع، عمان،الأردن، 2009، ص 21.

[2]– البركه الطيبي، **المرجع السابق**، ص 29.

للحدود صعبة الاكتشاف (البند الأول)، كما أن المجرم فيها يمتلك من الصفات ما يميزه عن المجرم التقليدي، بحيث يكون في الغالب شخص ذكي ذو خبرة فائقة في مجال الحاسب الآلي (البند الثاني).

البند الأول: خصائص الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات

تتميز الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات باعتبارها جريمة معلوماتية عن غيرها من الجرائم التقليدية بمجموعة من السمات والخصائص تكمن أساسا في كونها جريمة ناعمة ترتكب في صمت ودون أي عنف كما أنها تتميز بالخفاء وصعوبة الإثبات وغيرها من الخصائص المعالجة كما يلي:

أولا- جريمة صامتة وناعمة:

الجرائم التقليدية غالبا ما ترتكب باستخدام العنف سواءا العضلي أو اللفظي على العكس من ذلك تتسم الجرائم الناشئة عن استخدام الأنظمة المعلوماتية بأنها جرائم خالية من كل أشكال العنف المادي فسلاح المجرم فيها يكون جهاز معلوماتي متصل بشبكة مع وجود مجرم ذو كفاءة عالية في التعامل مع العالم الرقمي ومعرفة معمقة بتقنيات الكمبيوتر،[1] فهي بذلك من الجرائم الصامتة كما يطلق عليها أيضا الجرائم الناعمة لخفتها ولكونها مستترة في أغلبها، كما أن الضحية لا يلحظ ارتكابها رغم أنها قد تقع أثناء وجوده، فالجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، ومثال ذلك إرسال الفيروسات المدمرة و سرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وغيرها من الجرائم،[2] كما يستفيد المجرمون فيها من مختلف المواقع الإلكترونية ومنتديات القرصنة التي تضمن لهم التواصل فيما بينهم بهدف تبادل الخبرات والأفكار بعيدا عن أعين الأمن.[3]

ثانيا- جريمة سريعة وعابرة للحدود:

تتسم جرائم المساس بأنظمة المعالجة الآلية بأنها جرائم لا تتطلب مجهودا كبيرا في التنفيذ، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من الجهد العضلي، كما هو الحال في جرائم القتل

---

[1]- عومرية حساين، **أثر التكنولوجيا في استفحال الجريمة المعلوماتية وسبل مكافحتها في ظل التشريع الجزائري**، كتاب الملتقى الدولي حول القانون الجنائي في ظل التطور التكنولوجي – إشكالات ومعالجات- بيت الأفكار، الجزائر، 2023، ص 57.

[2]- يوسف صغير، **الجريمة المرتكبة عبر الأنترنت**، رسالة ماجستير، جامعة مولود معمري بتيزي وزو، كلية الحقوق والعلوم السياسية قسم الحقوق، السنة الجامعية 2011-2012، ص 14-15.

[3]- عبد المومن بن صغير، **الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن**، مداخلة مقدمة ضمن فعاليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر ، الموسوم بالجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة ،الجزائر، يومي 15 و16 نوفمبر 2015، ص 08.

أو الاختطاف،[1] حيث أن الجرائم التقليدية يحتاج مرتكبها إلى قوة عضلية لتنفيذها عكس جرائم نظام المعالجة الآلية للمعطيات التي تحتاج إلى قوة علمية وذكاء ومهارة ولا تحتاج من الوقت إلا ثوان أو دقائق معدودة لارتكابها، وفي بعض الأحيان يكون الدافع لارتكابها مجرد اللهو والتسلية أو تحقيق انتصارات تقنية، دون أن تكون لمرتكبها سوء نية، فمن هذا المنطلق تعد الجريمة المرتكبة عبر الأنظمة من الجرائم النظيفة فلا أثر فيها لأي عنف أو دماء، وإنما مجرد أرقام وبيانات يتم تغييرها من السجلات المخزنة فهي تنفذ في عالم افتراضي رقمي.

كما أنها عابرة للحدود بالنظر لتوسع استخدام الشبكات والأنظمة المعلوماتية، إذ لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر مختلف الدول، فالقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل العدد الهائل من المعلومات وتبادلها بين أنظمة تفصل بينها ألاف الأميال، جعلت من الممكن ارتكاب الجريمة من أماكن متعددة في دول مختلفة، ويتحقق الفعل الإجرامي في دولة أخرى بواسطة أنظمة التقنية الحديثة،[2] وذلك راجع إلى مجتمع المعلومات الذي لا يعترف بالحدود الإقليمية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان دون أن تخضع لحراس الحدود، الأمر الذي يطرح التساؤل حول الاختصاص القضائي لهذه الجرائم، علاوة على أن امتداد أنشطة الملاحقة والتحري والضبط والتفتيش خارج الحدود، الأمر الذي يحتاج إلى تعاون دولي شامل يستهدف مكافحة هذه الجرائم، مع احترام السيادة الوطنية للدول المعنية.[3]

ثالثا- جريمة صعبة الاكتشاف :

جريمة المساس بأنظمة المعلوماتية باعتبارها جريمة خفية ومتسترة، لا يتم في غالب الأحيان اكتشافها وتقديم شكوى بشأنها، إما لعدم اكتشاف الضحية لها وإما خوفا من التشهير،[4] حيث أن معظم هذه الجرائم تكتشف بالمصادفة، وأحيانا بعد وقت طويل من ارتكابها، وتبدو هذه الظاهرة أكثر وضوحا في المؤسسات المالية، كالبنوك والمؤسسات الادخارية ومؤسسات الاقتصادية والسمسرة، حيث تخشى مجالس إداراتها عادة

---

[1]- صالح بن محمد المسند ،عبد الرحمان بن راشد المهيني، "***جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات*** المجلة العربية للدراسات الأمنية والتدريب ، جامعة نايف العربية ، السعودية ،م15، ع29، افريل 2000، ص 202.

[2]- عومرية حساين ، **المرجع السابق** ، ص 52.

[3]- عبد المومن بن صغير، **المرجع السابق** ، ص 11.

[4]- أمير فرج يوسف، **الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت**، ط1 مكتبة الوفاء القانونية، الإسكندرية، مصر، 2011، ص 157.

من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية بشأنها إلى نقص ثقة عملائها فيها وانصرافهم عنها.[1]

وبالمقابل من ذلك وجود صعوبات تتعلق بإجراءات الضبط وإضفاء الوصف القانوني المناسب الذي ينطبق على الوقائع المتعلقة بهذا النوع من الإجرام، ولعل سبب ذلك يرجع إلى الطبيعة الخاصة لها فهي تتم في فضاء إلكتروني رقمي يتميز بالتغيير والديناميكية والانتشار الإقليمي العابر للحدود.[2]

رابعا- جريمة صعبة الإثبات:

ان البيانات والمعلومات المتداولة عبر الشبكة المعلوماتية تكون في هيئة رموز مخزنة في وسائط تخزين ممغنطة بلغة الصفر والواحد، لا تقرأ إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمرا صعبا، خاصة وأن الجاني يسعى إلى عدم ترك أثر لجريمته، ضف إلى ذلك ما يتطلب منه فحص دقيق لموقع الجريمة من قبل المتخصصين في هذا المجال، للوقوف على إمكانية وجود دليل ضد الجاني، وما يتبع ذلك من فحص للكم الهائل من الوثائق والمعلومات والبيانات المخزنة،[3] وتتم الجريمة المرتكبة عبر الأنظمة المعلوماتية خارج إطار الواقع المادي الملموس، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق، فداخل هذه البيئة الرقمية تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية، مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة،[4] كما يسعى مرتكب هذه الجريمة إلى إعاقة سلطات التحقيق في الوصول إلى الدليل بشتى الوسائل الممكنة، كحذف البرامج أو وضع رموز سرية وكلمات للمرور، وقد يلجأ لتشفير التعليمات لمنع إيجاد أي دليل يدينه،[5] حيث من السهل مسح الدليل من جهاز الكمبيوتر في زمن قياسي باستخدام البرامج المخصصة لذلك، إذ يتم بمجرد لمسة خاطفة على لوحة المفاتيح، على اعتبار أن الجريمة تتم بأوامر وتعليمات تصدر إلى الجهاز الالي.[6]

---

[1]- محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت**، ط2، دار النهضة العربية، القاهرة مصر، 2009، ص 37.

[2]- أمير فرج يوسف، **المرجع السابق**، ص 158.

[3] - محمد عبيد الكعبي، **المرجع السابق**، ص 38.

[4] - يوسف صغير، **المرجع السابق**، ص 45.

[5]- عبد المؤمن بن صغير، المرجع السابق، ص 10.

[6]- موسى مسعود أرحومة، **الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية**، مداخلة مقدمة ضمن فعاليات المؤتمر المغاربي الأول الذي نظمته أكاديمية الدراسات العليا بطرابلس، بعنوان: المعلوماتية والقانون، ليبيا ، يومي 28-29 أكتوبر 2010، ص 03.

البند الثاني: المجرم المعلوماتي في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات

إن مرتكب الجرائم الماسة بالأنظمة المعلوماتية هم في الغالب أشخاص تتوفر لديهم بعض الميزات التي لا نجدها عند الجميع، كما أنه ليس بمقدور كل شخص تنفيذ هذه الجرائم متى أراد ذلك، وقد اختلف الفقهاء والباحثون في مجال الجريمة المعلوماتية بشكل عام بخصوص تحديد شخصية المجرم المعلوماتي ومدى جسامة جرمه كدليل لتبرير العقوبة المنجرة عن فعلته، وبالرغم من عدم وجود نموذج محدد لهؤلاء المجرمين، غير أنه توجد صفات مشتركة توحد بين هؤلاء المجرمين،[1] وفيما يلي سمات وأصناف هذا النوع من المجرمين الملقبين بذوي الياقات البيضاء.

أولا- سمات المجرم المعلوماتي :

يتميز المجرم المعلوماتي بمجموعة من الصفات تميزه عن المجرم التقليدي، نجمل هذه الصفات فيما يلي:

1- **مجرم متخصص:** المجرم المعلوماتي له القدرة الفائقة والمهارة العالية للتحكم في التقنية المعلوماتية، حيث يستغل كل هذه المكتسبات في اختراق الشبكات وكسر كلمات المرور و الشيفرات، ويسبح في العالم الرقمي ليحصل على كل غال وثمين من البيانات والمعلومات الموجودة على أجهزة الحواسيب المتصلة بالشبكات.[2]

2- **مجرم محترف:** إن مجرمي المعلوماتية يتمتعون بقدر لا يستهان به من المهارة والمعرفة بتقنيات الحاسوب والانترنت، بل وأكثر من ذلك أن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا، فالمجرم المعلوماتي يتمتع باحترافية كبيرة في تنفيذ جرائمه، حيث أنه يرتكب هذه الجرائم عن طريق الكمبيوتر، الأمر الذي يقتضي الكثير من الدقة والتخصص والاحترافية في هذا المجال، بغية التغلب على العقبات التي أوجدها المتخصصون والمبرمجون لحماية أنظمة الكمبيوتر، كما في حالة البنوك والمؤسسات العسكرية والمواقع الخاصة بالحكومات.[3]

3- **مجرم ذكي:** يتمتع مرتكب الجريمة المعلوماتية بنظرة غير تقليدية للإجرام، على اعتبار أنه يوصف غالبا بدرجة عالية من الذكاء المعلوماتي الذي يمكنه من التعديل والتطوير في الأنظمة الأمنية حتى لا يكون من الممكن ملاحقته وتتبع أعماله الإجرامية عبر الشبكات وداخل أجهزة الحواسيب، مما يجعل من الصعب

---

[1]- عبد الكريم بلعزوق، **دراسة في ماهية الاجرام الإلكتروني ومجرم الأنترنت**، مداخلة مقدمة ضمن فعآليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، بعنوان: "الاجرام السيبراني المفاهيم والتحديات، برج بوعريريج، الجزائر ، يومي 11 و12 أفريل 2017، ص 07.

[2]- مليكة عطوي، **الجريمة المعلوماتية**، حوليات جامعة الجزائر، ع21، جوان 2012، ص 13.

[3]- فتيحة رصاع، **الحماية الجنائية للمعلومات على شبكة الأنترنت**، مذكرة ماجستير، جامعة أبي بكر بلقايد تلمسان، كلية الحقوق والعلوم السياسية، قسم الحقوق، تلمسان ، الجزائر ، السنة الجامعية 2011-2012، ص 51.

تصنيفه بحسب التصنيف الإجرامي المعتاد، لذا يعتمد في تحديد أنواع الجناة في الجرائم المرتكبة عبر الأنترنت على الهدف المراد تحقيقيه من ارتكاب هذه الجرائم كمعيار للتمييز فيما بينهم.[1]

4- **عائد للإجرام بطبعه:** يتميز المجرم المعلوماتي بأنه عائد للإجرام دائما، إذ يستخدم مهارته وخبراته في طريقة عمل الحاسب الآلي وكيفية تخزين البيانات والمعلومات فيها، وكذا طريقة التحكم في أنظمة الشبكات عن بعد، لإظهار قدراته وتفوقه على النظام فهو قد لا يرتكب الجريمة بهدف الإيذاء أو سرقة البيانات، بقدر ما يكون نوع من التحدي بهدف اختبار مهاراته ورغبته في تطويرها أكثر فأكثر، خاصة ما لم يتم القبض عليه.[2]

ثانيا- أصناف المجرمين المعلوماتي :

يصنف المجرم المعلوماتي مرتكبي الجرائم الماسة بالأنظمة المعلوماتية إلى أصناف عدة استنادا إلى الدافع او الغاية من ارتكابهم للجريمة التي تكون أما بهدف المتعة أو الانتقام وفي غالب الأحيان من اجل تحقيق الكسب المادي.

1- **الموظفون العاملون في مجال الأنظمة المعلوماتية:** باعتبار أن النظام المعلوماتي هو مجال عملهم الأساسي، ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها، فإنهم يقترفون بعض الجرائم المعلوماتية التي يمكن أن تحقق أهدافهم الشخصية ومنها الكسب المادي، كما أن هذه الفئة يمثلون الغالبية العظمى من مرتكبي هذه الجرائم. [3]

2- **الحاقدون:** هم افراد لا يسعون إلى إثبات قدراتهم ولا لتحقيق مكاسب مادية أو سياسية أو غيرها، وإنما يرتكبون أنشطتهم الإجرامية بدافع الرغبة في الانتقام والثأر، لذا فهم ينقسمون إما إلى مستخدمي النظام بوصفهم على علاقة ما بالنظام محل الجريمة، او غرباء عن النظام و تتوفر لديهم أسباب للانتقام من الشخص المستهدف في نشاطهم، ومثال ذلك من يقومون باستخدام الكمبيوتر لمسح بعض المعلومات الخاصة بالشركة أو المؤسسة، كطريقة للانتقام من المؤسسة لأسباب يعرفها مرتكب هذا الفعل.[4]

---

[1]- عبد اللطيف معتوق، **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، مذكرة ماجستير، كلية الحقوق و العلوم السياسية ،جامعة العقيد الحاج لخضر باتنة، الجزائر،السنة الجامعية 2011-2012، ص 16.

[2]- عبد الفتاح مراد، **شرح جرائم الكمبيوتر والإنترنت**، دار الكتب والوثائق المصرية، د س ن، ص 45.

[3]- مليكة عطوي، **المرجع السابق**، ص 13.

[4]- علي جعفر، **جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة**، ط1، منشورات زين الحقوقية، بيروت، لبنان، 2013، ص 117.

3- **القراصنة:** وهم عادة المبرمجون من أصحاب الخبرة، حيث يسعون إلى الدخول إلى الأنظمة المعلوماتية غير المسموح لهم بدخولها، وكسر كل الحواجز الأمنية المحيطة بهذه الأنظمة، ويمكن تصنيف القراصنة إلى صنفين هما:[1]

أ- **القراصنة الهواة (الهاكرز):** يكون هذا الصنف من القراصنة عادة من هواة الحواسيب والتكنولوجيا، ينطلقون من فكرة التسلية والرغبة في المعرفة، ويرون في اختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية، فالفضول وحب التعمق في الأنظمة المعلوماتية هو دافعهم الأول، وفي العادة لا تكون لديهم دوافع تخريبية وراء أعمالهم، لكنها قد تتولد بالعودة لارتكاب الجريمة،[2] وهناك سمة مميزة لهذه الفئة، وهي تبادلهم للمعلومات والخبرات فيما بينهم، حيث يتم ذلك عن طريق النشرات الإعلانية الإلكترونية ومجموعات الأخبار والمنتديات المخصصة لهذا الغرض.[3]

ب-**القراصنة المحترفون (الكرا كرز):** بالنسبة لهذا الصنف، فهو الأخطر على الإطلاق لأن المجرم يدرك ماذا يريد، وكيفية الوصول إلى أهدافه المحددة مسبقا، وذلك باستخدام ما لديه من مهارة وعلم يطوره باستمرار، فهدفه سحب الأموال من الأرصدة، والوصول إلى أخطر المواقع وأكثرها حساسية واختراقها والتلاعب ببياناتها، فهذه الفئة من المجرمين وبالنظر إلى السلوكات المرتكبة من طرفهم نجد أن لديهم ميولات اجرامية خطيرة وواضحة، تفصح عن رغبتهم في إحداث التخريب والسرقة والنهب[4]، و مهما قيل عن المجرم السيبراني بأنه متكيف اجتماعيا وأنه ليس مجرما بطبعه أو أنه لم يكشف عن أي عداء للمجتمع، يبقى رغم ذلك مجرما يتطلب توقيع العقاب عليه، فتعدد الجرائم المعلوماتية وتنوع صورها، يقتضي عدم التهاون في مكافحة مرتكبيها.[5]

الفرع الثالث: عناصر المعطيات المعالجة آليا محل المساس وتقنيات الاعتداء عليها.

تنفرد البيانات والمعطيات المعالجة آليا بمجموعة من العناصر الواجب توفرها حتى تحظى بالحماية القانونية، كما ان طرق وأساليب الاعتداء عليها تتميز وتختلف عن الطرق التقليدية.

---

[1]- يوسف صغير ، المرجع السابق، ص 26، 27.

[2]- نائلة عادل محمد فريد قورة، **جرائم الحاسب الآلي الاقتصادية**، ط1، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005، ص 61-62.

[3]- مليكة عطوي، **المرجع السابق**، ص 13.

[4]- عبد الفتاح مراد، **المرجع السابق**، ص 47.

[5]- عبد اللطيف معتوق، **المرجع السابق**، ص 16.

البند الاول: عناصر المعطيات المعالجة آليا محل المساس.

تعتبر السرية، التحديد والتوافر والتكاملية وسلامة المحتوى ضرورة حتمية تتعلق بالمعطيات حتى تدخل في نطاق الحماية الجزائية المقررة لهو بما يلي توضيح لذلك .

أولا- سرية البيانات المعالجة آليا :

إن إضفاء الطابع السري على البيانات أمر هام حيث يجب أن تكون المعطيات محاطة بجدار من السرية وهذا بضرورة الاحتفاظ بها في نطاق محصور ومحدد من الأشخاص، وبالتالي فان تلك المعطيات التي لا تتصف بالسرية تعتبر بيانات عامة ،وشائعة بين الناس ومجال حركتها غير محدد ،مما يجعلها قابلة للتداول ،ولا يمكن حينها الحديث عن المساس بها من خلال سرقتها او الاطلاع عليها دون وجه حق، لان ذلك متاح أصلا لعدم وجود عنصر السرية، وتستمد المعطيات سريتها من حيث كونها موجودة داخل نظام المعالجة الآلية وان هذا النظام مغلق وغير متاح للجمهور ولا يتم الدخول إليه إلا بشروط معينة أو من طرف أشخاص معينين تتوفر فيهم الصفة كالموظف مثلا.[1]

ثانيا- التحديد في المعطيات المعالجة آليا :

يعتبر التحديد خاصية أساسية وعنصرا ضروريا في المعطيات ،حيث يفرض نفسه حتى قبل السرية وبانعدامه تنعدم المعطيات، فمن البديهي أن تكون هذه الأخيرة محددة حتى تكون موجودة أساسا أي من الضروري تحديد جوانبها وحصرها في نطاق معين، لان الاعتداء يجب أن ينصب على شيء محدد،[2] بمعني يجب أن يفرغ في صورة مادية تبرز من خلالها إلى الوجود، ولا تكون مجرد فكرة دون إطار، ولا يهم الشكل الذي تتخذه سواءا كان كلمات أو رموز أو أرقام أو حقائق أو إحصائيات ...الخ حتى يمكن معالجتها بواسطة أنظمة المعالجة الآلية للمعطيات، وهذا الشكل هو الذي يحدد المعطيات، فلابد في جريمة التلاعب بالمعطيات على سبيل المثال ان تكون المعطيات محددة حتى يتم التلاعب بها، لان التلاعب هو تغيير لحالة او حقيقة وعليه لا يمكن تصور تغيير شيء لم يحدد بعد أو يفرغ في شكل معين.[3]

ثالثا: التوافر في المعطيات المعالجة آليا .

إن نظام المعالجة الآلية السليم والآمن يجب أن يحافظ على المعلومات ،ويوفر الوصول الموثوق اليها عند الحاجة إليها من قبل الأشخاص المخول لهم ذلك ،والمفهوم المخالف للتوافر هو إنكار الخدمة، ويعني ذلك أن الدخول إلى نظام المعالجة الآلية للمعطيات لا يكون ممكنا حتى بالنسبة للمصرح لهم، لذلك فان

[1] - محمد خليفة، المرجع السابق، ص 91.

[2] - نائلة عادل محمد فريد قورة، **المرجع السابق**، ص 112.

[3] - محمد خليفة، المرجع السابق، ص 91.

عنصر التوافر يرتبط ارتباطا وثيقا بالسرية لان هذا الأخير يتضمن فكرة السماح للأشخاص المخول لهم الولوج إلى أنظمة المعالجة الآلية للمعطيات وفي حال عدم توافرها سيظهر ذلك.[1]

رابعا: التكاملية وسلامة محتوى المعطيات المعالجة آليا .

في نظام المعالجة الآلية للمعطيات يجب الحفاظ على سلامة المعطيات المخزنة ودقتها، وتتجلى فكرة التكامل من خلال العناصر المادية والمعنوية التي يتكون منها النظام، ونذكر من ذلك الذاكرة والبرامج المعطيات و أجهزة الربط.. الخ ،وهذا يفتح المجال أمام إمكانية إضافة عناصر جديدة آو حذف البعض منها وفقا لما يفرزه التطور التكنولوجي في هذا المجال،[2] ومن تم لا تقع جرائم المساس بأنظمة المعالجة الآلية للمعطيات إذا وقع الاعتداء على عنصر بمفرده معزول عن النظام، كأن يتم الاعتداء على برامج معروضة للبيع او أنظمة خرجت عن الخدمة ،في حين يعتبرا اعتداءا إذا وقع على عناصر النظام في حالة عطل جزئي أو كلي وكان من الممكن إصلاحه انطلاقا من فكرة التكامل.[3]

هذا من جهة ومن جهة أخرى فإن الاعتداء على العناصر السالفة الذكر، يؤدي إما إلى تدمير المعلومات والمعطيات أو محوها أو تشويهها بشكل يؤثر سلبا على قيام النظام بالوظائف المخولة له.

البند الثاني: تقنيات الاعتداء على الأنظمة المعالجة آليا.

تتنوع وتتعدد التقنيات والأساليب المستخدمة في الاعتداء والتي لا تقبل الحصر لعدم إمكانية التبؤ بالوسائل التقنية التي قد تستحدث في مجال تكنولوجيا المعلومات،[4] ولعل أبرز أساليب الاعتداء على الأنظمة المعلوماتية التي يستخدمها مجرمو نظام المعالجة الآلية للمعطيات في تنفيذ جرائمهم هي أساليب الإدخال غير المشروع للمعطيات والبرامج ،ومن أشهر هذه البرامج نجد الفيروسات، برامج الدودة والقنابل، أما الأسلوب الثاني فيكمن في الاختراق .

أولا- ارتكاب جرائم نظام المعالجة الآلية للمعطيات عن طريق الإدخال غير المشروع للمعطيات.

يكون الاعتداء على المعطيات المعالجة آليا عن طريق الإدخال غير المشروع للمعطيات باستعمال تقنية الفيروسات، أو برامج الدودة أو ما يعرف بالقنابل:

1- **الفيروسات:** يعرف الفيروس بأنه: "برنامج حاسب مثل أي برنامج تطبيقي آخر، ولكن يتم تصميمه بواسطة أحد المجرمين لهدف محدد، وهو إحداث أكبر ضرر ممكن بنظام الحاسب، ولتنفيذ ذلك يتم

---

[1]- رشيدة بوكر، **المرجع السابق**، ص 84.

[2]- امال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري، ط2**، دار هومة، الجزائر ، 2007، ص 102.

[3]- علي عبد القادر القهواجي، **الحماية الجنائية لبرامج الحاسب الالي**، الدار الجامعية للطباعة والنشر، الاسكندرية، مصر 1999، ص 121.

[4]- نهلا عبد القادر المومني، **المرجع السابق** ص 125.

إعطاؤه القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر ويتوالد ذاتيا، وهذا ما يتيح له قدرة كبيرة على الانتشار ببرامج الحاسب المختلفة، وكذلك بين مواقع مختلفة في الذاكرة، حتى يحقق أهدافه التدميرية،[1] كما ينتشر أيضا عن طريق منافذ الدخول (USB) والأقراص الصلبة المتحركة أوعن طريق الاتصال بجهاز حاسوب مصاب بفيروس ما...إلخ،[2] كما تتمتع الفيروسات بمجموعة من الخصائص تجعلها في غاية الخطورة كالقدرة على الاختفاء، حتى أنّ بعضها تقوم بإخفاء آثارها الدالة عليها، فتضل البرامج المحتوية على هذه الفيروسات تعمل بكفاءة دون أخطاء لمدة طويلة وتنتشر بسرعة كبيرة تفوق سرعة الفيروس البيولوجي، كما لها القدرة على الاختراق وكذلك القدرة على التدمير بمجرد الدخول إلى ذاكرة الحاسوب،[3] وهناك عدة أصناف من الفيروسات بحسب الضرر الذي تحدثه من ذلك نجد فيروس الإبطاء وينحصر دوره في إبطاء عمل جهاز الحاسوب بصورة تدريجية تمهيدا لإيقافه عن العمل، الفيروسات النائمة وهي فيروسات خطيرة حيث تظل منكمشة لفترة ما ثم تنطلق لتنفيذ أهدافها التخريبية، الفـيروسات التطورية وهي فيروسات لها القدرة على تغيير شكلها بمرور الوقت لتقوم بتدمير برامج وبيانات الحاسوب دون أي صعوبة.

2- **برامج الدودة:** الديدان برامج مصممة للانتقال من شبكة إلى أخرى عبر وحدات الاتصال الرابطة بينها وخلال عملية انتقالها تتكاثر عن طريق إنتاج نسخ منها، بغية حيازة أكبر مجال ممكن من سعة الشبكة لأجل تقليل أو خفض كفاءتها، كما يمكن أن تتعدى أهدافها لتبدأ في التكاثر والانتشار مخربة بذلك مختلف الملفات والبرامج ونظم التشغيل وبروتوكولات الاتصال، هذا وتكمن خطورتها في استقلاليتها عن أي برامج أخرى مما يعطيها حرية كاملة في الانتشار السريع.

3- **القنابل المنطقية والزمنية:** القنبلة المعلوماتية هي اصطلاح يطلق على أنواع البرامج المعلوماتية التي تهدف إلى تدمير المعلومات كوسيلة لارتكاب جريمة الإتلاف وتنقسم إلى قسمين:

أ- **القنابل المنطقية:** هي برنامج أو جزء من برنامج يتم وضعها بطريقة غير مشروعة في شبكة معلوماتية يظل في حالة سكون ولا يتم اكتشافه فإذا توفرت شروط منطقية معينة حسب الرمز الذي يحدده برنامج القنبلة تنشط في القيام بمهام تخريبية.[4]

ب-**القنابل الزمنية الموقوتة:** هي برامج يتم إدخالها بطرق مشروعة متخفية مع برامج أخرى وتهدف إلى تدمير برامج ومعلومات النظام وتقوم على مبدأ التوقيت حيث تنفجر في وقت معين.[5]

---

[1]- حسن طاهر داود، **جـرائم نظــم المعلــومات ، ط1**، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 2000 ص71 .

[2]- Myriam Quéméner et Joel Ferry, **Cybercriminalité Défi mondial**, Economica, France, 2e édition 2009, p 75-78.

[3]- عثمان خرشي، **المرجع السابق**، ص 48.

[4]- نهلا عبد القادر المومني، **المرجع السابق**، ص 132.

[5]- نهلا عبد القادر المومني، **المرجع نفسه**، ص 133.

ثانيا– ارتكاب جرائم نظام المعالجة الآلية للمعطيات عن طريق الاختراق :

الاختراق هو الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات ويكون ذلك عن طريق انتهاك الإجراءات الأمنية، وبمعنى أخرى هو القدرة على الوصول لنظام معلوماتي معين بطريقة غير مشروعة عن لوجود ثغرات في نظام الحماية الخاص بالهدف أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروعة، وينقسم الاختراق إلى ثلاثة أنواع،[1] اختراق الأجهزة الخادمة و يتم عن طريق ما يسمى بالمحاكاة وهي القيام بانتحال شخصية مسموح لها بالدخول إلى هذه الأجهزة، التعرض للبيانات أثناء انتقالها وتستخدم هذه الطريقة للتعرف على أرقام بطاقات الائتمان أثناء انتقالها من المشتري إلى موقع التسوق، وثالثا اختراق الأجهزة الشخصية وهي الطريقة الأكثر شيوعا نظرا لتوفر العديد من برامج الاختراق سهلة الاستخدام.

الفرع الرابع: علاقة الحماية التقنية لأنظمة المعالجة الآلية للمعطيات بالمسؤولية الجزائية.

إن الحماية التقنية لأنظمة المعالجة الآلية للمعطيات لها ما يبررها في ظل التطور السريع والهائل لمختلف التقنيات والبرامج المستعملة في الاعتداء على هذه الأخيرة، هذه الحماية كأصل عام تكمن فائدتها في منع هذه الاعتداءات غير أنها في أحيان كثيرة تتسم بالقصور وتعجز عن ردع مجرمي المعلوماتية وتحتاج إلى تعزيزها بالشق العقابي.

البند الأول: أهمية الحماية التقنية لأنظمة المعالجة الآلية للمعطيات

تباينت الآراء الفقهية بين مؤيد ومعارض في مدى اعتبار الحماية الأمنية والتقنية لنظام المعالجة الآلية للمعطيات شرط أساسي وضروري كي يحظى هذا النظام بالحماية الجزائية من عدمها.

حيث ذهب جانب من الفقه إلى عدم اشتراط توفر الحماية الفنية للنظام المعالجة الآلية للمعطيات لقيام الجريمة،[2] وذلك راجع لكون نظام الأمن والحماية الفنية أو التقنية لا يكون له سوى دور وقائي، وأن ثبوت سوء نية المنتهك لهذا النظام ودخوله إليه بطريقة غير شرعية هي متوفرة أساسا،[3] في حين تمسك اتجاه آخر من الفقه بضرورة وجود نطاق كاف من الحماية الأمنية للمختلف الأنظمة المعلوماتية المعالجة آليا لقيام المسؤولية الجزائية، مقسما الأنظمة المعلوماتية بذلك إلى ثلاث أقسام، أنظمة مفتوحة للجمهور، أنظمة قاصرة على أصحاب الحق فيها ولكن دون حماية فنية، أنظمة قاصرة على أصحاب الحق فيها مع توفرها على حماية فنية لها.

---

[1]– الطيبي بركة، **المرجع السابق**، ص 70.

[2]– نعيم سعيداني، **المرجع السابق** ، ص 45.

[3]– احمد حسام طه تمام، **الجرائم الناشئة عن استخدام الحاسب الآلي–دراسة مقارنة–**، ط1، دار النهضة العربية للنشر والتوزيع، مصر، 2000، ص 264.

ومن ذلك اعتبر أن النوع الأخير من الأنظمة المعلوماتية هو الذي يتمتع بالحماية الجزائية، وحجتهم في ذلك أن الحماية الجزائية يجب أن تقتصر على الأنظمة المحمية تقنيا، لأنه من الطبيعي أن يقوم باستغلالها أي شخص، لذا فإن القانون الجزائي لا يحمي إلا الأشخاص الذين لديهم حرص على أموالهم بتوفير الحماية الأمنية ولو بقدر أدنى،[1] و من الناحية العملية أصبح من غير المعقول تقبل فكرة وجود نظام معلوماتي لا يحتوي على عنصر الحماية التقنية له، كما أن وجود هذه الحماية له دور كبير في تحديد القصد الجنائي لدى المجرم المعلوماتي.

هذا الرأي تعرض للانتقاد كون الشرط الذي استند عليه لا يكون له سوى دور واحد وهو إثبات سوء نية الشخص الذي قام بانتهاك النظام والدخول إليه بطريقة غير مشروعة، ويدخل ذلك في عبء إثبات القصد الجنائي حيث يكفي لقيام الجريمة أن يتم ذلك ضد إرادة المسؤول عن النظام، وهذا الرأي هو الراجح كما أن النصوص القانونية تؤيده، حيث أن هذه الأخيرة لم تشترط خضوع الأنظمة لأية حماية تقنية .

حيث نجد التشريع الجزائري و على غرار التشريع الفرنسي وبعض التشريعات الأخرى لم تنص صراحة على وجوب حماية تقنية لنظام المعالجة الآلية للمعطيات، ومن تم فإنها تكفل الحماية الجزائية لكافة الأنظمة حتى ولو لم تكن خاضعة لنظام حماية تقنية، لاسيما وأن هذا النوع من الجرائم يتم ارتكابها من طرف مجرم فائق الذكاء، له قدرة على التحكم في تقنيات الحاسوب واستخدام أنظمته، ويواكب كل تطور يحدث في هذه الأنظمة، ويجد له الطريق لتجاوزه وخرقه، بحيث أنه كلما استحدثت أنظمة جديدة فإنه يطور بالمقابل وسائل لاختراقه .

ورغم ذلك شكك البعض في جدوى هذه الحماية بل هناك من ذهب إلى القول بأنها تؤدي إلى نتائج عكسية وأن الرد المناسب على هذا الإجرام هو من طبيعة تقنية وذلك بإيجاد حماية فنية تمنع كل اعتداء على هذه الأنظمة فيؤدي ذلك إلى تلافي هذه الظاهرة بالكامل،[2] وتدخل المشرع الجنائي ليس بالضروري، إذ يمكن الاستغناء عنه بوسائل أخرى، وعندما تفشل كل تلك الوسائل يمكن أن يتدخل قانون العقوبات.

لكن الواقع يكشف عدم صحة هذا الرأي، فالإجرام المعلوماتي سابق في وجوده على تدخل القانون الجنائي وليس العكس، والحماية التقنية لنظام المعالجة الآلية للمعطيات و إن كانت هامة في الحد من الجرائم الواقعة على المعطيات الموجودة داخل نظام المعالجة الآلية للمعطيات إلا إنها غير كافية،[3] والتجربة كشفت أن مجرمي نظام المعالجة الآلية للمعطيات بصفة خاصة ومجرمي المعلوماتية بصفة عامة لهم قدرة

[1] – قارة أمال، **المرجع السابق**، ص 29.

[2] – نعيم سعيداني، **المرجع السابق**، ص 43.

[3] – احمد حسام طه تمام، **المرجع السابق**، ص 266.

فائقة على تجاوز أنظمة الأمان التي تزود بها الأنظمة المعلوماتية،[1] مما اشعل فتيل الحرب بين شركات تصنيع برامج الآمان والمجرمين المعلوماتيين الذين يتمتعون بمعرفة واسعة بتلك الأنظمة وبخباياها يطورون وسائل جرائمهم بما يخترق أنظمة الأمان الموجودة بطرق مختلفة، ولا يمكن حمايتها بطرق تقنية على نحو مطلق، وقد كشف الواقع أن أكبر الأنظمة المعلوماتية وأكثرها توفر على الحماية الفنية تم اختراقها تحديا للقائمين عليها وطرق الحماية التي استعانوا به.[2]

هذا ونظرا لاعتماد مختلف المؤسسات حآليا في عملها على نظام معلومات فإنّها بذلك عرضة لهجوم الفيروسات والمتسللين، مما قد يتسبب لها في خسائر كبيرة ، كما يؤثر على سمعتها وتسريب معلوماتها ،[3]لذلك كان لازما أن تواكب التشريعات المقارنة هذا التطور الملحوظ من خلال إقرارها قواعد قانونية غير تقليدية تتعامل بشكل عصري متقدم مع الجرائم المعلوماتية المختلفة وفي مقدمتها جرائم نظام المعالجة الآلية للمعطيات ، وعليه يمكن القول أن الحماية الفنية والتقنية لنظام المعالجة الآلية و إن كانت لازمة وهامة فإنها تظل قاصرة وغير كافية لمواجهة الاعتداءات التي يتعرض لها النظام مما استدعى تدخل المشرع الجزائي لفرض حماية جزائية خاصة.[4]

البند الثاني: أهمية الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات.

إن النظام القانوني من خلال تحديده للمصالح المشروعة المتعلقة بنظام المعالجة الآلية للمعطيات وقيامه بوضع نصوص جزائية تحميه يكون قد وفر حماية جزائية للنظام، وتتخذ هذه الحماية شكلين وقائي وعقابي ،فمن الناحية الوقائية يكون لنصوص قانون العقوبات دور وقائي لمنع الجريمة قبل وقوعها، ذلك أن التطور المعلوماتي الكبير يجد صداه في نصوص قانون العقوبات، ولابدا أن يتم إقراره وحمايته بواسطة قاعدة قانونية جزائية نظرا للخسائر الكبيرة التي تهدد الأشخاص والمؤسسات جراء الجرائم التي تمس بالمعطيات المدرجة ضمن نظام المعالجة الآلية ،وكذا المخاطر الجمة التي تمس حياتهم الخاصة، لاسيما مع تفاقم الأخطار في المجتمع الدولي المعاصر الذي يتميز بالحرب الاقتصادية، مما يلزم الدولة معه أن تتدخل فتبسط الحماية الجزائية على مشروعاتها الوطنية ضد هذا النوع من الإجرام.[5]

---

[1]– محمد محمد شتا، **فكرة الحماية الجنائية لبرامج الحاسب الآلي** ، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2001، ص 18.

[2]– محمد خليفة، **المرجع السابق**، ص 29–30.

3 – Bokhari Namrata Agrawal, Dharmendra Saini, Cyber Security Proceedings of CSI 2015 Springer Nature Singapore Pte Ltd, 2018, p216.

[4]– البركه الطيبي، **المرجع السابق**، ص 73–74.

[5]– محمد خليفة، **المرجع السابق**، ص 31.

ومن تم فإن هذه الحماية تقي المصالح المحمية من الكثير من الاعتداءات التي كانت ستحصل بالنظر لقصور الحماية التقنية في أغلب الأحيان، ما يجعل المستخدمين يعتمدون على وسائل تقنية لحماية برامجهم من خطر النسخ والنقل بوضع كلمة مرور، لا يتم تشغيل البرنامج دونها، أو وضع رقم سري في بداية البرنامج يمنع نقله أو استنساخه من طرف الآخرين، إلا أنّ هذه التقنيات غير كافية لحماية النظام المعلوماتي كونه قابل للاختراق من قبل أشخاص محترفين مقارنة بالأشخاص العاديين، ولا شك في أنّ فعالية الوسائل التقنية للحماية الموضوعة من قبل منتجي البرامج مرهونة بحجم المال والوقت الذي ينفق لأجل الحماية، فكل ما كان المال والوقت كبير تكون الحماية على قدر عال، والعكس كلما كانت البرامج أقل تكلفة وأقل وقت كلما كان احتمال الاختراق كبير ويسير، من جهة أخرى أصبحت تقنية المعلومات الجديدة قادرة على تخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل الأفراد والمؤسسات والدوائر والأجهزة الحكومية ومن قبل الشركات الخاصة، وأكثر من ذلك يمكن مقارنة المعلومات المخزونة في ملف مؤتمن بمعلومات في قاعدة بيانات أخرى، أين يمكن نقلها داخل البلد الواحد أومن بلد لآخر في ثوان وبتكاليف منخفضة نسبيا[1] .

من هنا نخلص إلى اتسام الجرائم الماسة بنظام المعالجة الآلية للمعطيات بالخطورة، فهي تقع على برامج ومعلومات ذات قيمة، وقد تتسبب في خسائر باهظة في الجهد والأموال، بل وقد تقضي على مؤسسات اقتصادية بمجرد معرفة رقم حسابها أو الرقم السري لها من قبل مجرم ذو دراية وخبرة في مجال المعلوماتية مما يؤدي إلى كشف أسرارها الإدارية أو أسرارها المالية، فالمجرم المحترف يستطيع في لحظات أن يدمر كل البيانات السرية لتلك المؤسسة أو أن يفشي سر صناعتها عن طريق وضعها على الشبكة المعلوماتية بحيث يكون في متناول الجميع، فالحواسيب الآلية لم يعد استخدامها مقتصرا على الشركات أو المؤسسات المالية والاقتصادية والتجارية بل أصبح في متناول الأفراد حتى في مدارسهم ومنازلهم مما يتيح للجميع الاتصال بالنظام الرقمي العالمي.[2]

المطلب الثاني: إرساء قواعد تجريم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

على غرار باقي الدول المسايرة للتطور والتكنولوجيا عملت الجزائر على حماية أنظمتها المعلوماتية بتعزيز الحماية التقنية السابقة وبالمقابل وضع إستراتيجية ردعية وعقابية من جهة أخرى جاهدة من خلال ذلك لقمع ومكافحة الجريمة المعلوماتية بشكل عام بما في ذلك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، متبنية بذلك الجهود والمساعي الدولية والإقليمية الرامية للتصدي لكل أشكال الجرائم المستحدثة الناجمة عن التطور التكنولوجي والناشئة ضمن البيئة الرقمية فعملت على تعديل قوانينها وتكييفها وفقا

[1]– عثمان خرشي، **المرجع السابق**، ص 65.

[2]– عثمان خرشي ، **المرجع نفسه**، ص 66.

للتطورات والمستجدات التقنية، بدأ بتعديل قانون العقوبات، بموجب القانون رقم 04-15 المؤرخ في 25 أوت 2004، والذي تم من خلاله إدراج جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضمن نطاق الأفعال المجرمة، تلى ذلك إصدار القانون رقم 09-04 المؤرخ في 05 أوت 2009، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما وعديد القوانين الخاصة في ذات الإطار، هذا ونحاول من خلال هذا المطلب التعرف أولا على مبررات الحماية الجزائية ثم التطرق إلى الإستراتيجية التي انتهجها المشرع الجزائري في إرساء قواعد الحماية بداءا بتبني الاتفاقيات الدولية والإقليمية ومن تم تكييف القوانين الداخلية وفقا لذلك.

الفرع الأول: مبررات الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات

تعتبر الحماية الجزائية لنظم للمعالجة الآلية للمعلومات، من الموضوعات التي أثارت الجدل الكبير في مدى قدرة القواعد الجزائية التقليدية على مواجهة ومسايرة واقع الثورة المعلوماتية وما أفرزته من تحديات إجرامية، الأمر الذي استدعى ضرورة التوصل لحلول غير تقليدية لموضوع مستحدث ذو تداعيات قانونية جزائية غير مسبوقة ولعل ذلك راجع بالأساس لعديد الأسباب والمبررات من ذلك حداثة الظاهرة الإجرامية.

البند الأول: الأسباب المتعلقة بحداثة الظاهرة الإجرامية.

أصبحت النظم المعلوماتية تشكل موضوعا قانونيا جديدا للحماية،لما صاحب الظواهر الإجرامية المعلوماتية الحديثة من أساليب إجرامية مبتكرة لم تعرفها مبادئ القانون الجزائي التقليدي، هذه الظواهر الإجرامية ذات خصائص تقنية عالية تتخطى وتتجاوز طرق المواجهة الجنائية التقليدية، وتفاديا لفكرة الفراغ التشريعي الذي يتيح إفلات الكثير من المجرمين من العقاب، تعين البحث عن أساليب مستحدثة للمواجهة،[1] لاسيما وأن النظم المعلوماتية هي أساليب تقنية وضعت لكي يتم من خلالها تبادل المعلومات المعالجة إلكترونيا، التي أصبحت بدورها محلا للجريمة المعلوماتية هي والنظم التي تعالجها، الأمر الذي حتم إعادة التفكير وإعادة صياغة المفاهيم الجنائية التقليدية لأجل مواجهة هذه الظاهرة الإجرامية بتطوير وإثراء الترسانة القانونية.

كما أن هذه الجريمة تميز بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها ودقة وسرعة محو آثارها وهي تعتمد في الأساس على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها وتحتاج لخبرة تقنية يصعب على الخبير التقليدي التعامل معه، نذكر أيضا أن ما زاد من خطورة هذا النوع من الجرائم، أنها انصبت على قيم معنوية لا تلمسها الأيدي ولا تبصرها الأعين، تتخطى حدود المكان في ظل انفتاح شبكة الإنترنت وتجاهلها للحدود الجغرافية للدول وزادها تعقيدا أنها جرائم ترتكب من قبل أشخاص من أصحاب

[1]- ناصر حمودي،" ***الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري"***، المجلة الأكاديمية للبحث القانوني ،جامعة عبد الرحمان ميرة، بجاية ، الجزائر، م14، ع2، 2016، ص 70.

المعارف والمهارات الفنية، وفي الغالب من المتخصصين في مجال المعلوماتية، وعلى قدر عال من الذكاء، يضاف لذلك خفاء الجريمة المعلوماتية كونها تتم عبر منصات إلكترونية لا تجيد قراءاتها سوى برامج الكمبيوتر، كل ذلك في ظل ندرة الكفاءات وقلة الخبرة لدى الأجهزة الأمنية والقضائية.[1]

البند الثاني: الأسباب المتعلقة بخصوصية المفاهيم وحاجتها لحلول مبتكرة.

تغيرت المفاهيم القانونية التقليدية وحل مكانها مفاهيم مستحدثة لم تكن معروفة من قبل لاسيما بظهور دعائم رقمية الكترونية ذات طابع دولي اوجب حمايتها جزائيا وإضفاء الحجة القانونية عليها، لاسيما وأن الشبكة العنكبوتية ليست ملكا لأي جهة ولا يسيطر عليها أحد مما أضعف الكثير من المبادئ التي كانت متأصلة في مبادئ السيادة الإقليمية للدولة، إضافة إلى أن الأدوات والمعدات الإلكترونية المستحدثة باتت تعكر صفو الإنسان وصار يضيق بها لأنها ستصيبه بأذى وضرر ناجم عن الجرام الحديثة التي تتمخض عنها، وسوف تسهل وتوسع من مجالات انتهاك حياته وخصوصياته الشخصية وأسراره المالية بل أن هذه الوسائل قد تنتهك كذلك الأسرار المهنية والاقتصادية للمؤسسات والشركات والبنوك،[2]ومن تم كان لازما أن تواكب هذه التطورات المعلوماتية تطورات في المتطلبات القانونية لتجاوز قصور القواعد الجنائية التقليدية ومواجهة الظواهر الإجرامية المستجدة تحت مسمىالإجرام المعلوماتي أو الإجرام إلكتروني أو الإجرام الرقمي.[3]

البند الثالث: الأسباب المتعلقة بأهمية المعطيات المدرجة ضمن النظم المعلوماتية.

إن المادة محل الحماية في البيئة الرقمية هي المعطيات المدرجة بأنظمة الحواسيب وأنظمة الاتصالات بمكوناتها المادية والمعنوية، وما نتج عن استعمالها من سرعة فائقة في نقل وتخزين وتبادل المعلومات داخل شبكات المعلومات التي تربط بين مختلف الحاسبات الآلية في مختلف أنحاء العالم، أدت إلى تقريب المسافات بين دول العالم وتسهيل التواصل بين مختلف الجنسيات وتطور عالم الاقتصاد والثقافة، وبروز موازين وتكتلات جديدة قوامها المعلومة فمن يملك المعلومة في وقتها يملك القوة.[4]

كما أن وجود بيئة رقمية افتراضية نجم عنه إزالة كافة الحدود وتلاشي المسافات، مما أدى إلى احدث انقلاب حقيقي وجذري في المفاهيم الجزائية التقليدية، وطرح تساؤل عن مدى قدرتها على التأقلم مع هذا التحول، ، وما إن كان يتعين هجرها والبحث عن بدائل قانونية حديثة تساير التطورات التقنية وما أفرزته من

[1]– ناصر حمودي، **المرجع السابق، ص** 71.

[2]– يوسف مناصرة، **المرجع السابق،** ص 41–42.

[3]– البركه الطيبي، **المرجع السابق،** ص 57.

[4]– يوسف مناصرة، **المرجع السابق،** ص 09.

نظم معلوماتية لازمة للتعامل مع هذا الوسط الحديث،[1] ذلك أن التطورات التكنولوجية غيرت كثيرا من المفاهيم القانونية التقليدية، وأدخلتنا في عصر العولمة وتدويل الرقمنة.[2]

البند الرابع: الأسباب المتعلقة بإلزامية مواكبة الفكر القانوني لتطور الفكر الإجرامي.

إن ظهور الانترانت وما أسفر عنها من تطور لظاهرة الإجرام المعلوماتي، استلزم بالضرورة مواجهة جزائية جديدة كون الإجرام يقوم على انتهاك النظم المعلوماتية وسرقة بياناتها وأموالها، ووجوب أن يكون هناك تطور مواز ومواكب في الفكر القانوني لاسيما في ظل واقع تكنولوجي يتسم بالحركية والتحول المستمر بروز الحاجة الملحة إلى الحماية الجنائية للنظم المعلوماتية والبيانات التي تتداول عبرها[3] .

إن التطرق إلى المراحل التي مرت به مواجهة ظاهرة مكافحة الجرائم المعلوماتية منذ نشأتها بينت أنها في تطور دائم ومستمر وفي كل مرة تظهر بشكل جديد مسايرة بذلك التقنيات والتطبيقات الجديدة، ففي ستينيات القرن العشرين عندما ظهرت الأنظمة المعلوماتية بالترانزيستور أصبحت الحواسيب تلاقي رواجا كبيرا تم التركيز في تجريم الأفعال المرتكبة على الأضرار المادية التي تلحق بالنظم الحاسوبية والبيانات المخزنة فيها، وخلال مطلع السبعينات تم استحداث أشكال جديدة من الجريمة منها الاستخدام غير المشروع للنظم الحاسوبية والتلاعب بالبيانات الإلكترونية وأفضى الانتقال من المعاملات اليدوية الى المعاملات الحاسوبية إلى نشوء شكل جديد من الجريمة وهو الاحتيال الحاسوبي، وفي الثمانينات ومع استخدام الحواسيب الشخصية أكثر فأكثر ظهر أول شكل من أشكال قرصنة البرمجيات الحاسوبية، وفي التسعينيات أدى التزايد السريع في مستخدمي الأنترنت إلى ظهور أساليب جديدة من السلوك الإجرامي حولت الجريمة الإلكترونية الى جريمة دولية، وأتسم العقد الأول من القرن الحادي والعشرين مرة أخرى بانتشار أساليب إجرامية جديدة ومعقدة للغاية مثل التصيد الاحتيالي والحساب الإلكتروني السحابي.[4]

المشرع الجزائري اقر الحماية الجزائية باستحداث نصوص تشريعية، مستفيدا في ذلك ببعض التجارب الدولية والإقليمية، مثلما هو الشأن بالنسبة لاتفاقية بودابست، والتي برغم من كونها اتفاقية أوروبية إلا أن طابعها وتوجهها عالميين كما وجد تجربة أخرى على المستوى العربي وهي تجربة وضع القانون العربي النموذجي أو الاسترشادي الذي يعد عملا مشتركا بين مجلس وزراء الداخلية والعدل العرب، في نطاق الأمانة العامة لجامعة الدول العربية في شأن مكافحة جرائم تقنية المعلومات.

---

[1]– ناصر حمودي، **المرجع السابق** ، ص 70.

[2]– البركه الطيبي، **المرجع السابق**، ص 56.

[3]– البركه الطيبي، **المرجع السابق**، ص 57.

[4]– يوسف مناصرة، **المرجع السابق**، ص 286.

الفرع الثاني: ارساء قواعد الحماية من خلال تبني بنود اتفاقية بودابست .

تعد اتفاقية بودابست (Convention Sur La cyber Criminality, Budapest)، أول اتفاقية قانونية دولية تعتمد تدابير وأحكام حول جرائم الحاسوب فهي وإن كانت أوروبية المنشأ ،فهي دولية النزعة كما أنها مفتوحة لجميع الدول الأخرى لتطلب الانضمام إليها قصد تعميم الفائدة على الجميع بهدف ضبط مجتمع المعلوماتية والاتصالات،[1] وإرساء سياسية جنائية مشتركة تهدف إلى حماية المجتمع من الإجرام في البيئة الافتراضية بتبني تشريع ملائم للتعاون الدولي ذلك أن مكافحة الإجرام المعلوماتي لا يكون إلا في إطار دولي مع تبني سلطات كافية لمكافحة هذا النوع من الجرائم بتسهيل البحث والتحري والمتابعة الجزائية على المستويين الداخلي والدولي مع إيجاد توزان بين أهداف الدعوى الجزائية واحترام حقوق الإنسان والحريات الأساسية.[2]

البند الأول: مضمون اتفاقية بودابست .

تضمنت اتفاقية بودابست كل ما يتعلق بالجرائم المعلوماتية سواء ما يقع على الشبكات والمعلومات آو الجرائم التقليدية التي تستخدم في ارتكابها الشبكات الرقمية،[3] كما تم استعراض أهداف الاتفاقية ومرجعياتها، وبعض التدابير التشريعية الإقليمية والدولية المتعلقة بمكافحة الجرائم المعلوماتية حيث ثمنت المقدمة التعاون الدولي في هذا المجال ووزعت الجرائم إلى أربع مجموعات كبرى تضم الأولى الجرائم التي تتعرض لخصوصية وسلامة وتوفر الأنظمة والبيانات من ذلك الاعتراض غير الشرعي وتشويه البيانات وسلامة النظام، وتضم المجموعة الثانية جرائم التزوير والاحتيال المعلوماتي في حين تطرقت المجموعة الثالثة إلى جرائم المحتوى أما المجموعة الأخيرة فضمت جرائم الاعتداء على الملكية الفكرية والحقوق المجاورة.[4]

هذا وقد جاءت الاتفاقية بأربعة فصول، الفصل الاول تحت مسمى **"استخدام المصطلحات"** أما الفصل الثاني فقد شمل التدابير الواجب اتخاذها على الصعيد المحلي بموجب القوانين الموضوعية وكذا

---

[1]– يوسف مناصرة، **المرجع السابق**، ص 287.

[2]– هشام عبد الكريم،" ***التمييز العنصري وصور الاستخدامات الجديدة للأنترنت"*** ، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، بعنوان: الإجرام السيبراني المفاهيم والتحديات الجزائر، يومي 11 و12 أفريل 2017، ص 09.

[3]– يوسف مناصرة، **المرجع السابق**، ص 291.

[4]– سليمان قطاف،عبد الحكيم بوقرين، ***"الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست التشريع الجزائري"***، المجلة الأكاديمية للبحوث القانونية والسياسة، جامعة عمار ثلجي، الأغواط، الجزائر، م 06، ع 01 2022، ص 340.

الإجرائية، في حين عالج الفصل الثالث مجال التعاون الدولي، أما الفصل الرابع فتناول الأحكام الختامية للاتفاقية، ومن اهم الجرائم التي تضمنها الاتفاقية نجد:

- **جرائم سرية وسلامة بيانات وأنظمة الكمبيوتر:** تطرقت إليها المواد من 2 إلى 6 من الاتفاقية التي حددت الافعال المجرمة ذات العلاقة بسرية وسلامة بيانات وأنظمة الكمبيوتر، والمتمثلة في النفاد غير الشرعي "Accès illegal" الذي عرفته المادة الثانية من اتفاقية بودابست،[1] والاعتراض غير الشرعي "Interception illégale" الذي عالجته المادة 03 من ذات الاتفاقية.[2]
- **المساس بسلامة المعطيات:** "Atteinte à l'intégrité des données"عرفته المادة 04 من الاتفاقية.[3]

إن تجريم هذه الأفعال يهدف بالدرجة الأولى إلى حماية بيانات وبرامج الكمبيوتر ويعتبر "**الاضرار**" و"التخريب" عملان متداخلان، وكلاهما بهدف إلى التغيير السلبي في سلامة البيانات والبرامج أو محتواها الإعلامي، بينما يعتبر "حذف" البيانات مطابقا لتدمير الشيء المادي، حيث يتم تدميرها وجعلها غير قابلة للتعرف،[4] ويقصد ب "إتلاف" بيانات الكمبيوتر كل عمل يمنع أو ينهي توافر البيانات للشخص الذي لديه حق المرور إلى الكمبيوتر أول وسيلة حفظ البيانات التي تم تخزين البيانات عليها، بينما يعني مصطلح "التغيير" تعديل البيانات القائمة، ومنه فإن إدخال رموز خبيثة، مثل الفيروسات والقنابل، مشمولة في هذه الفقرة، كما هو الحال بالنسبة للتعديل الناجم عن البيانات.[5]

البند الثاني: مدى توافق نظام بودابست مع التشريع الجزائري.

شكلت اتفاقية بودابست لمكافحة الجريمة السيبرانية خطوة رائدة على مستوى التعاون الدولي وهي بذلك تشكل المرجعية الأساسية الى غاية اليوم من حيث فعاليتها في إقرار الإجراءات العملية التي تلتزم الدول المنظمة في إدراجها ضمن قوانينيها الداخلية،[6] هذا وقد نهج المشرع الجزائري نهجها والتزم بتشريعاتها لاسيما الجانب الموضوعي للتصدي للجريمة المعلوماتية بشكل عام ونلمس مطابقة التشريع الداخلي الجزائري مع ما جاء في الاتفاقية الدولية بودابست في النقاط التالية:

---

[1] - art 2 de la convention stipule que: "..l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique."

[2]- art 3 de la convention stipule que: "..l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques .."

[3]- art 4 de la convention stipule que " .. le fait, intentionnel et sans droit,d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des donnéesinformatiques".

[4]– التقرير التفسيري لاتفاقية الجريمة الالكترونية "بودابست":
http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm تاريخ الاطلاع 2024/04/02 ، 18.00 سا

[5] – التقرير التفسيري لاتفاقية الجريمة الالكترونية، المرجع السابق.

[6]– سليمان قطاف، عبد الحكيم بوقرين، **المرجع السابق** ، ص 334.

- استخدام ذات المصطلحات وهي تلك المعمول بها في مجال الإعلام الآلي وتكنولوجيات الاتصال.[1]
- اعتماد ذات التعريف المتعلق بنظام المعالجة الآلية للمعطيات الوارد في اتفاقية بودابست.[2]
- الدخول الغير شرعي للأنظمة المعلوماتي.[3]
- الاعتراض الغير شرعي للمكالمات والمعطيات المتبادلة.[4]
- المساس بنزاهة أو استماتة المعطيات.[5]
- المسؤولية المعنوية للجهات المكلفة بتسيير مجالات تكنولوجيا الإعلام تبقى قائمة، لأنهم في نظر القانون الضامن الوحيد على حسن وسلامة الأنظمة المعلوماتية.[6]
- التعاون الدولي بمطابقة المواد 713-614 من قانون الإجراءات الجزائية والمادة 15 من القانون رقم 04-09 مع ما جاءت به اتفاقية بودابست في بابها الثالث.

الفرع الثالث: إرساء قواعد الحماية من خلال التعاون العربي .

إن اتساع رقعة الجريمة المعلوماتية، وفرض سيطرتها على الصعيد العالمي، وبعد أن تجسيد محاصرة مجلس أروبا لهذا التوغل بموجب اتفاقية بودابست وجدت الدول العربية نفسها مجبرة على توحيد الجهود العربية في سبيل مواجهة كل أشكال هذه الجريمة المستحدثة و التي أسفرت عن وضع قانون نموذجي استرشادي إضافة لتوقيع اتفاقيات في ذات الإطار .

البند الأول: القانون العربي النموذجي الاسترشادي .

جاء القانون العربي النموذجي الاسترشادي[7] كمحاولة للتصدي للجريمة المعلوماتية وهو نتيجة عمل مشترك بين وزراء الداخلية العرب ومجلس الوزارء العرب في نطاق الأمانة العامة لجامعة الدول العربية بعد أن قدم كلا المجلسين مشروعا بخصوص مكافحة الجريمة المعلوماتية، اعتمد هذا القانون من قبل مجلس وزراء العدل العرب في دورته التاسعة عشر بموجب القرار رقم 495 المؤرخ في 2003/10/08 ومن قبل مجلس وزراء الداخلية العرب في دورته الحادية والعشرين، هذا وقد جرم القانون السالف الذكر عمليات

---

[1]- يراجع في ذلك : المادة الأولى من اتفاقية بودابست و المادة الأولى من القانون رقم 04-09 السالف الذكر .

[2]- يراجع في ذلك :المادة 02 فـ2 من القانون رقم 04-09 السالف الذكر.

[3]- يراجع في ذلك: المادة الثانية والمادة 394 مكرر ق.ع.ج.م.م.

[4]- يراجع في ذلك: المادة الثالثة من الاتفاقية والمادة 303 من ق.ع.ج.م.م..

[5]- يراجع في ذلك: المادة الرابعة من الاتفاقية والمادة 394 مكرر من ق.ع.ج.م.م.

[6]- يراجع في ذلك المادة 12 من الاتفاقية والمادة 394 مكرر من ق.ع.ج.م.م..

[7]- القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات، اعتمده مجلس وزراء العرب في دورته التاسعة عشر بالقرار رقم رقم 495 د19في 2003/10/08، و مجلس وزراء الداخلية العرب في دورته الحادية و العشرون بالقرار رقم417- د21-2004.

اختراق النظم المعلوماتية بموجب المادة الثالثة منه والتي تنص على أن كل من توصل بطريقة التحايل لاختراق المعالجة الآلية للبيانات يعاقب بالحبس والغرامة، وتركت تقدير العقوبة للدولة المعنية، كما أضافت نفس المادة في فقرتها الثانية اعتبار انه إذا نتج عن هذا الفعل محو أو تعديل البيانات المخزنة بالحاسب أو تعطيل تشغيل النظام بسبب تسريبات للفيروسات أو غيرها من الأساليب المعلوماتية[1]، يكون معرضا صاحبها إلى العقوبة والحبس، يظهر تأثر واضح في هذا النص باتفاقية بودابست لاسيما في المفاهيم وفي كيفية التعامل مع فكرة أنظمة المعالجة الآلية للمعطيات، هذا وقد تلى صدور هذا القانون ابرام اتفاقيات عربية تهدف لمكافحة هذا النوع من الجرائم نذكر منها الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

البند الثاني: الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.

حررت هذه الاتفاقية بالقاهرة بتاريخ 2010/12/21، وهي تضم دول العربية المنظمة لجامعة الدول العربية، صادقت عليها الجزائر بتاريخ 2014/09/08[2].

و تهدف هذه الاتفاقية إلى تعزيز التعاون العربي لمنع ومكافحة الجريمة المنظمة عبر الحدود الوطنية وفقا لما جاء النص عليه ضمن أحكام المادة الأولى من الاتفاقية وقد جاء في ديباجتها أن الدول العربية توقع على هذه الاتفاقية التزاما منها بالمبادئ الأخلاقية والدينية السامية، ولاسيما أحكام الشريعة الإسلامية السمحة، وبأهداف ومبادئ ميثاق جامعة الدول العربية وميثاق الأمم المتحدة والاتفاقيات والمعاهدات العربية والدولية في مجال التعاون القضائي والأمني لمنع ومكافحة الجريمة والتي تكون الدول المتعاقدة طرفا فيها، ولاسيما منها اتفاقية الرياض للتعاون القضائي، واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، وإدراكا منها لأهمية التصدي للجريمة المنظمة عبر الحدود الوطنية، لما تمثله هذه الجريمة من تهديد لأمن الأمة العربية واستقرارها وعرقلة للتنمية الاقتصادية والاجتماعية للبلدان العربية، وحرصا منها على تعزيز التعاون العربي في مجال منع ومكافحة الجريمة المنظمة عبر الحدود الوطنية في المجالين القضائي والأمني وتجريم الأفعال المكونة لهذه الجريمة، واتخاذ تدابير وإجراءات منعها ومكافحتها وملاحقة ومعاقبة مرتكبيها وشركائهم وفق أحكام الشريعة الإسلامية السمحة أو القوانين الوطنية مع مراعاة النظام العام لكل دولة وتسليمهم إلى الدول الطالبة وأخذا في الاعتبار عدم تعارض أحكام الاتفاقية مع دساتير الدول الأطراف أو أنظمتها الأساسية.

---

[1]- بدري فيصل، **مكافحة الجريمة في القانون الدولي والداخلي**، أطروحة دكتوراه في القانون العام، كلية الحقوق جامعة الجزائر، السنة الجامعية2017- 2018، ص 34-35.

[2]-المرسوم الرئاسي رقم 251-14 بتاريخ 2014/09/08، المتضمن المصادقة على الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية.، ج.ر 56، الصادرة بتاريخ 2014/09/25.

كما جاء النص ضمن أحكام المادة 21 منها على: "تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع لتقنية أنظمة المعلومات، الاختراق غير المشروع أو تسهيل الاختراق غير المشروع على نحو كلي أو جزئي لأحد نظم المعلومات، تعطيل أو تحريف تشغيل أحد نظم المعلومات، إدخال بيانات بطرق غير مشروعة في أحد نظم المعلومات أو مسح أو تعديل أو نسخ أو نشر البيانات التي يحتويها هذا النظام بطريق غير مشروع، استيراد أو حيازة أو عرض أوترك أو إتاحة إحدى المعدات أو الأدوات أو برامج تقنية المعلومات بدون سبب مشروع بهدف ارتكاب إحدى الجرائم المنصوص عليها السابقة أي كل جريمة من الجرائم التقليدية ترتكب بإحدى وسائل تقنية أنظمة المعلومات".[1]

البند الثالث: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

تعتبر الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من الاتفاقيات العربية الحديثة في مجال مكافحة جرائم تقنية المعلومات على مستوى الدول العربية، وهي عبارة عن اتفاق دولي إقليمي معقود بين هذه الدول في نطاق جامعة الدول العربية بصورة خطية وقد حررت هذه الاتفاقية بمدينة القاهرة بتاريخ 21 ديسمبر 2010. صادقت عليها الجزائر بتاريخ 2014/09/08،[2] وهي تتويج لجهود الدول العربية في التصدي لهذا النوع المستحدث من الجرائم، تتكون الاتفاقية من ديباجة وثلاثة وأربعين (43) مادة موزعة على خمسة فصول، حيث تظهر الديباجة رغبة الدول العربية الموقعة في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها؛ واقتناعها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات؛ وأخذا بالمبادئ الدينية والأخلاقية السامية ولاسيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة، والتزامها بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها.

تهدف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات أساساً إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات بهدف الحفاظ على أمن وسلامة مجتمعاتها وأفرادها حسب ما جاءت به المادة الأولى من هذه الاتفاقية، كما جاءت نصوص هذه الاتفاقية لتخاطب الدول الأطراف فيها وتلزمهم لاتخاذ كافة الإجراءات التشريعية والتنظيمية المناسبة

[1] – يراجع في ذلك المرسوم الرئاسي رقم 251–14 المؤرخ في 2014/09/08 السالف الذكر.

[2] – المرسوم الرئاسي رقم14– 252، المؤرخ في 2014/09/08، المتضمن المصادقة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ج.ر57، المؤرخة في 2014/09/28.

لوضع الأحكام التي وردت فيها موضع التنفيذ سواء كانت هذه الأحكام موضوعية[1] ،أو أحكام إجرائية:[2] أو تلك المتعلقة بالتعاون الدولي[3] ،وذلك وفقاً لتشريعاتها وأنظمتها الداخلية، وأما بخصوص الأحكام الموضوعية التي وردت في الاتفاقية العربية فقد نصت المادة الخامسة منها على ضرورة التزام كل دولة طرف بتجريم الأفعال الواردة في الفصل الثاني منها المعنون ب "التجريم" ،حيث تضمن هذا الفصل جملة من النصوص على شكل مواد من المادة السادسة إلى الثامنة عشر وهذه المواد تتضمن الأفعال المجرمة التي تشكل جرائم تقنية المعلومات.

الفرع الرابع: إرساء قواعد الحماية ضمن التشريع الداخلي.

تعاظمت المصالح المرتبطة بمعطيات النظام في وقتنا الحاضر، إلى حد أصبح معه تدخل المشرع الجزائي أمرا لا بد منه لحمايتها لتشتمل حماية كل المعطيات مع تشديد الحماية على طوائف معينة تحظى بأهمية استثنائية، وتطال مختلف صور المعالجة ومواضيعها، وذلك بالنظر للخسائر الكبيرة التي باتت تهدد مصالح الأشخاص والدول من جراء هذه الجرائم.[4]

يطلق المشرع الجزائري على الجريمة المرتبطة بتكنولوجيا المعلومات مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا النظام المعلوماتي في حد ذاته محلا للجريمة اذ يمثل نظام المعالجة الآلية

---

[1]– تتضمن هذه المواد جرائم مرتبة حسب ترتيب مواد هذا الفصل من المادة، 5 إلى المادة 21 وهي: جريمة الدخول غير المشروع، جريمة الاعتراض غير المشروع، الاعتداء على سلامة البيانات، جريمة إساءة استخدام وسائل تقنية المعلومات جريمة التزوير، جريمة الاحتيال، جريمة الإباحية، الجرائم الأخرى المرتبطة بالإباحية، جريمة الاعتداء على حرمة الحياة الخاصة، الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات، الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة، الاستخدام غير المشروع لأدوات الدفع الإلكترونية، الشروع والاشتراك في ارتكاب الجرائم، المسؤولية الجنائية للأشخاص الطبيعية والمعنوية، تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات.

[2]– وهذه الأحكام الإجرائية تتمثل في نطاق تطبيق الأحكام الإجرائية، التحفظ العاجل على البيانات المخزنة في تقنية المعلومات، التحفظ العاجل أو الكشف الجزئي لمعلومات تتبع المستخدمين، أمر تسليم المعلومات، تفتيش المعلومات المخزنة، ضبط المعلومات المخزنة، الجمع الفوري لمعلومات تتبع المستخدمين، اعتراض معلومات المحتوى.

[3] – وتتمثل في: الاختصاص القضائي، تسليم المجرمين، المساعدة المتبادلة، المعلومات العرضية المتلقاة، الإجراءات المتعلقة بطلب التعاون والمساعدة المتبادلة، رفض المساعدة، السرية وحدود الاستخدام، التحفظ العاجل على المعلومات المخزنة في أنظمة المعلومات، الكشف العاجل للمعلومات تتبع المستخدمين المحفوظة، التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة: الوصول إلى معلومات تقنية المعلومات عبر الحدود، التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين، التعاون أو لمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى، جهاز متخصص.

[4]– يزيد بوحليط، **المرجع السابق**، ص 212– 213.

للمعطيات شرطا أساسيا في الجريمة السيبرانية،[1] هذا وقد أرسى المشرع الجزائري العديد من القوانين المكملة لقانون العقوبات للتصدي لجريمة المساس بأنظمة المعالجة الآلية للمعطيات في إطار الجهود المبذولة لمحاربة القرصنة الالكترونية.

البند الاول: أحكام تقنين العقوبات

تطرق المشرع الجزائري في أحكام قانون العقوبات الى تجريم الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وهذا كنتيجة حتمية لتأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة للإجرام حيث كان حاول تكييف قانون العقوبات وفقا لذلك فعدل فيه سنة 2001 بموجب القانون رقم 09/01 المؤرخ في 2001/06/26 المعدل والمتمم لقانون العقوبات في القسم الأول تحت عنوان الاهانة والتعدي على الموظفين ومؤسسات الدولة فنص في المواد 144 مكرر 144 مكرر2 والمادة 146 على جرائم الاهانة والقذف على رئيس الجمهورية باستعمال مختلف الوسائل الالكترونية وقد كان هدف المشرع منع استخدام الفضاء الافتراضي للمساس بأجهزة الدولة.

في سنة 2004 قام المشرع الجزائري بتعديل آخر لقانون العقوبات بموجب القانون رقم 15/04 المؤرخ في 2004/11/10 وقصد من ذلك مكافحة الجرائم الالكترونية الناشئة عن إساءة استخدام هذه التقنية بإضافة قسم سابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات حيث تضمن هذا القسم تسع مواد من 394 مكرر إلى 394 مكرر 7 وأدرج ضمن هذه المواد جملة من الجرائم المعلوماتية التي تجعل من جهاز الحاسوب وسيلة لارتكاب الجرائم الإرهابية المعلوماتية أو ما يسمى بجرائم امن الدولة المرتكبة في الفضاء السيبراني أو التي تجعل جهاز الحاسب الآلي هدفا لارتكاب الجريمة من ذلك جريمة الدخول والبقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات،[2] وجريمة تخريب نظام اشتغال المنظومة المعلوماتية...إلخ، ، هذا ويمكننا الجزم بأن المشرع الجزائري تدارك ولو نسبيا الفراغ القانوني في مجال مواجهة الإجرام المعلوماتي وهذا ما يشكل قفزة نوعية، كما تجدر الإشارة إلى أن المشرع الجزائري ركز في هذا القانون على الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، وأغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير المعلوماتي.[3]

---

[1]–جيلالي شويرب ، فائزة مراد ، ***"الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية"***، مجلة الدراسات القانونية والسياسية، *جامعة عمار ثليجي، الاغواط* ،الجزائر، م09، ع02، الجزائر، جوان 2023، ص 161.

[2]– عطاء الدين فشار، **مواجهة الجريمة المعلوماتية في التشريع الجزائري**، الملتقى المغاربي حول القانون والمعلوماتية أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص 28.

[3]– يزيد بوحليط، **المرجع السابق**، ص 101.

في العام 2009 سن المشرع الجزائري قواعد خاصة ضمن قانون العقوبات تهدف إلى الوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وهذا بموجب القانون رقم 01/09 الذي اعتبر المعلوماتية مال يمكن سرقته وفقا لأحكام المادة 350 مكرر.

في سنة 2016 عدل المشرع الجزائري في قانون العقوبات بإضافة المادة 394 مكرر 8وهذا بموجب القانون 02/16 المؤرخ في 19 جوان 2016 والتي حددت العقوبات المقررة لمقدم خدمة الانترانت حال ثبوت مسؤوليته الجنائية لما لهذه الفئة من دور في التحكم بالأنترانت.[1]

في العام 2024 عدل قانون العقوبات بموجب القانون رقم 24-06 المؤرخ في 28افريل 2024 [2] أحكام المواد 394 مكرر، 394مكرر1 و 394مكرر2و 394مكرر 3و هذا بتشديد العقوبات للجرائم المساس بالأنظمة المعلوماتية لاسيما إذا استهدفت هذه الجرائم مؤسسات الدفاع الوطني و الهيئات التابعة لها و المؤسسات الخاضعة للقانون العام .

البند الثاني: أحكام قانون الإجراءات الجزائية.

إن المواجهة الفعالة لجرائم المساس بأنظمة المعالجة الآلية للمعطيات لا يكون فقط بإرساء قواعد موضوعية فقط لذلك كان لازما على المشرع الجزائري استكمال سياسته الجنائية الخاصة بمكافحة الجرائم المعلوماتية في شقها الإجرائي، حيث قام بتعديل قانون الإجراءات الجزائية بغية استحداث إجراءات جديدة تتوافق والطبيعة الخاصة لجرائم المساس بالأنظمة المعلوماتية فجاء بالقانون رقم22-06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية وضمنه جملة من الإجراءات الجديدة في الفصل الرابع تحت عنوان: "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" من المادة 65 مكرر5 إلى المادة 65 مكرر 10، كما نص أيضا في الفصل الخامس تحت عنوان: "التسرب "بموجب المادة 65 مكرر11 إلى المادة 65 مكرر 18، وهي إجراءات تمكن سلطات البحث والتحري من الكشف عن المجرم الإلكتروني في هذه البيئة الافتراضية التي يصعب التحقيق فيها بسبب طبيعتها الخاصة.

البند الثالث: إرساء قواعد الحماية ضمن نصوص القوانين المكملة

إلى جانب القسم السابع مكرر من قانون العقوبات، نص المشرع الجزائري في بعض القوانين الخاصة على تجريم بعض السلوكات المعتبرة من ضمن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و في مايلي عرض لهذه الأخيرة.

---

[1]- نادية بوراس، **الاستراتيجيات الوطنية لمواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات**، مجلة الحقوق والحريات جامعة سطيف، الجزائر، المجلد10، العدد 03،2023، ص 587.

[2]-القانون 24-06 ، المؤرخ في 28افريل 2024 ، ج ر 30 ، المؤرخة في 30أفريل 2024 ،يعدل و يتمم قانون العقوبات.

أولا–القانون المتعلق بحقوق المؤلف والحقوق المجاورة :

جاء القانون رقم03–05، المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة [1] ،من اجل تجريم كل أشكال الاعتداء بطريق التقليد، الاستنساخ، والمساس بسلامة المصنف حيث ربط هذه الأخير بكل شيء له علاقة بمنظومة معلوماتية أو يجرى بواسطة منظومة معلوماتية كبرامج الحاب مثلا أو أداء الفنانين عن طريق أي منظومة معلوماتية، هذه الجرائم نصت عليها المادتين 151 و152 من القانون المذكور.

ثانيا– القانون المتعلق بالتأمينات الاجتماعية :

المشرع الجزائري من خلال القانون رقم 08–01 المؤرخ في 23 جانفي 2008 [2] ، يكون قد استبق الأحداث تحسبا للتطور الهائل في مجال استعمال التكنولوجيا الحديثة، وتعميم استعمال الشبكة المعلوماتية في شتى المجالات، إذ نص في المادة 06 مكرر من ذات القانون على: "أنه تثبت صفة المؤمن له اجتماعيا ببطاقة إلكترونية....." ونظرا لاحتواء هذه البطاقة على معلومات سرية تتعلق بالحياة الخاصة للأفراد، أحاطها بالحماية الجزائية اللازمة، فنص في المادة 93مكرر 2 على: "دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين إلى خمس سنوات من 100.000دج إلى 200.000دج، كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الإلكترونية للمؤمن له اجتماعيا أو المفتاح الإلكتروني لهيكل العلاج أو المفتاح الإلكتروني لمهني الصحة"، كما تضاعف العقوبة حسب نص المادة 93 مكرر 3 على كل من يقوم عن طريق الغش بتعديل أو حذف للمعطيات.

ثالثا– القانون المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية التقنية، تطلب تدخلا تشريعيا صريحا حيث أرسى هذا القانون رقم 09–04 المؤرخ في 05اوت 2009 [3] ،ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينه والقيام بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية سعيا منه للحفاظ على النظام العام ومستلزمات التحقيق القضائي.[4]

رابعا– القانون المتضمن القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين :

---

[1]– القانون رقم 03–05، المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر 44، المؤرخة في 2003/06/23 .

[2]– القانون رقم 08–01 المؤرخ في 23 جانفي 2008 ، ج.ر 04، المؤرخة في 27 جانفي2008 ،يتمم القانون 83–11 المؤرخ في 02 جوان 1983 يتعلق بالتأمينات الاجتماعية.

[3] – القانون رقم 09–04 المؤرخ في 05 اوت 2009، السالف الذكر.

[4]– نادية بوراس، **المرجع السابق**، ص 587.

تم استحداث القانون رقم 15-04 المؤرخ في 01 فبراير 2015 المتضمن التوقيع و التصديق الالكترونيين[1] ، في ظل التوجه نحو الحكومة الإلكترونية ومقتضيات التجارة الإلكترونية، وبعد أن أدرج المشرع الجزائري نظام الإثبات بالكتابة في الشكل الإلكتروني ضمن قواعد الإثبات ،حيث أقر بنظام التوقيع والتصديق الإلكترونيين والاعتراف بحجتيهما في الإثبات، وقصد توفير الحماية اللازمة لوسائل الدفع الإلكتروني بالنسبة لمعاملات التجارة الإلكترونية وزرع الثقة لدى المتعاملين لما يمتاز به من مستوى عالي للسرية والخصوصية تم تجريم كل فعل من شأنه المساس بنظام التوقيع والتصديق الالكتروني.

خامسا- القانون المتعلق بعصرنة العدالة:

يهدف القانون 15-03 المؤرخ في 01فبراير 2015 [2] ،إلى عصرنة سير قطاع العدالة من خلال وضع منظومة معلوماتية مركزية لوزارة العدل، واستخدام تقنية المحادثة المرئية عن بعد، إرسال الوثائق والمحررات القضائية بطريقة الكترونية، و عليه تم تجريم كل الأفعال التي من شأنها المساس بهذه الأنظمة.

سادسا- قانون البريد والاتصالات الإلكترونية :

صدر القانون رقم 18/04 المؤرخ في 10ماي 2018المتعلق بالبريد و الموصلات[3] ،ليلغي **القانون المتعلق بالمواصلات السلكية واللاسلكية**[4] ، حيث شدد القانون المنوه عنه من العقوبات المفروضة على الموظفين متعاملي الشبكات العمومية الذين ينتهكون سرية المراسلات أو المساعدة بالإحالة بعقوبة تتراوح من 03أشهر إلى 05 سنوات وغرامة مالية تقدر ب 30000 دج إلى500000 دج، كما أحال إلى تطبيق أحكام المادة 394 مكرر8 من قانون العقوبات، كل متعامل لا يقوم رغم إنذاره من طرف سلطة الضبط بالتدخل الفوري لمنع النفاذ إلى شبكات و/أو خدمات الاتصالات الإلكترونية.

سابعا- القانون المتعلق بحماية الأشخاص الطبيعية في مجال المعطيات ذات الطابع الشخصي :

[1]-القانون رقم 15-04 المؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر 06، المؤرخة في 10 فبراير 2015.

[2]- القانون رقم 15-03 المؤرخ في 2015/02/01، يتعلق بعصرنة قطاع العدالة، ج.ر 06، المؤرخة في 2015/02/10.

[3]- القانون رقم 18-04 المؤرخ في 2018/05/10، يتعلق بالبريد والاتصالات الالكترونية، ج.ر27، المؤرخة في 2018/05/13.

[4] - القانون رقم 2000-03 المؤرخ في 2000/08/05، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، ج.ر 48، المؤرخة في 2000/08/06.

تناول القانون 07/18 المؤرخ في 10جوان 2018 [1] بشكل مفصل حماية الأشخاص الطبيعيين في مجال معالجة المعطيات الشخصية، هذا وقد عرف معالجة المعطيات ذات الطابع الشخصي بأنها كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي، وقرن المشرع الجزائري المعالجة ب **"موافقة الشخص المعني"** الذي عرّفه على انه: "كل تعبير عن الادارة المميزة يقبل بموجبه الشخص المعني أو ممثله الشرعي معالجة المعطيات الشخصية المتعلقة به بطريقة يدوية أو إلكترونية".

ثامنا –القانون المتعلق بالانتخاب:

جرم قانون الانتخاب رقم 01/21 الصادر بتاريخ 10مارس 2021 [2] الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات الانتخابية أو محاولة المساس بها وفقا لأحكام المادة 283 من هذا القانون.

تاسعا–قانون مكافحة التزوير :

التزوير الالكتروني جريمة أفرزها التطور التكنولوجي و هي تختلف تماما عن جريمة التزوير التقليدي سواءا في أركانها و أساليب ارتكابها و البيئة الافتراضية واللامادية التي تقع فيها وكذا لخصوصية مرتكبها، يقصد بالتزوير حسب ما عرفته المادة 3 من القانون رقم 24–02 المؤرخ في 2024/02/26 المتعلق بمكافحة التزوير و استعمال المزور [3] هو كل تغيير للحقيقة عن طريق الغش في أحد المحررات أو الوثائق أو الدعائم المنصوص عليها في هذا القانون بأي وسيلة من شأنه إحداث ضرر و بهدف أو من شأنه أن يترتب عليه اقرار حق أو صفة أو واقعة ترتب آثارا قانونية و يشمل التزوير التقليد و التزييف المنصوص عليهما في هذا القانون."

ترتكب جريمة التزوير الالكتروني في أي مرحلة من مراحل المعالجة الآلية سواءا مرحلة الإدخال أو مرحلة المعالجة أو مرحلة الإخراج، فأثناء مرحلة الإدخال يستطيع الجاني إدخال معلومات غير صحيحة أو ترك معلومات ضرورية بهدف تغيير الحقيقة أو إدراج أسماء أشخاص غير موجودين حقيقة ، أما أثناء مرحلة المعالجة فيمكن إدراج تعديلات عن طريق التلاعب في برنامج نظام المعلومات وأثناء مرحلة الإخراج

[1]– القانون رقم 18–07 المؤرخ في 2018/06/10، المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، ج.ر 34، المؤرخة في 2018/06/10.

[2]– الأمر رقم 21–01، المؤرخ في 2021/03/10، المتضمن القانون العضوي المتعلق بنظام الانتخابات، ج.ر 17، المؤرخة في 2021/03/10.

[3]- القانون رقم 24–02 المؤرخ في 2024/02/26 المتعلق بمكافحة التزوير و استعمال المزور،ج .ر15، المؤرخة في 2024/02/29

يمكن تغيير النتائج التي تم إدخالها و معالجتها بطريقة صحيحة بالدخول الى نظام المعالجة الآلية من أجل تغيير الحقيقة.

تعد جريمة التزوير الالكتروني جريمة غير ملموسة لا تظهر آثارها كونها تتم خلال الوصول إلى معلومات عن طريق النظام المعلوماتي و تغير مضمونها ، و من جرائم الغش في مجال المعلوماتية جريمة التزوير في المحررات الالكترونية الرسمية و العمومية و التزوير في بعض الوثائق الادارية و كذا الشهادات إضافة إلى التزوير في المحررات العرفية أو التجارية أوالمصرفية ، و نلاحظ أن الوثائق الالكترونية غير محصورة لارتباطها بالتطور التكنولوجي و العالم الرقمي الذي يشهد تطور مستمرا و تتخد البطاقات الالكترونية أشكالا متعددة ووظائف مختلفة ، من بينها جواز السفر و بطاقة التعريف الوطنية، شهادة الجنسية و صحيفة السوابق القضائية ، البطاقات البنكية أو المصرفية، وغيرها... [1]

المبحث الثاني: أوجه الاعتداء على أنظمة المعالجة الآلية للمعطيات وجزاءات المساس بها

إن الجريمة المعلوماتية باعتبارها مستحدثة أثارت ضجة بخصوص تحديد الأفعال الإجرائية التي تدخل في نطاقها، ومن أوجه الاعتداء على أنظمة المعالجة الآلية للمعطيات جرائم الدخول والبقاء غير المشروع في نظام المعالجة الآلية للمعطيات ،وجريمة التلاعب بمعطيات الحاسب الآلي، الإتلاف الغير العمدي للمعطيات، وأخيرا جريمة التعامل في معطيات غير مشروعة، وذلك بالمقارنة مع مختلف التشريعات التي أكست نظام المعالجة الآلية للحماية الجزائية على غرار المشرع الجزائري واتفاقية بودابست وكذلك الجزاءات المقررة في القانون15-04 المعدل والمتمم لقانون العقوبات وذلك من خلال المواد من 394 مكرر إلى غاية المادة 394 مكرر 05 من نفس القانون.

حيث متى تبت توافر الشرط الأول لقيام الجريمة المعلوماتية ألا وهو نظام المعالجة الآلية للمعطيات أمكن الانتقال إلى المرحلة التالية وهي البحث عن توافر أركان أية جريمة من الجرائم المعلوماتية ، هذا ونقسم هذا المبحث الى مطلبين نتناول خلال المطلب الأول أوجه الاعتداء على أنظمة المعالجة الآلية للمعطيات ، أما المطلب الثاني فيعالج الجزاءات التي اقرها قانون العقوبات في ذات الاطار.

[1]- ليلى بومدين ، **دور المؤسسات و الادارات في مكافحة التزوير – الجريمة السيبرانية** –، مداخلة القيت خلال اليوم الدراسي بعنوان "**القانون 24-02 المؤرخ في 2024/02/26 المتعلق بمكافحة التزوير و استعمال المزور** " مجلس قضاء عين تموشنت ، الجزائر ، يوم 15ماي2024 .

المطلب الأول: أوجه الاعتداء على أنظمة المعالجة الآلية للمعطيات

إن المعطيات باعتبارها مجموعة من الحقائق أو البيانات ،تتخذ شكل أرقام أو حروف أو رموز أو أشكال خاصة وتصف فكرة أو موضوعا أو حدثا معينا ، وهي عبارة عن مادة خام يستخرج منها بعد معالجتها معلومات معينة تمثل ثروة هامة يمكن أن تكون عرضة لعدة اعتداءات[1] ،نص عليها المشرع الجزائري في المادة 394 مكرر 1 و394 مكرر 2 من القانون 04-15 السالف الذكر، ونظرا لأهميتها وخطورة المساس بها فقد جرم المشرع الجزائري كل سلوك يؤدي إلى المساس بسلامة معطيات النظام سواء كانت موجودة بداخله أو التي لها علاقة به، وذلك بالإدخال أو التعديل أو الإزالة المقصودة غير المصرح بها لمعطيات نظام المعالجة الآلية، كما انه عزز من هذه الحماية عند إدراجه جريمة أخرى تهدف إلى منع وقوع الجرائم السابقة أو التخفيف من أثارها أن وقعت وهي جريمة التعامل في معطيات غير مشروعة.

لذلك فان الجرائم التي تمس بمعطيات النظام تكون مرتكزة بحق على معطيات النظام أو على استخدام هذه المعطيات لأغراض غير مشروعة، وتكون هذه الأخيرة هي المستهدفة بالدرجة الأولى من الاعتداء وليس النظام الذي يتضمنها. ولدراسة أوجه الاعتداء على أنظمة المعالجة الآلية للمعطيات سنقوم بمعالجة صور هذه الجرائم بالتطرق إلى أركان كل جريمة على حدى.

الفرع الأول: الدخول أو البقاء غير المصرح به .

يمثل نظام المعالجة الآلية للمعطيات المفهوم الأولي الذي يمكن أن يتحقق به الاعتداء والمساس بالمعطيات والبيانات ومنه توافر أركان هذه الجريمة[2]، لكونها جريمة تقع في بيئة المعالجة المعلوماتية للبيانات لتصحيحها وتعديلها وتشكل محلا للاعتداء أو كوسيلة للاعتداء[3] ، وتقوم جريمة الدخول والبقاء في النظام المعلوماتي بمجرد ما يتم الدخول غير المرخص به وعن طريق الغش إلى النظام المعلوماتي، سواء مس الدخول أو البقاء كامل النظام المعلوماتي أو جزء منه فقط.[4]

لم يحدد المشرع الجزائري تعريف الدخول كما لم يحدد وسيلة للدخول، لذا يمكن الدخول إلى النظام المعلوماتي بأية وسيلة كانت، سواء عن طريق كلمة السر الحقيقية، أو عن طريق استخدام برنامج أو شفرة

---

[1]- سمير برادل ، " ***الجريمة المعلوماتية في التشريع الجزائري***"، مجلة القانون، كلية الحقوق والعلوم السياسية، المركز الجامعي، جامعة غليزان ، الجزائر ، م1، ع2، جويلية 2010، ص 190.

[2]- جابر بومعيزة ، **الاعتداء على المعطيات الآلية في الحوكمة الالكترونية**، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة ، الجزائر،ع12،2017 ، ص 127.

[3]- عفاف خديري، **الحماية الجنائية للمعطيات الرقمية**، أطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق جامعة العربي التبسي، تبسة،الجزائر ، السنة الجامعية 2017-2018، ص 154.

[4]- يوسف صغير، المرجع السابق، ص 108.

خاصة أو حتى بواسطة استخدام الرقم الكودي لشخص أخر فالمهم أن يكون هذا الدخول مخالفا لإرادة صاحب النظام، ولم يذكر الأفعال المادية لفعل الدخول أو الطريقة التي يتم بها الدخول إلى النظام، لذلك جرم أي طريقة سواء تم الدخول بطريقة مباشرة أو غير مباشرة، ولا تتحقق الجريمة إلا إذا اقتصر دور الجاني على مجرد قراءة الشاشة دون الولوج إلى داخل النظام المعلوماتي.[1]

وفي هذا الصدد يرى الفقه الفرنسي أن "الدخول" يحمل مدلولان: معنوي ومادي،[2] أما بالنسبة لجريمة البقاء فهي التواجد داخل النظام المعلوماتي ضد إرادة من له حق السيطرة على هذا النظام، ويتحقق فعل البقاء سواء كان مستقلا عن فعل الدخول غير المشروع أين يكون الدخول مسموحا به ومع ذلك لا يقطع الفاعل الاتصال عند إدراكه ان وجوده داخل النظام والبقاء فيه غير مشروع، او كان مقترنا بفعل الدخول غير المشروع أين يكون الفاعل غير مصرح له بالدخول ومع ذلك يدخل إلى النظام ليبقى فيه بعد ذلك، كما عرف البقاء بأنه: "كل تواجد غير عادي كالاتصال بواسطة الشبكة المعلوماتية بالنظام المعلوماتي بالدخول والنظر فيه، أي في المعطيات التي يتضمنها وغيرها من التصرفات الغير مسموح بها والتي تشكل بدورها بقاء احتيالي".[3]

بعد الوقوف على مفهوم جريمة الدخول وكذا جريمة البقاء في النظام والإحاطة بأهم التعاريف التي قيلت بشأنها، سنتناول تحديد أركانها من جهة أخرى وتنقسم أركان جريمة الدخول أو البقاء في النظام ألمعلوماتي إلى ثلاثة أركان وهما:

البند الأول: الركن الشرعي لجريمتي الدخول أو البقاء في النظام المعلوماتي

يعد نظام المعالجة الآلية للمعطيات الشرط الأول الذي يجب توافره قبل الانتقال للتحقق من وجود اعتداء عليه أولا، وفيما يخص الدخول والبقاء غير المصرح به في هذا النظام، فإنه جريمة معاقب عليها بموجب نص المادة 394 مكرر المعدل والمتمم من خلال العبارة الآتية: "يعاقب بالحبس.... كل من

---

[1]– مسعود خثير، **الحماية الجنائية لبرامج الكومبيوتر (أساليب وثغرات)**، دار الهدى، الجزائر، 2010، ص 115–116.

[2]– **المدلول المعنوي:** حيث يعتبر الدخول إلى نظام معالجة البيانات أو النظام المعلوماتي أو النظام الالكتروني يشبه الدخول إلى ذاكرة الإنسان، **المدلول المادي:** ويتمثل في أن الشخص يكون متى دخل الجاني إلى النظام كله أو جزء منه وكذلك يتحقق الدخول غير المشروع متى كان مسموحا للجاني بالدخول إلى جزء معين في النظام وتجاوز ذلك إلى جزء آخر غير مسموح له بالدخول، وحتى نكون بصدد جريمة الدخول غير المصرح به يجب أن يكون النظام مفتوحا أمام الجمهور، لأنه لو كان كذلك لما اعتبر جريمة ومعظم الذين يدخلون بطريقة غير مشروعة عن طريق التوصل إلى الأرقام والكلمات أو الشفرات أو الحروف او المعلومات السرية التي تكون بمثابة النظام الأمني لجهاز الحاسب الآلي أو البرامج والنظم المعلوماتية، نقلا عن : بهاء فهمي الكبيحي، **مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني**، رسالة ماجستير في القانون العام، جامعة الشرق الأوسط،عمان الأردن، السنة الجامعية 2012–2013، ص 26.

[3]– بسمة مامن، **المرجع السابق**، ص 479.

يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"، فتعد هاته الجريمة أبسط صور جرائم المساس بأنظمة المعالجة الآلية للمعطيات، فبمجرد القيام بفعل "دخول" أو "بقاء" في نظام معلوماتي، بطريقة احتيالية، أي عن طريق الغش، تقوم جريمة الدخول أو البقاء غير المصرح.

لكن بالرغم من ذلك، هناك جدل فقهي حول مدى تجريم فعلي "الدخول" و"البقاء" غير المصرح بهما في نظام معلوماتي، فالاتجاه الأول يرى أنه لا توجد ضرورة تستدعي تجريم مجرد الدخول أو البقاء غير المصرح بهما على النظام المعلوماتي، وخاصة إذا لم يكن لدى الفاعل نية لارتكاب جريمة لاحقة على هذا الدخول أو البقاء، ويبرر هذا الاتجاه رأيه أن هذا السلوك لا يخرج عن كونه طريقة لعرض القدرات التقنية أو الذهنية التي يتمتع بها الشخص الذي قام بهذا الفعل، وهذا الأمر لا يشكل بحد ذاته جريمة تستدعي معاقبة الفاعل، أما الاتجاه الثاني فيذهب إلى ضرورة تجريم الدخول والبقاء غير المصرح بهما إلى النظام المعلوماتي، حتى ولو لم يكن ذلك بقصد ارتكاب جريمة لاحقة فيما بعد.[1]

فالاتجاه الثاني يرى أن فعلي الدخول والبقاء غير المصرح بهما، لهما تبعات مادية تتمثل في خسائر متعددة، حيث تشير التقديرات إلى أن هناك الآن ما يزيد عن 100 ألف خبير استشاري في المجال المعلوماتي يعملون في أكثر من 20 ألف شركة في العالم وبلغ مجموع ما أنفقته الشركات على خدمات الاستشارة المعلوماتية 4.5 مليون دولار، وكل ذلك من أجل ضمان امن المبادلات الالكترونية.[2]

ويعاقب المشرع الفرنسي على جريمة الدخول والبقاء غير المصرح به، أو كما تسمى أيضا بجريمة الدخول الاحتيالي في الأنظمة المعلوماتية، بموجب نص المادة 323-1 الفقرة الأولى في إطار الفصل الثالث بعنوان: "الاعتداء على أنظمة المعالجة الآلية للمعطيات" وجاء نص المادة كما يلي:[3]

Art 323-1 : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de , 60000 € d'amend.

أي أن المشرع الفرنسي يعاقب بالحبس لمدة عامين وبغرامة قدرها 60000 أورو، كل من يدخل أو يبقى عن طريق الاحتيال في كل أو جزء من نظام المعالجة الآلية للمعطيات، فنلاحظ عدم وجود اختلاف مع ما هو منصوص عليه في التشريع الجزائري، إلا فيما يخص العقوبة.

تنص المادة 02 من اتفاقية بودابست على ما يلي: "..... عند ارتكابها عن قصد، وذلك من حيث الدخول على منظومة الكمبيوتر كليا أو على أي جزء منها دون وجه حق، وقد يلزم على الدولة

[1]– نهلا عبد القادر المومني، **المرجع السابق** ، ص 156.

[2]– محمود أحمد عبابنة، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر و التوزيع، عمان، الأردن، 2005، ص 81.

[3]- Chapitre 3: «Des atteintes aux systèmes de traitement automatisè de données»

الطرف..."،[1] كما تنص المادة 06 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في فقرتها الأولى على ما يلي: "الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به"، فنلاحظ أن كلا الاتفاقيتين قد جرمت فعل الدخول غير المشروع إلى أي نظام معلوماتي، إلا أن اتفاقية بودابست لم تنص على فعل البقاء.[2]

البند الثاني: الركن المادي لجريمتي الدخول والبقاء في النظام المعلوماتي

يتمثل الركن المادي في جريمتي الدخول أو البقاء بغش في نظام المعالجة الآلية للمعطيات في فعل الدخول أو البقاء بغش دون إحداث إتلاف وتخريب للنظام وهي الصورة البسيطة للجريمة في الفقرة الأولى، وتتحقق الصورة المشددة لها بتوافر نتيجة عن فعل الدخول أو البقاء بغش إما بمجرد حذف أو تغيير في المعطيات الموجودة في النظام وإما إتلاف وظيفة تشغيل هذا النظام.

فتقع جريمتي الدخول أو البقاء بطريق الغش إذا وقع الاعتداء على عنصر يشكل جزءا من أنظمة متعددة، فإذا تصورنا عدة أنظمة ترتبط فيما بينها أجهزة اتصال ووقع اعتداء على جهاز حاسب إلي في نظام من تلك الأنظمة المرتبطة فالجريمة تكون واقعة، فما ينطبق على الكل ينطبق على الجزء سواء كانت الشبكة مفتوحة أو مغلقة حسب طبيعة الشبكة ، وما ينوه إليه أن جرائم الاعتداء على نظم المعالجة الآلية للمعطيات تقع على محل أو موضوع واحد هو نظام المعالجة الآلية.[3]

أولا: الركن المادي لجريمة الدخول .

يمثل الركن المادي الجانب المادي للجريمة الذي يدخل في تكوينها، ويبرز هذا الجانب إلى العالم الخارجي بمظهر مادي يعبر عن سلوك ونتيجة ويتكون الركن المادي من ثلاث عناصر وهي، السلوك الاجرامي والنتيجة التي تحققت والعلاقة السببية التي تربط بين السلوك والنتيجة، وقد لا يتوفر الركن المادي دائما على هذه العناصر في جميع الجرائم، فقد يكتفي المشرع بالسلوك وحده للقول بقيام الركن المادي للجريمة دون اشتراط أن تتحقق النتيجة وصورة ذلك ما يسمى بالجرائم الشكلية وبالرجوع إلى قانون العقوبات الجزائري نجده يعاقب كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات آو يحاول ذلك.[4]

---

[1]– يراجع المادة 02، إتفاقية بودابست الخاصة بالإجرام المعلوماتي، 2001.

[2]– يراجع المادة 06، الإتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3]– يوسف مناصرة، **المرجع السابق**، ص 120– 121.

[4]– بسمة مامن، **المرجع السابق**، ص 480.

فقد نص المشرع الجزائري على فعل مادي وهو الدخول عن طريق الغش، إلا انه لم يقدم تعريفا له بل اكتفى بالقول في المادة 394 مكرر من قانون العقوبات المعدل و المتمم : ".... كل من يدخل او يبقى عن طريق الغش".[1]

ومن اهم الطرق التي تستخدم للدخول إلى النظام المعلوماتي ، الاتصال المادي المباشر بالنظام المعلوماتي والاتصال المعنوي عن بعد بالنظام المعلوماتي.

ثانيا: الركن المادي لجريمة البقاء الاحتيالي .

لقد اعتبر المشرع الجزائري البقاء الاحتيالي جريمة بموجب نص المادة 394 مكرر في فقرتها الأولى من قانون العقوبات المعدل و المتمم بقوله: "كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات...".[2]

ويتحقق الركن المادي في جريمة البقاء الاحتيالي إذا اتخذ صورة البقاء داخل النظام ويقصد بفعل البقاء كما سبق وأن وضحنا التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.

وتعتبر هذه الجريمة من الجرائم المستمرة، فالجريمة تستمر كلما زادت مدة البقاء غير المشروع داخل النظام المعلوماتي، كما أن جريمة البقاء الاحتيالي لا يشترط فيها أن تتوافر لدى المجرم نية الإضرار بالنظام المعلوماتي بل يكفي أن يقوم بمجرد البقاء فقط إذا كان غير مشروع، وقد يتسبب المجرم زيادة عن بقائه الغير مشروع في النظام إلى الإضرار بهذا الأخير.[3]

البند الثالث: الركن المعنوي في جريمة الدخول والبقاء .

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

وعليه لا يتوافر الركن المعنوي إذا كان دخول الجاني أو بقاؤه داخل النظام مسموح به أي مشروع، كما لا يتوافر هذا الركن إذا وقع الجاني في خطأ في الواقع سواء كان يتعلق بمبدأ الحق في الدخول أو الحق في البقاء، كان يجهل وجود حظر للدخول أو البقاء أو كأن يعتقد خطأ انه مسموح له بالدخول، فإذا توافر القصد الجرمي بعنصرية العلم والإرادة بالمعنى السابق لا تتأثر بالباعث من الدخول أو البقاء بالفضول أو مجرد

[1]– يراجع نص المادة 394، مكرر من ق.ع.ج، م.م.

[2]– يراجع في ذلك نص المادة 394، مكرر من ق.ع، المعدل والمتمم.

[3]– بسمة مامن، **المرجع السابق**، ص 481.

التصفح والاطلاع أو رفع التحدي وإثبات القدرة على الانتصار على النظام ووسائل الحماية فاختراق نظم الأمن الخاصة بنظام المعالجة الآلية للمعطيات يجعل فعل الدخول إليه أكثر خطورة ، فوجود هذه الأنظمة قرينة على أهمية المعلومات التي يحتوي عليها نظام المعالجة الآلية للمعطيات الذي تم الدخول إليه وإصرار الفاعل على اختراقها قرينة قاطعة على توافر القصد الجنائي لديه.[1]

الفرع الثاني: الإتلاف غير العمدي للمعطيات .

تعد جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات وإتلافها في مجال المعالجة الآلية للمعطيات من اخطر الجرائم التي تقع في هذا المجال ولاسيما بعد تراجع المحررات والمستندات والوثائق والصكوك الورقية في حين غزت المحررات الالكترونية كل المجالات مما زاد صعوبة اكتشاف وإثبات الجرائم التي ترتكب في هذا المجال ولقد عالج المشرع الجزائري هذا النمط من الجرائم من خلال نص المادة 394 مكرر من قانون العقوبات المعدل والمتمم والتي نصت على ما يلي: "يعاقب بالحبس من ستة (06) أشهر إلى سنتين (02) وبغرامة مالية من ستون ألف 60.000دج إلى مئتي ألف 200.000دج ، كل من يدخل او يبقى وعن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".[2]

ومن أركان جريمة الاعتداء على سير نظام المعالجة الآلية وإتلاف المعلومات هناك كل من الركن المادي وكذا الركن المعنوي لجريمتي الغش المعلوماتي وكذا جريمة إتلاف المعلومات:

البند الأول: الركن الشرعي لجريمة الإتلاف الغير العمدي للمعطيات

تنص المادة 394 مكرر في فقرتها الثانية والثالثة من قانون العقوبات الجزائري المعدل والمتمم على ما يلي: "...تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة"، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من سنة (1) إلى ثلاث (3) سنوات والغرامة من 100.000 دج الى 300.000دج".[3]

ويستخلص من نص المادة انها تتضمن صورة مشددة لجنحتي الدخول أو البقاء الغير الشرعي متى ترتب عليه نتيجة معينة تتمثل في إتلاف المنظومة إما بالحذف أو التغيير أو التخريب، على ان لا يكون بصورة عمدية وهذا ما سيتم تبيانه في كل من الركنين المادي والمعنوي.

---

[1]– يوسف مناصرة، **المرجع السابق**، ص 133، 134.

[2]– يراجع في ذلك نص المادة 394، مكرر من ق.ع، م .م.

[3]– نسيمة جدي، **المرجع السابق**، ص 58.

البند الثاني: الركن المادي لجريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات وإتلاف المعلومات

يتم التمييز بين الركن المادي في جريمة الغش المعلوماتي و الركن المادي في جريمة اتلاف المعلومات و هذا على النحو المذكور ادناه:

أولا: الركن المادي في جريمة الغش المعلوماتي

تعد جريمة الغش المعلوماتي في مجال المعالجة الآلية للمعطيات من أخطر طرق الغش التي تقع في هذا المجال ولا سيما بعد تراجع المحررات والمستندات والوثائق والصكوك الورقية في حين غزت المحررات الالكترونية كل المجالات مما زاد صعوبة اكتشاف وإثبات الغش في هذا المجال، أو هو تغيير الحقيقة في مستند رسمي ولكن المستند هنا ليس مستندا عاديا بل هي عبارة عن تسجيلات الكترونية أو محررات الكترونية.[1]

وقد أشار المشرع بخصوص الغش بقوله :.... عن طريق الغش .... خاصة مع تزايد حجم الاعتداءات الواقعة على المعطيات المخزنة داخل الحاسب الآلي التي تمس الأفراد في حقوقهم وأموالهم وحياتهم الخاصة وأمام تزايد فرص الأشخاص للعبث والتلاعب في معطيات الحاسب بتبديلها وتحويرها بالشكل الذي يفقد الثقة بالتقنية ويمس مراكز الأفراد بات من الواجب بسط الحماية لهذه المعلومات وضمان أمنها وسلامتها من كل تبديل وغش.[2]

ويتمثل الركن المادي لجريمة الغش المعلوماتي في تغيير الحقيقة في محرر معلوماتي بإحدى الطرق ولقيام هاته الجريمة التي نص عليها القانون وهو تغيير من شانه أن يسبب ضرر لا بد من توفر ثلاثة عناصر أساسية: وجود محرر، تغيير الحقيقة، الضرر.[3]

ثانيا: الركن المادي لجريمة إتلاف المعلومات

إن هذه الجريمة مستقلة بذاتها عن الجريمة السابقة بالرغم من أن الفعل يرد من بعد، أي لاحق لجريمة الدخول بغش والوسائل المستعملة للمساس بالنظام متعددة ونعد منها تخريب الجهاز، فيروس، قنبلة منطقة، تغيير في الرقم السري ... الخ والنتائج المترتبة عنها توقف كامل أو جزئي للنظام، استحالة استعمال النظام أو نقص ملحوظ في قدرة المعالجة للنظام (تباطؤ في المعالجة).[4]

---

[1]– محمود احمد عبابنة، **المرجع السابق**، ص 107.

[2]– محمود احمد عبابنة، **المرجع نفسه**، ص 108.

[3]– بسمة مامن، **المرجع السابق**، ص 485.

[4]– يوسف مناصرة ، **المرجع السابق**، ص 138.

قد يتخذ الركن المادي لجريمة إتلاف المعلومات إما صورة إجراء تعديلات غير مشروعة لها، أو تدميرها أو الإدخال غير المشروع للمعلومات داخل أنظمة الحاسبات الآلية:

1- **فعل الإدخال:** هو إضافة معطيات جديدة على الدعامة الخاصة بها سواء خالية أو يوجد عليها معطيات من قبل وقد يكون بإدخال معطيات وهمية إلى النظام المعلوماتي بقصد التشويش على صحة البيانات القائمة.

2- **تدمير المعلومات:** يعد تدمير المعلومات بدوره صورة من صور الإتلاف وإن كان ابعد أثار من مجرد إجراء بعض التعديلات للمعلومات ويتم ذلك من خلال ما يلي:

3- **فعل المحو أو الإزالة:** يقصد به إزالة كل أو جزء من المعطيات الموجودة داخل النظام أو نقل وتخزين المعطيات إلى المنطقة الخاصة بالذاكرة، ويعتبر المحو جريمة إتلاف طالما وقع إتلاف أو تخريب للشيء موضوع الجريمة وتعطيله أيا كانت الوسيلة المستخدمة.

4- **فعل التعديل:** يقصد به تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، وقد يكون عن طريق المصيدة أو المداخل المميزة التي هي عبارة عن ممرات خالية يمكن من خلالها الولوج إلى التعليمات المخزنة ومن ثمة التوصل إلى الشفرات والتعليمات، وقد ترتكب هذه الجريمة من قبل أشخاص معيين كان يكون المسؤول عن المعالجة هو مرتكب الجريمة نفسه أو المعالج من الباطن هو الذي قام بارتكاب الجريمة.[1]

البند الثالث: الركن المعنوي لجريمة إتلاف المعلومات

إن جريمة تعطيل أو إفساد نظام المعالجة الآلية للمعطيات جريمة قصدية يتخذ الركن المعنوي فيها صورة القصد الجنائي بعنصر العلم والإرادة فيجب أن تتجه الإرادة إلى فعل عرقلة، تعطيل أو فعل الإفساد كما يجب أن يعلم بأن نشاطه الإجرامي يؤدي إلى تعطيل أو إفساد نظام المعالجة الآلية للمعطيات وأن يعلم أن ذلك يتم بدون رضا صاحب الحق في السيطرة على ذلك النظام ضد إراداته فإذا توافر الركن المعنوي بعنصريه السابقين إلى جانب الركن المادي قامت الجريمة واستحق مرتكبها العقوبة المنصوص عليها في المادة 394 مكرر فقرة 03 من قانون العقوبات الجزائري المعدل و المتمم.[2]

إن فعل الإتلاف يتطلب وجود القصد الجنائي وهنا يكفي فقط قيام القصد العام أي وجود نية الجاني إلى إتلاف الأموال الثابتة أو المنقولة وكذلك وجوب علم الجاني بان فعله يؤدي إلى إتلاف أموال مملوكة للغير، وعدم العلم ينفي القصد الجنائي، ففي الجريمة المتعلقة بإعاقة سير نظام معلوماتي أو الجريمة المتعلقة بإعاقة سير نظام معلوماتي أو الجريمة المتعلقة بالاعتداء على المعلومات الموجودة داخل الجهاز

---

[1]- عائشة بن قارة مصطفى،" ***آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم 18/07"***، مجلة العلوم القانونية والسياسية، جامعة الوادي ، الجزائر، م10، ع01، أفريل 2019، ص 746.

[2]- يوسف مناصرة ، **المرجع السابق**، ص 142.

فيجب أن تتجه إرادة الجاني إلى قصد إتلاف المال وذلك بالقيام بوضع برنامج من شانه أن يغير المعلومات ا وان يقوم بمحو البيانات إذا فمن يعمل هذا العمل الإجرامي يجب أن يكون على درجة عالية من الناحية التقنية في مجال المعلوماتية، وبالتالي فهو يعلم أن هذه الأموال المعلوماتية التي تتجه إرادته إلى إتلافها تعود للغير فان القصد الجنائي يكون متوافرا وتقوم الجريمة المنصوص عليها باكتمال أركانها.

الفرع الثالث: التلاعب بالمعطيات .

يطلق عليها أيضا اسم "جريمة المساس العمدي للمعطيات"، وهي الجريمة المنصوص عليها في المادة 394 مكرر من قانون العقوبات الجزائري المعدل و المتمم ، وتتمثل هاته الجريمة في القيام بجملة من الأفعال التي تعتبر اعتداءات عمدية على المعطيات، والنشاط الإجرامي في هذه الجريمة يتمثل في أفعال الإدخال والمحو والتعديل، ويكفي توافر احدها لقيام الجريمة فلا يشترط اجتماعها حتى يقوم النشاط الإجرامي، ومن ثمة فان القاسم المشترك في هذه الأفعال جميعا فهو انطوائها على التلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة غير صحيحة أو محو أو تعديل أخرى قائمة.[1]

فالجريمة في هذه الحالة تقع على المعطيات أي البيانات المعالجة دون المعلومات ذاتها، فموضوع السلوك الإجرامي في هذه الجريمة محدد، وهو الاعتداء على معطيات في نظم المعالجة أي البيانات التي أدخلت لمعالجتها وتحولت إلى معطيات عبارة عن رموز أو إشارات تمثل تلك المعلومات، أي بيانات تمت معالجته.

البند الأول: الركن الشرعي لجريمة التلاعب بالمعطيات

تنص المادة 394 مكرر 1 من قانون العقوبات الجزائري المعدل و المتمم على ما يلي: "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية للمعطيات أو أزال أو عدل بطريق الغش، المعطيات التي يتضمنها"،[2] فنلاحظ أن المشرع الجزائري قد جرم فعل التلاعب بمعطيات الحاسب الآلي، سواء كان ذلك عن طريق الإدخال، التعديل أو الإزالة، والتي يترتب عنها تغيير في حالة المعطيات.

كما نص عليه المرسوم الرئاسي رقم 14 -252 الذي يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، في المادة 08 منه على ما يلي: "تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق".

---

[1]- محمد نجيب حسني، **الموجز في شرح ق.ع القسم الخاص**، دار النهضة العربية، القاهرة، مصر، 2003، ص 253.

[2]- يراجع في ذلك نص المادة 394 مكرر 01، ق.ع، م .م.

أما بالنسبة لاتفاقية بودابست الخاصة بالإجرام المعلوماتي، فقد نصت على جريمة التلاعب بمعطيات الحاسب الآلي في نصوص المواد 04، 08 كالآتي وعلى التوالي المادة 04: "..... وذلك من حيث إتلاف، أو إلغاء، أو إفساد أو تغيير أو تدمير البيانات الموجودة بالكمبيوتر دون وجه حق...."،[1] المادة 08: "..... وذلك من حيث إحداث خسائر بممتلكات الغير عن طريق: (أ) أية عمليات إدخال برامج تشغيل على الكمبيوتر أو تزويده بمعلومات أو بيانات، أو تبديلها أو تغييرها، أو إلغائها أو تدميرها، (ب) أي نوع من التدخل في طبيعة عمل منظومة الكمبيوتر، بقصد يشوبه التدليس وعدم الأمانة أو بقصد غير شريف للحصول بدون وجه حق على منفعة أو فائدة الكترونية لصالح الشخص ذاته أو لصالح الغير".[2]

إضافة إلى ما نص عليه المشرع الفرنسي في المادة 323-03 كالآتي:

Art 323-3: «Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les donnes qu'il contient est puni de cinq ans d'emprisonnement et de 150.000 € d'amende»,[3]

ويقصد بذلك، أن المشرع الفرنسي يعاقب كل من أدخل بيانات عن طريق الغش لنظام المعالجة الآلية للمعطيات أو قام بمحوها أو نقلها أو إزالتها أو تعديلها، بعقوبة الحبس لمدة خمس سنوات وغرامة تساوي 150.000 يورو، فنلاحظ أن مختلف التشريعات والاتفاقيات السابقة، قد جرمت كل اعتداء قد يقع على نظام المعالجة الآلية للمعطيات، وذلك بإتيان أي سلوك يؤدي إلى هذا الاعتداء، وهوما قام به المشرع الجزائري من خلال نص المادة 394 مكرر 01 من قانون العقوبات الجزائري المعدل و المتمم.

البند الثاني: الركن المادي لجريمة التلاعب بالمعطيات

الركن المادي لجنحة المساس بالمعطيات أو التلاعب بها يتحقق بإتيان الجاني لفعل من الصور الثلاث التالية: الإدخال، المحو أو الإزالة، التعديل وهي الصور المنصوص عليها بالمادة 394 مكرر 1 من قانون العقوبات الجزائري المعدل و المتمم السالف الذكر، ولا يشترط الركن المادي توافر الصور الثلاث بل يكفي أن يقوم الجاني بإدخال معطيات مغلوطة جديدة لم تكن موجودة أو محو معطيات موجودة أو تعديل أخرى كانت موجودة أصلا يحتويها النظام، فغاية الأمر أن يرد الأمر على معطيات بإحدى الصور الثلاث التي سوف نقوم بشرحها شرحا مفصلا.[4]

أولا- الإدخال غير المشروع للمعلومات :

[1]- يراجع المادة 04، اتفاقية بودابست الخاصة بالإجرام المعلوماتي، 2001.

[2]- يراجع المادة 08، اتفاقية بودابست الخاصة بالإجرام المعلوماتي، 2001.

[3]- يراجع المادة 323-03، القانون الفرنسي، رقم 88-19.

[4]- نسيمة جدي، **المرجع السابق**، ص 63.

ويقصد به إضافة معلومات جديدة على الدعامة الخاصة بها، سواء كانت خالية أم توجد عليها معطيات من قبل، ويتم ذلك من خلال تغدية الحاسب الآلي ونظامه بالمعلومات والبيانات المراد معالجتها آليا، أو بتعليمات لازمة لعملية المعالجة.

إن إدخال المعلومات بصورة غير مشروعة في نظام الحاسب الآلي قد ينتج عنه إضافة إلى تعديل ذاكرة الحاسب الآلي تعديل في المعلومات ذاتها أو تدميرها، وذلك بمحوها كما في حالة إدخال احد البرامج الخبيثة إلى نظام الحاسب الآلي، والذي يؤدي إلى إلحاق تعديل أو محو بالمعلومات الموجودة داخله إذ يتحقق فعل الإدخال المكون لجريمة الإتلاف المعلوماتي في كل حالة يتم فيها إدخال برنامج خبيث إلى الحاسب الآلي أو يؤدي إلى إضافة معلومات جديدة إلى المعلومات القائمة أصلا والتي قد يلحقها تعديل أو محو في النهاية كنتيجة لهذه الإضافة.[1]

كما توجد طريقة يطلق عليها اسم (بلوف) تتمثل في استخدام النظام من اجل طبع فواتير مصطنعة يقوم العملاء بتسديدها، أيضا في حالة أخرى قام المدعو فلادمبير بوريليت وهو مهاجر روسي بإدخال فواتير وهمية لا حصر لها وتحويل ما تم تسديده لحساب شركات وهمية اصطنعها أيضا.

ويعد اصطناع المعلومات هو الصورة الأكثر سهولة لاسيما في المنشآت المالية خاصة من المسؤول عن القسم المعلوماتي الذي يمكنه خلق مستخدمين غير موجودين أو عدم حذف المصروفين من مناصب عملهم وتحويل حقوقهم المالية إلى حساب الجاني أو لحساب فتح خصيصا لهذا الغرض وهي المعطيات التي لم تكن موجودة.[2]

ثانيا– المحو أو الإزالة:

إن فعل الإزالة ليس له مصطلح موحد ، نصت عليه المادة 394 مكرر 1 من ق.ع.ج المعدل والمتمم، ويختلف التعبير الذي يستعمله كل تشريع في تجريمه لهذا الفعل، فاتفاقية بودابست عند تجريمها لمختلف أشكال العدوان على سلامة المعطيات ضمنت المادة الرابعة (4) منها عدة مصطلحات تصب في سياق الإزالة وهي مصطلحات الإضرار، المحو، الإتلاف، الطمس.

ويعرف فعل الإزالة بأنه إزالة جزء من المعلومات المسجلة على الدعامة الموجودة داخل النظام أو تحطيم تلك الدعامة أو نقل أو تخزين جزء من المعلومات إلى المنطقة الخاصة بالذاكرة.

[1]– البركه الطيبي، **المرجع السابق**، ص 191.

[2]– نسيمة جدي، **المرجع السابق**، ص65.

إن محو المعلومات هي مرحلة لاحقة على عملية إدخال المعلومات فالمحو (الإزالة) تفترض الوجود السابق لعملية الإدخال، بمعنى ان محو المعلومات يعني إزالتها أي تدميرها بصورة كلية أو جزئية.[1]

ثالثا– التعديل :

ويقصد بالتعديل تغيير المعطيات الموجود داخل النظام واستبدالها بمعطيات أخرى، كما يشير إلى أي تغيير غير مشروع للمعلومات والبرامج والذي يتم عن طريق استخدام ووظائف نظام المعالجة الآلية.

ويعرف التعديل أيضا بأنه تغيير لحالة المعطيات الموجودة دون تغيير الطبيعة الممغنطة لها أو هو كل تغيير غير مشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى ووظائف الكمبيوتر ويتحقق فعل التغيير عن طريق برامج غريبة تتلاعب بالمعطيات.[2]

وكقاعدة يتم تعديل المعطيات باستعمال الفيروسات والقنابل المعلوماتية التي يصنعها شخص على درجة عالية من الذكاء وذو قدرة عالية وتحكم بالتقنيات المعلوماتية وهو الملقبون ب "المجرمين ذوي آلياقات البيضاء" كفيروس الدودة الذي يمكن له في مرحلة متقدمة ليس تعديل النظام فقط بل قد يصل لتعطيل النظام، أيضا نجد القنابل الموقوتة التي يرتبط بدأ تشغيلها بواقعة أو كلمة محددة أو تاريخ أو ساعة معينة متى قام بها المستخدم نشط البرنامج لتغيير محتوى المعطيات وهي الوسائل التي تحقق الجريمة في صورة المحو السالفة الذكر أو التعديل، وبهذا المفهوم يخرج من هذه الصور نسخ المعلومات الموجودة ونقلها إذ لا تنطوي هذه الأعمال على إدخال ولا تعديل.[3]

البند الثالث: الركن المعنوي لجريمة التلاعب بالمعطيات

إن جريمة التلاعب بالمعطيات تعتبر من الجرائم العمدية، والتي لا بد لقيامها من توافر قصد جنائي عام لدى مرتكبها، ومع ذلك ذهبت بعض التشريعات إلى طلب قصد جنائي خاص إضافة إلى القصد الجنائي العام.

أولا– القصد الجنائي العام :

يتحقق القصد الجنائي العام وفق القواعد العامة بتوافر عنصريه العلم والإرادة وانصراف كليهما الى كافة العناصر التي يتكون منها الركن المادي للجريمة، وفي جريمة الاتلاف المعلوماتي (جريمة التلاعب بالمعطيات) ينبغي أن ينصرف علم الجاني إلى انه يقوم بإدخال أو تعديل أو محو (إزالة) المعلومات وأن يعلم بأن نشاطه غير مشروع، ويشكل اعتداء على صاحب الحق في المعلومات أومن له السيطرة عليها، وأن

[1]–البركه الطيبي، **المرجع السابق**، ص 195.

[2]– أمال قارة، **الحماية الجزائية للمعلوماتية في التشريع الجزائري** ، ط1، دار هومة، الجزائر ، 2008، ص 122.

[3] – نسيمة جدي، **المرجع السابق**، ص 68.

من شأن نشاطه هذا أن يؤدي إلى نتيجة هي تغيير حالة المعلومات ومن تم تتجه إرادته إلى هذا النشاط وتلك النتيجة.[1]

ولا يشترط أن يكون القصد الجنائي مباشرا، بل يكفي لقيام العمد أن تتخذ الإرادة شكل القبول أي قبول النتيجة، وهذا ما يسمى بالقصد غير المباشر أو القصد الاحتمالي، وفيه يستوي لدى الجاني وقوع النتيجة من عدمها، كما لا يشترط أن يكون القصد محددا إذا تقوم الجريمة سواء حدد القصد بمعلومات معينة أولم يحدد.

ثانيا– القصد الجنائي الخاص :

يستفاد من نص المادة 394 مكرر 1 من ق.ع.ج المعدل والمتمم أن المشرع الجزائري لا يتطلب توافر قصد خاص لدى الجاني لقيام جريمة التلاعب بالمعطيات، ذلك أن القصد الخاص هو انصراف العلم والإرادة إلى وقائع لا تدخل ضمن عناصر الجريمة وأركانها.

في الواقع أن اغلب التشريعات التي جرمت أفعال الإتلاف المعلوماتي (التلاعب بالمعطيات) لم تتطلب قصد خاص يقوم عليه الركن المعنوي لهذه الجريمة إلا فئة قليلة من هذه التشريعات.

من بناء المادة 394 مكرر 1 ومن خلال مصطلح "الغش" الذي استعمله المشرع، نستنتج أن هذا الأخير اشترط أن تكون الجريمة عمدية، وبالتالي هذه الجريمة لا تتطلب قصد جنائي خاص.[2]

الفرع الرابع: التعامل في المعطيات غير المشروعة

إن جرائم المعطيات من اخطر الجرائم وأكثرها ضررا، خاصة إذا كانت تلك المعطيات التي يتم الاعتداء عليها تتعلق بأمن الدولة أو تتعلق بالحياة الخاصة أو تمثل فيها قيمة مالية مهمة ولهذا حرص المشرع في خطته لمكافحة هذه الجرائم على التصدي لها قبل وقوعها وذلك بمنع كل الأفعال التي تشكل مقدمة لها فقام بتجريم مجموعة من الأفعال تصب كلها في التعامل في معطيات صالحة لا ترتكب بها إحدى جرائم المعطيات فإذا لم ينجح فردع الجناة عن القيام بجرائمهم فقد حرص المشرع على التقليل من الضرر أن تسببه جرائم المعطيات التي يتم الحصول عليها من إحدى الجرائم.

حيث قامت المادة 394 مكرر 2 من ق.ع.ج.م.م من تجريم التعامل في كل المعطيات غير المشروعة سواء كانت صالحة لان ترتكب بها جريمة أو كانت متحصلة من جريمة.

لم يكتف المشرع بتجريم التعامل في المعطيات الصالحة لارتكاب جريمة بل جرم أيضا التعامل في معطيات متحصلة من جريمة، وإذا كان المشرع يهدف من خلال تجريمه التعامل في المعطيات الأولى إلى

[1]– نائلة عادل محمد فريد قورة ، **المرجع السابق** ، ص 368.

[2]– ناصر حمودي ، **المرجع السابق** ، ص 81.

منع حدوث الجريمة فانه في حالة حدوث هذه الأخيرة يحاول أن يقضي قدر ما أمكن القضاء عليه من أثار هذه الجريمة.[1]

فهذه الجريمة قد تفسر الحصول على معطيات معينة ويكون من الخطر وجودها في حوزة غيره صاحبها أو استعماله أو إفشاؤه أو نشره فالمشرع أراد أن يضيق إلى أكبر قدر ممكن من دائرة الأشخاص الذين يمكن أن يتعاملوا في هذه المعطيات التي تم الحصول عليها بطريقة غير مشروعة سعيا منه للحفاظ على سريتها فجرم أنواعا من السلوك يمكن أن ترد على هذه المعطيات فتفقدها هذه السرية.[2]

ومن هنا سنتناول أركان جريمة التعامل في معطيات غير مشروعة:

البند الأول: الركن الشرعي لجريمة التعامل في معطيات غير مشروعة

لقد نص المشرع الجزائري في المادة 394 مكرر 02 من قانون العقوبات الجزائري المعدل والمتمم على ما يلي: "يعاقب بالحبس من سنة (1) إلى خمس (5) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا وعن طريق الغش بما يأتي: 1- تصميم أو بحث أو تجميع أو توفير أو نشر أو 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".[3]

وهوما نص عليه المشرع الفرنسي أيضا في نص المادة 323-1-3 من قانون العقوبات بقوله:

«Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, de céder ou de mettre à disposition un équipement, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines est prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus , sévèrement réprimée».[4]

فالمشرع الفرنسي من خلال هذه المادة، يعاقب على كل عملية بحث أو جلب "Recherche ou Importation "، عبر شبكات الاتصال المعلوماتية أو أي مصدر أخر، وكذلك عملية تجميع Reuinir ou rassembler et detenir معطيات معلوماتية، أو عملية توفير أو نشر

[1]- محمد خليفة، **المرجع السابق**، ص 194.

[2]-محمد خليفة ، **المرجع السابق** ، ص 196.

[3]- يراجع المادة 394، مكرر 02، ق.ع.م.م.

[4]- يراجع المادة، 323-1-3، **من القانون الفرنسي**، رقم 88-19.

Offrir ceder, mettre a disposition معطيات معلوماتية مغرضة، ما يلاحظ على نص المادة السالفة المتعلقة بجريمة التعامل في معطيات غير مشروعة م (323-1-2-3) ،أن المشرع الفرنسي قد وسع في تعريف المعطيات، عندما قال Equipement تجهيز،Instriment آلة، Programme informatique أو أي معطيات أخرى تعد لارتكاب جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات .

على عكس المشرع الجزائري الذي حصرها في مصطلح واحد وهو "معطيات معلوماتية"، فصياغة المشرع الفرنسي كانت أوسع وأشمل لأنه حسب نص المادة، 323-3-1 فالوسيلة يمكن أن تكون مادية أو معنوية، عكس المشرع الجزائري الذي حصرها في الوسيلة المعنوية فقط "المعطيات"،[1] وعليه، فإنه يفترض على المشرع الجزائري أن يستدرك هذا الفراغ القانوني، ويوسع من الوسيلة المستعملة في هاته الجريمة.

نصت المادة 06 من اتفاقية بودابست لمكافحة الإجرام المعلوماتي، على جريمة التعامل في معطيات غير مشروعة، تحت عنوان **"إساءة استخدام الأجهزة"**، وهوما نص عليه أيضا، المرسوم الرئاسي رقم 14-252، المؤرخ في 8 سبتمبر 2014 المتضمن **"التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات"**، في نص المادة 09 تحت عنوان **"جريمة إساءة استخدام وسائل تقنية المعلومات"**.

غير أنه يوجد اختلاف بين ما نص عليه المشرع الجزائري وما نصت عليه اتفاقية بودابست لمكافحة الإجرام المعلوماتي، وكذا المرسوم الرئاسي رقم 14-252 المتضمن **"التصديق على الاتفاقية العربية لمكافحة وسائل تقنية المعلومات"**، وذلك فيما يخص **"عبارة كلمة سر"**، فالمرسوم الرئاسي رقم 14-252 قد ذكر في الفقرة الأولى من المادة 09 عبارة (ب) كلمة سر نظام معلومات أو....،[2] واتفاقية بودابست لمكافحة الإجرام المعلوماتي في المادة 06،[3] قد ذكرت أيضا في الفقرة الأولى منها عبارة **(-2 كلمة السر الخاصة بالكمبيوتر، أو الكود الشفري للدخول ....)**، على غرار المشرع الجزائري الذي لم يتناول هذه الجزئية.

---

[1]- المعطيات المعلوماتية: هي المعلومات و البيانات التي يتم تنظيمها ومعالجتها داخل نظام المعالجة الآلية للمعطيات، وتخزينها بغية استرجاعها عند طلبها، و المعطيات عبارة عن نبضات الكترونية داخل الحاسب غير ملموسة، أنظر: محمد خليفة، المرجع السابق، ص 25. وتعرفها اتفاقية بودابست، 2001، باللغة الفرنسية، في نص المادة الأولى بقولها:

-« données informatique » désigne tout représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction »

يراجع: المادة 01، اتفاقية بودابست الخاصة بالإجرام المعلوماتي، 2001.

[2]- يراجع المادة 09، اتفاقية بودابست لمكافحة الإجرام المعلوماتي، 2001.

[3]- يراجع المادة 06، اتفاقية بودابست لمكافحة الإجرام المعلوماتي، 2001.

البند الثاني: الركن المادي لجريمة التعامل في معطيات غير مشروعة

هي جريمة شكلية أو جريمة خطر لا يعتد المشرع في قيامها بتحقيق نتيجة معينة، فيكفي أن يقوم الجاني بأحد الأفعال التي تنص عليها المادة 394 مكرر 2 ق.ع.م.م، ليكتمل الركن المادي لهذه الجريمة.

محل جريمة التعامل في معطيات صالحة لارتكاب جريمة كما أشارت إليه المادة 394 مكرر 2 ق.ع.م.م هو المعطيات المخزنة أو المعالجة أو المرسلة عن طريق منظومة معلوماتية، ويلاحظ أن هذه المادة تختلف عن المادتين السابقتين لهما والمتعلقتين بجريمتي الدخول والبقاء غير المصرح بها والتلاعب بالمعطيات، وذلك في نقطتين:

- أولهما نقل بالحالة التي توجد عليها المعطيات محل الجريمة.
- ثانيهما تتعلق بالنظام الذي توجد به هذه المعطيات.[1]

فجريمة التعامل في معطيات صالحة لارتكاب جريمة فهو أي منظومة معلوماتية، ولا شك أن هذه الأخيرة تختلف عن نظام المعالجة الآلية للمعطيات أضيق منه، ونرى أن المشرع من خلال هذا التغيير لم يرد حصر هذه الجريمة في المعطيات المعالجة عن طريق نظام المعالجة الآلية وإنما أراد أن يتسع مجالها إلى مختلف المعطيات مهما كانت حالتها سواء كانت مخزنة (ثابتة) أو مرسلة (متحركة) أو معالجة وهذا مسلك يبرره كثيرا من المعطيات التي يمكن أن ترتكب بها الجرائم قد لا توجد داخل نظام المعالجة الآلية للمعطيات وإنما تكون مخزنة داخل وسائط أخرى أو تكون مرسلة بين نظم المعلومات وبالتالي فعدم تقييد النص بأنظمة المعالجة الآلية والمعطيات المعالجة كان الهدف منه أن يشمل مختلف المعطيات الصالحة لارتكاب الجريمة،[2] وإذا كان قانون العقوبات الجزائري قد اقتصر على المعطيات كمحل للجريمة فان قانون العقوبات الفرنسي كان أكثر توسعا في ذلك وهو ما أقرته المادة 323ف01-03 إن التعاملات المجرمة يمكن أن تقع على تجهيزات أو أدوات أو على برنامج معلوماتي أو على كل معطيات مصممة أو معدة لارتكاب واحد أو أكثر من جرائم الدخول أو البقاء غير المصرح بهما، أو إعاقة إفساد أنظمة المعالجة الآلية للمعطيات أو التلاعب بالمعطيات وهو في هذا يختلف عن المشرع الجزائري الذي لا يشترط أن تكون المعطيات مخصصة ومعدة لارتكاب الجريمة وإنما يكتفي بان تكون صالحة أو قابلة لان ترتكب بها الجريمة والظاهر أن المشرع الفرنسي قد سلك في هذا الأمر اتفاقية بودابست، والتي حددت نطاق هذه الجريمة بالأجهزة التي يمكن القول موضوعيا بأنها مصممة أساسا من اجل لارتكاب جريمة، فالمادة 06 من هذه

[1]- أمال قارة، **المرجع السابق** ، ص 66.

[2]- محمد خليفة، **المرجع السابق**، ص197.

الاتفاقية تجعل محلا لهذه الجريمة كل جهاز يحتوي على برامج معلوماتي مصمم أو موفق بشكل أساسي بغرض ارتكاب إحدى الجرائم المنصوص عليها.[1]

أما السلوك الإجرامي في جريمة التعامل في معطيات غير مشروعة يتخذ صورتين اثنين:

- **الصورة الأولى:** تتمثل في التعامل في معطيات صالحة لارتكاب جريمة.
- **الصورة الثانية:** هي التعامل في معطيات متحصلة من جريمة ولا يتطلب المشرع لقيام هذه الجريمة تحقق نتيجة معينة ولهذا فهي تقوم بمجرد ارتكاب أحد أنواع السلوك أو الأفعال التي تنص عليها المادة 394 مكرر 2 من قانون العقوبات الجزائري المعدل و المتمم.

أولا- التعامل في معطيات صالحة لارتكاب جريمة :

تجرم المادة 394 مكرر 2 من قانون العقوبات الجزائري المعدل و المتمم، في البند الأول منها مجموعة من الأفعال الخطرة والتي تركت دون تجريم لأدت إلى حدوث جرائم أخرى هذه الأفعال تشمل كافة أشكال التعامل الواقعة على معطيات الحاسب الآلي، والتي تسبق عملية استعمال هذه المعطيات في ارتكاب هذه الجريمة،[2] فالمعطيات قبل هذه المرحلة الأخيرة تمر بالعديد من المراحل حتى تصل إلى يد الجاني فيرتكب بها جريمته، وهذه المراحل تبدأ من تصميم هذه المعطيات والبحث فيها وتجميعها وصولا إلى جعلها في متناول الغير، وتحت تصرفه وذلك بتوافرها أو نشرها أو الاتجار فيها ولا يشترط أن تقع هذه الأفعال مجتمعة لتقوم الجريمة، بل يكفي أن تقع إحداها فقط والمقصود بالتعامل هنا ليس هو التعامل بمفهومه في القانون المدني، وإنما هو تعامل بمفهوم أوسع إذ يقصد به في الجريمة محل الدراسة كل سلوك له علاقة بإعداد وإنتاج المعطيات غير المشروعة أو كل سلوك يكشف عن وجود صلة معينة بين شخص ومعطيات غير مشروعة، هذه الصلة تتمثل في القيام بأحد أنواع السلوك التي نصت عليها المادة 394 مكرر 2 قانون العقوبات الجزائري المعدل و المتمم ، والتي أطلقنا عليها اسم "التعامل" وتتمثل في السلوكيات التالية: التصميم- البحث- التجميع- التوفير- النشر- الاتجار.....[3]

- **التصميم:** هي أول عملية في سلسلة التعامل في المعطيات وهي تتمثل في إخراج المعطيات إلى الوجود أي القيام بخلق وإيجاد معطيات صالحة لارتكاب جريمة، وهذا العمل يقوم به المختصون في هذا المجال كمصممي البرامج ومثال هذه الجريمة تصميم برنامج يحمل فيروسا وهذا ما يطلق عليه بالبرامج الخبيثة.
- **البحث:** يقصد بالبحث في نص المادة 494 مكرر 2 من قانون العقوبات الجزائري المعدل و المتمم ، البحث عن الوسيلة التي يمكن ترتكب بها الجريمة لا يعد جريمة فمن يبحث عن سكين لا يعد مرتكبا لجريمة، وعلى

[1]- ناصر حمودي ، **المرجع السابق**، ص 97.

[2]- محمد زكي أبو عامر، **قانون العقوبات القسم الخاص**، دار الجامعة الجديدة، الإسكندرية، مصر، 2005، ص 761.

[3]- محمد زكي أبو عامر **المرجع نفسه**، ص 762.

هذا نرجح ان المشرع يقصد بهذه العبارة البحث في كيفية تصميم هذه المعطيات وإعدادها وليس مجرد البحث عن هذه المعطيات ولهذا جاءت عبارة البحث بعد عبارة التصميم مباشرة.

- **التجميع:** وهو القيام بجمع العديد من المعطيات التي يمكن أن ترتكب بها جريمة الدخول غير المصرح بها وجريمة التلاعب ويفترض هذا السلوك أن صاحبه يحتفظ بمجموعة من المعطيات التي تشكل خطرا والتي من الممكن استعمالها في ارتكاب تلك الجرائم، وقد استخدمت اتفاقية بودابست مصطلح "الحصول للاستخدام" وما يميز هذا المصطلح عن مصطلح التجميع أن الأول يقتضي وجود نية استخدام المعطيات المتحصل عليها ولا يشترط عددا معينا فيها بينما الثاني التجميع لا مثل تلك النية ويشترط تعدد المعطيات.
- **التوفير:** (الوضع تحت التصرف أو العرض).

من الأفعال التي تجرمها المادة 394 مكرر 2 من قانون العقوبات الجزائري المعدل و المتمم ، أيضا فعل التوفير، أي توفير معطيات تمكن أن ترتب بها جريمة دخول أو بقاء أو جريمة تلاعب، وتعاقب المادة 323ف1-3 على نفس السلوك تحت مصطلح ceder كما تعاقب عليه المادة 6 من اتفاقية بودابست تحت عبارة أي أشكال للوضع تحت التصرف، والمراد بذلك هو تقديم المعطيات وإتاحتها لمن يريدها، أي جعلها في متناول الغير، ووضعها تحت تصرف.[1]

ثانيا- التعامل مع معطيات متحصلة من جريمة :

الصورة الثانية من صورتي جريمة التعامل في معطيات غير مشروعة هي التعامل في معطيات متحصلة من جريمة وتتحقق الجريمة في صورتها بواحد من أربعة أفعال هي حيازة معطيات متحصلة من جريمة أو إفشاؤها أو نشرها أو استعمالها، أي انه يكفي تحقق واحد من هذه الأفعال فقط لكي يقوم السلوك الإجرامي وتتمثل في الحيازة والإفشاء والنشر والاستعمال.

أما النتيجة الإجرامية لا تتطلب حدوث نتيجة ولا تتطلب تحقق ضرر فعلي وحال يقع على معطيات ما أو على أنظمة معالجته، فهو إنما يجرم تلك الأفعال ليس بوصفها أفعالا خطيرة يمكن أن تؤدي معالجتها فهو إنما يجرم تلك الأفعال ليس بوصفها أفعالا خطرة يمكن أن تؤدي إلى ضرر مباشر وحال، وإنما يجرمها بوصفها أفعالا خطرة يمكن أن تؤدي إلى ضرر فعلي.[2]

البند الثالث: الركن المعنوي لجريمة التعامل في معطيات غير مشروعة

جريمة التعامل في المعطيات غير المشروعة في صورتيها هما: التعامل في معطيات صالحة لارتكاب جريمة من جرائم المعطيات والتعامل في معطيات متحصلة من جريمة تقومان على القصد الجنائي العام ولا

[1] – محمد زكي أبو عامر، **المرجع السابق**، ص 763.

[2] – محمد خليفة، **المرجع السابق**، ص 212.

تطلب قصداً خاصاً في الصورة الثانية، وسنتكلم فيما يلي عن القصد الجنائي العام وعناصره، ثم نتكلم القصد الخاص.

أولا: القصد الجنائي العام

بالرجوع إلى نص المادة 394 مكرر 02 قانون العقوبات الجزائري المعدل و المتمم ، نجد أن جريمة التعامل في معطيات غير مشروعة جريمة عصرية ولا بد لقيامها توافر القصد العام وهذا الأخير يقوم على العلم والإرادة.

1- **العلم:** هو أن يعلم الجاني بكل العناصر التي تدخل في بناء الجريمة إذ يلزم أن يعلم انه يقوم بالتعامل في معطيات غير مشروعة ولا بد أن يعلم بما يحمله سلوكه من قدرة على تهديد المصلحة المحمية، وذلك بان يعلم أن من شان المعطيات التي يتعامل فيها أن تستعمل في ارتكاب الجرائم، وهذا بالنسبة للصورة الأولى من الجريمة أو يعلم أن من شأن تعامله في المعطيات المتحصل من الجريمة أن يزيد من الضرر المترتب على تلك الجريمة أولا بد أن يعلم الجاني بالصفة غير المشروعة للمعطيات، أي يعلم بأنه يمكن أن ترتكب بها جريمة أو أنها متحصلة من جريمة فإذا اعتقد إنها معطيات عادية لا علاقة لها بالجريمة انتفى عنها القصد الجنائي.[1]

2- **الإرادة:** بالإضافة إلى العلم لا بد من توافر الإرادة لقيام القصد الجنائي، إذ رغم علم الجاني بالصفة غير المشروعة للمعطيات فانه يقوم بإرادته بالتعامل فيها، والإرادة هنا تنصب على السلوك الإجرامي فحسب وهو مختلف أشكال التعامل السابق بيانها.[2]

ثانيا: القصد الجنائي الخاص

سوف تناول توافر القصد الجنائي الخاص في الصورتين التاليتين:

1- **القصد الخاص في التعامل في معطيات صالحة لارتكاب الجريمة:**

لا يكفي لقيام جريمة التعامل في معطيات صالحة لارتكاب جريمة ان يتوفر لدى الفاعل القصد العام وحده بالمعنى الذي سبق بيانه وإنما يلزم فصل عن هذا القصد ان يتوافر لدى الفاعل القصد الخاص أي اتجاه بعلم والإرادة إلى وقائع معينة لا تدخل في تكوين أركان الجريمة، أي أن التعامل في المعطيات الصالحة لارتكاب الجريمة لا بد أن يكون بقصد الإعداد أو التمهيد لاستعمالها في ارتكاب الجريمة، ومع هذا فاستعمال هذه المعطيات في ارتكاب جريمة ليس ركنا في جريمة التعامل هذه فقد لا يقوم احد باستعمال هذه

[1] – محمد زكي أبو عامر، **المرجع السابق**، ص 765.

[2] – محمد خليفة، **المرجع السابق**، ص 212.

المعطيات ومع ذلك تقوم الجريمة إذا توافر قصد الإعداد والتمهيد واستعمال هذه المعطيات في ارتكاب الجريمة.[1]

2- مدى اشتراط القصد الخاص في التعامل مع معطيات متحصلة من جريمة:

قد رأينا أن جريمة التعامل في صورتها الأولى التعامل مع معطيات صالحة لارتكاب جريمة، تتطلب قصدا خاصا، نظرا لان المعطيات بها قد يتم التعامل فيها لأغراض مشروعة، وهذا ما لا يوجد في الصورة الثانية للجريمة وهي واحة، فكلها متحصلة من جريمة وصفتها الثانية هذه تجعل من القصد العام كافيا لقيام الجريمة، إذا لا يسأل الفاعل عن قصده الخاص من التعامل في هذه المعطيات مادام يعلم أنها متحصلة من جريمة وهذا ما يكون القصد العام فليس ما يبرر تطلب المشرع لقصد خاص من هذه الناحية.

المطلب الثاني: الجزاءات المترتبة على المساس بأنظمة المعالجة الآلية للمعطيات

لقد نصت المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي بموجب أن تكون العقوبات المقررة نتيجة ارتكاب الجرائم المعلوماتية رادعة ومتضمنة لعقوبات سالبة للحرية، كما نصت على وجوب تطبيق عقوبات على الشخص المعنوي بناء على مبدأ له مساءلة الشخص المعنوي الوارد في المادة 12 من نفس الاتفاقية.

حاول المشرع الجزائري خلال الفترات الأخيرة من الزمن تدارك الفراغ القانوني الذي عرفه مجال الإجرام الالكتروني، فقام بتعديل أحكام قانون العقوبات الجزائري، بموجب القانون رقم 15-04، مستحدثا فيه مجموعة من النصوص، التي جرم من خلالها كل الأفعال والسلوكيات المرتبطة بالمعالجة الآلية للمعطيات، وحدد لكل فعل منها جزاء وذلك من المادة 394 مكرر إلى غاية المادة 394 مكرر7 من قانون العقوبات الجزائري المعدل و المتمم ، نجد أن المشرع الجزائري قد تبنى في تقريره للجزاءات الواجبة على هذا النوع من الجرائم فسن عقوبات تطبق على الشخص الطبيعي وعقوبات تطبق على الشخص المعنوي وذلك سنتطرق إليه بالتفصيل فيما يلي:[2]

الفرع الأول: الأحكام المتعلقة بالشروع والاتفاق الجنائي في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات .

يتطلب مبدأ العقاب وقوع الجريمة، فهي تمثل عدوانا على المصالح محل الحماية القانونية ونظرا للطبيعة الخاصة للجريمة الإلكترونية وما تثيره من إشكالات في هذه البيئة الافتراضية، سنوضح أولا مسألة

[1]- محمد زكي أبو عامر، **المرجع السابق**، ص 766.

[2]- أمال قارة، **المرجع السابق**، ص 24.

الشروع في الجريمة الإلكترونية، وموقف المشرع الجزائري منه، ثم نتطرق ثانيا إلى موضوع الاتفاق الجنائي في الجريمة الإلكترونية وموقف المشرع الجزائري.

البند الأول: الشروع في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات،وموقف المشرع الجزائري منه .

إذا كان الهدف من العقاب على الجرائم بمختلف أنواعها وخاصة الجرائم المعلوماتية المستحدثة، هو تعديها على المصالح التي يحميها القانون، فإن العلة من العقاب على الشروع بوصفه جريمة هو وجود خطر يهدد هذه المصالح، فهو بمثابة اعتداء محتمل فالمشرع لا يحمي المصالح القانونية من الضرر الذي يلحقها فقط، وإنما يوفر لها حماية إزاء الخطر الذي يهدد باحتمال القضاء عليها.[1]

إذا كانت الجريمة لا تكتمل إلا بتوافر ركن مادي، فإنه ليس من الضروري أن يترتب على هذا الفعل نتيجة ضارة حتى يعاقب عليها، فإذا تحققت النتيجة نكون بصدد الجريمة التامة، وإذا لم تتحقق نكون بصد الشروع، عادة تمر الجريمة قبل تمامها بعدة مراحل منها ما هو مؤثم قانونا وتمتد إليه يد العقاب، ومنها ما هو غير مؤثم ويفلت من العقاب، وهذه المراحل هي مرحلة التفكير في الجريمة، ومرحلة التحضير للجريمة ومرحلة البدء في التنفيذ.[2]

تتعلق المرحلة الأولى بالجانب النفسي إذ تكون الجريمة عبارة عن فكرة محضة لا عقاب عليها إلا إذا نص القانون على خلاف ذلك مثل: نص المادة (176) من قانون العقوبات الجزائري المعدل و المتمم التي عاقبت على مجرد التصميم المشترك بخصوص تكوين جمعيات الأشرار وهو ما يتعلق بالاتفاق الجنائي، أما المرحلة الثانية فتتعلق بالأعمال التحضيرية التي تتوسط التفكير في الجريمة والبدء في التنفيذ، وهي تتخذ جانبا ماديا يقتضي من الجاني مباشرة أعمال استعدادا للتنفيذ، فهي تختلف عن مرحلة التفكير من كونه سلوكا ماديا خارجيا، كما تختلف عن مرحلة الشروع من حيث كونه سابقا عن البدء في تنفيذ الجريمة، فهو بمثابة ممهد للبدء في التنفيذ، ويعتبر من قبيل الأعمال التحضيرية.[3]

هذه المرحلة غير معاقب عليها إذ ترك المشرع فرصة للجاني للعدول عن جريمته، لكن إذا ارتقت هذه الأفعال إلى درجة الخطورة التي تمس المصالح المحمية، اعتبرها المشرع جريمة مستقلة بذاتها، ومثال ذلك

---

[1]– عبد الله سليمان، **شرح قانون العقوبات الجزائري**، القسم العام،ج1، ط6، ديوان المطبوعات الجامعية، الجزائر، 2005 ص 164.

[2]– عمر أبو الفتوح عبد العظيم الحمامي، **الحماية الجنائية للمعلومات المسجلة الكترونيا**، دراسة مقارنة، دار النهضة العربية القاهرة، مصر، 2010، ص 1003.

[3]– أحمد حسام طه تمام، **الجرائم الناشئة عن استخدام الحاسب الآلي**، دراسة مقارنة، دار النهضة العربية، القاهرة، مصر 2000، ص 594.

نص المادة (394 مكرر 2) من قانون العقوبات الجزائري المعدل و المتمم، التي اعتبرت بعض الأفعال التحضيرية كالبحث والتصميم جريمة مستقلة، كذلك نص المادة (394 مكرر 5) من قانون العقوبات الجزائري المعدل و المتمم، التي تعاقب على الأعمال التحضيرية في صورة الاتفاق الجنائي، وأخيرا تأتي مرحلة الشروع التي تنصرف فيها إرادة الجاني إلى تنفيذ الجريمة فعلا، فيبدأ في تنفيذ الركن المادي غير أن الجريمة لا تتم لأسباب لا دخل لإرادة الجاني فيها، وهي مرحلة معاقب عليها قانونا.

أما بالنسبة لموقف المشرع الجزائري من الشروع في الجرائم المعلوماتية نص على الشروع (المحاولة) في المادة (30) من قانون العقوبات الجزائري المعدل والمتمم: "كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أولم يخب أثرها الا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"، غير أن المشرع لا يعاقب على الشروع في مواد الجنح إلا بنص ولا يعاقب إطلاقا على الشروع في مواد المخالفات، إذ تنص المادة (31) من قانون العقوبات الجزائري المعدل و المتمم على: "المحاولة في الجنحة لا يعاقب عليها إلا بناء على نص صريح في القانون والمحاولة في المخالفة لا يعاقب عليها إطلاقا". أما بخصوص الجرائم المعلوماتية ونظرا لخطورة هذا النوع المستحدث من الجرائم وبوصفها جنحا، لم يخرج المشرع الجزائري في رسم سياسته الجنائية في هذا المجال عن نظام العقاب الذي رسمته القوانين والاتفاقيات الدولية،[1] مثل نص المادة (11) من الاتفاقية الدولية للإجرام المعلوماتي التي تجرم المحاولة، نص المشرع الجزائري في المادة (394 مكرر 7) من القسم السابع مكرر قانون العقوبات الجزائري المعدل و المتمم بعنوان: "المساس بأنظمة المعالجة الآلية للمعطيات" على: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"، يظهر لنا من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال التي تضم الجرائم الماسة بنظام المعالجة الآلية للمعطيات نظرا لخطورتها، فعاقب على الشروع بنفس عقوبة الجريمة التامة، وهو مسلك محمود في سياسته الجنائية الرامية لمواجهة هذه الجرائم المستحدثة وسد كافة المنافذ أمام المجرم الإلكتروني، لكن بالمقابل عاقب المشرع الجزائري على الاتفاق الجنائي في الجرائم الإلكترونية،و هذا ما سيتم التطرق إليه فيما يأتي:

البند الثاني: الاتفاق الجنائي في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات وموقف المشرع الجزائري منه.

لم يعط المشرع الجزائري تعريفا للاتفاق أو الجمعية، إلا أنه لاكتساب الصفة الإجرمية لهذا الفعل يجب انعقاد إرادتين أو أكثر للقيام بذلك و"الجمعية والاتفاق عبارتان تفيدان المعنى نفسه تقريبا ولكن الجمعية أكثر

[1]– يزيد بوحليط، المرجع السابق، ص 96.

هيكلة من الاتفاق الذي يغلب عليه الطابع الفكري"،[1] فنصت المادة (176) من قانون العقوبات الجزائري المعدل و المتمم على: "كل جمعية أو اتفاق مهما كانت مدته وعدد أعضائه تشكل أو تؤلف بغرض الإعداد لجناية أو أكثر، أو لجنحة أو أكثر، معاقب عليها بخمس (5) سنوات حبس على الأقل، ضد الأشخاص أو الأملاك تكون جمعية أشرار، وتقوم هذه الجريمة بمجرد التصميم المشترك على القيام بالفعل".

رغم أهمية تجريم هذا السلوك إلا انه أثار جدليا فقهيا، حيث يرى بعض من الفقه أن الاتفاق الجنائي وان كان للجاني عزم إجرامي، فإن المعاقبة عليه لا يعد استثناء على قاعدة عدم العقاب على مجرد العزم على ارتكاب الجريمة، بسبب أن المشرع لا يعاقب على الاتفاق الجنائي كخطوة للجريمة إنما يعاقب عليه في حد ذاته كجريمة مستقلة، في حين يرى جانب آخر الفقه أن هذه الحجج غير سديدة، فحينما نقارن بين خطورة الاتفاق الجنائي وخطورة الأعمال التحضيرية التي يسعى فيها المجرم للقيام بفعله بمفرده، فالاتفاق الجنائي يعتبر مرحلة نفسية مبكرة للتحضير للجريمة.

يمكن استخلاص أركان الاتفاق الجنائي من نص المادة (394 مكرر 5) من قانون العقوبات الجزائري المعدل و المتمم كما يأتي: أ- **تعدد الجناة**، ب- **موضوع الاتفاق الجنائي**، ج-**المشاركة في الاتفاق**، د- **القصد الجنائي**.[2]

أما بالنسبة لموقف المشرع الجزائري من الاتفاق الجنائي في الجرائم الالكترونية، يمكن القول أنه جعل عقوبة الاتفاق الجنائي تتناسب وطبيعة الجرائم الواقعة على نظام المعالجة الآلية للمعطيات، على خلاف نص المادة (177) من من قانون العقوبات الجزائري المعدل و المتمم التي حددت العقوبة على الاتفاق الجنائي العام على أساس خطورة الجريمة، حيث تنص على: "يعاقب على الاشتراك في جمعية الأشرار اوفي الجماعة الاجرامية المنظمة، بالسجن المؤقت من خمس (5) سنوات إلى (10) عشر سنوات وبغرامة من 500.000 دج إلى 1.000.000 دج، إذا تم الإعداد لارتكاب جنايۃ أو أكثر، وتكون العقوبة الحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 100.000 دج إلى 500.000 دج، إذا تم الإعداد لارتكاب جنحة أو أكثر، ويعاقب منظم جمعية الأشرار أوالجماعة الإجرامية المنظمة أومن يباشر فيها أية قيادة كانت بالسجن المؤقت من عشر (10) سنوات إلى عشرين (20) سنة وبغرامة من 1.000.000 دج إلى 5.000.000دج"، كما يلاحظ أن المشرع الجزائري تجاوب مع نصوص الاتفاقيات الدولية ومقررات المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات بشأن جرائم الكمبيوتر وما تضمنه القرار الصادر عن

[1]- أحسن بوسقيعة ، **الوجيز في القانون الجنائي الخاص**، ج 1 ،ط9، دار هومة، الجزائر، 2008، ص 480.

[2]- رشيدة بوكر، **المرجع السابق**، ص 341-345.

مؤتمر الأمم المتحدة الثامن عشر لمنع الجريمة ومعاملة السجناء المتعلق بالجرائم ذات الصلة بالكمبيوتر، والتي خلصت في مجملها إلى تجريم الاتفاق الجنائي.[1]

الفرع الثاني: العقوبات المطبقة على الشخص الطبيعي .

سنتناول في هذا الفرع كل من العقوبات الأصلية والعقوبات التكميلية تم ظروف تشديد العقوبة.

البند الأول: العقوبات الأصلية المطبقة على كل جريمة من جرائم المعطيات

من خلال استقراء النصوص المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي هذا التدرج في العقوبات يحدد الخطورة الإجرامية التي قدرها المشرع لهذه التصرفات إذا نجد سلم خطورة يتضمن ثلاثة درجات، جريمة الدخول أو البقاء بالغش في الدرجة الأولى، وبعدها الدرجة الثانية جريمة الدخول والبقاء المشددة، أما الدرجة الثالثة، فتحتلها الجريمة الخاصة بالمساس العمدي بالمعطيات.[2]

أولا- جريمة الدخول والبقاء :

1- **الدخول والبقاء بالغش (الجريمة البسيطة):** العقوبة المقررة هي 06 أشهر إلى سنتين حبس و60.000دج إلى 200.000دج غرامة (المادة 394 مكرر ق.ع.ج.م.م).[3]

2- **الدخول والبقاء بالغش (الجريمة المشددة):** تضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات العقوبة من سنة (1) إلى ثلاث (3) سنوات وغرامة من 100.000دج إلى 300.000دج إذا ترتب عن الدخول أو البقاء غير المشروع لنظام اشتغال المنظومة (المادة 394 مكرر من قانون العقوبات الجزائري المعدل و المتمم فقرة 02.

ثانيا- جريمة التلاعب بالمعطيات :

حسب نص المادة 394 مكرر 1، قانون العقوبات الجزائري المعدل و المتمم فإن العقوبة المقررة هي الحبس من سنة (1) إلى ثلاثة 03 سنوات وغرامة تتراوح من خمسة مائة ألف 500.000دج إلى مليوني 2.000.000دج.

ومن الملاحظ أن عقوبة التلاعب بالمعطيات تفوق جريمة الدخول والبقاء غير المصرح بهما سواء كانت هذه الأخيرة في صورتها البسيطة أو المشددة، لان في صورتها البسيطة لا تؤدي إلى إضرار معينة تلحق بالمعطيات أو بنظام معالجتها وحتى في صورتها المشددة، وإن أدت إلى نفس النتائج التي تؤدي إليها

---

[1]- يزيد بوحليط، **المرجع السابق**، ص 99.

[2]- أمال قارة، **المرجع السابق**، ص 127.

[3]- رشيدة بوكر ، **المرجع السابق**، ص 345.

جريمة التلاعب بالمعطيات وهي إزالة المعطيات أو تعديلها، فان العقوبة المقررة لجريمة التلاعب تبقى اكبر لأنها جـريمة عمـدية يتـوافر لـدى مرتكبها القصد الجنائي بينما لا يتوافر هذا القصد لدى مرتكب جريمة الدخول أو البقاء المشددة.[1]

ثالثا- جريمة التعامل في معطيات غير مشروعة :

تعاقب المادة 394 مكرر 2 من قانون العقوبات الجزائري المعدل و المتمم ، على جريمة التعامل في معطيات غير مشروعة بعقوبة الحبس من سنة (01) إلى (05) سنوات وبالغرامة المالية من مليون 1.000.000دج إلى خمسة ملايين 5.000.000دج وبهذا يكون ترتيب هذه الجريمة من حيث عقوبة الحبس هو الثاني بين جريمتي الدخول والبقاء غير المصرح بهما سواء في صورتها البسيطة أو المشددة وبين جريمة التلاعب بالمعطيات.[2]

ذلك أن حدها الأقصى يزيد عن الحد الأقصى لجريمة الدخول أو البقاء في صورتيها (سنة أو ثلاث سنوات) ويفوق مع الحد الأقصى لجريمة التلاعب بالمعطيات (ثلاثة 03 سنوات).

البند الثاني: العقوبات التكميلية

تتمثل هذه العقوبة في المصادرة والغلق، وسنتعرض لهما فيما يلي:

أولا- المصادرة :

نصت المادة 394 مكرر 6 من ق.ع.ج.م.م على ما يلي: "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة" ويقصد بالمصادرة [3]أن يؤول المال إلى الدولة، وتعد المصادرة في مجال المعلوماتية وجوبية، تتعلق بالأجهزة والبرامج والوسائل المستخدمة، ويقصد بها كل وسيلة مهما كانت طبيعتها ونوعها تستخدم في ارتكاب الجريمة، إلا أن المشرع الجزائري قيد المصادرة بعدم المساس بحقوق الغير حسن النية، وهم الأشخاص الذين لم يكونوا محل متابعة أو إدانة من اجل الوقائع التي أدت إلى المصادرة ولديهم سند ملكية أو حيازة صحيح ومشروع على الأشياء القابلة للمصادرة، وتعد حماية حسني النية أثر طبيعي لمبدأ الشرعية.[4]

ثانيا- الغلق :

---

[1]- نائلة عادل محمد فريد قورة ، **المرجع السابق**، ص 228.

[2]- محمد خليفة، **المرجع السابق**، ص 219.

[3]- أحسن بوسقيعة، **المرجع السابق** ، ص 448.

[4]- عبد الله سليمان، **المرجع السابق**، ص 73- 76.

إلى جانب عقوبة المصادرة نص المشرع الجزائري على عقوبة تكميلية وجوبية أخرى وهي عقوبة الغلق وذلك بموجب أحكام المادة 394 مكرر 6 من ق.ع.ج.م.م كما يلي: "... 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" أن المشرع الجزائري هنا قد جعل لعقوبة الغلق محلين الأول: هو المواقع محل الجريمة والثاني هو: محل أو مكان الاستغلال، ويقصد المشرع الجزائري بالمواقع التي تكون محلا للجريمة، المواقع التي تستعمل في ارتكاب الجريمة، أما مكان الاستغلال فهو المكان الذي يستعمله المتهم في ارتكاب الجريمة، وكان يحتوي على الوسائل الالكترونية التي استعملت في عملية الدخول غير المصرح بها وفي عملية التلاعب أوفي عملية التعامل بمعلومات غير مشروعة، ولم تحدد المادة 394 مكرر 6 من القانون السالف الذكر، مدة الغلق وبالتالي تطبق على ذاك القواعد العامة المنصوص عليها بالمادة 16 في فقرتها الأولى التي تنص على "يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي ارتكبت الجريمة بمناسبته ويحكم بهذه العقوبة إما بصفة نهائية أو لمدة تزيد عن عشر سنوات في حالة الإدانة لارتكاب جناية أو خمس سنوات في حالة الإدانة لارتكاب جنحة...".[1]

البند الثالث: الظروف المشددة

نصت المادة 394 مكرر 2-03 من من قانون العقوبات الجزائري المعدل و المتمم على ظرف التشديد في عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام ويتحقق هذا الظرف عندما ينتج عن الدخول أو البقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة.

- في الحالة الأولى تضاعف العقوبات المقررة في الفقرة الأولى من المادة 394 مكرر من نفس القانون وفي الحالة الثانية تكون عقوبة الحبس سنة (1) إلى ثلاث (3) سنوات والغرامة من مئة ألف 100.000دج إلى ثلاثة مائة ألف و300.000دج.
- كذلك نصت المادة 394 مكرر 3 من قانون العقوبات الجزائري المعدل و المتمم على أن تضاعف العقوبات المقررة للجرائم الماسة بالأنظمة المعلوماتية وذلك إذا استهدفت الجريمة الدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام.[2]

الفرع الثالث: العقوبات المطبقة على الشخص المعنوي

نص المشرع الجزائري والفرنسي على مسالة الشخص المعنوي وتطبيق عقوبات خاصة به تطبيقا للتوصية الواردة بنص المادة 12 من الاتفاقية الدولية للإجرام المعلوماتي التي نصت على وجوب ان يسأل الشخص المعنــوي على هذه الجـرائم سـواء بصفته فاعــلا أصلــيا أو شــريكا أو متـدخلا، كما يسأل عن

[1]- عبد الله سليمان ، **المرجع نفسه**، ص 76-77.

[2]- يراجع في ذلك نص المادة 394، مكرر 5، من ق.ع.ج، م.م.

الجريمة التامة أو الشروع فيها شرط أن تكون قد ارتكبت لحساب الشخص المعنوي وبواسطة احد أعضائه أو ممثليه، وتجدر الملاحظة أن المسؤولية الجزائية للشخص المعنوي لا تستبعد المسؤولية الجزائية للأشخاص الطبيعيين بصفتهم فاعلين أو شركاء أو متدخلين في نفس الجريمة.

البند الأول: العقوبات الأصلية

نصت المادة 394 مكرر 3 من قانون العقوبات الجزائري المعدل و المتمم "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي"، إن الأشخاص المعنوية لم تعد أشخاص وهمية، بل لها وجود قانوني وتتحمل المسؤولية، ولها إرادة خاصة بها ومستقلة عن أعضائها، وهي ترجمة لإرادة جماعية متميزة عن إرادة الأعضاء المكونين له،[1] ولقد نص قانون العقوبات الجزائري المعدل و المتمم بموجب أحكام المادة 51 مكرر على ما يلي: "باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك".

حيث يتضح من هذا النص أن المشرع استثنى الأشخاص المعنوية العامة من الخضوع للمسؤولية الجزائية وعلى رأسها الدولة والحكمة من ذلك مرتبطة بدور الدولة في حماية المصالح العامة الجماعية والفردية،[2] ولكونها المكلفة قانونا بمتابعة المجرمين، ولها دور ريادي في مكافحة الجريمة ووضع السياسة الجنائية العامة في البلاد، ومن بين العقوبات التي يمكن توقيعها على الأشخاص المعنوية بالمادة 18 مكرر من ذات القانون ما يلي:

الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

لقد ألزمت المادة 394 مكرر 4 من قانون العقوبات الجزائري المعدل و المتمم ، القاضي على تطبيق الحد الأقصى للغرامة المساوي لخمس أضعاف ما قررته للشخص الطبيعي، أما إذا ارتكبت الجريمة على الجهات العامة فتضاعف الغرامة مرتين، إذا تضاعف إلى خمس مرات عما هو مقرر للشخص الطبيعي لان الجريمة ارتكبت من شخص معنوي.[3]

---

[1]– أحسن بوسقيعة، **المرجع السابق**، ص450.

[2]– مبروك خزينة، **المسؤولية الجزائية للشخص المعنوي في التشريع الجزائري**، مكتبة الوفاء القانونية، مصر، 2010، ص 35.

[3]– سفيان حديدان ،" ***الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات***"، مجلة الأستاذ الباحث للدراسات القانونية و السياسية ، جامعة 8 ماي 1945 قالمة، الجزائر، ع8، م2، ديسمبر 2017، ص 682.

البند الثاني: العقوبات التكميلية

وهي ذات العقوبات التكميلية المطبقة على الشخص الطبيعي والمنصوص عليها بالمادة 394 مكرر 6 من قانون العقوبات الجزائري المعدل و المتمم والتي جاءت شاملة والتي سبق أن تناولنها بالشرح في الفرع الأول الخاص بالجزاءات المطبقة على الشخص الطبيعي والتي نصت على ما يلي: "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة".[1]

[1]– يراجع في ذلك نص المادة 394، مكرر 6، من ق.ع.ج، م.م.

الفصل الثانـي

الأحكام الاجرائية لمواجهة جرائم

المساس بأنظمة المعالجة الآلية للمعطيات

إن كانت الحماية الموضوعية لأنظمة المعالجة الآلية للمعطيات تقوم على تبيان أركان ونوع الجريمة المعلوماتية الواقعة على النظام وتحديد العقوبة اللازمة لها، فان الحماية الإجرائية للنظام المعلوماتي تقوم على مواجهة وكشف الجريمة فهي عبارة عن حماية عملية لهذا النظام،[1] وإذا كانت النصوص الجنائية الموضوعية محكومة بمبدأ لا جريمة ولا عقوبة إلا بنص[2] فان القواعد الإجرائية الجزائية محكومة بمبدأ الشرعية الإجرائية والذي يقوم على أساس تحديد الإجراءات الواجبة الإتباع خلال مختلف مراحل الخصومة الجنائية من لحظة وقوع الجريمة والى غاية صدور الحكم نهائيا فيها وتنفيذه وأن تكون هذه الإجراءات صادرة من الجهة المختصة وفقا لمقتضيات قانون الإجراءات الجزائية الجزائري.

ونذكر في هذا الجانب أن التطور التقني الذي لحق نظم المعالجة الآلية، فضلا عن الطبيعة الخاصة للدليل الرقمي، أدى إلى تغيير المفاهيم السائدة حول إجراءات وطرق الحصول على الدليل، وهوما أدى إلى ضرورة إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية حيث أقدم المشرع الجزائري على أحداث تعديلات في النصوص الإجرائية برصد إجراءات وأساليب مستحدثة للكشف وتتبع الجريمة المعلوماتية بشكل عام وباستحداث مؤسسات حماية من جهة أخرى، ذلك أن إجراءات التحقيق الجنائي في الجرائم المرتكبة في العالم الافتراضي هي إجراءات إما قانونية وإما تقنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والامتثال، أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته،[3] لاسيما وان التحقيق في الجرائم بشكل عام إجراء جوهري يترتب عليه آثار قد تمس حياة الأفراد وحريتهم، كما يترتب عليه حقوق والتزامات، ومن تم وجب ان تكون التحريات جدية وأن يكون القائم عليها جاد في اتخاذها، فليس للإهمال أو الرعونة مكانا فيها لأنه يمس حياة الإنسان وحقوقه وحريته.[4]

هذا وتمر الدعوى الجزائية الرامية إلى تعقب الجاني وتوقيع الجزاء عليه بمراحل متسلسلة تتوزع فيها الأدوار بين الضبطية القضائية المنوط بها مهام التحري وجمع الاستدلالات في مرحلة تحقيق تمهيدي وبين الدور الذي تؤديه النيابة العامة كجهة اتهام يلي ذلك مرحلة التحقيق القضائي لتنتهي بالمحاكمة المخولة للقاضي الجزائي، وفي ذات الصدد تواجه هذه المراحل جملة من الصعوبات والتحديات الإجرائية بالنظر لطبيعة البيئة المعلوماتية التي تنشا فيها الجريمة.

لكل ما سبق نعالج في هذا الفصل خصوصية أساليب البحث والتحري وأهم أجهزة الحماية المستحدثة ضمن المبحث الأول، ومراحل سير الدعوى العمومية وأهم التحديات التي تواجهها ضمن المبحث الثاني.

---

[1]–عثمان خرشي، **المرجع السابق**، ص 69.

[2]– يراجع نص المادة 01 من ق.ع.ج المعدل و المتمم .

[3]– خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الالكترونية** ، ط01، دار الفكر الجامعي، مصر، 2009، ص 56.

[4]– عبد الواحد إمام مرسي، **الموسوعة الذهبية في التحريات**، ، دار المعارف والمكاتب الكبرى، مصر، د.س ن، ص331 .

المبحث الأول: المساس بأنظمة المعالجة الآلية للمعطيات خصوصية الإجراءات وإرساء أجهزة الحماية.

إن التطور السريع الحاصل في مجال المعلوماتية وما صاحبه من انعكاسات على الجرائم من حيث الوسائل المستعملة لارتكابها والمحل الذي تقع عليه ونوع الجناة الذين يرتكبونها، جعل من القوانين الكلاسكية غير مواكبة للتصدي لها حيث أضحت القواعد الإجرائية غير مجدية لإثباتها، الأمر الذي دفع المشرع الجزائري إلى توسيع نطاق تطبيق إجراءات التحقيق التقليدية لمتابعة هذه الأخيرة، بهدف إزاحة الإشكالات و العقبات العملية التي تعود إلى خصوصية هذه الجرائم كالإجراءات المتعلقة بالتفتيش والضبط والمعاينة، كما برزت الحاجة إلى تطوير هذه الإجراءات كي تتناسب مع طبيعة الدليل الذي يصلح لإثباتها.

في المقابل فان تفاقم الظاهرة الإجرامية المعلوماتية المصاحب للطبيعة الخاصة التي تتميز بها لاسيما تلك الماسة بالمعالجة الآلية للمعطيات، اوجب استحداث أجهزة للحماية والتصدي لها لتواكب هذا التطور المتنامي، لهذا عمد المشرع الجزائري على غرار نظرائها في التشريعات المقارنة إلى الدول إلى إنشاء هيئات ووحدات متخصصة متخصصة أبرزها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال إضافة إلى أجهزة قضائية متخصصة وأخرى تابعة لسلك الأمن والدرك الوطني،[1] وعلى هذا الأساس، فإننا سوف نركز دراستنا في هذا المبحث على مطلبين الأول يتعلق بخصوصية إجراءات البحث والتحري عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والثاني نخصصه لأجهزة الحماية المستحدثة في متابعة هذه الأخيرة.[2]

المطلب الأول: خصوصية آليات البحث والتحري عن جرائم الماسة بأنظمة المعالجة الآلية .

تبنى المشرع الجزائري في القانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيا المعلومات، تدابير إجرائية جديدة مكملة لتلك الإجراءات المنصوص عليها في قانون الإجراءات الجزائية الجزائري المعدل و المتمم موجب التعديلين رقم 04-14 المؤرخ في 10 نوفمبر 2004 ،و06-22 المؤرخ في 20 ديسمبر 2006، بما يتلائم وخصوصية البحث والتحري في الكشف عن جرائم الإعلام و الاتصال بصفة عامة وعن جرائم نظام المعالجة الآلية للمعطيات بصفة خاصة، وتتمثل في التفتيش في النظام المعلوماتي وحجز المعطيات المعلوماتية، باعتبارهما إجراءين حاسمين خلال التحقيق [3]في هذه الجرائم، وملائمين كذلك

[1]- سعيدة بوزنون، ***"مكافحة الجريمة الإلكترونية في التشريع الجزائري"***، مجلة العلوم الإنسانية، ع3، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2019، ص 52.

[2]- محمد قدري حسن عبد الرحمن، "**جرائم الاحتيال الالكتروني**"، مجلة الفكر الشرطي، ع79، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، أكتوبر 2011، ص 159.

[3]- حددت اتفاقية بودابست أفضل الطرق الواجب إتباعها في التحقيق في جرائم الأنترنت والتي تعهدت الدول الموقعة بالتعاون الوثيق من أجل محاربتها، أنظر: جعفر حسن جاسم الطائي، **جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة**، دار البداية، الأردن، ط1، 2007، ص 228.

لخصوصية الدليل الرقمي الذي يتم الحصول عليه من خلالهما، بحيث لا يكفي مجرد الإلمام بالجانب التقني لهذه الجرائم بل لا بدا من وجود تدابير إجرائية فعالة وملائمة للبحث والتحري في الكشف عن هذا النوع من الإجرام، وهو ما يستوجب وجود نصوص إجرائية تكميلية تكون ضرورية من أجل ضمان أن يكون الحصول على هذه البيانات المعلوماتية يتم بطريقة فعالة مساوية لعملية تفتيش وضبط حاملات البيانات المادية أو دعامات المعلومات المادية.[1]

الفرع الأول: تفتيش المنظومة المعلوماتية .

إن التفتيش في الجريمة المعلوماتية إجراء صعب بالنظر إلى طبيعة الدليل المراد تحصيله والذي يسهل إخفاءه وتدميره، كما أن التفتيش في الأنظمة الالكترونية يحتاج إلى معرفة علمية وفنية قد لا تتوفر لدى رجال الضبطية القضائية والقضاة، هذا ويعتبر التفتيش من أخطر الحقوق التي منحت للمحقق وذلك لمساسه بالحريات التي تكفلها الدساتير، لذا نجد أن المشرع الجزائري كباقي التشريعات أوجد له ضوابط وشكليات عديدة سواء فيما يتعلق بالسلطة التي تباشره وتأذن بمباشرته والأحوال التي تجوز فيها مباشرته وشروط اتخاذ هذا الإجراء بما، ضمانا للحرية الفردية وحرمة المسكن، وعلى العموم نحاول بداية تعريف التفتيش في البيئة الرقمية.[2]

البند الأول: تعريف التفتيش في البيئة التقنية .

التفتيش لغة من فتش وفتش الشيء أي تصفحه وفتش عنه سال واستقصى في الطلب،[3] وفي المعنى الاصطلاحي هو السؤال عن الشيء والاستقصاء في طلبه بالسعي والبحث وهو بهذا المعنى يتطرق إلى حرية الإنسان، هذا ولم يتضمن التشريع الجزائري تعريفا خاصا ودقيقا للتفتيش بقدر ما اعتبره إجراء من إجراءات التحقيق وأحاطه بضوابط صارمة نظرا لأهميته في كشف الأدلة وخطورته فيما قد يترتب عنه من مساس بحرية الأشخاص وكرامتهم ومما يؤكد ذلك تكريسه دستوريا فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة، أما عن التعريفات الفقهية فقد تعددت غير أنها أجمعت على انه إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن

---

[1] – هلالي عبد الله أحمد، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001)**، ط1، دار النهضة العربية، القاهرة، مصر، 2006، ص 231.

[2] – يراجع في ذلك المادة 48 من التعديل الدستوري الجزائري 2020، الصادر في 2020/12/30، ج.ر82 ،المؤرخة في2020/12/30.

[3] – الكفوي أبو البقاء أيوب موسى الحسني، **معجم في المصطلحات والفروق اللغوية**، ط2، مؤسسة الرسالة، بيروت، لبنان 1998، ص 88.

أدلة مادية لجناية أو جنحة ونسبتها إلى متهم، تحقق وقوعها في محل يتمتع بحرمة وذلك وفقا للضمانات والقيود القانونية المقررة.[1]

هذا ويقع التفتيش في البيئة الرقمية على المكونات المادية لنظام لمعالجة الآلية وأوعيتها المختلفة بحثا عن شيء يتصل بالجرائم المرتبطة به وتفيد في كشف الحقيقة واكتشاف مرتكبها، كما يقع على المكونات المعنوية اي الجانب غير المادي لنظام المعالجة الآلية للمعطيات والمتمثلة أساسا في المعلومات المعالجة الكترونيا من ذلك فحص البرمجيات، كما يقع على شبكات نظام المعالجة وهوما يعرف بالتفتيش عن بعد بالنظر لتوزع المعلومات عبر شبكات حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش،[2] وهذا وفقا لضوابط وشروط شكلية وموضوعية.

البند الثاني: الشروط الشكلية والموضوعية للإذن بالتفتيش في الجرائم المتصلة بتكنولوجيا المعلوماتية

المقصود بالشروط الشكلية تلك الإجراءات التي أوجب المشرع مراعاتها عند إجراء عملية التفتيش والهدف من وضع هذه الشروط من قبل المشرع هو إحاطة عملية التفتيش بإجراءات وشكليات تضمن صحة ودقة النتائج التي يصل إليها القائم بالتفتيش وإحاطة المتهم بضمانات كافية للحفاظ على حريته الفردية فالشكلية في الإجراءات الجزائية تعد ضمانة لعدم تعسف الجهات القائمة بالتفتيش ومن أهم القواعد الشكلية أن يتم بناءا على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق، ويجب على ضابط الشرطة القضائية أن يستظهر الإذن قبل الدخول أو الشروع في التفتيش طبقا لنص المادة 44 من قانون الإجراءات الجزائية الجزائري ، كما يجب أن يتضمن الإذن وصف الجرم محل التحري وعنوان الأماكن التي ستتم تفتيشها تحت طائلة البطلان، مع التنويه أن التفتيش يكون بحضور المشتبه فيه، أو ممثل عنه، أما إذا امتنع عن الحضور أو كان في حالة فرار، يعين ضابط الشرطة القضائية المكلف بالتفتيش شاهدين من غير موظفيه[3] وفي حالة ما إذا كان المشتبه فيه موقوف وكان نقله يشكل خطورة على النظام العام، فله الحق في أن يختار وكيلا عنه أو يكتفي بحضور شاهدين بعلم وموافقة وكيل الجمهورية.

كما لا يجوز بدء التفتيش داخل المساكن قبل الخامسة صباحا ولا بعد الثامنة مساء إلا بطلب من صاحب المسكن، غير انه يمكن إجراء التفتيش خارج الأوقات المذكورة إذا تعلق الأمر بالجرائم الستة المحددة بالمادة 47 ف 3 من ق.إج.ج والتي تعطي لضابط الشرطة القضائية الصلاحيات للتفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في أي ساعة من الليل أو النهار بإذن مسبق من وكيل الجمهورية.[4]

---

[1]– رشيدة بوكر، **المرجع السابق**، ص 394.

[2]– رشيدة بوكر **المرجع نفسه**، ص 401.

[3]– يراجع في ذلك المادة 45–1، ق. الإ.ج.ج .م.م .

[4]– لحسن ناني، **المرجع السابق**، ص 103.

أما بالنسبة للشروط الموضوعية للتفتيش بصفة عامة في الجرائم التقليدية وبصفة خاصة في الجرائم الماسة بالمعطيات المعالجة آليا فـيمكن حصرها في ثلاث شروط أساسية وهي سبب التفتيش، محل التفتيش، السلطة المختصة بالقيام بالتفتيش، ويتمثل سبب التفتيش في الجرائم الماسة بالأنظمة المعالجة آليا في ارتكاب الجريمة المعلوماتية بشكل عام، أما محل التفتيش فيقصد به مستودع سر الإنسان، ويكون أما محل له حرمة خاصة كالمسكن أوقد يكون الشخص ذاته أو رسائله، هذا بالنسبة للجرائم التقليدية، أما بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية والمعلوماتية فمحل التفتيش هو الحاسب الآلي ويعد التفتيش إجراء من إجراءات التحقيق الابتدائي التي تمس حقوق وحريات الأفراد،، لذا حرص المشرع على إسنادها لجهة قضائية تكفل تلك الحقوق والحريات وتتمثل الجهة القضائية في قاضي التحقيق أو النيابة العامة كسلطة أصلية، أو استثناءا في رجال الضبط القضائي، كم خول قانون الإجراءات الجزائية صلاحية إصدار الإذن استثناء إلى سلطات أخرى غير السلطات المختصة ففي حالة وقوع جريمة من نوع الجنايات أو الجنح ولم يكن قاضي التحقيق المختص موجودا فإن على المسؤول عن التحقيق عندما تقتضي الضرورة عرض الأمر على أي قاضي يمارس اختصاصه في نفس دائرة اختصاص قاضي التحقيق أو أي منطقة قريبة لاتخاذ ما يلزم على أن تعرض الأوراق على قاضي التحقيق المختص في أقرب وقت.[1]

ولم يشترط المشرع الجزائري شكلا معينا لأمر التفتيش، ولكن بالرجوع إلى القواعد الأساسية للتحقيق الابتدائي، فإنه يحب أن تكون الإجراءات مدونة في محاضر وموقعة عليها من القاضي.

ومن المتعارف عليه في معظم التشريعات الإجرائية أن حالة التلبس تعتبر إحدى الحالات التي تتسع فيها سلطات الضبطية القضائية، حيث تباشر اختصاصات موسعة في التحقيق ومنها التفتيش بحثا عن أدلة الجريمة وتحديد فاعلها، سواء تعلق الأمر بتفتيش المساكن أو الأشخاص، ولما كانت الجرائم الماسة بأنظمة المعالجة الآلية كغيرها من الجرائم يمكن أن تتوفر فيها شروط الجريمة المتلبس بها كان من الجائز إجراء تفتيش شخص المشتبه به وما قد يحمله من حاسوب نقال أو هاتف نقال أو حاسوب صغير أو مسكنه وما يتضمنه من موجودات.

البند الثالث: إجراءات التفتيش في الجرائم الماسة بالمعطيات الرقمية

لا يكفي في التفتيش مجرد توافر شروطه الموضوعية أو الشكلية، بل يلزم أيضا ضرورة مراعاة حدوده الداخلية والتي يتمثل أهمها في ضرورة التقيد بالغرض من التفتيش أثناء تنفيذه وفقا لما نص عليه قانون الإجراءات الجزائية والذي يقضي بأن الأصل في التفتيش هو البحث عن الأشياء المتعلقة بالجريمة موضوع

[1]– عز الدين عثماني، "**اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية**"، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، المركز الجامعي مرسلي عبد الله ، تيبازة الجزائر، ع4، 2018، ص 57– 59.

التحقيق، ويلاحظ أنه في الحالات التي يجوز فيها لضابط الشرط القضائية القيام بإجراء التفتيش والضبط فإن مشروعية هذا الإجراء تتوقف على محل ارتكاب الجريمة ومدى تبعيته للمجني عليه.

هذا ويطرح التفتيش في الجرائم المتصلة بتكنولوجيا المعلوماتية لاسيما التفتيش في الأنظمة المعالجة آليا عديد الإشكالات عديدة منها مدى قابلية المكونات الرقمية أو المنطقية للحاسب الآلي لعملية التفتيش وهو أمر محل جدل فقهي، فهناك رأي يرى بجواز ضبط البيانات الإلكترونية بمختلف أشكالها ويستند هذا الرأي في ذلك إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط "أي شيء فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسب المحسوسة وغير المحسوسة، بينما ذهب رأي آخر إلى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، فذهب إلى أنه يجب أن يقع الضبط على بيانات الحاسب الآلي إذا اتخذت شكلاً مادياً، وهنا يجب إيجاد نص صريح يخص المكونات المنطقية أو الرقمية للحاسب الآلي.[1]

ويثور الخلاف أيضا حول شبكات الحاسب الآلي ومدى خضوعها للتفتيش "التفتيش عن بعد" فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماماً عن الموقع المادي[2] للتفتيش وإن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية الجاري تفتيشها، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتى في بلد آخر، ففي الإحتمال الأول وهو اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة، يُثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم.[3]

بالرجوع إلى التشريع الداخلي نجد أن المشرع الجزائري قد تعرض لعملية تفتيش المنظومة المعلوماتية من خلال الفصل الثالث من القانون 04-09 المعنون بالقواعد الإجرائية –تفتيش المنظومة المعلوماتية ضمن المادة 05 منه حيث تنص على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية الجزائري وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض، التفتيش ولوعن بعد، إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها ومنظومة تخزين معلوماتية.

[1]– خالد ممدوح إبراهيم، **المرجع السابق**، ص 228.

[2]– عز الدين عثماني، **المرجع السابق**، ص 228.

[3]– لحسن ناني، **المرجع السابق**، ص 103.

الفرع الثاني: إجراء الضبط في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات.

يعتبر الضبط الأثر المباشر للتفتيش[1] ،وحتى يحقق التفتيش غايته في جمع الأدلة لابد من وسيلة التقاط تلك الأدلة، وهذه الوسيلة هي الضبط،[2] بحيث تكون الغاية من التفتيش هو حجز أي شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأنها، سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئا نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة وبالتالي ينبغي القيام بضبط ما يترتب عليه التفتيش وتحريزه بطريقة علمية حتى لا يفقد قيمته القانونية حال تفقده أمام القضاء إذا تطلب الأمر ذلك.

يعرف الضبط بأنه العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها والتحفظ على هذه الأدلة، فالضبط هو الغاية من التفتيش ونتيجته المباشرة المستهدفة ولذلك يتعين عند إجرائه أن تتوافر فيه نفس القواعد التي تطبق بشأن التفتيش،[3] ويترتب على هذا الارتباط؛ أن الضبط لا يجوز أن يقع على شيء إلا بـوصفه دليلا من أدلة الجريمة التي يجري التفتيش بشأنها.

ونذكر في هذا الشأن أن المشرع الجزائري قد قام بسن التدابير الإجرائية الخاصة بحجز المعطيات المعلوماتية في الفصل الثالث من القانون 09-04 السالف الذكر،[4] واعتمد طريقتين في حجز هذه المعطيات المعلوماتية، حيث تتمثل الطريقة الأولى في الحجز عن طريق نسخ المعطيات المعلوماتية التي تفيد في الكشف عن الجرائم وعن مرتكبيها، أما الطريقة الثانية فتتمثل في الحجز عن طريق منع الوصول إليها وهذا تفاديا لإتلافها أو تغييرها.[5]

البند الأول: الحجز عن طريق نسخ المعطيات المعلوماتية

إن المعطيات الرقمية المعلوماتية المجمعة يمكن نسخها على جميع دعائم التخزين وهذا ما يطلق عليه الحجز المعلوماتي الذي هو غير متعارض مع الضبط المادي التقليدي لدعائم التخزين المعلوماتية المستخرجة من نفس مكان التفتيش، فالنسخ يعد أحد أساليب الضبط المستخدمة في حالة عدم وجود إمكانية

---

[1]- المعيني سرحان حسن، "**التحقيق في جرائم تقنية المعلومات**"، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات، م20، ع79، أكتوبر 2011، ص 46.

[2]- صالح شنين، "***إجراءات التحري و التحقيق في جرائم تكنولوجيا الإعلام و الاتصال في التشريع الجزائري (قانون 09-04)***"، مجلة الدراسات الحقوقية، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي سعيدة.،الجزائر،ع1، 2014 ص 283.

[3]- عبد الله سيف الكيتوب، **الأحكام الإجـرائية لجريمة الاحتيال المعلوماتي**، دار النهضة العربية، القاهرة، مصر، 2013 ص 142.

[4]- يراجع في ذلك نص المواد 6-7-8-9 من القانون رقم 09-04 السالف الذكر .

[5]- درياد مليكة، "***المساس بأنظمة المعالجة الآلية للمعطيات***"، حوليات جامعة الجزائر، ج1، ع33، مارس 2019، ص 251.

لضبط القطع الصلبة المتضمنة للمواد غير المشروعة[1]، ويمكن عن طريقه الاستيلاء على كافة أنواع المعطيات، والتي تشمل البيانات والمعلومات والأوامر والبرمجيات وغيرها، فيتم مثلا نسخ المواد التي تحتاج إلى فك شفرتها لكي يتم التعرف على محتوياتها أو نسخ البيانات التي يتم وضعها في إطار برمجية تحوي قنبلة زمنية موقوتة"، وهنا نجد أسلوب النسخ يصلح تماما أن ينتج عنه دليل رقمي مقبول أمام القضاء هذا ما اعتمده المشرع الجزائري،[2] باعتماد طريقة نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية سواء بحجز النظام المعلوماتي برمته إذا كان ضروريا لمصلحة التحقيق أو القيام بحجز المعطيات المعنية بالذات وذلك بعد نسخها على دعامة مادية أو أي وعاء للبيانات كطبعها على الورق أو ضبطها على الشاشة قصد تسهيل قراءتها والتعامل معها.[3]

كما أنه حاليا يتم استخدام برامج متخصصة في النسخ مثل برنامج lap link[4] ،كما يوجد أسلوب تجميد التعامل بنظام المعالجة الآلية أو إحدى القطع المكونة له التي استخدمت في ارتكاب الجريمة.

البند الثاني: الحجز عن طريق منع الوصول إلى المعطيات

أعطى القانون رقم 09-04[5] للجهات المختصة سلطة الأمر بالتحفظ عليها، وذلك خشية محو أو إتلاف أو نقل أو ضياع الأدلة التي يتم الحصول عليها بطريق التفتيش، وهذا باستعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها وحصر بذلك حالات اللجوء إلى الحجز عن طريق منع الوصول في حالة واحدة وهي استحالة الحجز، مع التحفظ على جميع البيانات محل الجريمة، وكذلك الأدوات التي استخدمت في ارتكابها، أو الآثار المخلفة عنها والتي من شأنها كشف

---

[1]- محمد عبد الله إبراهيم، **المواجهة الأمنية لجرائم شبكات المعلومات الدولية**، مطابع الشرطة للطباعة والنشر والتوزيع القاهرة ،مصر، 2016، ص 16.

[2]- يراجع في ذلك المادة 06 ف 01 من القانون 09-04السالف الذكر.

[3]- رشاد خالد عمر، **المشاكل القانونية و الفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)**، المكتب الجامعي الحديث، الإسكندرية ، مصر، 2018، ص 148.

[4]- يوصي الأستاذ Sieber بضرورة استعانة الجهات القائمة بالضبط و التحقيق بخبراء فزيئين للقيام بعملية الاستنساخ عامة، وأن تتم عملية إنتاج النسخ من قبل هؤلاء من خلال أنظمة الحاسبات التي يألفونها فقط، وأن يستخدموا -إذا كان ذلك ممكنا- نظام التشغيل (الآمن) الخاص بهم. أنظر: هشام محمد فريد رستم، **الجوانب الإجرائية للجرائم المعلوماتية**، ط1، مكتبة الآلات الحديثة، أسيوط، مصر ، 1994، ص 132.

[5]- يراجع في ذلك نص المادة 07 من القانون رقم 09-04 السالف الذكر .

الحقيقة، بالإضافة إلى تكليف شخص مؤهل باستعمال الوسائل التقنية المناسبة لذاك وهوما نصت عليه المادة 08 من القانون 09- السالف الذكر04.[1]

البند الثالث: التعامل مع المحجوزات في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات

يتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق عقب أي عملية تفتيش أو معاينة ايجابية، في حال عدم حجز المنظومة كاملة وتبقى المحجوزات تحت تصرفها إلى حين انتـهاء المحاكـمة، ويـرى البعـض بضرورة حفظ نسخة أخرى لدى الجهة التي قامت بالتفتيش، خشية تلف أو ضياع النسخة الوحيدة الموضوعة تحت تصرف جهة التحقيق أو المحكمة، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل وإعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات ويواجه عملية الحجز للبيانات المعالجة إلكترونيا صعوبات منها حجم الشبكة التي تحتوي على المعلومات المعالجة إلكترونيا والمطلوب ضبطها، من أمثلة ذلك البحث في نظام إلكتروني لشركة متعددة الجنسيات، احتمال وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أو دول أجنبية، مما يستدعي تعاونها مع جهات الشرطة والتحقيق في عملية التفتيش والضبط والتحفظ.[2]

الفرع الثالث: إجراء التسرب الالكتروني

يقصد بالتسرب قيام ضابط عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم انه فاعل معهم أو شريك لهم،[3] ويعتبر بدلك واحد من أهم واخطر طرق البحث والتحري وأكثرها تعقيدا حيث يعتمد على المهارات والقدرات الشخصية لضباط وأعوان الشرطة القضائية القائمين بالعملية المعينين بناءا الكفاءة والخبرة والحيلة والذكاء، وتستخدم فيها مختلف الأساليب من اجل كسب ثقة المشتبه فيهم وتحديد طبيعة ومدى النشاط الإجرامي، حيث يقوم ضابط أو عون الشرطة القضائية باختراق جماعة إجرامية باستعمال هوية مستعارة أو بغية مراقبة الأشخاص بإجرامهم بأنه فرد لا يتجزأ من العصابة الإجرامية المشتبه فيهم والحصول على المعلومات المتعلقة بمخططاتهم للكشف عن أنشطتها الإجرامية والوسائل التي تستعملها في ذلك، وغيرها من المعلومات المتعلقة بالجريمة والمجرمين والتصرف في الوقت المناسب شرط ألا يشكل هذا التصرف تحريضا

---

[1]- يراجع في ذلك أحكام المادة 8 من القانون رقم 09-04 "يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك".

[2]- لحسن ناني، **المرجع السابق**، ص 124.

[3]- يراجع المادة 65 مكرر 12 من ق.الإ.ج.ج.م.م.

على ارتكاب الجريمة، وقد أطلق المشرع الجزائري على هذا الأسلوب مصطلح "التسرب" في أحكام قانون الإجراءات الجزائية الجزائري المعدل و المتمم بينما أطلق تسمية "الاختراق" في المادة 56 من قانون مكافحة الفساد.[1]

هذا تعتبر الجريمة المعلوماتية من بين الجرائم التي يمكن فيها اللجوء إلى إجراء التسرب وذلك عندما تقتضي ضرورة التحري والتحقيق في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات ولا يمكن أن تتجاوز مدة عملية التسرب 04 أشهر إلا في حالة التمديد من طرف القاضي الذي رخص بها والذي يمكنه أن يأمر في أي وقت بوقفها قبل انقضاء الأجل المحدد، وقد اقر قانون الإجراءات الجزائية الجزائري المعدل و المتمم عقوبات صارمة ضد من يكشف هوية ضابط أو عون الشرطة القضائية المتسرب في أي مرحلة من مراحل الإجراءات.[2]

البند الأول: شروط التسرب الالكتروني

في هذا الصدد أعطى المشرع الجزائري لسلطات التحقيق إمكانية اعتراض المراسلات كأسلوب مستحدث للبحث عن الدليل يتماشى مع الأساليب المتطورة التي يلجأ إليها الجناة في تنفيذ جرائمهم وإخفاءه أي اثر يدل عليهم، فمن ناحية أخرى لم يفتح الباب على مصرعيه في اللجوء إلى هذه الوسيلة بل أحاط استخدامها بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية وتتمثل هذه الشروط في:

أولا- الشروط الشكلية :

تنحصر الشروط الشكلية للتسرب في الإذن وما يجب أن يتضمنه فلا يمكن أن يباشر ضابط الشرطة القضائية عملية التسرب بمفرده دون إذن من قبل الجهات القضائية،[3] ويجب أن يكون الإذن مكتوبا وإلا كان الإجراء باطلا كما يجب أن يتضمن ذكر هوية الضابط الذي تتم على يديه عملية التسرب وتحديد المدة المطلوبة في عملية التسرب والتي لا يتجاوز إجراء التسرب 04 أشهر تحدد حسب المقتضيات.

ثانيا- الشروط الموضوعية:

هو أن يكون إذن التسرب مسببا، فمن خلال التسبيب تتبين العناصر التي أقنعت الجهات القضائية المختصة لمنح الإذن وكذا العناصر التي دعت ضابط الشرطة القضائية للجوء إلى هذا الإجراء والتي تكون ضمن موضوع طلبه الإذن، لذلك فكان لزاما عند إصدار الإذن بالتسرب سواء من طرف وكيل الجمهورية

---

[1]- معزيز أمينة،" ***التسرب في ق.إ.ج الجزائري***"،مجلة القانون والمجتمع، كلية الحقوق والعلوم السياسية ،جامعة مستغانم الجزائر ،2015، ص 246- 247.

[2]- يراجع في ذلك المادة 65، مكرر 16، من ق الإ.ج.ج.م.م.

[3]- يراجع في ذلك المادة 65، مكرر 11، من الإ.ج.ج.م.م.

أومن قاضي التحقيق إظهار جميع الأدلة بعد تقدير العناصر المعروضة عليه من طرف ضابط الشرطة القضائية.[1]

البند الثاني: طرق التسرب الالكتروني

يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى العلم الافتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات الكترونية فيها، أو اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم مستخدما في ذلك أسماء أو صفات هيئات مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام الهاكر للموقع، من اجل القيام بعملية التسرب فقد أجاز المشرع استعمال أساليب وطرق خاصة أتاحت بدورها إمكانية اللجوء إلى استخدام عدة وسائل وتقنيات هي في الأصل ليست مسموح بها قانونا لأنها تعتبر مساسا لمبدأ حرمة الحياة الخاصة غير انه لكل قاعدة استثناء وهو ما فعله المشرع الجزائري عندما تدخل بواسطة القواعد الإجرائية ليقيد أحيانا هذه الحرمة للحياة الخاصة.[2]

حيث يجب أن يتم الإذن بعملية التسرب من طرف وكيل الجمهورية أومن طرف قاضي التحقيق، بعد إخطار وكيل الجمهورية، يجب أن يكون الإذن المسلم مكتوبا ومسببا وذلك تحت طائلة البطلان، مع ذكر الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (04) أشهر ويمكن أن تجدد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية، ويجوز للقاضي الذي رخص إجرائها أن يأمر في أي وقت، بوقفها قبل انقضاء المدة المحددة، وتودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب، ولا يجوز إظهار الهوية الحقيقية لضباط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات، وإذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة إجراءات التسرب للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألا تتجاوز ذلك مدة أربعة (4) أشهر، وفي هذه الحالة يتعين إخبار القاضي الذي رخص إجراء عملية التسرب تلك في اقرب الآجال، فإذا انقضت مهلة الأربعة (04) أشهر تلك دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه، أمكن لهذا القاضي أن يرخص بتمديدها

1- نادية غرباوي ، **أساليب البحث والتحري في الجرائم المعلوماتية**، مذكرة ماستر تخصص قانون عام ، كلية الحقوق والعلوم السياسية ،جامعة أكلي محمد اولحاج، البويرة، الجزائر،السنة الجامعية 2016-2017، ص 78.

2- وردة شرف الدين ، سامية بلجراف ،" ***الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري"*** مجلة المنار للبحوث والدراسات القانونية والسياسية، جامعة يحي فارس ،المدية الجزائر ، ع3، ديسمبر 2017، ص 37 .

لمدة أربعة (4) أشهر على الأكثر، ويجوز سماع ضابط الشرطة القضائية الذي تجري عملية التسرب تحت مسؤوليته دون سواه بوصفه شاهدا عن العملية.[1]

الفرع الرابع: الوسائل الأخرى للبحث والتحري في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات

إن الاستخدام المفرط للشبكات المعلوماتية في الآونة الأخيرة، جعل المشرع يدرك الصعوبات الكثيرة التي تثيرها محاولةّ مد نطاق إجراءات الاعتراض والمراقبة وفق النصوص التقليدية لتشمل المراسلات والاتصالات عبر الشبكات المعلوماتية، لذلك عمد المشرع إلى مراجعة قوانينه الإجرائية، بوضع نصوص صريحة تنظم هذه العملية فتدخل بموجب قانون الإجراءات الجزائية 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم فاستحدث لهذا الإجراء الفصل الرابع تحت عنوان: "اعتراض المراسلات وتسجيل الأصوات والتقاط صور" تناول فيه المقصود بهذا الإجراء نطاقه وضمانات استخدامه ثم عززه بالقانون رقم 09-04 المؤرخ في 05 أوت 2009 السالف الذكر ، وسنبين كل ذلك من خلال ما يلي:

البند الأول: اعتراض المراسلات

حدد المشرع الجزائري المراسلات التي تصلح أن تكون محلا للاعتراض[2] بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها (كتابة، رموز، أشكال، صور) أو (الدعامة التي تنصب عليها) ورقية أو رقمية أو الوسيلة المستعملة لإرسالها سلكية كانت (كالفاكس أو تليغرام) أم لاسلكية (البريد الالكتروني، الهاتف النقال) باستثناء الكتب والمجلات والرسائل والحوليات، التي تعد مراسلات خاصة.

وهذا ما أكدته المادة 02 فقرة 06 من القانون رقم09 -04 التي عرفت الاتصالات الالكترونية بأنها: **"أي إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أية وسيلة الكترونية"**،[3] وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون أو علم موافقة المعنيين،[4] وذلك

---

[1]- علاوة هوام، ***"التسرب كآلية للكشف عن في جرائم القانون الجزائري"***، مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية جامعة الحاج لخضر، باتنة، الجزائر، 2012، ص 03.

[2]- زورو هدى، ***"التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري"***، مجلة دفاتر السياسة والقانون كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، ع11، 2014، ص 1.

[3]- وهو التعريف الذي كرره المشرع الجزائري في المادة (05) من المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08، المحدد تشكيلة وتنظيم وكيفيات تسيير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج.ر53، صادر بتاريخ 2015/10/08.

[4]- مصطفى محمد موسى، **المراقبة الالكترونية عبر شبكة الانترنت**، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية الكتاب الخامس، دار الكتب والوثائق القومية المصرية، القاهرة، مصر، 2003، ص 1.

لغرض التصنت والتقاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل لمواجهة المتهم،[1] ولعل من أهم المراسلات الالكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض والمراقبة وتعتبر مصدرا غنيا لأدلة إثبات الجرائم الالكترونية، المراسلات عبر البريد الالكتروني، كون هذه التقنية من أكثر الوسائل الحديثة استخداما للاتصال عبر الانترنت ومجالا خصبا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة ودون حواجز.

فهو بمثابة نظام تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة، كما يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه بسهولة لأنه محاط بحماية فنية، ومن هنا فعملية اعتراض ومراقبة البريد الالكتروني التي تجري بغرض ضبط، المراسلات الالكترونية وتجدر الإشارة إلى أن المشرع الجزائري لم يتبني في القانون رقم 09 -04 مراقبة الاتصالات الالكترونية كإجراء تقتضيه التحريات والتحقيقات القضائية فقط مثلما هو في قواعد الإجراءات الجزائية، إنما أعطى تصريحا للجهات القضائية باستعمال هذا الإجراء التقني في إطار الوقاية من بعض الجرائم التي يحتمل أن تشكل خطرا على أمن الدولة وهي كما حددتها المادة (04) من القانون السالف الذكر، الأفعال الموصوفة بجرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة، وجرائم الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة،[2] والمثير للانتباه أن المشرع سمح بإجراء عمليات المراقبة للاتصالات الالكترونية لأشخاص أو مجموعات بمجرد وجود احتمال تورطهم مستقبلا في ارتكاب إحدى هذه الجرائم لان الوقاية في اعتقاده لا تفرض القيام بأعمال تحضيرية لارتكاب هذه الأفعال إنما مجرد تكهنات أو حتى قرائن بسيطة تنبئ بأن هؤلاء الأشخاص قد يقدمون على ارتكاب تلك الجرائم، على أن تكون الترتيبات التقنية الموضوعة لمراقبة الاتصالات الالكترونية في هذه الحالة موجهة حرصاً لتجميع وتسجيل معطيات ذات صلة بالوقاية من تلك الأفعال ومكافحتها، تحت طائلة العقوبات المنصوص عليها في قانون العقوبات بالنسبة للمساس بالحياة الخاصة للغير.

البند الثاني: مراقبة الاتصالات الإلكترونية

يقصد بالاتصالات الالكترونية إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية، وقد نص المشرع الجزائري على مراقبة الاتصالات

[1]- زيبحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى، الجزائر، 2011، ص 157.

[2]- يراجع في ذلك نص المادة 04 من القانون رقم 09-04 السالف الذكر.

الالكترونية،[1] ونظم الحالات التي تسمح للجوء إلى هذا الإجراء، وهي الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية، في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.[2]

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة سابقا إلا بإذن مكتوب من السلطات القضائية المختصة، ولقد أوكل المشرع الجزائري مهمة مراقبة الاتصالات الالكترونية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تحت سلطة القاضي المختص.[3]

البند الثالث: التقاط الصور

الصورة كأصل عام تعتبر وسيلة هامة تم استخدامها الاستعانة بها في تحقيق العديد من الأغراض والأهداف، وهي سلاح ذو حدين فقد يستعان بها من أجل تحقيق المصلحة العامة كما قد يتعدى بها على الحق في الخصوصية، والصورة قد تكون في شكلها العادي (الثابت) كما قد تكون في شكلها المرئي الذي يعد مرحلة متقدمة على التصوير العادي والذي بات له خصوصية واضحة حتى أن البعض قد أطلق على حضارة القرن العشرين بأنها حضارة الصورة وذلك للأهمية والمكانة الواضحة التي نالتها هذه الأخيرة.

فقد أصبح يعتمد عليها في المجال الجنائي باعتبار الناتج عن عملية التصوير من الأدلة العلمية المهمة في الإثبات الجنائي نظرا لما تحتويه من تفاصيل معلوماتية بالغة الأهمية والتي تعد توثيقا لمواقع وشخصيات أو آثار وأحداث ومواقف، وهذا ما دفع المشرع الجزائري إلى الأخذ بهذه الآلية ونظمها دون موافقة المعنيين بها وتكون بوضع ترتيبات تقنية من أجل التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص، ولعل المشرع من خلال تفعيله هذه الآلية وجعلها مقصورة على المكان الخاص فقط دون المكان العام كان لاعتبارات تقنية أو لاعتبارات تتعلق بحقوق الآخرين غير المعنيين بالجريمة أو لاعتبارات تتعلق بصعوبة إثبات وجود هؤلاء الأشخاص في تلك الأماكن.[4]

---

[1]– يراجع في ذلك : نص المادة 09-04 من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال السالف الذكر .

[2]–وردة شرف الدين ،سامية بلجراف ، **المرجع السابق**، ص 48- 49.

[3]– يراجع في ذلك أحكام المادة 04 ف 03 من قانون 09-04، والمادة 04 ف 02 من 04 من المرسوم الرئاسي رقم 15-261 المؤرخ في 2015/10/08، المحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[4]– عثمان خرشي، **المرجع السابق** ، ص 117.

وحصرها في جرائم معدودة كانت الجرائم المعلوماتية إحداها، أين أجاز لضابط الشرطة القضائية التقاط الصور بمختلف أشكالها لكن وفق الشروط محددة تحت طائلة البطلان؛ من ذلك وجوب الحصول على إذن من وكيل الجمهورية أومن قاضي التحقيق والدي يتضمن نوع الجريمة التي تبرر اللجوء لمثل هذه ال‌آليات والوقت المحدد واللازم لتفعيلها والذي لا يتجاوز أربعة (04) أشهر وتكون هذه المدة قابلة للتجديد حسب مقتضيات التحري والتحقيق، ويجب أن تفعل هذه العمليات تحت المراقبة المباشرة لمصدر الإذن سواء وكيل الجمهورية قبل فتح تحقيق قضائي أو قاضي التحقيق في حالة فتح تحقيق قضائي.

البند الرابع: تسجيل الأصوات

هو وضع تقنية دون موافقة المعنيين من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة او سرية من طرف شخص أو عدة أشخاص تشمل كل أدوات الاتصال سواء سلكية أو لاسلكية، وهو عبارة عن تسجيل ل‌أحاديث المتهم وشركائه، حيث يأخذ اعتراف المتهم ضد نفسه بشكل خفي ودون رضاه وموافقته عن طريق تسجيل كل ما يقوله من كلام بصفة خاصة أو سرية، هذا الكلام عبارة عن حديث يعبر فيه الشخص عن نفسه وينقل مكنوناته إلى المتحدث إليه، وبغض النظر عن مكان التسجيل الذي قد يكون عاما كالشارع أو خاصا كالمسكن والأداة التي يتم بها، فالمهم في العملية هو الكلام المتفوه به والذي قد يشكل دليلا لإظهار الحقيقة،[1] وبالرجوع للمشرع الجزائري فقد أجاز لضابط الشرطة القضائية بالنسبة لجرائم حددها على سبيل الحصر كجرائم المعلوماتية التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية لشخص أو عدة أشخاص في أي مكان بناء على إذن من وكيل الجمهورية أو قاضي التحقيق.[2]

المطلب الثاني: أجهزة وهيئات الحماية من الجرائم المساس بأنظمة المعالجة الآلية للمعطيات

تتعدد أسباب إنشاء أجهزة مكلفة بالتحقيق في الجرائم المعلوماتية ، و لعل أهم سبب هو حماية أفراد المجتمع من مخاطر هذه الجرائم ،والحد منه إضافة إلى ضبط الجرائم المعلوماتية والحصول على مختلف الأدلة الالكترونية التي تساعدنا في إثبات الجريمة، كما يعتبر التهديد الذي يطال أمن الدول سببا ثانيا لإنشاء أجهزة متخصصة في التحقيق في مثل هذه الجرائم نتيجة استخدام تقنية المعلومات والتفاعل معها من قبل مختلف فئات المجرمين من إرهابيين ومهربي الأسلحة والمتاجرين بالمخدرات ومبيضي الأموال وجماعات الجريمة المنظمة،[3] ونظرا لانتشار الجريمة الإلكترونية بشكل ملفت للانتباه، ولأن أجهزة التحقيق في الجرائم التقليدية لم تكن كافية للتصدي لهذا النوع من الإجرام، أنشئت أجهزة خاصة بالتحقيق فيها.

---

[1]– فوزي عمارة، ***اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية"***، مجلة العلوم الإنسانية، جامعة الإخوة منتوري، قسنطينة، الجزائر ،ع33، جوان 2010، ص 237.

[2]– المادة 65 مكرر5ف4 من ق الإج. ج .ج .م .م .

[3]– مصطفى محمد موسى، **المرجع السابق**، ص 228.

بدأت التشريعات ومن بينها التشريع الجزائري تواجه خطورة الجرائم المعلوماتية من خلال استحداث هيئات قضائية وهيئات شبه قضائية، فالهيئات المتخصصة في مجال مكافحة الجريمة المعلوماتية هي وحدات تسند مهام الوقاية ومكافحة الجرائم الإلكترونية بالنظر إلى تشكيلتها البشرية الخاصة التي تضم محققين من نوع خاص تجمع لديهم صفة الشرطة القضائية إضافة إلى المعرفة الواسعة بالنظم المعلوماتية والمجرم الالكتروني.[1]

الفرع الأول: الأجهزة الأمنية لمكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات

سنتطرق خلال هذا الفرع إلى استعراض أبرز الهيئات والوحدات المتخصصة في مجال مكافحة الجرائم المساس بأنظمة المعالجة الآلية للمعطيات، والتي ما تسند إليها عادة مهام الوقاية ومكافحة الجرائم المعلوماتية بشكل عام، نظرا لتشكيلتها البشرية الخاصة والتي تضم محققين من نوع خاص تجتمع لديهم صفة ضابط شرطة قضائية إضافة إلى المعرفة الواسعة بمجال النظم المعلوماتية والإجرام المعلوماتي، مما يسمح لهم ويؤهلهم لتولي مهام البحث والتحقيق في ميدان الجرائم المعلوماتية، ولعل أن أبرز هذه الهيئات والوحدات هي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال إضافة إلى تلك الأجهزة الأمنية سواء التابعة لسلك الأمن الوطني أو التابعة لقيادة الدرك الوطني.

البند الأول: الأجهزة التابعة لسلك الأمن الوطني

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم وبالخصوص تلك المستحدثة منها كالجرائم المعلوماتية، والتي تعتبر نتاج التطور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات.

أولا: على مستوى المركزي

بادرت المديرية العامة للأمن الوطني إلى تحديث بنيتها الهيكلية بغية خلق وحدات متخصصة تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها، ولذلك قامت المديرية العامة للشرطة القضائي باستحداث مصلحة مختصة في لمكافحة الجريمة المعلوماتية سميت بنيابة مديرية مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، بالإضافة إلى نيابة مديرية الشرطة العلمية والتقنية، هذه الأخيرة التي تضع لخدمة هذا الهدف مصالح عملية مختصة بذلك، تتولى أعمال البحث والتحري والتحقيق بشأن الجرائم

[1]– حسين ربيعي، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة دكتوراه، تخصص قانون عام ، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر ، السنة الجامعية 15-2016، ص 171.

المتصلة بتكنولوجيات الإعلام والاتصال، وهذه الوحدة هي المخبر المركزي للشرطة العلمية والكائن مقره بالجزائر العاصمة.

يتولى المخبر المركزي مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها، ولأجل ذلك يضم المخبر دائرة تقنية تتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الأسلحة والقذائف بمختلف أنواعها، وكذلك الجرائم التزوير، إضافة إلى الجرائم المعلوماتية، وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى.[1]

ثانيا: على المستوى الجهوي

قامت المديرية العامة للأمن الوطني بإنشاء مخابر جهوية للشرطة العلمية بداية في كل من ولايتي قسنطينة وهران، بالإضافة إلى ثلاث مخابر أخرى لاحقا على مستوى ورقلة، بشار، تمنراست ،على مستوى كل مخبر مصلحة تسمى دائرة الأدلة الرقمية والآثار التكنولوجية التابعة لمخبر الأدلة الجنائية، تتولي هذه المصلحة أعمال البحث والتحقيق القائمة بشأن الجرائم المعلوماتية، وذلك تحت تسمية دائرة الأدلة الرقمية والأثار التكنولوجية والتي لم تكن عند استحداثها سنة 2004 سوى قسم، غير أن الارتفاع الملحوظ لعدد القضايا الناتجة عن الجرائم المعلوماتية، بسبب الانتشار المتزايد لتقنية المعلوماتية عجل بترقيتها إلى دائرة تضم ثلاث 03 أقسام فرعية هي: **قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات، قسم استغلال الأدلة الناتجة عن الهواتف النقالة، قسم تحليل الأصوات.**

تضم الدائرة في صفوفها ثمانية 08 أعضاء محققين أربع 04 منهم عناصر شرطيون رسميون يتمتعون بصفة ضابط شرطة قضائية، والبقية هم أعوان شبيهون، يحمل كل منهم شهادة جامعية في تخصص الإعلام الآلي، إضافة إلى إلمامهم بالجانب القانوني، ومما يزيد من فعاليتهم في مجال مباشرتهم لمختلف إجراءات البحث والتحقيق في الجرائم المعلوماتية هو خضوعهم بصفة دورية لدورات تكوينية لأجل الاطلاع على كل المستجدات القانونية منها والتقنية في مجال الإجرام المعلوماتي.[2]

ومن مهام هذه المخابر ضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية في مجال التحريات الالكترونية، وذلك من خلال القيام بعمليات البحث عن المعطيات المشبوهة والمعلومات الرقمية على مختلف أشكالها: ملفات، رسائل الكترونية، برامج، صور،... هذا البحث يتم عن طريق استعمال برامج ووسائل خاصة تمكن من استرجاع كل المعطيات المحذوفة، و الاطلاع على محتوى كل الوسائط الرقمية.[3]

---

[1]– فريدة سعيدي ،هشام معزوز ، ***"دراسة سوسيو قانونية لمهام الشرطة العلمية في التحقيقات الجنائية"*** ،مجلة الدراسات القانونية م8 ،ع 02،جامعة يحي فارس المدية، الجزائر ،جوان 2022 ، ص 953 .

[2]– حسين سعيداني، **المرجع السابق**، ص 180.

[3]– فريدة سعيدي،هشام معزوز ،**المرجع السابق**، ص 954.

تلعب الدائرة دورا مهما للغاية في الكشف عن أسرار الجرائم المعلوماتية، من خلال مختلف الإجراءات التي تباشرها إما أثناء مرحلة البحث والاستدلال، أو أثناء مرحلة التحقيق القضائي.

ثالثا: على المستوى المحلي

في سبيل تدعيم المصالح الولائية للشرطة القضائية في مجال مكافحة الجرائم المعلوماتية، خلقت المديرية العامة للأمن الوطني فرق لمكافحة الجرائم المعلوماتية على مستوى مصالحها بأمن كل الولايات، ويتمثل دورها في تلقي الشكوى والبحث والتحقيق في الجرائم المعلوماتية وتقريب مصالح الأمن من المواطن.

البند الثاني: الأجهزة التابعة للدرك الوطني

تضع قيادة الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية وهي تباعا: قيادة الدرك الوطنية، الوحدات الإقليمية، الوحدات المشكلة، الوحدات المتخصصة وحدات الإسناد، هياكل التكوين، المعهد الوطني للأدلة الجنائية وعلم الإجرام، المصالح والمراكز العلمية والتقنية، مصلحة المركزية للتحريات الجنائية، المفرزة الخاصة للتدخل.[1]

تعمل مؤسسة الدرك الوطني جادة إلى التطلع بمختلف الجرائم المرتكبة على شبكة الإنترنت وهذا لتسهيل مهمة البحث والمعاينة والتفتيش في أنظمة الحواسيب والعمل على مراقبة مختلف الشبكات وبالتالي فقد تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه الأهداف، وذلك حسب الاختصاص والصلاحيات وطبيعة الجريمة إلى ثلاث 03 مستويات مركزية، جهوية، محلية.

أولا- على المستوى المركزي :

تعمل مصالح الدرك الوطني من خلال أجهزتها المركزية على مكافحة الجرائم المعلوماتية ودعم أعمال البحث والتحقيق بشأنها من خلال الهيئات التالية:

1- المعهد الوطني للأدلة الجنائية وعلم الإجرام في مكافحة جرائم المعطيات المعلوماتية:

يشكل المعهد لوطني للأدلة الجنائية وعلم الإجرام أداة مستلهمة من الخبرات التطبيقية والتحاليل

[1]- الموقع الرسمي لقيادة الدرك الوطني، الرابط الإلكتروني: http://www.mdn.dz ، تاريخ الدخول يوم 2024/05/01، على الساعة 10:00.

الحديثة والمدعومة بالتكنولوجيات المناسبة الخدمة الأساسية التي يقدمها هذا المعهد هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية.[1]

أنشئ المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب المرسوم الرئاسي رقم 04-183 وذلك من خلال المادة رقم 01 منه، والمعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، يوضع تحت وصاية وزير الدفاع الوطني، ويمارس قائد الدرك الوطني سلطات الوصاية بتفويض منه، وبهذه الصفة فإنه يخضع إلى جميع الأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية.[2]

حدد مقر المعهد بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني، كما يمكن إحداث ملحقات عند الحاجة بقرار من وزير الدفاع الوطني.[3]

يقوم بالإشراف على إدارة المعهد مدير عام ويسيره مجلس توجيه، ويزود بمجلس علمي، ويتكون المعهد من الهياكل التالية: مديرية الأدلة الجنائية، مديرية الدراسات والبحوث الإجرامية، مصلحة التنظيم والمناهج، مصلحة الإدارة والوسائل[4].

يساهم المعهد الوطني للأدلة الجنائية وعلم الإجرام في معاينة الجريمة الإلكترونية من خلال تقديم الخبرات التطبيقية والمعاينات اللازمة التي تساعد في التحقيقات القضائية والكشف عن الجرائم بالأدلة العلمية وذلك من خلال الدوائر المتخصصة في مجالات مختلفة أهمها دائرة الإعلام الآلي والإلكترونيك المتخصصة، هي دائرة مكلفة بمعالجة وتحليل وتقديم دليل رقمي وتماثلي للعدالة، كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة وكذلك تأمين اليقظة لتكنولوجية من أجل تحيين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية،[5] تنقسم الدائرة إلى ثلاثة مخابر وذلك حسب نوع المعلومات سمعية، بصرية وإعلام آلي كل مخبر مزود بفصيلة مهمتها اقتناء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل.[6]

---

[1]- الموقع الرسمي للدرك الوطني الجزائري http://www.mdn.dz ، تاريخ الدخول يوم 2024/05/01، على الساعة 10:30.

[2]- يراجع المادة 02 من المرسوم الرئاسي رقم 04- 183، مؤرخ في 2004/06/26، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانون الأساسي، ج.ر 41 .مؤرخة في 2004/06/27.

[3]- يراجع المادة 03 من نفس المرسوم السالف الذكر.

[4]- يراجع المادتين 05 و06 من نفس المرسوم السالف الذكر.

[5]- هواري عياش، **المعهد الوطني للأدلة الجنائية وعلم الإجرام مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة، الجزائر، يومي 16، 17نوفمبر 2015، ص 04.

[6]- هواري عياش ، **المرجع نفسه**، ص 05.

2- **مديرية الأمن العمومي والاستغلال:**

وهي الهيئة التي تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي، في مجال أعمال البحث والتحري في الجرائم المعلوماتية.

3- **المصلحة المركزية للتحريات الجنائية:**

وهي هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة المرتبطة بتكنولوجيا الإعلام والاتصال.

4- **مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية:**

أنشأ هذا المركز حديثا ويعتبر بمثابة نقطة وصل وطنية في مجال دعم أعمال البحث والتحقيق في الجرائم المعلوماتية،[1] إذ يوفر المساعدة التقنية للمحققين ويساهم في توجيه التحقيقات المرتبطة بتكنولوجيا الإعلام والاتصال، فهو هيئة تقنية تعمل تحت وصاية مديرية الأمن العمومي والاستغلال لقيادة الدرك الوطني ويحقق المهام التالية:

ضمان المراقبة الدائمة والمستمرة على شبكة الإنترنت، القيام بمراقبة الاتصالات الإلكترونية بما يسمح به القانون لفائدة وحدات الدرك الوطني والجهات القضائية، مساعدة الوحدات الإقليمية للدرك الوطني في معاينة الجرائم المرتبطة بتكنولوجيا الإعلام والاتصال والبحث عن الأدلة في شبكة الانترنت، المشاركة في عمليات التحري والتسرب عبر شبكة الانترنت الفائدة وحدات الدرك الوطني والسلطات القضائية، المشاركة في قمع الجرائم المعلوماتية، من خلال التعاون مع مختلف مصالح الأمن والهيئات الوطنية.

إذن تعتبر هذه الهيئات التابعة للدرك الوطني مسؤولة عن تنفيذ إجراءات البحث والتحقيق بشأن الجرائم المعلوماتية، وذلك على نطاق وطني بحيث تعتبر هيئات دعم وإسناد ونقاط وصل بين مختلف الوحدات الأخرى المتخصصة والتي توجد كذلك على مستويات أدنى منها الجهوية والمحلية.

ثانيا- على المستوى الجهوي:

تختص المصالح الجهوية للشرطة القضائية التابعة للدرك الوطني بمهمة تنسيق النشاطات بين مختلف الوحدات التابعة للشرطة القضائية وكذلك دعمها بالوسائل الخاصة للتحريات والأبحاث المعقدة كالجرائم المعلوماتية.

[1]- هواري عياش، المرجع السابق ، ص 29.

يلعب الدرك الوطني دورا هاما في ميدان الشرطة القضائية نظرا لانتشار وحداته على مستوى كامل التراب الوطني، ونظرا للوسائل المادية الموضوعة تحت تصرفه وعدد أفراده الهائل، والصلاحيات التي خولها لهم القانون، وهم في الواقع حسب الرتب والوظائف ضباط وأعوان الشرطة القضائية.

ثالثا- على المستوى المحلي:

يحوز الدرك الوطني على فصائل للأبحاث التي ينتمي إليها أفراد ذو وخبرة واختصاص واسعين في ميدان الشرطة القضائية، هذه الفصائل مكلفة خصوصا بمكافحة الأشكال الخطيرة للإجرام المنظم كالجرائم المعلوماتية، وذلك عن طريق القيام بتحقيقات تتطلب تحريات معقدة، هذه الوحدات المختصة تساهم في تدعيم نشاط الأبحاث والتحريات التي تقوم بها الفرق الإقليمية للدرك الوطني، وهوما سمح بإنشاء خلية متخصصة لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال في كل مجموعة ولائية، وهوما يسمح بتطبيق سياسة فعالة في مكافحة الجرائم المعلوماتية من خلال توفير الخلايا المتخصصة في مجال أعمال البحث والتحقيق في هذا النوع من الجرائم.

الفرع الثاني: الهيئات القضائية الجزائية المتخصصة

تعتبر الأقطاب الجزائية المتخصصة توجها جديدا من المشرع الجزائري، من أجل مكافحة الجريمة المنظمة، التي صارت تشكل خطرا حقيقيا على أمن سلامة المجتمع، ويعتبر انشاء هيئات قضائية جزائية متخصصة توجها جديدا لتطويق نطاق الجرائم الخطيرة ومن بينها الجرائم المعلوماتية.

البند الأول: الأقطاب الجزائية المتخصصة

رغم الأهمية التي خص بها المشرع الجزائري الأقطاب الجزائية المتخصصة، الى أنه لم يضع لها تعريفا محددا، وكانت بداية ظهور هذه الأقطاب مع صدور القانون: 14-04 المعدل والمتمم للأمر: 66-155 المتضمن قانون الإجراءات الجزائية، الذي تطرق في المواد: 37، 40، 329 إلى إمكانية تمديد الاختصاص الإقليمي لوكيل الجمهورية، قاضي التحقيق وقاضي الحكم، عندما يتعلق الأمر بالبحث والتحري عن جرائم محددة "جرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف"،[1] ثم صدر المرسوم التنفيذي رقم: 348-10 المؤرخ في 2010/10/05، المعدل والمتمم بالمرسوم التنفيذي

[1]- تنص المادة: 37ف2 من ق.الإ.ج ج م م : يجوز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى، عن طريق التنظيم، في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.

رقم 16-267 المؤرخ في: 2016/10/17،[1] الذي تضمن توسيع الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، وأعطى بذلك للجهات القضائية المتخصصة اختصاصا أوسع، ويمكن تعريف الأقطاب الجزائية المتخصصة من خلال استقراء النصوص القانونية المتعلقة بسيرها بأنها: "جهات قضائية متخصصة للنظر في بعض الجرائم التي حددها القانون، وليست جهات قضائية خاصة تنشط بإجراءات قانونية خاصة تخرج عن النظام القضائي ساري المفعول".[2]

وتتميز الأقطاب الجزائية عن المحاكم العادية بعدة خصائص، من أهمها اعتبار الأقطاب الجزائية جهات قضائية جزائية، مثل المحاكم الجزائية العادية، تتشكل من قضاة تحقيق، قضاة حكم، قضاة نيابة، وأمناء ضبط، تخضع الدعوى العمومية فيها لنفس القواعد الإجرائية العامة،[3] مع مراعاة بعض الأحكام الخاصة بها، وتتميز كذلك باختصاصها الإقليمي الموسع الذي يمتد ليشمل الاختصاص الإقليمي لمجالس قضائية أخرى ،وتختص الأقطاب الجزائية بالنظر في نوع معين من الجرائم، ويعد اختصاصها تفضيليا وليس مانعا، أي أن المحاكم العادية تبقى مختصة لمعالجة هذه الجرائم إلى حين إحالة الملف أمام القطب المتخصص.

ومن مبررات استحداث الأقطاب الجزائية المتخصصة عجز الآليات التقليدية للقضاء على مواجهة الأشكال الجديدة للإجرام المنظم، الذي عرف تطورا متسارعا، ومستوى عال من التنظيم، الاختصاص المحلي المحدود للجهات القضائية العادية شكل عقبة في مواجهة الإجرام المنظم، الذي يتسم باتساع رقعة نشاطه الإجرامي، حيث يمتد غالبا إلى اختصاص عدة محاكم، بل قد يتعدى حدود الدولة، مواكبة التوجه الدولي الجديد، بالعمل على تخصص القضاة، من أجل الارتقاء بالعمل القضائي لمواجهة التحديات المعاصرة، في ظل عولمة الجريمة، وما يتطلبه من تعاون دولي لمكافحة الإجرام المنظم.

البند الثاني: القطب الجزائي الوطني المستحدث

استحدث المشرع الجزائري قطب جزائي وطني واعتبره جهة متخصصة لمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، ومنحه اختصاصا وطنيا من أجل تجاوز العوائق التي تواجهها الجهات القضائية، وعليه يمكن القول بأن القطب المستحدث عبارة عن جهة قضائية متخصصة في

---

[1]- المرسوم التنفيذي رقم: 06-348 المؤرخ في: 2006/10/05، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر63، المؤرخة في 2006/10/08، ص 29.

[2]- عميور خديجة، **قواعد اختصاص الأقطاب الجزائية للنظر في جرائم الفساد**، مجلة دراسات في الوظيفة العامة، جامعة جيجل، الجزائر ،ع02، 2014، ص 134.

[3]- تنص المادة: 40 مكرر من ق.الإ.ج:ج م م تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد: 37 و40 و329 من هذا القانون، مع مراعاة أحكام المواد من 40مكرر 1 إلى 40 مكرر 5.

معالجة الجرائم الإلكترونية، جاء كخطوة إضافية، بعد إنشاء القطب الاقتصادي والمالي سنة 2020[1] لمواصلة إرساء نظام التخصص القضائي في الدولة، ولذلك سنتطرق لاختصاصه النوعي والإقليمي.

منح المشرع الجزائري القطب المستحدث اختصاصا وطنيا بموجب المادة 211 مكرر23من قانون الإجراءات الجزائية المعدل و المتمم ، ليمارس بذلك كل من وكيل الجمهورية وقاضي التحقيق ورئيس القطب اختصاصهم عبر كافة الإقليم الوطني، وذلك وفق نمطين كما يلي :

أولا–الاختصاص الحصري:

ويقصد به اختصاص القطب المستحدث حصريا ودون سواه بمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال عبر كافة الإقليم الوطني، ويكون ذلك في حالتين:

الحالة الأولى: بالنسبة للجرائم المحددة قانونا والجرائم المرتبطة بها

يختص القطب المستحدث عبر الإقليم الوطني ودون سواه، بمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المحددة على سبيل الحصر، والجرائم المرتبطة بها، وقد حصرت المادة 211 مكرر 24 من قانون الإجراءات الجزائية المعدل و المتمم.

الحالة الثانية: بالنسبة للجرائم الأكثر تعقيدا والجرائم المرتبطة بها

يختص القطب المستحدث كذلك دون سواه، بمعالجة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا والجرائم المرتبطة بها،[2] عبر كافة الإقليم الوطني حسب نص المادة:211 مكرر 25 من قانون الإجراءات الجزائية المعدل و المتمم.

ثانيا: الاختصاص التفضيلي

يتمتع القطب المستحدث عند معالجته لباقي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، التي تخرج من اختصاصه الحصري المحدد بنصوص المواد: 211 مكرر24، 211 مكرر25 مثل ما سبق توضيحه،[3] باختصاص مشترك مع باقي الجهات القضائية المختصة إقليميا، مع تمتعه بأفضلية

---

[1]– تم إنشاء القطب الاقتصادي والمالي بموجب الأمر 20–04 المؤرخ في: 2020/08/30 المتمم لقانون الإجراءات الجزائية ج.ر51، المؤرخة في 2020/08/31.

[2]– يراجع في ذلك نص المادة 211مكرر 25،ف 01، من الأمر 11–21.

[3]– تنص المادة: 211، مكرر 27ف 01، من الأمر 11–21، دون الإخلال بأحكام المواد: 211 مكرر 24 و211 مكرر 25 يمارس وكيل الجمهورية لدى القطب الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب اختصاصا مشتركا مع الاختصاص الناتج عن تطبيق المواد: 37، 40، 329 من هذا القانون بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

معالجتها، حيث يمارس وكيل الجمهورية لدى القطب المستحدث وكذا قاضي التحقيق ورئيس القطب اختصاصا مشتركا مع الجهة القضائية المختصة محليا، بموجب المواد: 37،40 329 من قانون الإجراءات الجزائية المعدل و المتمم، والتي تضبط معيار الاختصاص المحلي بمكان ارتكاب الجريمة أو محل إقامة أحد المتهمين، أو محل القبض على أحدهم، مع جواز تمديده لدائرة اختصاص محاكم أخرى عندما يتعلق الأمر بجرائم المخدرات، الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف، وفي هذه الحالة فإن وكيل الجمهورية لدى القطب المستحدث يتمتع بسلطة تقديرية للمطالبة بالملف أو عدم المطالبة به، وذلك بعد أخذ رأي النائب العام لدى مجلس قضاء الجزائر.

الفرع الثالث: الهيئات الشبه القضائية

تتمثل الهيئات الشبه القضائية المكلفة بالتحقيق في الجرائم المعلوماتية في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إضافة إلى السلطة الوطنية لمعالجة المعطيات ذات طابع شخصي، ووكالة أمن الأنظمة المعلوماتية.

البند الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

لضمان فعالية هذه الأحكام أحدث المشرع الجزائري من خلال القانون 04-19 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ونظمها بالمرسوم الرئاسي 261-15، الذي تضمن جملة من الإجراءات الخاصة لمكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

أولا: الإطار التنظيمي للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

أصدر رئيس الجمهورية المرسوم الرئاسي رقم 261-15، بتاريخ 08 أكتوبر2015 الذي حدد من خلاله تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتهما، و هذا إعمالا لأحكام المادة 13 من القانون 04-09 التي تنص على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والتي أحالت تنظيم الهيئة إلى المرسوم الرئاسي السالف الذكر.

وبموجب المادة 13 من قانون رقم 04-09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فان الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ،هي هيئة تنسيقية تعمل على اتخاذ الإجراءات اللازمة للوقاية من هذه الجرائم، وتتولى تنشيط

وتنسيق عملية الوقاية من الجرائم المعلوماتية، وكذا مصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم.[1]

تعد الهيئة بمثابة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي وضعت لدى الوزير المكلف بالعدل،[2] وبمقرها بمدينة الجزائر العاصمة.[3]

ثانيا: تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

تضم التشكيلة البشرية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ضباط وأعوان الشرطة القضائية من دوائر الاستخبارات العسكرية والدرك الوطني والشرطة، وفقا لأحكام قانون الإجراءات الجزائية، وتضم الهيئة من حيث تشكيلتها التقنية لجنة مديرة، مديرية عامة، مديرية المراقبة الوقائية واليقظة الإلكترونية مديرية التنسيق التقني، مركز للعمليات التقنية وملحقات جهوية.

ثالثا: الصلاحيات الإجرائية للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في معاينة الجريمة الإلكترونية

لقد جاء القانون04-09 رقم السالف الذكر ،بمجموعة من التدابير الوقائية و بإجراءات الخاصة ، منها ما يتعلق بمراقبة الاتصالات الإلكترونية، ومنها ما يتعلق بإجراءات التفتيش والحجز، كما ألزم القانون المتعاملين في مجال تكنولوجيات الإعلام والاتصال بتقديم المساعدة بهدف الوقاية، بمراقبة الاتصالات، وتفتيش المنظومات المعلوماتية، حجز المعطيات، التزامات مقدمي الخدمات وخدمة الانترنت.[4]

البند الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي

استحدث المشرع الجزائري بموجب القانون رقم 18-07 المؤرخ في 10جوان 2018 المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي، سلطة وطنية تسهر على مطابقة ومعالجة المعطيات ذات الطابع الشخصي ،وهي عبارة عن سلطة إدارية مستقلة تتمتع بالشخصية المعنوية وبالاستقلال المالي والإداري تضمن عدم انطواء استعمال تكنولوجيات الإعلام والاتصال على أي أخطار

[1]- نعيم سعيداني، المرجع السابق، ص 98.

[2]- المادة 02 من المرسوم الرئاسي رقم 261/15، مؤرخ في 2015/10/08، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر53، مؤرخة في 2015/10/08.

[3]- المادة 03 من نفس المرسوم الرئاسي.

[4]- حليمة حوالف، فاطمة الزهراء مهاجي ، **معالم الجريمة المعلوماتية في القانون الجزائري**، مجلة البحوث القانونية والسياسية جامعة تلمسان ، الجزائر ، م3، ع16، 2021، ص 151- 152.

تجاه حقوق الأشخاص والحريات العامة والحياة الخاصة، توضع لدى رئيس الجمهورية وذلك بهدف حماية المعطيات.

ومن المهام المسندة للسلطة الوطنية لحماية المعطيات ذات الطابع الشخصي، تلقي التصريحات المسبقة المتعلقة بمعالجة المعطيات ذات الطابع الشخصي، حيث تضمنت المواد من 13 الى 16 من القانون كل ما يخص إجراء التصريح الذي يجب أن يودع مسبقا لدى السلطة الوطنية، وباستقراء نص للمادة 13 من القانون السالف الذكر، نجد أن طريق تقديم التصريح المسبق يكون بأي شكل من الأشكال، حيث يمكن تقديمه الكترونيا، ويسلم وصل إيداع أو يرسل فورا بالطريق الالكتروني في مدة محددة ب 48 ساعة.[1]

كما تتولى السلطة الوطنية لحماية المعطيات الشخصية إخضاع المعالجة لنظام الترخيص المسبق، وفقا لأحكام المواد من 17 إلى 21 من ذات القانون ، و لها أن تتدخل متى تبين لها أن المعالجة محل التصريح تتضمن أخطار ظاهرة على احترام وحماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص، كذلك تمنح التراخيص بنقل المعطيات ذات الطابع الشخصي نحو الخارج وفقا شروط محددة قانونا، كما تقوم بنشر التراخيص الممنوحة والآراء المدلى بها في السجل الوطني، و تقدم الاستشارات والاقتراحات اللازمة، حيث تسهر على إعلام الأشخاص المعنيين والمسؤولين عن المعالجة بحقوقهم وواجباتهم، وتسهر على تقديم الاستشارات للأشخاص والكيانات التي تلجأ لمعالجة المعطيات ذات الطابع الشخصي، أو التي تقوم بتجارب أو خبرات من طبيعتها أن تؤدي إلى مثل هذه المعالجة، كذا تختص بتقديم أي اقتراح من شأنه تبسيط وتحسين الإطار التشريعي والتنظيمي، لمعالجة هذه المعطيات.

تتولى أيضا السلطة الوطنية لحماية المعطيات الشخصية إصدار أوامر بالتغييرات اللازمة من أجل حماية المعطيات ذات الطابع الشخصي المعالجة، كما تأمر بإغلاق معطيات أو سحبها أو إتلافها، و تسهر على تطوير علاقات التعاون مع الســلطات الأجنبية المماثلة، ويشترط في ذلك مراعاة مبدأ المعاملة بالمثل، كما تقوم بوضع معايير وقواعد السلوك والأخلاقيات التي تخضع لها معالجة المعطيات، بالإضافة إلى إصدار عقوبات إدارية، مع الإعلام الفوري للنائب العام المختص، في حالة معاينة وقائع تحتمل الوصف الجزائي[2].

هذا وتكلف السلطة الوطنية لحماية المعطيات الشخصية بإعداد تقرير سنوي، حول نشاطاتها، وترفعه الى رئيس الجمهورية، ولقد اشترط القانون 18-07 الموافقة المسبقة من الشخص الطبيعي الذي تكون

---

[1]- أومدور رجاء، **خصوصية التحقيق في مواجهة الجرائم المعلوماتية**، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية قسم الحقوق، جامعة محمد البشير الإبراهيمي، برج بوعريريج، الجزائر،السنة الجامعية 2020-2021، ص 96.

[2]- عائشة بن قارة مصطفى،"***آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم 18/07***"، مرجع سابق، ص 606.

المعطيات ذات الطابع الشخصي المتعلقة به محل معالجة، وله الحق في التراجع عن موافقته في أي وقت، كما لا يمكن اطلاع الغير على المعطيات محل المعالجة إلا بعد الموافقة المسبقة منه، وإذا كان عديم أو ناقص الأهلية تكون الموافقة وفق القواعد المقررة قانونا،[1] ولا يمكن القيام بالمعالجة للمعطيات ذات الطابع الشخصي المتعلقة بالطفل إلا بعد حصول موافقة من ممثله الشرعي، أو بترخيص من القاضي المختص.[2]

وتجدر الإشارة أنه لا يمكن معالجة المعطيات ذات الطابع الشخصي المتعلقة بالجرائم والعقوبات وتدابير الأمن، إلا من قبل السلطة القضائية والسلطات العمومية أو الأشخاص المعنوية المسيرة لمصلحة عمومية، ومساعدي العدالة في إطار اختصاصاتهم القانونية، كما يجب تحديد المسؤول عن المعالجة والغاية منها والأشخاص المعنيين بها، والغير الذي يمكنه الاطلاع على المعلومات ومصدرها والإجراءات الواجب اتخاذها لضمان سلامة المعالجة.[3]

البند الثالث: المجلس الوطني لأمن الأنظمة المعلوماتية

تم استحداث منظومة وطنية لأمن الأنظمة المعلوماتية لدى وزارة الدفاع الوطني ، والتي تتكون من المجلس الوطني لأمن الأنظمة المعلوماتية، و الوكالة الوطنية لأمن الأنظمة المعلوماتية التي من بين مهامها إجراء التحقيقات الرقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية وتعتبر وكالة أمن الأنظمة المعلوماتية مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، يقع مقرها في مدينة الجزائر.[4]

تضم تشكيلة المجلس الوطني لأمن الأنظمة المعلوماتية رئيسا يتمثل في وزير الدفاع الوطني أو ممثله ويتكون المجلس من تشكيلة تضم :ممثل عن رئاسة الجمهورية، ممثل عن الوزير الأول، الوزير المكلف بالشؤون الخارجية، الوزير المكلف بالداخلية، الوزير المكلف بالعدل، الوزير المكلف بالمالية، الوزير المكلف بالطاقة، الوزير المكلف بالاتصالات، الوزير المكلف بالتعليم العالي، كما يمكن أن يستعين المجلس بأي شخص أو مؤسسة من شأنه تنويره في أعماله.

يتولى المجلس في إطار إعداد الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية، على الخصوص المهام الآتي، البت في عناصر الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها، دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليهما، دراسة التقارير المتعلقة

[1]– يراجع في ذلك المادة 07 من القانون رقم 18–07 السالف الذكر.

[2]– يراجع في ذلك نص المادة 08 من القانون رقم 18–07 السالف الذكر.

[3] – يراجع في ذلك نص المادة 10 من القانون رقم 18–07 السالف الذكر.

[4]– المرسوم الرئاسي رقم 20–05، المؤرخ في 02 جانفي 2020، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية ج ر 04 ،المؤرخة في 26–01–2020، ص 05.

بتنفيذ الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها، الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية، الموافقة على سياسة التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني، الموافقة على تصنيف الأنظمة المعلوماتية، اقتراح ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية، عند الحاجة، ويبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية.[1]

أولا- وكالة أمن الأنظمة المعلوماتية

تعتبر الوكالة حسب نص المادة 17 من المرسوم الرئاسي، مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية ويحدد مقر الوكالة في مدينة الجزائر وتتولى مهمة تحضير عناصر الإستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس، تنسيق تنفيذ الإستراتيجية الوطنية في مجال لأمن الأنظمة المعلوماتية المحددة من قبل المجلس، اقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية، إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السيبرانية التي تستهدف المؤسسات الوطنية، السهر على جمع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية، متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية، تقديم المشورة والمساعدة للإدارات والمؤسسات والهيئات العمومية والخاصة من أجل وضع إستراتيجية أمن الأنظمة المعلوماتية، ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتي، مرافقة الإدارات والمؤسسات والهيئات في مجال معالجة الحوادث المتصلة بأمن الأنظمة المعلوماتية بعد الرأي المطابق للمجلس، إعداد وتحديث المرجعيات والإجراءات والأدلة العملية وتقديم توصيات في ميدان أمن الأنظمة المعلوماتية، اعتماد منتجات أمن الأنظمة المعلوماتية والتصديق عليها، اعتماد منظومات إنشاء وفحص الإمضاء الإلكتروني، تحديد معايير وإجراءات منح علامة الجودة و/أو التصديق و/أو اعتماد المنتجات ومقدمي الخدمات في مجال أمن الأنظمة المعلوماتية طبقا للتشريع والتنظيم المعمول بهما، القيام بنشاطات التموين والتوعية ذات الصلة بأمن الأنظمة المعلوماتية.[2]

ثانيا- اللجنة العلمية للوكالة:

تتكون اللجنة العلمية من عشرة (10) أعضاء يتم اختيارهم لمدة 03 سنوات قابلة للتجديد، من قبل لجنة التوجيه من بين الأساتذة والباحثين والخبراء في مجال أمن الأنظمة المعلوماتية.[3]

[1]- يراجع في ذلك نص المادة 04 من المرسوم الرئاسي 20-05، السالف الذكر.

[2]- يراجع في ذلك نص المادة 19 من المرسوم الرئاسي 20-05، السالف الذكر.

[3]- يراجع في ذلك نص المادة 31 من المرسوم الرئاسي 20-05، السالف الذكر.

وتبدي اللجنة رأيها وتوصياتها فيما يأتي: تجانس البرامج والمشاريع المقترحة من المدير العام للوكالة، كيفيات تنفيذ برامج ومشاريع البحث والتطوير، اختيار واقتناء المراجع العلمية، التنظيم والمشاركة في الأحداث والتظاهرات العلمية المتعلقة بأمن الأنظمة المعلوماتية، نشاطات التكوين العلمي والإتقان وإعادة التأهيل لفائدة مستخدمي الوكالة، وكذا المستخدمين المكلفين بأمن الأنظمة المعلوماتية في الإدارات والمؤسسات والهيئات العمومية، كل المسائل ذات الطابع العلمي التي يعرضها عليها المدير العام للوكالة.

الفرع الرابع: أجهزة التعاون الدولي في مجال الجرائم المعلوماتية

مديرية الأمن الوطني لم تغفل عن استغلال عضويتها الفعالة في الأنتربول على المستوى الدولي،الأمر الذي يتيح لها مجالات للتبادل المعلوماتي وتسهيل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الإنابة القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا،[1] ومن خلال الهيكل التنظيمي للمكتب المركزي الوطني أنتربول الجزائر" يوجد مكتب الربط للأنتربول 58 ولاية، واستخدام قاعدة المعطيات، حيث يعمل الجهاز على تحديد المعلومات اللازمة حول الأشخاص والمركبات موضوع التحقيق.

نذكر أن التعاون الأمني الدولي في مواجهة الجرائم المعلوماتية مبني على أساس توفير المعلومات و البيانات اللازمة حول الجريمة ومرتكبيها، و ذلك كان لابد من إنشاء مركز دولي للمعلومات والبيانات الخاصة بهذه الجرائم بكافة صورها وأنماطها، بما في ذلك أسماء المتورطين والإجراءات المتخذة والتحقيقات والأحكام الصادرة بشأنهم، كما يفترض إعداد مدونة دولية توحد معايير وأركان الجريمة ،و ضمان أن يشكل نطاق التجريم كافة جوانبها ومراحلها،[2] و لنجاعة التعاون الدولي في مواجهة الجرائم المعلوماتية لابد من تنسيق دولي على المستوى الأمني وتحقيق تكامل بين الأجهزة الأمنية الدولية والإقليمية و هذا ما تم التطرق إليه فيما يأتي.

البند الأول: المنظمة الدولية للشرطة الجنائية "الأنتربول" .

في إطار مواجهة الجرائم العابرة للحدود الوطنية يبحث العديد من القضاة أو ضباط الشرطة القضائية أو الدرك عن أدوات وخدمات عملية تسمح لهم بإجراء تحقيقاتهم خارج الأراضي الوطنية،[3] وتعتبر المنظمة الدولية للشرطة الجنائية (الانتربول INTERPOL)، من الأجهزة التابعة لمنظمة الأمم المتحدة وهي منظمة

---

[1]– عبد الرحمان حملاوي، **دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة، يومي 16–17 نوفمبر 2015، ص 09.

[2]– عادل عبد العال إبراهيم خراشي، **إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، مجلة كلية الشريعة والقانون، مصر ، ع16، م1، 2014، ص 193.

[3]- Olivier B**, Les investigations judiciaires internationales**, 1er édition ,Berger-levrault, 2014, p 237.

شرطة دولية مقرها في ليون فرنسا، تم إنشاؤها في07-09-1923 تباشر مهامها بأربع لغات رسمية (الانجليزية، الفرنسية، الاسبانية، العربية).[1]

أولا: دور الأنتربول في مواجهة الجرائم المعلوماتية

يبرز دور الأنتربول في مواجهة الجرائم المعلوماتية من خلال تأكيد وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة من خلال جمع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية للشرطة الجنائية الدولية على مستوى إقليم الدول الأعضاء، وتتبادلها فيما بينها،[2] دعم جهود الشرطة في مواجهة الجرائم العابرة للحدود الوطنية، وتقديم الخدمات في مجال الأدلة الجنائية،[3] التعاون في ملاحقة المجرم وتسليمه إلى الدولة التي طلبته فهي مختصة بالجرائم ذات الطابع الدولي خاصة جرائم الاستغلال الجنسي للأطفال عبر الانترنت والاحتيال المعلوماتي، إضافة إلى دعم إجراءات البحث والتحقيق في الجرائم المعلوماتية من خلال جمع وتخزين المعلومات المتعلقة بالجرائم وتوفير هذا للدول الأعضاء عبر شبكة الاتصالات الشرطية الرابطة بين الدول الأعضاء[4] ،والتي تم تطويرها و دعمها بمنظومة (I-Link)، التي تعتبر مركز رئيسي لتبادل المعلومات الجنائية والتواصل بين الدول الأعضاء، لها عدة وظائف تضمن فعالية نقل وتبادل المعلومات الشرطية، حيث تسير قاعدة البيانات الجنائية الدولية، وتقدم الدعم لمصالح الشرطة على المستوى الدولي والداخلي، مع تكوين رجال الشرطة لتحسين مهاراتهم في مجال الاتصالات، كما تقوم بعمليات نوعية تستهدف الإجرام المعلوماتي، كعملية Anmask.[5]

---

[1]- الأنتربول منظمة مستقلة تهدف لتأكيد التعاون الدولي بين سلطات الشرطة للدول الأعضاء، ومكافحة جرائم القانون العام، والتعاون في إطار الإعلان العالمي لحقوق الإنسان بغض النظر عن الأبعاد السياسية والدينية والعنصرية، والعمل على منع الجرائم الدولية والحد منها. لها عدة تسميات منها: البوليس الدولي أو الشرطة الدولية، المنظمة الجنائية للشرطة الدولية CPOI، انتسبت الجزائر له في العام 1963.

[2]- **محمد** أحمد سليمان عيسى، **التعاون الدولي لمواجهة الجرائم الالكترونية، المجلة الأكاديمية للبحث القانوني**،جامعة المجمعة ،المملكة العربية السعودية ، م14، ع02، 2016، ص 53.

[3]-**عادل عبد العال إبراهيم خراشي**، المرجع السابق، ص 197.

[4]- منذ 2003 نفذ الأنتربول شبكة اتصالات جديدة تسمى 24/7I تربط هذه الشبكة بين الدول الأعضاء، مما يسمح لهم بالتواصل في الوقت الحقيقي وبشكل أساسي بين المكاتب المركزية الوطنية والهيئات الفنية الدائمة بطريقة آمنة، وللتواصل بين الهيئات الفنية التابعة للأنتربول مباشرة حيث تضمن هذه الشبكة الوصول الكامل أو الجزئي إلى قواعد بيانات الانتربول والمعلومات التي تنشرها هذه المنظمة.

Olivier B, op.cit, p 240.

[5]- حسين ربيعي، المرجع السابق، ص 149-151.

ثانيا- استراتيجيات عمل الانتربول :

يقوم الأنتربول بعملية ملاحقة مجرمي المعلوماتية بصفة عامة وشبكة الانترنت بصفة خاصة عن طريق تعقب الأدلة الالكترونية وضبطها، والقيام بعمليات التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة المعلوماتية شبكات الاتصال، وذلك بغرض البحث عما قد تحتويه من أدلة وبراهين على ارتكاب الجريمة المعلوماتية، وكلها أمور تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة وهي من شأنها تطوير واكتساب مهارات وخبرات القائمين على مواجهة هذه الجرائم والحد من انتشارها،[1] وقد وضع الأنتربول بالتعاون مع مجموعة الدول الثمانية الكبرى G8 استراتيجيات لمواجهة الجرائم المعلوماتية من خلال إنشاء مركز اتصالات أمني عبر الشبكة يعمل على مدار 24 ساعة وكامل ايام الأسبوع على مستوى مصالح الشرطة في الدول الأطراف، إضافة إلى استخدام وسائل حديثة لمواجهة هذه الجرائم كأستخدام قاعدة البيانات المركزية للصور الإباحية المحولة من قبل الدول الأطراف والتي تستخدم برامج معيّنة للتحليل ومقارنة أوتوماتيكية للصور، هذا ناهيك عن تزويد شرطة الدول الأطراف بإرشادات حول الجرائم المعلوماتية وكيفيات التدريب على مكافحتها والتحقيق فيها،[2] وبهذا يتوالى عمل الأنتربول بالتعاون بينه وبين الدول الأطراف.

وعلى غرار هذه المنظمة أنشأ المجلس الأوروبي في لكسمبورج عام 1991 شرطة أوربية لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة لملاحقة الجناة في الجرائم العابرة للحدود ومنها: الجرائم المعلوماتية، أما على المستوى العربي، فنجد مجلس وزراء العرب أنشأ المكتب العربي للشرطة الجنائية بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في مجال مكافحة الجريمة وملاحقة المجرمين في حدود القانون والأنظمة المعمول بهذا في كل دولة، إضافة إلى تقديم العون في مجال دعم وتطوير أجهزة الشرطة في الدول الأعضاء.[3]

البند الثاني: الأجهزة الأمنية الدولية الأخرى

بغرض نجاعة التعاون الدولي على المستوى الأمني اعتمدت عدة وكالات لمواجهة الجرائم المعلوماتية ،ومن بينها اليوروبول واليوروجست على مستوى الاتحاد الأوروبي، والأفريبول على المستوى الإفريقي.

---

[1]- المركز العربي للبحوث القانونية و القضائية، **ضرورة التعاون الإقليمي والدولي في مكافحة جرائم المعلوماتية**، ورقة عمل مقدمة إلى الاجتماع السادس للمختصين بتقنية المعلوماتية في النيابات العامة في الدول العربية، بيروت، لبنان، 2018، ص 04.

[2]- عادل عبد العال إبراهيم خراشي، **المرجع السابق**، ص 198.

[3]- نجاة بن مكي، **السياسة الجنائية لمكافحة جرائم المعلوماتية**، منشورات دار الخلدونية، الجزائر، 2017، ص 150.

أولا- وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون- اليوروبول - :

يعد **اليوروبول** من أكبر الهيئات الاستشارية لمكافحة الجرائم المعلوماتية من ذلك الجرائم المسماة بالأنظمة المعالجة آليا ، يقع مقره في لاهاي هولندا، وقد تم إنشاؤه من قبل الإتحاد الدولي للأمن المعلوماتي، لإنجاز مختلف الدراسات الخاصة بالجرائم المعلوماتية ، بهدف تحليل دوافعها ووضع تصور مستقبلي لتطورها، وهو ما يفسر الثقة الموضوعة فيه من قبل اللجنة الأوربية باعتباره مركز إعلام حول هذه الجرائم حيث يختص بالبحث والتحقيق فيها، خاصة ما يتعلق بالإرهاب الالكتروني، ويكمن دوره أساسا في العمل على تسهيل الإجراءات أمام رجال الشرطة، ومدهم بمختلف النشرات الأمنية والتقارير حول هوية المتهمين والأدلة المحصلة خارج حدود اختصاصهم،[1]و يهدف اليوروبول أيضا إلى تحقيق تنمية اقتصادية وتوازن اجتماعي وتطوير البرامج الرقمية والوصول إلى الثقافة وأمن المواطنين،[2] ومن الصلاحيات المخولة له مكافحة جرائم الكمبيوتر، وكل أشكال الجريمة التي يسهل ارتكابها بواسطة التقنيات الرقمية.

يهدف اليوربول أيضا إلى توفير الخبرة والمساعدة الفنية للتحقيقات والعمليات داخل الاتحاد الأوروبي و نشر نظام معلومات داخل الدول الأعضاء لتمكين إدخال البيانات والوصول إليها وتحليلها، ويمكنه تخزين واستخدام البيانات اللازمة لأداء وظائفه، وقد تم الإعلان عن منصة مشتركة لتتبع الجرائم المعلوماتية في 24 أكتوبر 2008 في لوكسمبورغ، تضمن التعاون الشرطي ، وتبسيط إجراءات الشرطة في القضايا التي تشمل عدة دول، ولعل أهم المهام المسندة لها مكافحة الإرهاب، والجريمة المنظمة.[3]

ثانيا:- وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية- اليوروجست- :

وكالة الاتحاد الأوروبي للتعاون في مجال العدالة الجنائية- اليوروجست- هو هيئة تابعة للإتحاد الأوروبي مسؤول عن تحسين كفاءة الهيئات المختصة في مكافحة الجريمة المنظمة العابرة للحدود من ذلك الجريمة المعلوماتية بكل أشكالها، مقره في لاهاي بهولندا، ويكمن دوره في مواجهة الجريمة السيبرانية من خلال دعم وتعزيز التنسيق والتعاون بشأن الجرائم الخطيرة التي تؤثر على دولتين فأكثر، ومن بين صلاحياته تحفيز وتحسين تنسيق التحقيقات والملاحقات القضائية بين السلطات المختصة في الدول الأعضاء،[4] دعم الدول الأعضاء لزيادة كفاءة التحقيقات والملاحقات القضائية، تنسيق التحقيقات وتنفيذ طلبات التسليم من قبل السلطات الوطنية من اجل تعزيز فعالية المساعدة القانونية الدولية.

[1]- حسين ربيعي، **المرجع السابق**، ص 154.

2- Freyssinet E, **La cybercriminalité en mouvement**, Lavoisier, France, 2012, p 184.

[3] Myriam Quéméner, Joel Ferry , **Cybercriminalité Défi mondial** .Op. cit, p 238.

[4]- Olivier B, op. cit ,p 237.

يعمل اليوروجست بالتعاون مع المكتب الأوروبي لمكافحة الاحتيال، يقوم بمناقشة خطط عمله لمكافحة الجرائم المعلوماتية داخل فضاء الاتحاد،[1] له دو كبير في تطوير آليات مكافحة الجرائم المعلوماتية من خلال تبادل المعلومات بصفة دورية مع محاكم الاتحاد الأوروبي، كما يمثل دعامة في فعالية التحقيق في الجرائم المعلوماتية من ذلك الجرائم الماسة بالأنظمة ، ويمهد لليوروبول عمله في مجال التحقيق.[2]

ثالثا-منظمة الشرطة الجنائية الإفريقية -الأفريبول- :

بدأت فكرة إنشاء منظمة الشرطة الجنائية الإفريقية -الأفريبول- تتجسد ابتداء من مؤتمر الأنتربول الإقليمي الإفريقي الثاني والعشرين، سنة 2013 بمدينة وهران، ويكمن دوره في المساعدة على تعزيز القدرة التحليلية للشرطة الإفريقية في إطار تقييم التهديدات الإجرامية وتطوير الاستجابة الملائمة، وتعزيز التنسيق بين قوات الشرطة المنتشرة في عمليات دعم السلام، إضافة إلى مهامه في تطوير قدرة السياسة الشرطية الإفريقية لمسايرة الجرائم المستحدثة، ومن بينها مواجهة الجرائم المعلوماتية بما في ذلك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ،من خلال تبادل الخبرات و تكثيف الدورات التدريبية، والمساعدة التقنية المتبادلة في مجال تبادل المعلومات واستخدام التكنولوجيا الحديثة لاستخراج الأدلة الالكترونية.[3]

المبحث الثاني: الدعوى العمومية للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وتحدياتها الإجرائية

الدعوى العمومية هي الطريق الأساسي والأداة القانونية الشرعية للوصول إلى المضمون التقليدي لسلطة الدولة في توقيع الجزاء، وعلى الرغم من انتهاج السياسة العقابية اتجاها إجرائيا بطريق العمل على تبسيط إجراءات الدعوى العمومية يبقى الأمر صعب في ظل وجود جرائم معقدة كالتي على شاكلة الجرائم المعلوماتية،[4] هذه الأخيرة تدفع النيابة العامة إلى سلك طريق الدعوى العمومية بمختلف مراحلها ابتداء من تحريكها ومتابعتها إلى غاية إصدار الحكم الفاصل فيها بصفة نهائية، متوخية في ذلك تحقيق توازن بين مقتضيات العدالة في الكشف عن الجريمة، وضمان أقصى حد من الحريات الأساسية لحقوق الإنسان وبطبيعة الحال تشرف على كل مرحلة من هذه المراحل جهة مخولة قانونا ، يتمتع عناصره بمهارات وذكاء ودقة في الملاحظة، خصوصا وأن الأمر يتعلق بمواجهة جرائم تمس بأنظمة معالجة آليا تنشأ في الخفاء وترتكب من طرف جناة أذكياء وتطال معطيات مخزنة ومعلومات منقولة عبر النظم والشبكات، ورغم ذلك فالأمر لا يكاد يخلو من العوائق والصعوبات التي تعترض مواجهة هذه الجرائم من الناحية الإجرائية من ذلك مسألة الاختصاص القضائي وقبول الدليل الرقمي وإشكالية التعاون الدولي.

---

[1]- Myriam Quéméner, Joel Ferry , **Cybercriminalité Défi mondial**, Op. cit, p 239.

[2]- حسين ربيعي، **المرجع السابق**، ص 155.

[3]-يوسف مناصرة ، **المرجع السابق**، ص 284.

[4]- عثمان خرشي، **المرجع السابق**، ص 134.

وعلى هذا الأساس نقسم هذا المبحث إلى مطلبين نتناول من خلال المطلب الأول مراحل سير الدعوى العمومية لجرائم المساس بأنظمة المعالجة الآلية للمعطيات ونخص المطلب الثاني بدراسة أهم التحديات التي تواجه التصدي لهذا النوع من الجرائم.

المطلب الأول: مراحل سير دعوى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

إن تحريك الدعوى العمومية ومباشرتها يعني كل ما من شانه نقل الدعوى من حال السكون الذي كانت عليها عند نشأتها إلى حال الحركة بأن يدخلها في حوزة السلطات المختصة باتخاذ إجراءاتها التالية،[1] هذا وقد وسع قانون الإجراءات الجزائية الجزائري من الدور الأصيل الذي تؤديه النيابة العامة في مجال تحريك ومباشرة الدعوى العمومية سواء بصفة مباشرة أو عن طريق الضبطية القضائية التي يعهد إليها دور التحري وجمع الاستدلالات للكشف عن الجريمة تماشيا مع المستحدثات والتطور المتنامي للجرائم المنظمة والجرائم العابرة للحدود ومن ذلك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وذات الأمر بالنسبة لسلطات قاضي التحقيق والقاضي الجزائي المخول بالفصل في الدعوى العمومية ذات الصلة بالجريمة المعلوماتية.

على هذا الأساس نتطرق خلال هذه المطلب بالدراسة لمختلف مراحل سير الدعوى الجزائية المقامة في مواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات، بداية بمرحلة التحري والتحقيق المنوطة بأجهزة الضبطية القضائية، يلي ذلك دور النيابة العامة في تحريك الدعوى و إدارتها ،ثم المهام المسندة لقاضي التحقيق وصولا إلى مرحلة المحاكمة وهذا ضمن أربعة فروع على التوالي.

الفرع الأول: مرحلة التحري وجمع الاستدلالات في الجرائم الماسة بالأنظمة المعلوماتية

يعتبر التحقيق الابتدائي من المهام التي منحها المشرع إلى جهاز الضبطية القضائية تحت الإشراف المباشر للنيابة العامة حرصا منه على ضمان سير التحقيق على أكمل وجه وصولا لكشف الحقيقة، ذلك أن إجراءات التحقيق الابتدائي يترتب عليها آثار تمس بالمواطنين وخصوصياتهم، قد تصل في بعض الأحيان إلى تقييد حريتهم، وتكمن أهمية مرحلة التحقيق الابتدائي في أنها مرحلة تحضيرية للمحاكمة،[2] وقد نص المشرع الجزائري ضمن أحكام قانون الإجراءات الجزائية على مهام واختصاصات الضبطية القضائية والمتمثلة أساسا في مهمة البحث والتحري عن الجرائم المنصوص عليها في قانون العقوبات، وكذلك جمع الأدلة المتعلقة بهاته الجرائم والبحث عن مرتكبيها،[3] ما دام لم يبدأ فيها بتحقيق قضائي وعلى هذا سنحاول

---

[1]– زبيحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى، عين مليلة، الجزائر، ص 108.

[2]– يوسف خليل يوسف العفيفي، **الجرائم الالكترونية في التشريع الفلسطيني دراسة تحليلية مقارنة**، رسالة ماجستير في القانون العام، كلية الشريعة القانون، الجامعة الإسلامية غزة، فلسطين،السنة الجامعية2012 – 2013، ص 114.

[3]– يراجع في ذلك نص المادة 12 من ق.الإ.ج.ج.م.م.

معرفة الاختصاص المخول لهذه الفئة وآليات اتصالها بالجريمة المعلوماتية وأهم القواعد الإجرائية الواجبة الإتباع.

البند الأول: اختصاص ضباط الشرطة القضائية في الجرائم المعلوماتية

بالنظر لخصوصية الجرائم الماسة بأنظمة المعالجة الآلية عمدت جل التشريعات إلى تحديد صفات الأشخاص المؤهلة للتحري والبحث على هذا النوع من الجرائم، حيث أسندت لهم مهمة الضبط القضائي وهوما أبرزه المشرع الجزائري ضمن نصوص خاصة أين حدد الأشخاص المخول لهم مهام الضبط القضائي في الجرائم المعلوماتية، وحدد لهؤلاء اختصاصهم الإقليمي الذي يباشرون فيه مهامهم والتي لا يجوز لهم تجاوزها تحت طائلة بطلان الإجراءات التي باشروها ،وطبقا لقواعد قانون الإجراءات الجزائية الجزائري فإنّ ضباط الشرطة القضائية غير العسكريين يمارسون مهامهم بدائرة اختصاص كل مجلس قضائي تحت إشراف النائب العام الذي يحدد التوجيهات العامة اللازمة لهم من أجل تنفيذ السياسة الجزائية بدائرة اختصاص المجلس القضائي أين يتول وكيل الجمهورية إدارتهم على مستوى كل محكمة تحت رقابة غرفة الاتهام ويناط كذلك بضباط الشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها ما دام لم يبدأ فيها تحقيق قضائي، هذا ويبقى ضباط الشرطة القضائية في الحالات العادية يمارسون اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة أمّ في حالة البحث والتحري عن جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، تمتد اختصاصهم إلى كامل الإقليم الوطني.[1]

البند الثاني: آليات اتصال الضبطية القضائية بالجريمة الماسة بالنظام المعلوماتي

تعتبر مرحلة التحري على مستوى الضبطية القضائية أول خطوة في الكشف عن الجرائم بشكل عام بما في ذلك الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، علما أن التحري في مجال الضبط القضائي يقصد به البحث عن الجرائم المرتكبة والتحقق من صحة الوقائع المبلغة لضباط الشرطة القضائية، وجمع القرائن التي تفيد في حصول الواقعة أو نفي وقوعها،[2] فهذه المرحلة تعد أهم مرحلة من بين جميع مراحل الدعوى العمومية، وهي الفاصل الإجرائي للوصول إلى الحقيقة، وفي هذا السياق فإن رجال الضبطية القضائية إذا أخطروا بأي جريمة من جرائم المساس بأنظمة المعالجة الآلية للمعطيات، فإنهم يقومون بالإجراءات الأولية المرتبطة بالبحث والتحري باعتبارها مرحلة تمهيدية للدعوى، فكلما قرب الزمن بين

[1]– يراجع في ذلك نص المادة 16 من ق.الإ.ج.ج.م.م.

2– محمد ماجد ياقوت، **أصول التحقيق الإداري في المخالفات التأديبية–دراسة مقارنة–**، دار الجامعة الجديدة، الإسكندرية مصر، 2007، ص 289.

الإجراء والجريمة، كانت الأدلة واضحة أكثر وأسلم، ولم يشبها أي تغيير أو تحريف ومن ثم كانت أدعى للثقة،[1] وتختلف سبل اتصال الضبطية القضائية بالجريمة بحسب طبيعة الجريمة بحد ذاتها فمنها ما هو تقليدي منها ما هو مستحدث ومن أهم آليات اتصال عناصر الضبطية القضائية بالجريمة هي التبليغ والشكوى إضافة إلى إجراء المعاينة.

أولا- آلية التبليغ عن الجريمة:

هو إجراء يقوم بواسطته شخص لم يتضرر من الجريمة بالإبلاغ عنها لدى الجهات المختصة، وقد يكون التبليغ رسمي إذا كان صادر من قبل جهات رسمية، كما قد يكون عادي إذا صدر من قبل الأشخاص العاديين، وقد يكون في شكل مكتوب أوفي شكل تصريحات، هذا وقد ظهرت صور جديدة للتبليغ نتيجة التطور التكنولوجي مثل التبليغ عن طريق البريد الالكتروني، والتبليغ من خلال مواقع مخصصة لذلك.

وتلقي البلاغات في التشريع الجزائري من اختصاص ضباط الشرطة القضائية طبقا لقانون الإجراءات الجزائية ونشير إلى أن المادة 17 من ذات القانون تجيز للضبطية القضائية مطالبة أي عنوان أو سند إعلامي بنشر إشعارات أو أوصاف أو صور لأشخاص مبحوث عنهم وذلك بعد الحصول على إذن من النائب العام وبالتالي يمكن تخصيص موقع أو إضافة صفحة على المواقع الرسمية للضبطية القضائية تختص بتلقي البلاغات والشكاوى المتعلقة بالجرائم المعلوماتية وكذا نشر كل ما من شأنه المساعدة في البحث عن مجرمي المعلوماتية .

ثانيا- آلية الشكـــوى :

وهو إجراء يقوم به المجني عليه أو ذوي الحقوق يهدف من خلاله إلى إخطار السلطات المختصة بوقوع الجريمة عليه، وتكون الشكوى أمام ضباط الشرطة القضائية طبقا للمادة 17 من قانون الإجراءات الجزائية المعدل و المتمم، كما قد تكون أمام قضاة النيابة طبقا لنص المادة 36 من ذات القانون كما قد تكون في شكل شكوى مصحوبة بادعاء مدني أمام قضاة التحقيق طبقا لنص المادة 72 من ذات القانون.

ثالثا- إجراء المعاينة :

تعتبر أهم إجراء من إجراءات التحقيق، وهي في التعريف الاصطلاحي رؤية محل ارتكاب الوقائع الجنائية، وإثبات حالتها بالشيء والشكل الذي تركها عليه الجاني عقب ارتكاب الجريمة، كما تتصرف إلى فحص وإثبات ما يوجد من آثار[2]، وتتمثل أهمية إجراء المعاينة في ضبط جميع الوسائل التي تم استعمالها

---

[1]- محمد محدة، **ضمانات المتهم أثناء التحقيق ،ج3 ، ط1**، دار الهدى، عين مليلة، الجزائر ، 1992 ،ص 105.

[2]- خالد ممدوح إبراهيم، **المرجع السابق** ، ص 147.

في ارتكاب الجريمة وكذا مجموع الآثار والمخلفات والأشياء التي تفيد في الكشف عن الجريمة، وعلى هذا الأساس يلزم رجال الضبطية القضائية بقواعد إجرائية غير تقليدية بغية الحفاظ على مسرح الجريمة.

البند الثالث: قواعد التحقيق الابتدائي في الجرام الماسة بأنظمة المعالجة الآلية للمعطيات

إن أساليب التحقيق التقليدية، قد لا تصلح لمكافحة جميع الجرائم المستحدثة المرتكبة في العالم الافتراضي، خصوصا جرائم "المساس بأنظمة المعالجة الآلية للمعطيات"، لذا تم استحداث جملة من القواعد الإجرائية الواجبة الإتباع بغية كشف تلك الجرائم وضبط مرتكبيها، والمحافظة على مسرح الجريمة الرقمي ومن بين أهم القواعد الواجب إتباعها نذكر ما يلي:

أولا- وضع خطة عمل:

أول ما يبدأ به ضابط الشرطة القضائية المحقق عند بداية جمع الاستدلالات هو وضع خطة عمل على ضوء المعلومات المستقاة، مع تحديد الفريق التقني اللازم للقيام لمساعدته ويكون هذا مباشرة بعد معاينة مسرح الجريمة يضاف إلى ذلك التخطيط التقني المسبق للتحقيق وذلك قصد الوصول إلى أفضل الطرق والأساليب للتعامل مع خصوصية الجريمة، مع تحديد الإجراءات المسبقة والتي من شأنها التقليل من الأخطار الفردية التي قد تنتج عن قلة الخبرة لنقص المعرفة، والتي تضمن نجاح الخطوات التي يقوم بها المحقق خلال باقي مراحل التحقيق.[1]

ثانيا- تشكيل فريق التحقيق :

إن التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يكون أكبر من أن يتولاه شخص واحد بمفرده، حتى ولو كانت المحجوزات هي مجرد حاسب شخصي واحد، ولذلك فإنه يفضل أن يتعاون عدة محققين في انجاز مهمة التحقيق والعثور على الأدلة، ويجب أن يتشكل فريق التحقيق من تقنيين أخصائيين ذوي خبرة في مجال المعلوماتية، ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بـشكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والانترنت ليتمكنوا من فك التعقيدات التي تفرقها ظروف وملابسات كل جريمة،[2] وغالبا ما يتكون هذا الفريق من:

- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.

---

[1]- محمد نصير السرحاني، **مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت**، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، 2004، ص 72- 73.

[2]- عبد الله حسين محمود، **إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية**، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات، 2003، ص 612.

- خبراء التصوير والبصمات والرسم التخطيطي.[1]

وفي ذات الإطار نجد أن المشرع الجزائري قد أشار إلى مسألة إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو ممن لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية، وذلك بغض مساعدة جهات التحقيق في إنجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك.[2]

ثالثا: الالتزام بإجراءات التحقيق الأولية

يلتزم فريق العمل ببعض الإجراءات الخاصة السابقة لبداية التحقيق في النظام المعلوماتي المعتدى عليه من ذلك:

- تحديد نوع نظام المعالجة الأولية للمعطيات إذا كان معزولا أم متصل بشبكة معلومات.
- تحديد أطراف الاتصال إذا وقعت الجريمة على شبكة لمعرفة الطريقة التي تمت بها عملية الاختراق.
- إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة وتخزينها في الأقراص المعدة لذلك ومنع حذفه.
- مراعاة خصوصية الدليل الرقمي وعودة الجاني لإتلاف كل المعلومات المخزنة داخل الشبكة وبالتالي العمل على فصل الأجهزة عن موقع المعاينة لشل فاعلية الجاني في محو آثار الجريمة.
- إبعاد الموظفين عن الأجهزة بعد الحصول منهم على كلمة السر وكذا الثغرات في حالة وجودها.
- تصوير الأجهزة المستهدفة من أمام والخلف لإثبات أنها كانت تعمل.

أما عن الإجراءات الواجب مراعاتها أثناء التحقيق فيمكن إجمالها فيما يلي:

- نسخ الأقراص الصلبة قبل استخدامها والتأكد تقنيا من دقة النسخ.
- العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول وخروج المعلومات إضافة إلى حفظ المعدات والأجهزة التي تضبط بطريقة تقنية سليمة.
- العمل على فحص التطبيقات مثل البرامج الحسابية التي تكون قد استخدمت في الجريمة.
- تحليل المعلومات الموجودة بمحتوى الأسطوانة والأقراص بغرض التوصل إلى معرفة المعلومات الملفات الممسوحة، وكذلك معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.[3]

---

[1]– عبد الله حسين محمود، المرجع نفسه، ص 613.

[2]– يراجع في ذلك نص المادة 05 من القانون 04-09 السالف الذكر.

[3]– نعيم سعيداني، **المرجع السابق** ، ص 112- 114.

نشير في الأخير أن ضباط الشرطة القضائية وفي إطار جمع الاستدلالات والتحري عن الجريمة يخطرون وكيل الجمهورية بدون تمهل بجميع الإجراءات التي يباشرونها كما يوافوه بأصول المحاضر وما يتبعها من مستندات ووثائق قصد استكمال إجراءات المتابعة الجزائية.

الفرع الثاني: دور النيابة العامة في تحريك الدعوى جرائم المعطيات المعلوماتية

يطلق مصطلح النيابة العامة في قانون الإجراءات الجزائية الجزائري على القاضي الذي يتولى مهمة تمثيل المجتمع أمام القضاء، وذلك بتوجيه الاتهام من أجل اقتضاء حق الدولة في العقاب، وأن ينوب عنه أمام قضاء التحقيق وأمام قضاء الحكم، كما يتولى إعداد أدلة الإثبات وتنفيذ واستئناف وأوامر قاضي التحقيق المتعلقة بالقبض والإيداع والإحضار،[1] كما تؤدي النيابة العامة دور هام كحارس للشرعية وأداة لحماية القانون، من خلال بتقديم طلباتها الافتتاحية لقاضي التحقيق لفتح تحقيق في الجرائم المرتكبة وكذا استئناف الأحكام والأوامر وتنفيذها،[2] فعمل النيابة العامة كجهاز قضائي يتمثل في مباشرة عملها من خلال سلطتها كجهة اتهام، وكذا سلطتها كجهة تحقيق تبعا لاختصاصها الاقليمي والنوعي.

البند الأول: الاختصاص الاقليمي والنوعي لوكيل الجمهورية

طبقا لأحكام قانون الإجراءات الجزائية يتحدد اختصاص وكيل الجمهورية محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولوكان هذا القبض قد حصل السبب آخر، كما يجوز تمديد الاختصاص المحلي لوكيل الجمهورية في دائرة اختصاص محاكم أخرى في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[3]

البند الثاني: دور النيابة العامة في مباشرة الدعوى العمومية

تحرك النيابة العامة الدعوى بمجرد تلقيها خبر الجريمة، دون الحاجة إلى شكوى أو طلب أيا كان موقف المجني عليه، ذلك لأن الضرر لا يمس المجني عليه فقط، وإنما هو ضرر عام يمس كافة المجتمع وتتمتع النيابة العامة باختصاصات بصفتها جهة اتهام وهو الاختصاص الأصلي لها وتنحصر في التصرف في محاضر جمع الاستدلالات بالحفظ لأسباب قانونية وأخرى موضوعية، فالقانونية تتمثل في الحفظ لعدم قيام الجريمة وذلك لتخلف أحد أركانها بحيث لا يمكن إعطاؤها الوصف الإجرامي ثم الحفظ لوجود مانع من

[1]– عبد الرحمان خلفي، **الإجراءات الجزائية في التشريع الجزائري**، ط03، دار بلقيس للنشر، الدار البيضاء، الجزائر، 2017، ص 106.

[2]– عبد الرحمان خلفي، **المرجع نفسه**، ص 107.

[3]– يراجع نص المادة 37 من ق.الإ.ج.ج م م .

موانع المسؤولية ويتحقق ذلك عندما يتوافر مانع من موانع المسؤولية طبقا للمادة 47 من قانون العقوبات المعدل و المتمم أما الأسباب الموضوعية فتتعلق بموضوع الدعوى وأطرافها كالحفظ لعدم معرفة المتهم.[1]

وتقوم النيابة العامة ممثلة في شخص وكيل الجمهورية بحكم وظيفته بإدارة نشاط ضباط وأعوان الشرطة القضائية في دائرة اختصاص المحكمة وله الصلاحيات المرتبطة بذلك.[2]

كما يجوز للنيابة العامة أن تطعن في أوامر قاضي التحقيق وقرارات غرفة الاتهام وكذلك في الأحكام التي تصدرها جهات الحكم، فيما يخص الطعن في أوامر قاضي التحقيق ، فيجوز للنيابة استئناف جميع أوامر قاضي التحقيق أما غرفة الاتهام خلال ثلاثة (03) أيام بالنسبة لوكيل الجمهورية من تاريخ صدور الأمر وعشرين (20) يوما بالنسبة للنائب العام للمجلس القضائي، أما بالنسبة للأحكام الجزائية فإذا كان الحكم صادرا عن محكمة الجنح او محكمة الجنايات الابتدائية فيكون قابل للطعن بطرق الطعن العادية وهي الاستئناف ، أما إذا كان الحكم صادرا عن محكمة الجنايات الإستئنافية أو الغرف الجزائية بالمجلس القضائي، فيكون قابلا للطعن بالنقض أمام المحكمة العليا.[3]

كما تلعب النيابة العامة دورا محوريا في تنفيذ الأوامر والأحكام والقرارات حيث يقع على عاتقها تنفيذ الأوامر التي يصدرها قاضي التحقيق كالأمر بالقبض والأمر بالإحضار والأمر بالإيداع في المؤسسة العقابية، كما تتولى تنفيذ مختلف الأحكام التي تصدرها المحاكم بعد أن استنفاد هذه الأحكام جميع الطرق الموقفة للتنفيذ.[4]

البند الثالث: السلطات المخولة لوكيل الجمهورية

الأصل أن وكيل الجمهورية باعتباره سلطة اتهام لا يملك مهام سلطة التحقيق، فكلا السلطتين مستقلتين عن بعضهما البعض، إلا أن المشرع الجزائري قد منح لوكيل الجمهورية بعض المهام المرتبطة بالتحقيق وذلك على سبيل الاستثناء في حدود معينة، وقبل اتصال قاضي التحقيق بملف الدعوى،[5] كالانتقال لمكان الجريمة طبقا لنص المادة57 من قانون الإجراءات الجزائية المعدل و المتمم وتشمل مهام النيابة العامة في هذا الإطار ما يلي:

أولا- إصدار الأمر بالإحضار :

[1]- مصطفى بن عودة، **المرجع السابق**، ص 50- 52.

[2]- يراجع في ذلك المادة 36 ف 1 من ق.الإج.ج م م .

[3]- يراجع في ذلك المادة 36 ف7 من ق.الإ.ج.ج م م .

[4]- يراجع في ذلك المواد 29 و36 من ق.الإ.ج.ج م م .

[5]- عبد الرحمان خلفي، **المرجع السابق**، ص 205.

الأمر بالإحضار هو ذلك الأمر الذي يصدره قاضي التحقيق إلى القوة العمومية لاقتياد المتهم لمثوله أمامه على الفور ولكن يجوز لوكيل الجمهورية إصداره استثناء إذا كنا بصدد جناية متلبس بها، إذا لم يكن قاضي التحقيق قد أبلغ بها، بعد تنفيذ امر ضبط واحضار مشتبه في مساهمته في الجريمة ويقوم وكيل الجمهورية باستجواب الشخص المقدم أمامه وجوبا وهذا بحضور محاميه إن وجد.[1]

ثانيا- إصدار أمر المنع من مغادرة التراب الوطني :

طبقا لأحكام قانون الإجراءات الجزائية فقد تم إعطاء وكيل الجمهورية ممارسة بعض إجراءات الرقابة القضائية، بحيث يمكنه وبناء على تقرير مسبب من طرف ضابط الشرطة القضائية أن يأمر بمنع كل شخص توجد ضده دلائل من مغادرة التراب الوطني،[2] ويسري هذا الأمر لمدة ثلاث (03) أشهر قابلة للتجديد مرة واحدة، غير أنه يمكن إذا تعلق الأمر بجرائم الإرهاب أو الفساد أن يمتد الأمر إلى غاية الانتهاء من التحريات ويرفع الأمر بنفس الأشكال.[3]

ثالثا: إجراءات الاستجواب في الجرائم المتلبس بها

إذا تقرر متابعة المتهم وإحالتهم على المحاكمة وفقا لإجراءات المثول يتعين على وكيل الجمهورية التحقق من هوية المتهم المقدم أمامه ثم يبلغه بالأفعال المنسوبة إليه ووصفها القانوني ويخطروه أنه سيمتثل فورا أمام المحكمة، كما يبلغ الضحية والشهود بذلك.[4]

هذا ويجوز للمشتبه فيه الاستعانة بمحام عند مثوله أمام وكيل الجمهورية وفي هذه الحالة يتم استجوابه في حضور محاميه وينوه عن ذلك في محضر الاستجواب.[5]

من خلال ما سبق فان وكيل الجمهورية يحرك ويباشر الدعوى العمومية متى توفرا تاركان الجريمة ويتصرف بناءا على ذلك إما بإحالة الملف على المحاكمة مباشرة في حال الجنح المتلبس بها أو عرض الملف على قاضي التحقيق بناءا على طلب افتتاحي لإجراء التحقيق إذا تعلق الأمر بجناية أو إذا كانت الوقائع المشكلة جنحة تحتاج إلى تعزيز التحقيق فيها وهذا ما نجده في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إذ أنها غالب ما تعرض على قاضي التحقيق بالنظر لخصوصيتها وطبيعة الأدلة الرقمية المرتبطة بها.

---

[1]- يراجع في ذلك المادة 110 من ق.الإج.ج م م .

[2]- يراجع في ذلك نص المادة 36 مكرر 01 من ق.الإ.ج.ج م م .

[3]- عبد الرحمان خلفي، المرجع السابق، ص 206.

[4]- يراجع في ذلك نص المادة 339 مكرر 02 من ق.الإ.ج.ج م م .

[5]- يراجع في ذلك نص المادة 339 مكرر 03 من ق. الإ.ج.ج م م

الفرع الثالث: مرحلة التحقيق القضائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

تكتسي مرحلة التحقيق لقضائي أهمية كبيرة في مكافحة جميع أنواع من الجرائم، بما في ذلك الجريمة المعلوماتية بوجه عام وجرائم المساس بأنظمة المعالجة الآلية للمعطيات على وجه الخصوص، وبما أن هذا النوع من الجرائم في تزايد مستمر، وتطور دائم، أصبح من الواجب على مختلف الدول أن تقوم بتطوير أساليب وإجراءات التحقيق في هذا النوع من الجرائم، لتحقيق الغرض المطلوب وهو مكافحة الجريمة المعلوماتية بكل أنواعها والحد من أضرارها، والأهم من ذلك الاستعانة بذوي الكفاءات، ويتميز قاضي التحقيق بخصائص تميزه عن القاضي العادي في الجرائم التقليدية، كما خول له المشرع الجزائري سلطات واسعة يمارسها بكل استقلال على أن يطلع النيابة العامة على مجريات ونتائج التحقيق.

البند الأول: اختصاص قاضي التحقيق

يتحدد الاختصاص المخول لقاضي التحقيق وفقا لأحكام قانون الإجراءات الجزائية استنادا إلى ثلاث معيار، تتمثل في الاختصاص الشخصي، الاختصاص النوعي الاختصاص الإقليمي.

أولا: الاختصاص المحلي لقاضي التحقيق

طبقا للأحكام قانون الإجراءات الجزائية يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولوكان هذا القبض قد حصل لسبب أخر، كما يجوز تمديد الاختصاص المحلي لقاضي التحقيق في دائرة اختصاص محاكم أخرى في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف.[1]

ثانيا: الاختصاص النوعي لقاضي التحقيق

يختص قاضي التحقيق في جميع الجرائم ويكون ذلك وجوبيا في الجنايات وجوازيا في الجنح، ما لم ينص القانون على خلاف ذلك كما يجوز إجراؤه في مواد المخالفات إذا طلبه وكيل الجمهورية.[2]

ثالثا– الاختصاص الشخصي لقاضي التحقيق:

يحقق قاضي التحقيق في الأصل مع جميع الأشخاص، إلا أن المشرع الجزائري أورد استثناء على بعض الفئات والمتمثلة أساسا في أعضاء الحكومة والولاة وقضاة المحكمة العليا [1]،حيث يحال ملف المتابعة

[1]– يراجع نص المادة 40 من ق.الإ.ج.ج م م .

[2]– يراجع أحكام المادة 66 ق.الإ.ج .ج .م .م

ضد هؤلاء من وكيل الجمهورية المختص في الجرائم المرتكبة من الأشخاص العاديين بالطريق السلمي على النائب العام لدى المحكمة العليا، الذي بدوره يرفعه إلى الرئيس الأول للمحكمة العليا ليتخذ ما يراه بشأنه، فإذا رأى أن هناك ما يقتضي المتابعة، يعين قاضيا من قضاة المحكمة العليا ليتولى التحقيق في القضية،[2] كذلك الأمر بالنسبة لقضاة المجالس القضائية ورؤساء المحاكم ووكيل الجمهورية وفقا لما جاءت به المادة 575 قانون الإجراءات الجزائية المعدل و المتمم الناصة على أنه إذا كان الاتهام موجه إلى أحد أعضاء المجلس القضائي أو رئيس محكمة أو وكيل الجمهورية أرسل الملف بطريقة التبعية التدريجية من وكيل الجمهورية إلى النائب العام لدى المحكمة العليا الذي يرفع الأمر إلى الرئيس الأول للمحكمة العليا إذا قرر أن ثمة محلا للمتابعة ويندب الرئيس الأول للمحكمة قاضيا للتحقيق من خارج دائرة اختصاص المجلس الذي يقوم بالعمل فيه رجل القضاء المتابع.

أما إذا كان الاتهام موجه إلى قضاة المحاكم وضباط الشرطة القضائية فيقوم وكيل الجمهورية بإرسال الملف إلى النائب العام لدى المجلس القضائي، الذي يعرض الأمر على رئيس المجلس القضائي من اجل الأمر بالتحقيق في القضية لأحد قضاة التحقيق من خارج دائرة الاختصاص القضائية التي يباشر فيها المتهم مهامه وفقا لأحكام المواد 576، 577من قانون الإجراءات الجزائية المعدل و المتمم [3].

في حين يختص قاضي التحقيق العسكري بالمحاكم العسكرية دون سواه في التحقيق في الجرائم التي يرتكبها العسكريون، ومن في حكمهم في الخدمة أو المرتكبة داخل مؤسسة أو لدى المضيف، ويستوي في ذلك أن يكون مرتكب الجريمة عسكريا أو مدنيا فاعلا أصليا أو مساعدا أو شريكا.[4]

البند الثاني: آليات اتصال قاضي التحقيق بملف الدعوى الخاص بجرائم المعطيات المعلوماتية

يتصل قاضي التحقيق بملف الدعوى الجزائية للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بذات الآليات في الجرائم التقليدية وهذا إما عن طريق وكيل الجمهورية وذلك بموجب طلب افتتاحي لإجراء التحقيق، وأما عن طريق شكوى مدنية مقدمة من الضحية أو المدعي المدني ضمن الشروط والإجراءات المنصوص عليها في قانون الإجراءات الجزائية.[5]

---

[1]– يراجع أحكام المادة 573 ق.الإ.ج .م .م

[2]– فوزي عمارة ، **قاضي التحقيق**، أطـروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة قسنطينة ، الجزائر ،السنة الجامعية 2009–2010، ص 46.

[3]– فوزي عمارة، **المرجع نفسه**، ص 46.

[4]– فوزي عمارة ، **المرجع نفسه**، ص 47.

[5]– يراجع في ذلك أحكام المادة 67 ف 03 من ق.الإ.ج .م .م.

أولا- الطلب الافتتاحي لإجراء التحقيق:

لا يجوز لقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب افتتاحي من وكيل الجمهورية لإجراء التحقيق حتى ولو كان ذلك بصدد جناية أو جنحة متلبس بها،[1] وفي المقابل من ذلك يملك سلطة اتهام أي شخص ساهم بصفته فاعلا أو شريكا في الوقائع المحال إليه من طف النيابة العامة، هذا ويتوجب عليه متى أخطر بوقائع أو محاضر جديدة لم يشر إليها في طلب إجراء التحقيق، أن يحيلها فورا إلى وكيل الجمهورية لإبداء التماساته بشأنها.[2]

ثانيا- الشكوى المصحوبة بادعاء مدني :

يجوز لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يقدم شكواه أمام قاضي التحقيق المختص،[3] وبالتالي فإن المشرع الجزائري أجاز تحريك الدعوى العمومية عن طريق الشكوى المصحوبة بالادعاء المدني، إذا كانت هناك جريمة تضرر منها الضحية أي المدعى المدني،[4] ويلجأ عادة المتضرر من الجريمة إلى هذه الطريقة تجنبا لطول الإجراءات وتقليصا للوقت وحرصا من على أن يكون الإشراف على الملف من طرف قاضي التحقيق لا أن يكون من طرف الضبطية القضائية التي عادة يكون لها تأثير مجرى التحقيق، إلا أن أخطر سلبيات الادعاء المدني يتمثل في سوء استعمال هذا الطريق لأن من شأن أن يعرض الطرف المدني إلى متابعة جزائية بتهمة الوشاية الكاذبة إذا ما خسر دعواه، ولهذا و عليه أن يتأكد من أن اتهامه كان مبنيا على دليل قوي في الدعوى.[5]

البند الثالث: سلطات قاضي التحقيق المختص في جرائم المعطيات المعلوماتية

يختلف المختصون بالتحقيق القضائي في الإجرام المستحدث عن أولئك المختصين بالتحقيق في الجرائم العادية من حيث البناء العلمي والتكنولوجي ذلك أنهم يتولون مهمة التحقيق في جرائم ذات طابع رقمي معلوماتي ومن أهم هذه المميزات:

- معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والانترنت والتي تتعلق بالجريمة الإلكترونية.
- معرفة آلية تشكيلات الحاسوب والانترنت والتمييز بين أنظم لحاسوب المختلفة، وأن يلم بجميع الأنظمة التشغيلية لأجهزة الحاسوب وما تتسم به من خصائص.[6]

---

[1]- يراجع في ذلك المادة 67 ف 1 من ق.الإ.ج .ج .م .م

[2]- يراجع في ذلك المادة 67 ف 03 من ق.الإ.ج .ج .م .م.

[3]- يراجع في ذلك المادة 72 من ق.الإ.ج .ج .م .م

[4]- مصطفى بن عودة، **المرجع السابق**، ص 190.

[5]- عبد الرحمان خلفي، **المرجع السابق**، ص 34.

[6]- نعيم سعيداني، **المرجع السابق**، ص 116.

- أن يكون ملما بالأساليب المستخدمة في ارتكاب الجريمة الإلكترونية وتقنيات الأمن المعلوماتي.[1]

وفي سبيل إجراء التحقيق يتمتع قاضي التحقيق بعدة سلطات نذكر أهمها:

أولا- اتخاذ إجراءات التحقيق:

يقوم قاضي التحقيق باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للوصول إلى الحقيقة والتحري عن أدلة الاتهام والنفي.[2]

ثانيا- استجواب المتهم وإجراء المواجهة:

أن قيام قاضي التحقيق باستجواب المتهم يهدف إلى مناقشة هذا الأخير حول علاقته بالجريمة ومواجهته بالأدلة القائمة ضده وكذا مطالبته بالرد عليها إثباتا أو نفيا، ولعل الغرض الأساسي من استجواب المتهم بالجريمة المعلوماتية هو الحصول على اعتراف هذا المتهم.

أما المواجهة فهي إجراء يتم من خلاله جمع المتهم مع متهم آخر أو مع شاهد في حالة ما إذا كان هناك تناقض في الأقوال لكلا طرفي المواجهة، وذلك بهدف رفع هذا التناقض وللوقوف على صحة دليل أو واقعة.[3]

ثالثا- الاستماع إلى أقوال الشهود :

يستدعي قاضي التحقيق للحضور أمامه كل شخص يرى فائدة من سماع شهادته، وبطبيعة الحال يختلف الشاهد المعلوماتي عن الشاهد العادي ذلك أنّ هذا الأخير عاين الواقعة بأحد حواسه، بينما الشاهد الأول هو شخص متخصص، استعمل خبرته في الولوج إلى الحاسب الآلي والشبكات بحثا عن أدلة الجريمة التي سيدلي فيها فيما بعد بشهادته حول ما توصل إليه من نتائج ضرورية ومساعدة في مرحلة التحقيق.[4]

رابعا: الانتقال إلى أماكن وقوع الجرائم

---

[1]- نعيم سعيداني ،**المرجع نفسه**، ص 117.

[2]- المادة 68 من ق.الإ.ج .ج .م .م.

[3]- عثمان خرشي، **المرجع السابق**، ص 164.

[4]-وردة شرف الدين ، **الإثبات الجنائي بالأدلة الإلكترونية دراسة مقارنة**، أطروحة دكتوراه، تخصص قانون جنائي كلية الحقوق الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر ،السنة الجامعية 2016-2017، ص 248.

يمكن لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء المعاينات اللازمة أو للقيام بتفتيشها ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، وتبعية قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات.[1]

خامسا: تنسيق سير إجراءات التحقيق

ينسق القاضي المكلف بالتحقيق تسيير إجراءات التحقيق وله وحده الصفة للفصل في مسائل الرقابة القضائية والحبس المؤقت واتخاذ أوامر التصرف في القضية.[2]

سادسا: التصرف في نتائج التحقيق

إن السلطات و الإجراءات المخولة لقاضي التحقيق تساعده في استقصاء مختلف الأدلة المساعدة في إظهار الجريمة المعلوماتية المرتكبة كما أن نتائج هذا التحقيق هي من تحدد نهاية هذه المرحلة من الدعوى وذلك بأحد الأمرين إمّا بان يصدر قاضي التحقيق بالأمر بأن لا وجه لمتابعة المتهمين المعلوماتيين في غياب الأدلة، وإمّا التصرف بالأمر بإحالة القضية إلى المحكمة المختصة بنظر هذه القضية، وننوه هنا أن الطبيعة الخاصة والمعقدة للجرائم المعلوماتية تجعل من قاضي التحقيق كثير الشك حول المتهم المعلوماتي باعتباره مجرما محترفا في إخفائه لآثار وأدلة جريمته مما يجعل قاضي التحقيق في غالب الأحيان يحيله إلى المحكمة المختصة بهذه الجريمة للتدقيق وتمحيص الأدلة المتوفرة أكثر.

الفرع الرابع: دور القاضي الجزائي في الفصل في دعوى المساس بأنظمة المعالجة الآلية للمعطيات

تمثل المحكمة سلطة الحكم ولا ينعقد لها الاختصاص بالنظر في الدعوى العمومية والفصل فيها من تلقاء نفسها حيث لا يكون لها ذلك إلا بموجب إحالة إليها من طرف النيابة العامة كأصل عام، والمحاكمة تعتبر المرحلة الختامية في الدعوى العمومية يكون الغرض منها الوصول إلى الحقيقة الواقعية والقانونية، لهذا وضع المشرع مجموعة من الإجراءات لسير المحاكمة، يتعين على المحكمة مراعاتها ابتداءا من تشكيلة المحاكمة إلى افتتاح الجلسة والنطق بالحكم.[3]

البند الأول: تشكيلة المحكمة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

إعمالا لقواعد قانون الإجراءات الجزائية الجزائري تفصل المحكمة الابتدائية بقاضي فرد، يساعده أمين ضبط، و يقوم بتمثيل النيابة العامة وكيل الجمهورية أو أحد مساعديه، وينطبق ذلك على محكمة الجنح

[1]– يراجع في ذلك نص المادة 79 من من ق.الإ.ج .ج .م .م

[2]– يراجع في ذلك نص المادة 73 ف 3 من من ق.الإ.ج .ج .م .م.

[3]– نجيمي جمال،**دليل القضاة للحكم في للجنح والمخالفات**، ج2، ط2، دار هومة للطباعة والنشر، الجزائر، 2014، ص 14.

أو المخالفات على مستوى المحاكم الابتدائية كدرجة أولى للتقاضي، أما الغرف الجزائية على مستوى المجلس القضائي باعتباره درجة ثانية فالتشكيلة فيها ثلاثية، حيث تتكون من رئيس غرفة ومستشارين أثنين بالإضافة إلى أمين ضبط و حضور النائب العام أو أحد مساعديه، في حين تتشكل محكمة الجنايات الابتدائية

أو الإستئنافية من رئيس المحكمة ومستشارين وأربعة محلفين وأمين الضبط وممثل النيابة العامة،[1] هذا ولم يتعرض المشرع لتنظيم توزيع الجلسات وتحديد القضاة المكلفين بها، وهو ما يعرف بأمر توزيع المهام الذي يصدره رئيس المحكمة، غير أن التشريع لم يتطرق لذلك، وهو ما يجعل هذه المسألة الحساسة في وضع غامض لأن في غياب النص القانوني تبقى المسألة ذات طابع إداري، وهو ما يسمح للسلطة الإدارية بالتدخل فيها بطرق ملتوية والتأثير على عمل رئيس المحكمة أو رئيس المجلس في هذا الشأن.[2]

البند الثاني: القواعد العامة لإجراءات المحاكمة في جرائم المساس بأنظمة المعالجة الآلية للمعطيات

ترتكز المحاكمة الجزائية على مجموعة من المبادئ الأساسية تحت طائلة الطعن بالنقض وهي ذاتها بالنسبة لجميع الجرائم بما في ذلك جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتتمثل هذه المبادئ فيما يلي:

أولا- مبدأ العلنية :

يسمح هذا المبدأ للجمهور بمراقبة عمل المحكمة إلا أن العلنية ليست في جميع الجلسات، ويمكن كذلك أن تكون الجلسة سرية إذا ما كانت العلنية تشكل خطرا على النظام العام والآداب العامة وفي هذه الحالة على المحكمة أن تصدر حكما علنيا بعقد جلسة سرية وهذا الحكم منصوص عليه في نص المادة 285من قانون الإجراءات الجزائية المعدل والمتمم حيث نصت على: "جلسات المحكمة علنية ما لم يكن مساس بالنظام العام أو الآداب العامة وفي هذه الحالة تصدر المحكمة حكما علنيا بعقد جلسة سرية، غير أن الرئيس أن يحظر على القصر الدخول لقاعة الجلسة، وإذا تقررت سرية الجلسة تعين صدور الحكم في الموضوع بجلسة علنية".[3]

ثانيا- مبدأ شفوية الجلسات :

ويقصد بها أن تجرى المحاكمة شفويا أي بصوت مسموع للكافة لكل ما يتم داخل الجلسة من إجراءات، حيث يتم إلقاء الاتهامات التي يحاكم المتهم من أجلها بصوت مسموع ويجب أن تطرح الأدلة كلها في الجلسة حتى تلك التي تم تدوينها في اوراق التحقيق ومحاضر جمع الاستدلالات.

---

[1]- عبد الرحمان خلفي، **المرجع السابق**، ص 472.

[2]-جمال نجيمي ، **المرجع السابق**، ص 16- 17.

[3]- يراجع في ذلك نص المادة 285 من ق.الإ.ج .م .م

ثالثا- حضور أطرف الخصومة:

لا يجوز إجراء المحاكمة دون حضور أطراف الدعوى أو الخصومة لذلك أوجب المشرع حضور كل من الضحية والمتهم أو صحة تبليغهم بتاريخ انعقاد الجلسة، أما بالنسبة للنيابة العامة فهي جزء من تشكيلة المحكمة.

رابعا- تدوين التحقيق النهائي:

لا يمكن أن تعقد المحكمة في حالة غياب أمين الضبط، ذلك لأن دوره يتجسد في تدوين كل ما يدور في الجلسة، حيث يقوم بالتوقيع عليها، كما يؤشر رئيس المحكمة عليها وذلك خلال ثلاث (03) أيام الموالية لكل جلسة على الأكثر طبقا لأحكام قانون الإجراءات الجزائية.[1]

خامسا: مباشرة القاضي لجميع إجراءات الدعوي

تصدر أحكام المحكمة وجوبا من القاضي الذي يترأس جميع جلسات الدعوى وإلا كانت باطلة وإذا طرأ مانع من حضوره أثناء نظر القضية يتعين نظرها كاملا من جديد.[2]

البند الثالث: إجراءات سير الجلسة المحاكمة

تفتتح المحكمة باسم الشعب الجزائري الجلسة ثم يعلن القاضي الجلسة مفتوحة، ليتولى بعد ذلك المناداة على أطـراف الخصومة بداية بالمتهم والضحية والشهود والمسؤول المدني على التوالي والتأكد من حضورهم أو غيابهم، يتم تدوين ذلك في محضر الجلسة المعد من طرف أمين الضبط، ثم يتم التحقيق من هوية المتهم وتبليغه بالتهمة المنسوبة إليه، فإذا كان المتهم قد سبق حبس من طرف قاضي التحقيق عن طريق الحبس المؤقت أو بموجب إجراءات المثول الفوري فإنه يساق بواسطة القوة العمومية لحضور الجلسة، ويخطره رئيس الجلسة بأن له الحق في اختيار محام للدفاع عنه فإن طلب ذلك أمهل القاضي مدة لتحضير دفاعه وإذا كانت الدعوى غير مهيأة للحكم أمرت المحكمة بتأجيلها إلى أقرب جلسة، وفي هذه الحالة وطبقا لأحكام المادة 339 مكرر من قانون الإجراءات الجزائية المعدل والمتمم تتخذ المحكمة إحدى الإجراءات التالية اما ترك المتهم حرا أو إخضاعه لتدبير أو أكثر من تدابير الرقابة القضائية المنصوص عليها في المادة 125 مكرر1 من ذات القانون، أو وضعه في الحبس المؤقت، مع التنويه بعدم قابلية هذه التدابير لأي طريق من طرق الطعن.

[1]- يراجع في ذلك نص المادة 236 من ق.الإ.ج .ج .م .م

[2]- يراجع في ذلك المادة 341 من ق.الإ.ج .ج .م .م

تتسم إجراءات المحاكمة كما سبق الإشارة بالعلنية والشفوية حيث يتم مواجهة المتهم بالأفعال المنسوبة إليه ويتاح له أن يعرف ما لدى خصمه وممثل للنيابة العامة من أدلة ضده، وعلى القاضي مناقشته عن كل واقعة بالتفصيل حتى وإن اعترف بالجرم المنسوب إليه، يلي ذلك سماع شهود الإثبات ثم النفي إن وجدوا، وبعدها سماع الطرف المدني، ثم تعطى الكلمة للنيابة العامة من أجل توجيه الأسئلة إلى المتهمين أو الشهود أو الضحايا، أما دفاع المتهم فيوجهه الأسئلة بواسطة رئيس الجلسة لا يكون له الحق في الاعتراض على أي سؤال، باستثناء محكمة الجنايات الابتدائية ومحكمة الجنايات الإستئنافية فيمكن للمحامي طرح أسئلة مباشرة مثل النيابة العامة طبقا لنص المادة 288 من قانون الإجراءات الجزائية المعدل والمتمم

وبعد الانتهاء من التحقيق تعطى الكلمة للطرف المدني أو محامية للمرافعة وتقديم طلبات المتمثلة في التعويض المدني فقط دون المطالبة بالعقوبات الجزائية لأنها حق عام، تقوم بعد ذلك النيابة العامة بالمرافعة وتقديم التماساتها في الشق الجزائي وفي الأخير يقوم دفاع المتهم بتقديم مرافعته وتقديم التماسه، ويكون بعدها للنيابة العامة والمدعي حق الرد على مرافعة محامي المتهم، وتعطى الكلمة الأخيرة بعدها للمتهم ومحاميه، ثم يعلن رئيس الجلسة إقفال باب المرافعات ويصدر حكم في نفس الجلسة أو يحدد تاريخ لاحق للنطق بالحكم، اين يبني هذا الحكم وفقا لقناعته الشخصية الخاصة،[1] وهنا تحديدا تظهر خصوصية جرائم المساس بأنظمة المعالجة الآلية للمعطيات من حيث تقدير القاضي للأدلة الرقمية وما تطرحه من تحديات تضاف الى باقي التحديات الأخرى ذات الصلة بعقبات التحقيق والاختصاص القضائي للجريمة العابرة للحدود ومتطلبات التعاون الدولي في ذات الإطار.

المطلب الثاني: التحديات الإجرائية في مواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

لم يعد خطـر الجـريمة الماسة بأنظمة المعالجة الآلية للمعطيات وآثارها محصورة في نطاق إقليمي أو زماني معين بذاته، الأمر الذي بات يثير عديد التحديات القانونية والإجرائية أمام الأجهزة المعنية بمكافحة الجريمة بجميع مستوياتها وعلى اختلاف أدوارها، وبالذات فيما يخص العقبات التي تعترض إجراءات جمع الاستدلالات والتحقيق فيها عبر البيئة الافتراضية ؛ لأنها تعد حجر الزاوية الذي سيتم على أساسه بناء الدعوى برمتها، فما يتم جمعه من معلومات وأدلة رقمية عقب ارتكاب الجريمة مباشرة قد لا يبق بعد مرور وقت قصير على ارتكابها بسبب الطبيعة التقنية لهذه الجرائم، ففي كثيرا من الجرائم المعلوماتية لا يترك الجاني ورائه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإعجاب والإحباط معا[2]،يضاف إلى ذلك ملاحقة الجناة وضبط الأدلة خارج الحدود والذي يصطدم بمبدأ السيادة الإقليمية للدول

[1]– عبد الرحمان خلفي، المرجع السابق، ص 475– 476.

[2]– محمد طارق عبد الرؤوف، **جريمة الاحتيال عبر الانترنت الاحكام الموضوعية والاحكام الاجرائية**،ط1، منشورات الحلبي الحقوقية، بيروت، لبنان ، 2011، ص 230.

عملاً بمبدأ إقليمية القانون الجنائي، الأمر الذي يفضي إلى تنازع الاختصاص القضائي بسبب صعوبة تحديد مكان وقوع الجريمة المعلوماتية يضاف إلى ذلك مسالة إثبات هذه الجرائم والإشكالية التي يطرحها الدليل الرقمي كذا إجراءات المسطرة في مجال التعاون الدولي ومن ثَم كان لابدّ من تسليط الضوء بالدراسة على هذه التحديات فيما يخص عقبات إجراءات التحقيق عبر الفضاء المعلوماتي وكذلك تحديد معايير الاختصاص وآلية قبول الدليل الرقمي وصولا إلى إجراءات التعاون الدولي.

الفرع الأول: التحديات الإجرائية ذات الصلة بإجراءات التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات

إن الضبطية القضائية تباشر الاختصاصات والمهام الموكلة إليها في إطار الدور الأساسي الذي تؤديه في صيانة أمن المجتمع وذلك إما بالقيام بدور وقائي يهدف إلى منع ارتكاب الجرائم والحيلولة دون وقوعها وتقليل فرص اقترافها، أو القيام بدور إجرائي في الكشف عن الجرائم وضبط مرتكبيها بعد حدوثها بإتباع مجموعة من الإجراءات تهدف للتأكد أولا من وقوع جريمة يعاقب عليها القانون، ومن ثمة معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكذا معرفة الوسائل التي استعملت في ارتكابها، ويكون ذلك وفقا لمنهج تحقيقي متميز يختلف في الجرائم المعلوماتية عن غيره في الجرائم التقليدية، وبالنظر لما تتميز به هذه الأخيرة من خصوصية جعلت المحققين يصطدمون بعدة تحديات إجرائية بعضها متعلق بشخص المحقق وأخرى متعلقة بطبيعة الجريمة في حد ذاتها.[1]

البند الأول: الصعوبات ذات الصلة بشخص المحقق

يعترض التحقيق في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات جملة من المعوقات والصعوبات التي تؤثر على عملية التحقيق وتؤدي بها إلى الخروج بنتائج عكسية تفقد ثقة المجتمع في أجهزة في أجهزة تنفيذ القانون غير القادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضا على المجرم نفسه حيث يشعر أن الجهات القضائية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق،لا تجاري خبرته وعلمه بالأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من الجرائم التي تكون اشد ضررا على المجتمع،[2] ومن أهم هذه التحديات:

---

[1]– عثمان خرشي، **المرجع السابق**، ص 69.

[2]– محمد بوعمرة، سيد علي بنينال، **جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماستر في قانون الأعمال، كلية الحقوق جامعة البويرة،الجزائر ،السنة الجامعية 2012– 2013، ص 28.

أولا: نقص خبرة القائمين بالتحقيق في هذه الجرائم

أضاف ظهور الجرائم المعلوماتية النابعة من التطور الإلكتروني أعباء جديدة على أجهزة التحقيق الابتدائي لما يتطلبه التصدي لهذه الجرائم من قدرات تقنية لم يألفها رجال الضبطية القضائية ولم يتعودوا عليها، وهوما يستدعي ضرورة توفير المهارات المطلوبة في هذا المجال، والإشكال الأساسي الذي يواجه المحققين ضباط الشرطة القضائيين في جرائم نظم المعالجة الآلية للمعطيات هو خلفية المحقق نفسه فالمتخصصين في الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دوافع الجريمة وجمع الأدلة لتقديم المتهم للمحاكمة، وفي كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول الجريمة الإلكترونية، ولكن يتضح فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى، بينما المحققون ذوي الخلفية القانونية قد تكون لديهم خبرة واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم،[1] كما أن شخصية المحقق لها دور كبير في نجاح التحقيق، فالتخوف من استخدام الكمبيوتر، وعدم الاهتمام بالمستجدات الحاصلة في المجال المعلوماتي أو نقص المعرفة بمتطلبات أمن المعلومات أو نقص المهارات الفنية المطلوبة للتحقيق في الجرائم المعلوماتية، وعدم فهم المصطلحات الخاصة بالمجال الرقمي قد يؤدي إلى فشل التحقيق.[2]

ثانيا: ارتفاع تكاليف وأعباء التكوين

إن التحقيق في هذه الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يحتاج إلى خبراء متخصصين في المجال التقني ،وهؤلاء يحتاجون إلى دورات تكوينية مستمرة ومتزامنة مع تطور التقنية الإلكترونية، وهذا الأمر مرتبط بتخصيص أعباء مالية وتكاليف باهظة قد ترهق خزينة الدولة، وكذلك الأمر بالنسبة لعملية البحث وضبط الأدلة التي تحتاج إلى فحص آلاف الصفحات خصوصا عندما لا تثبت تلك الصفحات شيئا[3] وكل ذلك يتطلب تخصيص موارد مالية قد لا تستطيع الدولة توفيرها في كل الحالات.

البند الثاني: صعوبات تتعلق بطبيعة الجريمة والجهات المتضررة منها

نميز هنا بين الصعوبات التي تعرض التحقيق من حيث الطبيعة الخاصة للجريمة الماسة بأنظمة المعالجة الآلية للمعطيات باعتبارها جريمة معلوماتية والدور التي تلعبه الجهات المتضررة من الجريمة في إعاقته التحقيق.

---

[1]– نعيم سعيداني، **المرجع السابق**، ص 115.

[2]– محمد بوعمرة، سيد علي بنينال، **المرجع السابق**، ص 30.

[3]– يوسف جفال، **التحقيق في الجريمة الإلكترونية**، مذكرة ماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولاي الطاهر، سعيدة،الجزائر ، السنة الجامعية 2016–2017، ص 42، 43.

أولا: الصعوبات المتعلقة بطبيعة الجريمة

من أهم المعوقات والتحديات التي تواجه التحقيق خصوصية الجريمة المرتكبة في العالم الافتراضي ومن أبرز هذه الصعوبات نذكر:

- خفاء الجريمة وغياب الدليل المرئي وصعوبة التعرف عليه.
- الإعاقات المتعلقة بالوصول إلى الدليل لإحاطته بوسائل الحماية الفنية.
- سهولة محو الدليل أو تدميره في زمن قصير جدا.
- صفات الجاني الذي يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدا بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعمل بها فإنه يستهدف بالمحو السريع عدم استطاعة السلطات إقامة الدليل ضده، وبالتالي تملصه من مسؤولية هذا الفعل وإرجاعه إلى خطأ نظام الحاسوب الآلي أو الشبكة أوفي الأجهزة.

ثانيا: الصعوبات المتعلقة بالجهات المتضررة من الجريمة

من بين الصعوبات التي تعرض التحقيق في هذا النوع الخاص من الجرائم هو عدم إدراك خطورة الجريمة من قبل المسؤولين بالمؤسسات المجني عليها، وكذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة الجرائم المتعلقة بالأنظمة، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، وهذا يؤدي إلى الإحجام عن الإبلاغ عن الجريمة التي تعتبر من أهم وأخطر الإشكالات التي تتعلق بعملية الإبلاغ عن الجريمة الإلكترونية، حيث يحجم البعض عن إبلاغ السلطات المختصة بالجرائم التي ارتكبت بحقهم خاصة وإذا تعلق الأمر بالمؤسسات المالية أو ما شابهها.[1]

ومن أهم أسباب الامتناع عن التبليغ عند التعرض للجريمة قد يعود إلى الجهل بالقانون وعدم معرفة الضحية بالإجراءات التي يمكنه إتباعها في حالة تعرض النظام للمساس كعدم معرفته الجهة التي يلجأ لها للتبليغ وكيفية التبليغ، وكذا تخوف المؤسسات التجارية من استغراق التحقيق لفترة زمنية طويلة، مع احتمالية احتفاظ جهات التحقيق بأجهزة الحاسب مما يؤثر على حسن سير العمل بتلك الشركات والمؤسسات، بضاف الى ذلك صعوبة تحديد نطاق الضحايا بسبب أنهم في اغلب الأحيان لا يعلمون شيئا عن الجريمة إلا بعد وقوع الفعل وفي هذه الحالة يرون من الحكمة عدم الإبلاغ عنها، كما لا يحبذ أكثرهم أن يعترف بأن نظامه المعلوماتي قد وقع ضده اعتداء، وهذا السلوك السلبي يعتبر مغريا لمرتكبي الجرائم للاستمرار في أنشطتهم[2]

[1]– يوسف جفال، المرجع السابق، ص 43– 44.

[2]–رجاء أومدور ، **المرجع السابق**، ص 36.

الفرع الثاني: التحديات الإجرائية ذات الصلة بالاختصاص القضائي في جرائم المساس بأنظمة المعالجة الآلية للمعطيات

أحدث التطور التكنولوجي المعلوماتي مسؤولية كبيرة على عاتق المشرع الجزائي لمواجهة الجرائم المعلوماتية بمختلف أنواعها، وسد كل الفراغات التشريعية بما فيها مسألة الاختصاص القضائي، التي أثارت عدة صعوبات قانونية منها التنازع الإيجابي للاختصاص القضائي ذلك أن القواعد التقليدية التي تحدد معايير الاختصاص لا يتلاءم تطبيقها مع طبيعة هذا النوع من الجرائم ذات الطابع المعلوماتي،[1] ويرجع ذلك إلى صعوبة تحديد مكان وقوع الفعل الإجرامي، فهي جرائم عابرة للحدود تتم في فضاء الكتروني معقد، لذا سنتناول المبادئ العامة للاختصاص القضائي الدولي في مجال مكافحة الجريمة العابرة للحدود، موقف المشرع الجزائري بشأن الاختصاص القضائي الإقليمي والدولي .

البند الأول: المبادئ العامة للاختصاص القضائي الدولي في مكافحة الجريمة

يقصد بالاختصاص السلطة التي يقرها القانون للقضاء بان ينظر في دعاوى من نوع معين،[2] كما انه ذلك النطاق الذي يحدده المشرع والذي تمارس فيه الجهة القضائية ولايتها القضائية وتبسط سلطتها بحيث يعتبر هذا النطاق حدا مانعا للجهات القضائية الأخرى،[3] ويكون النطاق إما محليا بتحديد الحيز المكاني أو نوعيا من حيث تحديد نوع القضايا التي يحق لها نظرها وللمعطيات البت فيها وفقا للقواعد التي رسمها القانون والحدود التي تبناها المشرع لهذه السلطات أثناء ممارسة مهامها.

غير أن اختلاف النظم القانونية،وتباين التشريعات في مكافحة جرائم نظام المعالجة الآلية للمعطيات نجم عنه تنازع في الاختصاص القضائي الدولي، فيؤدي تارة إلى تنازع إيجابي في الاختصاص القضائي بين محاكم أكثر من دولة لملاحقة نفس الجرم، وتارة أخرى يؤدي إلى تنازع سلبي في الاختصاص القضائي بأن تمتنع أي دولة من الدول المعنية بملاحقة الجاني، وهذا النوع الأخير من التنازع نادر الوقوع.[4]

وتعد مسألة تنازع الاختصاص القضائي من أكبر التحديات التي تواجهها عملية التصدي لجرائم نظام المعالجة الآلية للمعطيات، بالنظر لما تتميز به هذه الجرائم من طابعها المتعدي لحدود الدولة الواحدة، واتسامها بالطابع الدولي، بالإضافة إلى تجرد السلوك الإجرامي فيها من الطابع المادي لارتباطه بالعالم

---

[1]– Myriam Quéméner. Cybercriminalité. Droit pénal appliqué éd. Economica. Paris.2010. p157.

[3]– محمود نجيب حسني، **شرح قانون الإجراءات الجزائية** ، دار النهضة العربية، مصر، 2002، ص 132 .

[3]– مريم عراب،"" ***الاختصاص القضائي في الجرائم المعلوماتية***"، مجلة annales de facute de droit، كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد وهران، الجزائر، م7، ع3، ديسمبر2015، ص 276.

[4]– البركه الطيبي ، المرجع السابق ، ص 313.

الافتراضي أو الرقمي مما يجعلها ترتبط بأكثر من ولاية قضائية ويجتمع فيها أكثر من معيار واحد من معايير إسناد الاختصاص، ويؤدي إلى تنازع إيجابي في الاختصاص بين جهات قضائية عدة، كما ان الطبيعة الخاصة للجرائم المستحدثة تقتضي تجاوز المعايير التقليدية، لعدم ملائمة تطبيق القواعد لكلاسيكية لاسيما تحديد محل وقوع الجرم في العالم الرقمي، لذلك ذهب غالبية الفقهاء لحل مشكلة الاختصاص القضائي في العالم الافتراضي، إلى تطبيق مبادئ القانون الدولي المعمول بها فيما يخص الاختصاص الجزائي الدولي المطبق على الجرائم التقليدية وعلى رأسها مبدأ إقليمية القوانين،[1] حيث يطبق قانون الدولة على كل جريمة ترتكب على إقليمها، سواء أكان الجاني يحمل جنسية هذه الدولة أم يحمل جنسية دولة أجنبية، وسواء أكان المجني عليه مواطنا أم أجنبيا، ويجب التنويه بأن المحكمة المختصة وكذا سلطة التحقيق المختصة وفقا لمبدأ الإقليمية الذي يسود معظم التشريعات المقارنة هي محكمة المكان الذي وقعت فيه الجريمة، أي المكان الذي وقع فيه الركن المادي، وبالرغم من أن مبدأ الإقليمية هو المبدأ المهيمن عند تنازع الاختصاص القضائي الدولي، إلا أنه يثير عدة صعوبات تتعلق بتحديد معيار الاختصاص المكاني في جرائم نظام المعالجة الآلية للمعطيات، والتي لا يقتصر نطاقها على المستوى المحلي أو القومي، بل يمتد ليشمل المستوى الإقليمي والدولي، بحيث يقع بذلك جزء من النشاط أو الركن المادي في إقليم دولة معينة بينما تقع النتيجة في إقليم دولة أخرى، فتزعم كل من الدولتين اختصاصها استنادا إلى المبرر القانوني الخاص بها. وأصبح لمبدأ الإقليمية مفهوما واسعا فيما يتعلق بتحديد مكان وقوع هذه الجرائم ولم يعد يلازم وقوع الفعل المادي أو أحد العناصر المكونة له مثلما هو معروف في السابق، بل بلغ الأمر حد نزع الصفة اللامادية كلية من هذا الفعل، نظرا لارتباط هذه الجرائم بالعالم الافتراضي وكون تقنيات ارتكابها لا تترك أية آثار محسوسة.[2]

الأمر الذي عزز لاعتماد معايير أخرى تحكم الاختصاص الدولي كانت فيما مضى تعد احتياطية كمعيار العينية،[3] ومعيار الشخصية،[4] والعالمية،[1] ولم يعود هناك مانعا من تطبيق هذه المبادئ على سائر

---

[1]- هلالي عبد الله أحمد، المرجع السابق، ص 160.

[2]- البركه الطيبي، المرجع السابق، ص 314.

[3]- يقصد بمبدأ العينية تطبيق القانون الجزائي على الجرائم التي تمس المصالح الأساسية للدولة، والمرتكبة خارج إقليمها أيا كانت جنسية مرتكبها، وهذا المبدأ يفرضه حرص الدولة على حماية مصالحها الأساسية نقلا عن: مريم عراب، المرجع السابق ص 279.

[4]- يقصد بمبدأ الشخصية ملاحقة القانون الوطن الأشخاص الذين يحملون جنسية الدولة أينما وجدوا ليحكم أفعالهم الإجرامية المرتكبة بالخارج، ويطبق مبدأ الشخصية بطريقتين: إيجابية وسلبية، ويقصد بالطريقة الإيجابية تطبيق القانون الجزائي على مرتكب الجريمة الذي يحمل جنسية الدولة ولو ارتكبت الجريمة خارج إقليمها وهذا لتجنب فرار المجرم الذي يسيء إلى سمعة دولته، أما الطريقة السلبية فيقصد بها تطبيق القانون الجزائي على كل جريمة يكون المجني عليه حاملا لجنسية الدولة، ولو

الجرائم المعلوماتية المرتكبة، لأن القواعد الإجرائية الجزائية يمكن تفسيرها تفسيرا موسعا إضافة إلى إمكانية اللجوء إلى القياس عند فقدان النص الإجرائي وذلك بخلاف القواعد الموضوعية.

وبالتالي للتغلب على التنازع الإيجابي للاختصاص، يمكن لأي من الدول المتنازعة تطبيق أحد معايير الاختصاص الأكثر فعالية لضمان ملاحقة الجريمة، ويبدو أن مبدأ الإقليمية هو الأكثر قبولا، فالدولة التي في إقليمها تقع الجريمة كلها أو الجزء الأكبر من النشاط المكون لركنها المادي أو النشاط التبعي كله أو بصفة عامة الدولة التي في إقليمها توجد متحصلات الجريمة، تبدو أرجح الدول اختصاصا بملاحقة الجريمة ومحاكمة فاعلها ولا يجد هذا الحل مبررا فقط في اعتبارات السيادة الوطنية اللصيقة بمبدأ الإقليمية، وإنما أيضا في جدواه العملية حيث أنه أين تقع الجريمة كلها أوجلها، تصبح أدلة الإثبات متوافرة ويصبح من السهل إجراء التحقيقات الكفيلة لإظهار الحقيقة، ثم يأتي من بعد مبدأ الإقليمية، مبدأ العالمية، حيث يكون هو الملائم لمعظم الجرائم الإلكترونية التي يتوزع النشاط المكون للركن المادي لها في أكثر من دولة، ثم يأتي مبدأ الشخصية في شقه الإيجابي، بحيث ينعقد الاختصاص للدولة التي يحمل جنسيتها مرتكب هذه الجريمة فإن تعددت جنسياته.

البند الثاني: موقف المشرع الجزائري من مسالة الاختصاص الدولي والمحلي

منح المشرع الجزائري من خلال أحكام القانون09-04 السابق الذكر للمحاكم الجزائية الجزائرية وبصفة استثنائية اختصاص النظر في الجرائم المعلوماتية المرتكبة خارج الإقليم الوطني الجزائري عندما يكون مرتكبها أجنبي وتستهدف اعتداءاتها مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المساس المصالح الإستراتيجية للاقتصاد الوطني، ويكون بذلك ضيق من نطاق الاختصاص سواء كان نوعيا أو محليا لهذه المحاكم بالنسبة للجرائم المرتكبة خارج الحدود الإقليمية، أما بالنسبة للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات المرتكبة محليا فيتحدد الاختصاص فيها إقليميا وفقا للأحكام العامة المنصوص عليها بقانون الإجراءات الجزائية الجزائري،[2] وهذا إما بمكان وقوع الجريمة أو بمحل إقامة أحد المتهمين أو شركائهم أو محل القبض عليهم ، مع جوازية تمديد الاختصاص المحلي ليشمل اختصاص محاكم أخرى فيما يخص بعض الجرائم من ذلك جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وأنشئت في ذات الإطار أقطاب

ارتكبت الجريمة خارج إقليمها، وأيا كانت جنسية الجاني وهذا لضمان حماية رعايا الدولة من الاعتداءات الجرمية عليهم. نقلا عن: مريم عراب، المرجع السابق، ص 279- 280.

[1]- ينطوي هذا المبدأ على نوع من التعاون الدولي في مكافحة الإجرام، فهو يضمن عدم إفلات المجرمين الذين سولت لهم أنفسهم ارتكاب الجرائم في دولة ما، ثم الفرار إلى دولة أخرى تملصا من المسؤولية، وعليه فالأجنبي الذي يرتكب جريمة في دولة ويلقى القبض عليه في دولة أخرى، يمكن محاكمته في الدولة التي ألقي القبض عليه فيها بشرط أن لا تطلب الدولة التي أرتكب فيها الجرم تسليمه لها. نقلا عن: مريم عراب، المرجع السابق، ص 280.

[2]- يراجع في ذلك أحكام المادة 329 من ق.الإ.ج .م .م

قضائية جزائية متخصصة من خلال المرسوم التنفيذي رقم 06-348 تنظر في هذا النوع من الجرائم بغية وضع إطار إجرائي متماسك يمكنه التحقيق والفصل في هذا النوع من هذا الجرائم بكل احترافية، إضافة الى ذلك أحدث المشرع الجزائري من خلال الأمر رقم 20-04 المعدل و المتمم لقانون الإجراءات الجزائية الجزائري قطب جزائي ذو اختصاص وطني موسع، على مستوى محكمة مقر مجلس قضاء الجزائر متخصص في متابعة القضايا التي لها علاقة بالجريمة الاقتصادية والمالية وقضايا الجرائم المرتبطة بها من ذلك جرائم المساس بأنظمة المعالجة الآلية للمعطيات، وكذا الجرائم الاقتصادية والمالية الأكثر تعقيدا، حيث يتمتع هذا القطب باختصاص موسع يمتد إلى كامل الإقليم الوطني الجزائري.[1]

ورغم كل ما سبق ذكره تبقى مسالة الاختصاص تثير الكثير من الجدل فما يخص العلاقة التدريجية بين مختلف السلطات القضائية المختصة لاسيما في مجال التحري والتحقيق عن الجرائم المعلوماتية ومن ذلك:

- عدم إخطار النائب العام لدى الجهة القضائية المختصة إقليميا والنائب العام لدى الجهة القضائية ذات الاختصاص الإقليمي الموسع في التحقيق، وإبقائهما بعيدان عن تطوراته يؤثر على حقهما في المطالبة بالملف في الوقت المناسب.[2]
- تقليص الدور الذي يؤديه النائب العام لدى الجهة القضائية العادية في العلاقة الجديدة التي تنشأ بين وكيل الجمهورية لدى الجهة القضائية العادية ووكيل الجمهورية لدى الجهة القضائية المتخصصة عند مطالبة هذا الأخير بملف الإجراءات إثر التخلي لصالح القطب.[3]
- انتماء وكيل الجمهورية التابع للجهة القضائية المتخصصة ووكيل الجمهورية التابع للجهة القضائية العادية إلى مجلسين مختلفين، قد يؤدي إلى إثارة تنازع بين النائب العام لدى الجهة القضائية المتخصصة والنائب العام لدى الجهة القضائية العادية مما يستوجب إخطار المصالح المركزية بوزارة العدل للتدخل لحل الإشكال و هذا الأمر الذي يستغرق الوقت[4].
- الإشكال المثار في حال رفض قاضي تحقيق لدى القطب إجراء التحقيق أو التصريح بعدم اختصاصه، حين يرى أن الطلب جاء سابقا لأوانه لعدم اتضاح معالم الجريمة، وهل تأخذ وصف الجنحة أو وصف الجناية أين قد يتغير تكيفها من جريمة معلوماتية إلى جريمة اقتصادية ومالية أكثر تعقيدا، هذه الأخيرة تدخل في اختصاص القطب الجزائي الوطني المتخصص ، الموجود بمحكمة مقر مجلس قضاء الجزائر العاصمة

[1]- تم التطرق اليه تفصيلا ضمن المطلب الثاني المبحث السابق من اجهزة الحماية القضائية.

[2]- لحسن ناني، **المرجع السابق**، ص 61.

[3]- عثمان خرشي، **المرجع السابق**، ص 199 .

[4]- لحسن ناني، **المرجع السابق**، ص 63.

حيث يمارس فيه كل من رئيس القطب ووكيل الجمهورية وقاضي التحقيق التابعين له صلاحياتهم في كامل الإقليم الوطني.[1]

الفرع الثالث: التحديات الإجرائية ذات الصلة بتقدير الدليل الرقمي

يصدر القاضي الجنائي حكمه في الدعوى المعروضة عليه تبعا لاقتناعه الشخصي ويبني حكمه على أي دليل يراه ملائم ومنتج في الدعوى،[2] ويلعب القاضي الجزائي دورا ايجابي في توفير وتقدير الأدلة عكس القاضي المدني الذي يكتفي بما يقدمه الخصوم من أدلة حيث يمكن للقاضي الجزائي بناءا على طلبات الأطراف أومن تلقاء نفسه أن يتحرى وينقب عن الحقيقة باتخاذ أي إجراء من الإجراءات الذي يراها مناسبة لاستكمال قناعته الشخصية،[3] فالقاضي الجزائي يستعين بكل الوسائل التي تترجم أمامه تفاصيل الجريمة هذه الوسائل هي ما يعرف بوسائل الإثبات وبطبيعة الحال فان الجرائم الماسة بالمعالجة الآلية باعتبارها من الجرائم المعلوماتية تخضع لنوع معين من وسائل الإثبات وهو ما يعرف بالدليل الرقمي.

البند الأول: مفهوم الدليل الرقمي

بعرف الدليل الرقمي بأنه ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصالات من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميا أو تفسيريا في شكل نصوص مكتوبة، أو رسومات أو صور وأشكال وأصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها،[4] وهو أيضا الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات ونبضات مغناطيسية أو كهربائية، من الممكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة في شكل صور أو تسجيلات صوتية أو مرئية، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء،[5] وقيل انه الدليل الذي يحتاج إلى معالج رقمي لقراءته أوفهم محتواه،[6] من التعاريف السابقة بمكن القول أن الدليل الرقمي هو دليل علمي يحتوي على بيانات ومعلومات رقمية مستمدة من الأجهزة

---

[1]– عثمان خرشي، **المرجع السابق**، ص 200.

[2]– يراجع المادة 212 من ق.الإ.ج .ج .م .م

[3]– رشيدة بوكر، المرجع السابق، ص 485.

[4]– حسين طاهيري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية**، دار العلا للطباعة والنشر، أم البواقي 2023، ص ، نقلا عن: عبد الناصر محمد محمود فررلي، محمد عبيد اسيا سعيد المسماري، **الاثبات الجنائي بالأدلة الرقمية**، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايا للعلوم الأمنية، الرياض، السعودية، 2007 ص 13.

[5]– ممدوح عبد الحميد عبد المطلب، **البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت**، دار الكتب القانونية مصر، 2006، ص 77.

[6] -Lazetik G B, Koshevaliska O, Digital Evidence in Criminal Procedures(A comparative approach), Balkan Social Science Review, 2 (1), 2013, p16

الالكترونية وشبكات الاتصال، تكون في شكل نبضات مغناطسية أو كهربائية، تقبل القراءة والتحليل ويمكن تقديمها للقضاء كدليل لإثبات الجريمة ،ونشير هنا إلى أن الدليل الالكتروني يتميز بالنظر إلى البيئة الرقمية التي ينشأ فيها بمجموعة من الخصائص التي تميزه عن الدليل المادي التقليدي ويمكن حصرها في النقاط التالية:

أولا: الدليل الالكتروني دليل علمي

يتكون الدليل الكتروني من بيانات ومعلومات غير ملموسة ولا تدرك بالحواس العادية، بل يتطلب

لإدركها الاستعانة بالبرامج والوسائل الخاصة بذلك،[1] ويحتاج إلى مجال علمي يتعامل مع، فلا يخرج عما توصل إلي العلم الرقمي وإلا فقد معناه.[2]

ثانيا: الدليل الرقمي من طبيعة تقنية

إن الطبيعة التقنية للدليل تقتضي أن يكون هناك توافق بين الدليل، وبين البيئة التي نشأ فيها فهذه التقنية هي نبضات رقمية تكمن قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشمل الحاسوب على أية شاكلة يكون عليها.[3]

ثالثا: سهولة التخلص من الدليل الالكتروني

ان سهولة التخلص من الدليل تعد من أهم خصائص الدليل الالكتروني التي يتميز بها عن غيره من الأدلة التقليدية ، و لكن بالرغم من ذلك قد تتيح تقنية المعلومات استرجاع الأدلة و البيانات بعد محوها أو إتلافها باستعمال برامج حاسوبية متطورة ، سواء كانت هذه البيانات صورا أو رسوما أو كتابات ...إلخ.

رابعا: القابلية للنسخ

تتيح التقنية المعلوماتية استخراج نسخ من الأدلة الجنائية الرقمية مطابقة لأصل ولها القيمة العلمية نفسها، وهذه الخاصية لا تتوفر في الأدلة الجنائية التقليدية، مما يشكل ضمانة فعالة لعدم إتلاف الدليل أو فقده ، حيث يمكن نسخ البيانات على دعامة الكترونية تمهيدا لحجزها و تقديمها أمام القضاء،[4] حيث أجاز

---

[1]– عائشة بن قارة مصطفى، **حجية الدليل الإلكتروني في مجال الاثبات الجنائي في القانون الجزائري والمقارن**،ط1، دار الجامعة الجديدة، الإسكندرية، مصر، 2010، ص 62.

[2]– بحرية هارون، ***"دور الدليل الرقمي في أثبات الجريمة المعلوماتية في التشريع الجزائري"***، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة، كلية الحقوق جامعة محمد خيضر بسكرة، الجزائر، يومي 16-17 نوفمبر 2015، ص 62.

[3]– خالد ممدوح إبراهيم، **المرجع السابق**، ص 185.

[4]– يزيد بوحليط، **المرجع السابق**، ص 403.

المشرع الجزائري نسخ و إفراغ المعطيات على دعامة تخزين الكترونية تكون قابلة للحجز مثل القرص الصلب أو المضغوط أو الذاكرة الوميضية ... إلخ.[1]

البند الثاني: شروط صحة الدليل الالكتروني

إن الاحتكام إلى الدليل الرقمي كدليل من أدلة الإثبات الجنائي يهدف لتأكيد ارتكاب المتهم للجرم المنسوب إليه وإدانته على ذلك، لذا يجب من توافر شروط تجعله ذي قيمة ومحل ثقة، وأساسا يعتمد على لإصدار تلك الأحكام ومن تلك الشروط ما يلي:

أولا: أن يكون الدليل الالكتروني متحصلا بطريقة مشروعة

يقصد بالشرعية عدم مخالفة الأحكام التي تهدف إلى صيانة كرامة الإنسان وحماية حقوق، لذلك تتضمن الدساتير الحديثة قواعد أساسية تضبط مسائل التفتي والتوقيف والحجز والحبس وغيرها، بحيث يتقيد بها المشرع عند وضع قانون الإجراءات الجزائية، فكل دليل مستمد بصفة مخالفة لهذه الأحكام يعتبر باطلا بطلانا مطلقا.[2]

ثانيا: أن يكون الدليل الالكتروني ذا علاقة بموضوع الجريمة المعلوماتية

العلاقة بين الدليل الرقمي و محل الجريمة هو ما يشكل العلاقة الكاشفة، حيث يجب أن تكون هناك علاقة ما بين الدليل وما بين الواقعة محل الدعوى، وهو مبدأ لا يتحقق إلا بتحقيق شرط آخر، وهو مطابقة الدليل المعلوماتي المستخرج من الحاسوب مع المخزن بداخله.[3]

ثالثا: أن يكون الدليل الإلكتروني يقيني غير قابل للشك

يشترط في الأدلة الإلكترونية أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة بموجبها، ذلك أن لا مجال لدحض قرينة البراءة و إفتراض عكسها، إلا عندما يصل القاضي إلى درجة من القناعة تتسم بالجزم واليقين.[4]

---

[1]– يراجع في ذلك نص المادة 06 من قانون 04-09 السالف الذكر.

[2]– حسين ريعي، **البحث والتحقيق في الجرائم المعلوماتية**، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، 2015-2016، ص 265.

[3]– حسين ريعي، **المرجع نفسه**، ص 265.

[4]– سامية بلجراف، **سلطة القاضي الجنائي في قبول و تقدير الدليل الرقمي**، بحث مقدم إلى أعمال الملتقى الوطني حول- الجريمة المعلوماتية بين الوقاية و المكافحة، كلية الحقوق والعلوم السياسية، جامعة بسكرة، يومي 16-17 نوفمبر 2015، ص 09.

البند الثالث: ضمانات حرية القاضي في الأخذ بالدليل الرقمي

بالرغم من الحرية الكبيرة التي يتمتع بها القاضي في نظام الإثبات، إلا أن هذه الحرية ليست مطلقة بل وضع المشرع لها ضوابط وهي بمثابة صمام أمام إنحراف القاضي عند ممارسته لها كي لا تختل الأحكام ولا يحيد هذا الأخير ، إذ يلتزم بتسبيب الأحكام التي يصدرها،[1] في هذا الشأن يكون اقتناع القاضي بالأدلة التقنية المقدمة له مرهون بعديد الضوابط من ذلك الضابط المتعلق بشروط قبول الدليل الإلكتروني حيث لا يكون القاضي حرا في تقدير أي دليل كان بل هو حر فقط في تقدير الدليل الإلكتروني المقبول في الدعوى، بمعنى الدليل المحصل بطريقة مشروعة، إعمالا لمبدأ الشرعية الإجرائية، وبالتالي تستبعد سائر الأدلة الرقمية غير المقبولة ، لأنها لا تدخل ضمن عناصر تقديره،[2] والشرط الثاني يتعلق بوضعية الدليل الإلكتروني في حد ذاته حيث لا يجوز للقاضي أن يبني حكم على أدلة لم تطرح لمناقشة الخصوم في الجلسة، وبمقتضى ذلك يكون للدليل أصل ثابت في أوراق الدعوى وأن يتاح للخصوم فرصة الاطلاع عليه ومناقشته،3 أما عن الضوابط المتعلقة بالاقتناع الشخصي للقاضي فان مبدأ الإثبات الجنائي يتيح حرية كبيرة للقاضي في تقدير عناصر الإثبات بما في ذلك الأدلة الرقمية، و عليه فإن تقدير كفاية أو عدم كفاية الدليل الإلكتروني في إثبات الجريمة المعلوماتية ونسبتها إلى مرتكبيها أمر متروك لمحكمة الموضوع المعروض عليها الدليل، ولا تخضع في ذلك لرقابة المحكمة الناظرة في الطعن بالنقض التي يقتصر دورها على مراقبة المنطق القضائي لمحكمة الموضوع عن طريق رقابتها على صحة تسبيب الحكم.[4]

وفي سبيل بلوغ القاضي درجة الاقتناع التام للفصل في القضية، يجب ان تتوفر الشرطين التالين:

أولا- بلوغ الاقتناع القضائي درجة اليقين: تقتضي العدالة أن يصدر القاضي حكم عن اقتناع يقيني بصحة ما ينتهي إلي من وقائع لا مجرد الظن والاحتمال.

ثانيا-توافق الاقتناع مع مقتضيات العقل والمنطق: ومعنى ذلك أن يكون استخلاص محكمة الموضوع لوقائع الدعوى استخلاصا معقولا، من غير تعسف في الاستنتاج ولا تعارض مع مقتضيات العقل والمنطق.[5]

---

[1]- فاضل زيدان محمد، **سلطة القاضي الجنائي في تقدير الأدلة**، ط1، دار الثقافة للنشر والتوزيع،عمان ، الأردن، 2006 ص 232.

[2]- عائشة بن قارة مصطفى، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن** ،المرجع السابق، ص 269.

[3]- رشيدة بوكر، المرجع السابق، ص 508.

[4]- عائشة بن قارة مصطفى، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن** ، المرجع نفسه، ص 206.

[5]- فوزي عمارة، **المرجع السابق**، ص 78.

الفرع الرابع: التحديات ذات الصلة بالتعاون الدولي لمكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات

في إطار التصدي للجريمة العابرة للحدود، قامت مختلف دول العالم بما فيها الجزائر بالتعاون فيما بينها، من أجل التصدي لهذه الجرائم لاسيما تلك التي ترتكب في البيئة الافتراضية، وذلك باتخاذ إجراءات واستراتيجيات، فيما بينها لإنجاح ذلك الهدف، حيث أضحى التعاون الدولي في مكافحة الجرائم المعلوماتية ضرورة حتمية، ويتخذ هذا الأخير صورا عديدة منها المساعدة القضائية في مجال الإنابات القضائية الدولية وتبادل المعلومات يضاف إلى ذلك آلية تسليم المجرمين، رغم ذلك فان الدور الحيوي الذي يؤديه التعاون الدولي لا يخلو من تحديات ومعوقات تحول في غالب الأحيان من تحقيق الأهداف المرجوة منه،[1] وعلى العموم سنحاول إبراز أهم صور التعاون الدولي التي اعتمدها المشرع الجزائري والتحديات التي تواجهها.

البند الأول: المساعدة القضائية الدولية وتحدياتها

اكتست المساعدة القضائية الدولية المتبادلة أهمية كبيرة في مجال مكافحة جرائم نظام المعالجة الآلية للمعطيات باعتبارها الصورة الحقة للجرائم العابرة للحدود الدولية، وللمساعدة القضائية صور عديدة من أهمها:

أولا- الإنابة القضائية الدولية :

وهي طلب القيام بإجراء قضائي من إجراءات الدعوى الجزائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب منها ذلك الإجراء للفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها،[2] والأصل بالنسبة لطلبات الإنابة القضائية التي تعد من أهم صور المساعدة القضائية الدولية في المجال الجنائي أن تسلم عن طريق الدبلوماسية وهذا ما يجعلها تتسم بالبطء والتعقيد، إضافة إلى التباطؤ في الرد من طرف الدولة متلقية الطلب بسبب الصعوبات اللغوية أو الفوارق في الإجراءات التي تعقد الاستجابة للطلب،[3] هذا وقد تبنها المشرع الجزائري ضمن أحكام المادتين 16 و17 من قانون 09-04 بقولها: "تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل".[4]

---

[1]- عبد الفتاح بيومي حجازي، **الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجريمة المعلوماتية**، ط01، دار المعارف الإسكندرية ، مصر، 2009، ص 103.

[2]- بن محمد محمد،" **تنازع الاختصاص في الجرائم الالكترونية** "،مجلة الحقوق والعلوم السياسية، ، جامعة قاصدي مرباح ورقلة ، الجزائر ، ع02، 2010، ص 156.

[3]- خراشي إبراهيم عادل، **المرجع السابق**، ص 63.

[4]- المادة 17 القانون رقم 09-04 السالف الذكر .

ثانيا- تبادل المعلومات :

يشمل التبادل تقديم المعلومات والوثائق التي تطلبها سلطة قضائية أجنبية من سلطة أخرى عن الاتهامات التي وجهت إلى رعاياها في الخارج، والإجراءات التي اتخذت ضدهم، من ذلك الطلبات المتعلقة بصحيفة السوابق القضائية للمتهمين، قصد التعرف على الماضي الجزائي للشخص المحال على الجهات القضائية، والتي تساعد في تشديد العقوبة في حالة العود أوفي وقف تنفيذها، ولا يتم ذلك الا في إطار اتفاق ثنائي للدولتين،[1] ومن بين تلك الاتفاقيات الاتفاقية التي أبرمتها الجزائر مع اسبانيا، وقد جاء نص المادة 15 منها على ما يلي: *"تتبادل وزارتي العدل للطرفين بيانات عن الأحكام المقيدة في صحيفة السوابق القضائية والصادرة عن الجهات القضائية لكل منها ضد رعايا الدولة الأخرى والأشخاص المولودين في إقليمها وفي حالة المتابعة أمام جهة قضائية تابعة لحد الطرفين المتعاقدين يمكن للسلطة القضائية المختصة أن تحصل من السلطات المختصة للطرف الآخر على صحيفة السوابق القضائية الخاصة بالشخص محل المتابعة".*[2]

ثالثا: المساعدة القضائية المتبادلة في مجال الإجراءات الوقتية والعاجلة

تتميز لإجراءات الكلاسيكية في مجال تبادل المعلومات ونقل الإجراءات في إطار المساعدة القضائية الدولية بنوع من البطء والتعقيد الذي لا يتناسب مع طبيعة هذه الجرائم لذا كان من الواجب استحداث وسائل أكثر سرعة وفاعلية لمكافحة جرائم نظام المعالجة الآلية للمعطيات، قصد التمكن من الحصول على الأدلة والمعلومات بصورة عاجلة، وهو ما تضمنته الاتفاقيات الخاصة بالجرائم المعلوماتية لاسيما اتفاقية بودابست والاتفاقية العربية لمكافحة جرائم تقنية المعلومات،[3] من خلال استحداثها لبعض صور التعاون القضائي التي تتناسب مع طبيعة هذه الجرائم من ذلك:

- **التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي** : وهو عبارة عن إجراء ذو طبيعة وقتية للتدخل بطريقة أكثر سرعة دون المساس بسرية المعلومات والبيانات محل الإجراء الوقتي موضوع الطلب فلا يتم كشفها ولا فحصها من قبل سلطات إنفاذ القانون إلا في بعض الحالات ووفقا للشروط المقررة قانونا بما يكفله حق الشخص المعني بالخصوصية في سرية معلوماته، وهو أمر ضروري تستلزمه طبيعة الأدلة في جرائم نظام المعالجة الآلية للمعطيات، وذلك لتفادي إي تغيير في هذه الأدلة أو نقلها أو إتلافها أو محو آثار الجريمة خلال تلك المدة التي تستغرقها إجراءات طلب المساعدة المتبادلة للحصول على تلك البيانات بالطرق التقليدية.

---

[1]- طارق ابراهيم الدسوقي عطية، **المرجع السابق**، ص 598.

[2]- المرسوم الرئاسي رقم 04-23، الصادر في 2004/02/07، المتضمن التصديق على الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا الموقعة بمدريد في 2002/10/07، ج.ر 08 ، المؤرخة في 2004/02/08، المادة 15.

[3]- البركه الطيبي، **المرجع السابق**، ص 133.

- **الإفشاء العاجل لسرية بيانات المرور** :عندما يقوم الطرف المقدم إليه الطلب بتنفيذ ما طلب منه بالتحفظ على بيانات المرور فيكتشف أثناء ذلك أن هذه البيانات ارسلت من خلال مزود خدمات في إقليم دولة ثالثة أو حتى في إقليم الدولة مقدمة الطلب، ففي هذه الحالة يجب الكشف للدولة الطالبة عن خط سير هذه البيانات والمسار الذي سلكه الاتصال، حتى تتمكن الدولة الطالبة من خلال هذه المساعدة معرفة الدولة التي تقدم إليها طلب المساعدة العاجلة بشأن التحفظ على البيانات والمعلومات المخزنة في النظام المعلوماتي، وبالتالي يتم الوصول إلى المصدر الحقيقي للاتصال.

رابعا: المساعدة القضائية المتبادلة في مجال سلطات التحقيق

يمكن لسلطات التحقيق تبادل المساعدة القضائية الدولية في عدة مجالات تشمل المساعدة المتبادلة بالولوج إلى البيانات المعلوماتية المخزنة في النظم المعلوماتية حيث بمقدور كل طرف أن يطلب من الطرف الآخر أن يفتش أو أن يقوم بالولوج إلى البيانات المعلوماتية المخزنة في نظام معلوماتي يتواجد على أرض الطرف الآخر، لضبطها أو الحصول عليها أو الكشف عنها، كذلك الوصول عبر الحدود إلى البيانات المعلوماتية المخزنة بموافقة صريحة أومن خلال إتاحتها للجمهور، المساعدة المتبادلة في مسألة اعتراض بيانات المحتوى.

وعلى العموم يمكن القول أن المساعدة القضائية الدولية المتبادلة تعتبر آلية دولية فعالة لمكافحة جرائم نظام المعالجة الآلية المعطيات ذات البعد الدولي والمرتكبة في بيئة افتراضية، لذا فإن تنفيذها وفق القواعد المنصوص عليها في الاتفاقيات الدولية ذات الصلة والاتفاقيات الثنائية ومبدأ المعاملة بالمثل، واستحداث مجالات خاصة بالمساعدة القضائية الدولية للمواجهة هذا النوع من الإجرام، يتلائم مع طبيعة هذه الجرائم التي تقتضي التعامل مع أدلة رقمية غير ملموسة وسريعة الزوال.[1]

البند الثاني: تسليم المجرمين المعلوماتيين

تسليم المجرمين إجراء من إجراءات التعاون القضائي الدولي، تقوم بموجبه إحدى الدول، بتسليم شخص متواجد على إقليمها إلى دولة أخرى، أو إلى جهة قضائية دولية، إما بهدف محاكمته عن جريمة اتهم بارتكابها، وإما لأجل تنفيذ حكم الإدانة الصادر ضده من محاكم هذه الدولة أو المحكمة الدولية.[2]

وتعد الجزائر من بين الدول التي أدخلت نظام تسليم المجرمين في تشريعاتها الداخلية، وهوما نص عليه قانون الاجراءات الجزائية الجزائري المعدل و المتمم في الكتاب السابع **"في العلاقات بين السلطات القضائية الأجنبية"**، في الباب الأول **"في تسليم المجرمين"**، بالنص على انه يجوز للحكومة الجزائرية أن

[1]– طيبي البركة، المرجع السابق، ص 344.

[2]– سليمان عبد المنعم، **الجوانب الإشكالية في النظام القانوني لتسليم المجرمين–دراسة مقارنة–** ، دار الجامعة الجديدة، الإسكندرية ،مصر، 2007، ص 10.

تسلم شخصا غير جزائري الى حكومة أجنبية بناء على طلب.ها إذا وجد في أراضي الجمهورية وكانت قد اتخذت في شأنه إجراءات متابعة باسم الدولة الطالبة أو صدر حكم ضده من محاكمها.[1]

كما أنه مبدأ كرسه الدستور الجزائري بالنص على انه: "لا يسلم أحد إلا بمقتضى اتفاقية دولية مصادق عليها أو بموجب قانون".[2]

ننوه في ذات الإطار إلى أهمية تميز مصطلح **"تسليم المجرمين"** عن بعض المصطلحات المشابهة والتي من بين بينها **"التسليم المراقب"**، والذي يقصد به انه أسلوب السماح للشحنات غير المشروعة بمواصلة طريقها إلى خارج إقليم بلد، أو أكثر أو عبره أو إلى داخله بعلم سلطاته المختصة وتحت مراقبتها، بغية كشف هوية الأشخاص المتورطين في ارتكاب هذه الجرائم،[3] ولا يعد التسليم من قبيل الإبعاد الذي يعد عملا إداريا تستقل باتخاذ جهة إدارية في الدولة في حالات لا يمكن حصرها،[4] ويكون بإلزام شخص بمغادرة الإقليم
أو إخراجه منه بغير رضاه، إذا كان يشكل تهديد لأمنها وسلامتها، أما رعايا الدولة فلا يجوز إبعادهم،[5] ولا يعتبر التسليم كذلك من قبيل الطرد الذي تمارسه الدولة بما لها من سيادة على إقليمها، متى رأت أن بقاء الشخص على إقليمها، من شأنه أن يؤثر على وجودها أو أمنها.[6]

وتنبغي الإشارة إلى وجود بعض التحديات الخاصة بتسليم المجرمين والتي تظهر من جانبين يتعلق الأول بالتجريم المزدوج والثاني بتزاحم الطلبات.

أولا- التجريم المزدوج :

يعد التجريم المزوج من أهم الشروط الخاصة بنظام تسليم المجرمين وهو منصوص عليه في أغلب التشريعات الداخلية والمواثيق الدولية المعنية بتسليم المجرمين، ويجد أساسه الفقهي في أن التسليم إجراء يتضمن مساسا بالحرية الشخصية يستند إلى قضاء أجنبي، الأمر الذي يوجب أن يكون لهذا الإجراء ما يبرره

[1]- يراجع في ذلك نص المادة 696، ق.الإ.ج.ج.م. م

[2]- يراجع في ذلك أحكام المادة 50 ،من التعديل الدستوري 2020.

[3]- نصر الدين مروك، **جريمة المخدرات في ضوء القوانين و الاتفاقيات الدولية**، دار هومة للطباعة و النشر والتوزيع، الجزائر، 2004، ص 453.

[4]- سراج الدين محمد الروبي، **الانتربول وملاحقة المجرمين** ، الدار المصرية اللبنانية، مصر، 1998، ص 40.

[5]- علي صادق أبو الهيف، **القانون الدولي العام**، ط12، منشأة المعارف، الإسكندرية، مصر، 2015، ص 257.

[6]- جميل عبد الباقي الصغير، **المرجع السابق**، ص 88.

في النظام القانوني الوطني، وأن يكون الفعل المرتكب مجرما في القانون الوطني حتى لا تصطدم الجماعة بالقبض على شخص أو اعتقاله لارتكابه فعلا تعتبره تلك الجماعة مباحا ومشروع.[1]

وبالرغم من أهمية هذا الشرط إلا أنه غالبا ما يكون عقبة أمام التعاون الدولي في مجال تسليم المجرمين بالنسبة للجرائم المعلوماتية بما في ذلك الجرائم الماسة بالنظام المعالج آليا ، بالإضافة إلى صعوبة تحديد ما إذا كانت النصوص التقليدية لدى الدولة المطلوب منها التسليم يمكن أن تنطبق على الجرائم الرقمية و يضاف إلى ذلك أن الدول قد تفسر و توسع شرط ازدواج التجريم ،الأمر الذي يعوق تطبيق الاتفاقيات الدولية في هذا المجال، ويحول بالتالي دون جمع الأدلة ومحاكمة مرتكبي الجرائم المعلوماتية.

ثانيا- التزاحم في طلبات التسليم :

وهو تنازع وكثرت الطلبات من اجل تسليم ذات الشخص من عدة دول، سواء كان الطلب متعلق بنفس الجريمة أو بجرائم مختلفة، وسبب تعلق هذه الصعوبة بالجرائم المعلوماتية أن الشخص المطلوب تسليمه قد يرتكب جريمة أو أكثر من الجرائم المعلوماتية تمس في نفس الوقت بمصالح أساسية لأكثر من دولة، ففي هذه الحالة قد تتزاحم طلبات التسليم المقدمة من الدول المضرورة إلى الدولة المطلوب إليها.

وللقول بوجود تزاحم في طلبات التسليم ينبغي أن تقدم الدولة الطالبة أدلة تثبت فيها قيام الشخص المطلوب تسليمه بارتكاب الجريمة المعلوماتية، وكذلك إرسال طلبها بالفعل حيث لا تكفي التصريحات الشفوية أو إبداء الرغبة في استلام الشخص، ولا يشترط في تزاحم الطلبات أن تتعاصر في وصولها إلى الدولة المطلوب إليها، بل يكفي أن تتوالى إلى الدولة المطلوب إليها، طالما أن الشخص المطلوب ما زال متواجدة على إقليمها، ولم يتم تسليمه إلى أي من الدول التي تطالب بتسليمه.

هذا ويخضع تسليم المجرم المعلوماتي إلى مجموعة من الشروط أهمها:

- أن يكون الدخول إلى النظام أو البيانات قد تم دون وجه حق وبنية الإخلال بسرية البيانات أو إعاقة نظام الكمبيوتر.
- وجود اتفاقية تسليم مرتكبي الجرائم المعلوماتية مبرمة بين الدولة الطالبة والمطلوب منها التسليم.

لكل ما سبق وجب على الدول أن تكثف التعاون فيما بينها من خلال تطبيق وتفعيل أحكام المواثيق الدولية المتعلقة بالتعاون الدولي في المسائل الجنائية ذات الصلة بمكافحة الإجرام المعلوماتي.

[1]- أحمد محمد السيد عبد الله، **التعاون الدولي في الإجراءات الجنائية**، دراسة مقارنة بالنظام الإسلامي، رسالة دكتوراه، كلية حقوق، المنصورة، مصر ،السنة الجامعية 2008- 2009، ص 394.

الخـــاتمـــة

الخاتمة:

من خلال هذه الدراسة تم تناول الحماية الجزائية لأنظمة المعالجة الالية للمعطيات من الجانبين الموضوعي والإجرائي في ظل أحكام التشريع الجزائري، وهذا باعتبارها جريمة تنتمي إلى طائفة الجرائم المعلوماتية التي تحظى بالخصوصية من حيث أساليب ارتكابها و صفات مرتكبيها ، و قد تضمنت الدراسة تبيان أركان ونوع الجريمة الواقعة على النظام المعالج آليا وتحديد العقوبة المقررة لها المدرجة ضمن القسم السابع مكرر من قانون العقوبات المعدل والمتمم ، أما الجانب الإجرائي فتناول الإجراءات المستحدثة في البحث و التحري عن الجريمة ذات الصلة ، لعدم كفاية الإجراءات التقليدية و هذا على ضوء قانون الاجراءات الجزائية الجزائري المعدل و المتمم و القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وبالرغم من ذلك ومع كل الجهود التي بدلت ومازالت تبدل لتكريس حماية قانونية فعالة لنظام المعالجة الآلية للمعطيات ،إلا أنها تبقى غير كافية للتعامل مع هذا النوع من الجرائم و مرتكبيها لارتباطها بتكنولوجيا في تطور مستمر ، ما يستوجب المبادرة إلى تعديل و تحيين التشريعات بما يكفل تجاوز النصوص التقليدية التي تبقى عاجزة في ظل تطور و اتساع هذا النوع المستحدث من الجرائم .

هذا و على ضوء ما سبق ذكره ، فقد خلصت الدراسة إلى بعض النتائج التي يمكن إجمالها في السياق الاتي :

✓ لقد تعاظم الدور الذي يؤديه نظام المعالجة الآلية للمعطيات باعتباره مستودعا لكم هائل وضخم من البيانات والمعلومات الشخصية والاقتصادية والمالية والعسكرية، وأصبح عرضة للكثير من الاعتداءات التي تمس بسلامته، مما أدى إلى ظهور شركات متخصصة في صناعة برامج الحماية التقنية ونظم الأمان الهدف منها حماية هذه الأنظمة من الاختراقات والفيروسات، ورغم هذا التطور الذي بلغته هذه الصناعة فإن الاعتداءات لم تتوقف بل على العكس من ذلك ذهب مرتكبوها إلى تطوير تقنيات وسائل ارتكابهم لهذه الجرائم وأهمها تقنيتي الاختراق والفيروسات بما يحبط آمان هذه النظم و إلحاق أضرار اقتصادية كبيرة بالدول والمؤسسات من خلال الولوج إليها بطرق غير مشروعة، الأمر الذي جعل الشرائع الدولية والتشريعات الداخلية تأذن بوضع نصوص ومبادئ قانونية لتجريم مختلف أنواع العدوان على نظم المعالجة الآلية للمعطيات.

✓ إن المعطيات و البرامج هي جزء من نظام المعالجة الآلية للمعطيات، و الاعتداء على إحداها منفردا يعد اعتداء على هذا النظام أو مساسا به، ذلك أن الحماية الجنائية للنظام أوسع من الحماية الجنائية للمعطيات و البرامج .

✓ إن نظام المعالجة الآلية للمعطيات يعتبر الشرط الأولي للبحث في توافر أو عدم توافر أي جريمة من جرائم المساس بـنظام المعالجة، فإذا تخلف هذا الشرط لا يكون هناك مجال للبحث في مدى توافر أركان أي جريمة من الجرائم الماسة بنظام المعالجة الآلية للمعطيات، والتي تؤدي إما إلى المساس بالنظام في حد ذاته أو إلى المساس بالمعطيات الموجودة داخل نظام المعالجة الآلية أو التي لها علاقة به، وهو ما جعل الفقه يتجه إلى وضع معيارا للتفرقة بين الاعتداء على النظام والاعتداء على المعطيات التي يتضمنها وذلك على أساس ما إذا كان الاعتداء يشكل وسيلة أم غاية، فإذا كان الاعتداء مجرد وسيلة فإن العمل يشكل جريمة اعتداء على نظام المعالجة الآلية أما إذا كان الاعتداء غاية فهو يشكل جريمة اعتداء على المعطيات الموجودة داخل هذا النظام .

✓ عالج المشرع الجزائري جرائم المساس بأنظمة المعالجة الآلية باعتبارها من الجرائم المعلوماتية من خلال النص عليها في قانون العقوبات المعدل والمتمم، ولم يخصها بقانون خاص حيث اكتفى بتعديل كل من قانون العقوبات و قانون الإجراءات الجزائية .

✓ ثمة بعض الصعوبات في تطبيق بعض الإجراءات على الجرائم المعلوماتية مثل التفتيش والضبط خاصة فيما يتعلق بالمكونات المعنوية للحاسوب، صعوبة الحصول على الدليل الالكتروني من حيث طبيعته و دور الوسائل التقنية في ذلك ، و قيمة الدليل المتحصل عليه باستعمال هذه الطرق ، و تقديره من طرف القاضي في ظل مبدأ الاقتناع الحر للقاضي ، و يبقى له التقدير النهائي للدليل ما إذا كان كافيا لإدانة المتهم أو استبعاده أو إعمال قاعدة تفسير الشك لصالح المتهم، هذه الصعوبات التي لا تنحصر على المستوى الداخلي فقط بل و رغم الجهود المبذولة على المستوى الدولي إلا أنه توجد بعض الصعوبات أيضا التي تعترض سير عملية مكافحة الجريمة المعلوماتية.

هذا ومن خلال ما تم التوصل إليه في هذه الدراسة يمكن التماس مجموعة من المقترحات يتم ذكرها كما يلي :

✓ المتابعة الدورية للجريمة المعلوماتية لاسيما جرائم المساس بانظمة المعالجة الالية للمعطيات بحكم خصوصية هذا النوع من الجرائم ، وذلك بسن قواعد موضوعية و أخرى إجرائية تتلائم مع طبيعة الجريمة المعلوماتية حتى تكون هذه القواعد أكثر فعالية.

✓ لا بد من تكاثف الجهود الدولية و الإقليمية في حقل جرائم المعلوماتية لتخطي العقبات التي تطرحها هذه الجرائم، حيث ان التعاون الدولي ضروري لمواجهة الجرائم في البيئة المعلوماتية الالكترونية و ذلك من خلال الدخول في اتفاقيات و معاهدات تجرم صورة هذه الجرائم كلها و تبين كذلك الاختصاص المكاني في حال وقوعها ، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات و المعلومات وفي المسائل المتعلقة بالجرائم المعلوماتية ،و هذا ما يجب أن يحدث بالنسبة للجزائر و ضرورة انضمامها لاتفاقية بوداسبت 2001 لمكافحة الجريمة المعلوماتية .

✓ ضرورة تدريب وتأهيل أفراد الضبطية القضائية من العاملين و النيابة العامة والقضاء على كيفية التعامل مع هذا النوع من الإجرام و تحقيق التعاون مع التقنيين من أصحاب الخبرة ، و ذلك بعقد دورات تدريبية بشكل دوري و دائم للاستفادة من خبراتهم و إرشاداتهم ابتداء من مرحلة الاستدلال و جمع الأدلة و انتهاء بقرارات المحاكم .

✓ إن تطور الفكر الإجرامي في جرائم نظام المعالجة الآلية للمعطيات لا بدا أن يقابله تفعيل الفكر القانوني، بحيث يجب أن يكون هناك تطور موازي ومواكب في الإطار القانوني خاصة في ظل واقع المعلوماتية الذي يتسم بالحركية والتحول الدائمين وبالتالي العمل بشكل دائم على استحداث آليات وتدابير جديدة لتوفير الحماية الجنائية للنظم المعلوماتية و البيانات التي تتداول عبرها.

✓ تدريس مواد الأنظمة المعلوماتية والجرائم التي قد نشأ منها في كليات الحقوق والمعاهد القضائية.

✓ تفعيل دور الأسرة في متابعة الأبناء لوقايتهم من الآثار السلبية و المخاطر المترتبة عن الاستخدام الغير الأمن لشبكة الانترنت بخلق منصات رقمية تتكفل بتوعية الاباء و تدريبهم على التحكم في الاجهزة و الشبكات .

✓ التطور المستمر للتشريعات القائمة بما يحقق مرونتها و مواكبتها للتطورات المتسارعة في مجال تكنولوجيا المعلومات .

و في الأخير و في ضوء ما سبق عرضه و لاجل توفير حماية جزائية ناجعة لأنظمة المعالجة الآلية للمعطيات، يلتمس في هذا الصدد من المشرع الجزائري افراد قانون خاص يتضمن توفير حماية جزائية لأنظمة المعالجة الآلية للمعطيات من مختلف الاعتداءات المحتملة .

قائمة المصادر والمراجع

قائمة المصادر و المراجع

- **القران الكريم**

I. المراجع باللغة العربية:

أولا :المراجع العامة:

1) أحسن بوسقيعة، **الوجيز في القانون الجنائي الخاص** ، الجزء الأول، الطبعة التاسعة، دار هومة الجزائر، 2008.

2) جمال نجيمي ، **دليل القضاة للحكم في للجنح والمخالفات**، الجزء الثاني، الطبعة الثانية ، دار هومة للطباعة والنشر، الجزائر، 2014.

3) سراج الدين محمد الروبي، **الأنتربول وملاحقة المجرمين**، الدار المصرية اللبنانية، مصر.1998 .

4) سليمان عبد المنعم، **الجوانب الإشكالية في النظام القانوني لتسليم المجرمين – دراسة مقارنة –** دار الجامعة الجديدة، الإسكندرية، مصر، 2007.

5) عائشة بن قارة مصطفى، **حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن**،الطبعة الأولى، دار الجامعة الجديدة، الإسكندرية، مصر، 2010.

6) عبد الرحمان خلفي، **الإجراءات الجزائية في التشريع الجزائري**، الطبعة الثالثة، دار بلقيس للنشر، الدار البيضاء، الجزائر، 2017.

7) عبد الله سليمان، **شرح قانون العقوبات الجزائري**، القسم العام، الجزء الأول، الطبعة السادسة، ديوان المطبوعات الجامعية، الجزائر، 2005.

8) عبد الواحد إمام مرسي، **الموسوعة الذهبية في التحريات**، دار المعارف والمكاتب الكبرى، مصر،دون سنة نشر .

9) علي صادق أبو الهيف، **القانون الدولي العام** الطبعة الثانية عشر، منشأة المعارف، الإسكندرية، مصر، 2015.

10) فاضل زيدان محمد، **سلطة القاضي الجنائي في تقدير الأدلة**، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الأردن، 2006.

11) مبروك خزينة، **المسؤولية الجزائية للشخص المعنوي في التشريع الجزائري**، مكتبة الوفاء القانونية، مصر، 2010.

12) محمد زكي أبو عامر، **قانون العقوبات القسم الخاص**، دار الجامعة الجديدة، الإسكندرية، مصر، 2005.

13) محمد ماجد ياقوت، **أصول التحقيق الإداري في المخالفات التأديبية–دراسة مقارنة–**،الطبعة الثالثة دار الجامعة الجديدة، الإسكندرية، مصر، 2007 .

14) محمد محدة، **ضمانات المتهم أثناء التحقيق،الجزء الثالث**،الطبعة الأولى، دار الهدى، عين مليلة الجزائر ، 1992.

15) محمد نجيب حسني، **الموجز في شرح قانون العقوبات القسم الخاص**، دار النهضة العربية، القاهرة مصر، 2003.

16) محمود نجيب حسني، **شرح قانون الإجراءات الجزائية** ، دار النهضة العربية، مصر، 2002 .

17) مصطفى محمد موسى، **المراقبة الالكترونية عبر شبكة الانترنت**، دراسة مقارنة بين المراقبة الأمنية التقليدية والالكترونية، الكتاب الخامس، دار الكتب والوثائق القومية المصرية، القاهرة، مصر، 2003.

18) نصر الدين مروك، **جريمة المخدرات في ضوء القوانين والاتفاقيات الدولية**، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2004.

<u>ثانيا – المراجع المتخصصة:</u>

1) احمد حسام طه تمام، **الجرائم الناشئة عن استخدام الحاسب الآلي–دراسة مقارنة–**،الطبعة الأولى، دار النهضة العربية للنشر والتوزيع، مصر،2000.

2) أمال قارة، الحماية **الجزائية للمعلوماتية في التشريع الجزائري**، الطبعة الأولى، دار هومة، الجزائر 2008.

3) أمير فرج يوسف، **الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت**، الطبعة الأولى ، مكتبة الوفاء القانونية، الإسكندرية، مصر، 2011.

4) جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة، الطبعة الأولى دار البداية، الأردن، 2007.

5) حسن طاهر داود، **جـرائم نظـم المعلـومات**، الطبعة الأولى ،أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 2000.

6) حسين طاهيري، **إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية**، دار العلا للطباعة والنشر، أم البواقي، الجزائر ،2023.

7) خالد ممدوح إبراهيم، **فن التحقيق الجنائي في الجرائم الالكترونية**، الطبعة الأولى،دار الفكر الجامعي مصر ، 2009،

8) رشاد خالد عمر، **المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية (دراسة تحليلية مقارنة)** المكتب الجامعي الحديث الإسكندرية ، مصر ، 2018.

9) رشيدة بوكر، **جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن**، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012.

10) زيبحة زيدان، **الجريمة المعلوماتية في التشريع الجزائري والدولي**، دار الهدى، الجزائر، 2011.

11) عبد الفتاح بيومي حجازي، **الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجريمة المعلوماتية** الطبعة الأولى، دار المعارف، الإسكندرية، مصر، 2009.

12) عبد الفتاح مراد، **شرح جرائم الكمبيوتر والإنترنت، دار الكتب والوثائق المصرية**، مصر، دون تاريخ النشر.

13) عبد الله سيف الكيتوب، **الأحكام الإجـرائية لجريمة الاحتيال المعلوماتي**، دار النهضة العربية، القاهرة مصر، 2013.

14) علي جعفر، **جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة**، الطبعة الأولى منشورات زين الحقوقية، بيروت، لبنان، 2013.

15) علي عبد القادر القهواجي، **الحماية الجنائية لبرامج الحاسب الآلي**، الدار الجامعية للطباعة والنشر الإسكندرية، مصر، 1999.

16) عمر أبو الفتوح عبد العظيم الحمامي، **الحماية الجنائية للمعلومات المسجلة الكترونيا- دراسة مقارنة-** ، دار النهضة العربية، القاهرة، مصر، 2010.

17) محمد خليفة، **الحماية الجنائية لمعطيات الحاسب الآلي**، دار الجامعة الجديدة، الإسكندرية، مصر 2007.

18) محمد طارق عبد الرؤوف، **جريمة الاحتيال عبر الانترنت الأحكام الموضوعية والأحكام الإجرائية**،الطبعة الأولى ، منشورات الحلبي الحقوقية ، بيروت، لبنان ، 2011.

19) محمد عبد الله إبراهيم، **المواجهة الأمنية لجرائم شبكات المعلومات الدولية**، مطابع الشرطة للطباعة والنشر والتوزيع، القاهرة ، مصر، 2016.

20) محمد عبيد الكعبي، **الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت**، الطبعة الثانية، دار النهضة العربية، القاهرة، مصر، 2009.

21) محمد محمد شتا، **فكرة الحماية الجنائية لبرامج الحاسب الآلي** ، دار الجامعة الجديدة للنشر الإسكندرية، مصر، 2001.

22) محمود أحمد عبابنة، **جرائم الحاسوب وأبعادها الدولية**، دار الثقافة للنشر والتوزيع، عمان، الأردن 2005.

23) مسعود خثير، **الحماية الجنائية لبرامج الكومبيوتر (أساليب وثغرات)**، دار الهدى، الجزائر، 2010.

24) ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006.

25) ناني لحسن، **التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية**، النشر الجامعي الجديد، تلمسان، 2018.

26) نائلة عادل محمد فريد قورة ، **جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية**، منشورات الحلبي الحقوقية، بيروت، لبنان، 2005.

27) نجاة بن مكي، **السياسة الجنائية لمكافحة جرائم المعلوماتية**، منشورات دار الخلدونية، الجزائر 2017.

28) نهلا عبد القادر المومني، الجرائم المعلوماتية،الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الأردن، 2008.

29) هشام محمد فريد رستم، **الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة**، أسيوط مصر ، 1994.

30) هلالي عبد الله أحمد، **الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001)**، ط1، دار النهضة العربية، القاهرة، مصر، 2006.

31) يزيد بوحليط، **الجرائم الالكترونية والوقاية منها في القانون الجزائري**، دار الجامعة الجديدة، الإسكندرية مصر،2019 .

32) يوسف مناصرة ، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات (ماهيتها، صورها، الجهود الدولية لمكافحتها)– دراسة مقارنة–**، الطبعة الأولى، دار الخلدونية، الجزائر. 2018.

<u>ثالثا : الرسائل العلمية والمذكرات:</u>

أ- رسائل الدكتوراه :

1) أحمد محمد السيد عبد الله، **التعاون الدولي في الإجراءات الجنائية**، دراسة مقارنة بالنظام الإسلامي رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، مصر، السنة الجامعية 2008–2009.

2) البركه الطيبي، **الحماية الجنائية لأنظمة المعالجة الآلية للمعطيات**، دراسة مقارنة، أطروحة دكتوراه تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة احمد دارية ادرار، الجزائر، السنة الجامعية 2020–2021.

3) حسين ربيعي، **آليات البحث والتحقيق في الجرائم المعلوماتية**، أطروحة دكتوراه، تخصص قانون عام والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة1، الجزائر، السنة الجامعية 2015–2016.

4) رجاء أومدور، **خصوصية التحقيق في مواجهة الجرائم المعلوماتية**، أطروحة دكتوراه ، قسم الحقوق، جامعة محمد البشير الابراهيمي، برج بوعريريج، السنة الجامعية 2020–2021

5) عثمان خرشي، **إجراءات سير الدعوى العمومية في الجرائم المعلوماتية**، أطروحة دكتوراه ، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية جامعة مولاي طاهر سعيدة، الجزائر، السنة الجامعية 2020–2021.

6) عفاف خديري، **الحماية الجنائية للمعطيات الرقمية**، أطروحة دكتوراه، تخصص قانون جنائي، كلية الحقوق جامعة العربي التبسي، تبسة، الجزائر، السنة الجامعية2017–2018.

7) فـوزي عـمارة، **قــاضي التحقيــق**، أطـروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة قسنطينة، الجزائر، السنة الجامعية 2009-2010.

8) فيصل بدري، **مكافحة الجريمة في القانون الدولي والداخلي**، أطروحة دكتوراه في القانون العام، كلية الحقوق جامعة الجزائر، السنة الجامعية 2017- 2018.

9) وردة شرف الدين ، **الإثبات الجنائي بالأدلة الإلكترونية دراسة مقارنة**، أطروحة دكتوراه، تخصص قانون جنائي ، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر ، السنة الجامعية 2016-2017.

ب-<u>رسائل الماجستر</u>:

1) بهاء فهمي الكبيحي، **مدى توافق أحكام جرائم أنظمة المعلومات في القانون الأردني**، رسالة ماجستير في القانون العام، جامعة الشرق الاوسط، عمان، الاردن، السنة الجامعية 2012-2013.

2) عبد اللطيف معتوق، **الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن**، رسالة ماجستر ، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العقيد الحاج لخضر باتنة ،الجزائر، السنة الجامعية 2011-2012.

3) فتيحة رصاع، **الحماية الجنائية للمعلومات على شبكة الأنترنت**، رسالة ماجستر، كلية الحقوق والعلوم السياسية، قسم الحقوق جامعة أبي بكر بلقايد، تلمسان ،الجزائر،السنة الجامعية 2011-2012.

4) محمد نصير السرحاني، **مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنت**، رسالة ماجستير في القانون، جامعة نايف العربية للعلوم الأمنية، الرياض، السعودية، السنة الجامعية 2003- 2004.

5) نسيمة جدي ، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات**، رسالة ماجستر في القانون الجنائي كلية الحقوق، جامعة وهران، الجزائر، السنة الجامعية 2013- 2014.

6) نعيم سعيداني، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، رسالة ماجستير في العلوم القانونية، تخصص علوم جنائية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، السنة الجامعية 2012-2013.

7) يوسف خليل يوسف العفيفي، **الجرائم الالكترونية في التشريع الفلسطيني**، دراسة تحليلية مقارنة رسالة ماجستير في القانون العام، كلية الشريعة القانون، الجامعة الإسلامية غزة، فلسطين، السنة الجامعية 2012-2013.

8) يوسف صغير، **الجريمة المرتكبة عبر الأنترنت**، رسالة ماجستير، كلية الحقوق والعلوم السياسية قسم الحقوق جامعة مولود معمري، تيزي وزو ، الجزائر، السنة الجامعية 2011-2012.

ج- **<u>مذكرات الماستر</u> :**

1) محمد بوعمرة، سيد علي بنينال، **جهاز التحقيق في الجريمة الالكترونية في التشريع الجزائري**، مذكرة ماستر في قانون الأعمال، كلية الحقوق، جامعة البويرة ، الجزائر،السنة الجامعية 2012- 2013.
2) نادية غرباوي ، **أساليب البحث والتحري في الجرائم المعلوماتية** ، كلية الحقوق والعلوم السياسية، قسم قانون عام، جامعة أكلي محمد أولحاج ، البويرة ، الجزائر، السنة الجامعية 2016-2017.
3) يوسف جفال، **التحقيق في الجريمة الإلكترونية**، مذكرة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولاي الطاهر ،سعيدة، الجزائر، السنة الجامعية 2016-2017.

رابعا -المقالات:

1) أمينة معزيز ، ***التسرب في قانون الإجراءات الجزائية الجزائري***"، مجلة القانون و المجتمع" ، كلية الحقوق والعلوم السياسية بجامعة مستغانم، الجزائر،2015.

2) بسمة مامن، "***جرائم المساس بأنظمة المعالجة الآلية للمعطيات في التشريع الجزائري***"، مجلة الحقوق والعلوم السياسية، جامعة خنشلة، الجزائر، المجلد09، العدد01، 2022.

3) جابر بومعيزة ، "**الاعتداء على المعطيات الآلية في الحوكمة الالكترونية**"، مجلة البحوث والدراسات القانونية والسياسية، جامعة البليدة ، الجزائر، العدد12،2017 .

4) جيلالي شويرب ، فائزة مراد ، ***الآليات الدولية والوطنية لمكافحة الجريمة السيبرانية***"، مجلة الدراسات القانونية والسياسية، جامعة عمار ثليجي، الاغواط ، الجزائر، المجلد 09، العدد02، جوان 2023.

5) حليمة حوالف، فاطمة الزهراء مهاجي ، "***معالم الجريمة المعلوماتية في القانون الجزائري***"، مجلة البحوث القانونية والسياسية جامعة تلمسان ، الجزائر، المجلد 3، العدد 16، 2021.

6) خديجة عميور ،" ***قواعد اختصاص الأقطاب الجزائية للنظر في جرائم الفساد***"، مجلة دراسات في الوظيفة العامة، جامعة جيجل، الجزائر، العدد 02، 2014.

7) سعيدة بوزنون، "***مكافحة الجريمة الإلكترونية في التشريع الجزائري***"، مجلة العلوم الإنسانية، جامعة الإخوة منتوري، قسنطينة، الجزائر، العدد 03، 2019.

8) سفيان حديدان ، ***الدخول أو البقاء عن طريق الغش في نظام المعالجة الآلية للمعطيات***"، جامعة 8 ماي 1945، قالمة، الجزائر، المجلد 02، العدد08، ديسمبر 2017.

9) سليمان قطاف، عبد الحكيم بوقرين، ***الآليات القانونية الموضوعية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست التشريع الجزائري***"، المجلة الاكاديمية للبحوث القانونية والسياسة، جامعة عمار ثلجي الأغواط ، الجزائر، المجلد 06، العدد 01، 2022،

10) سمير برادل ، ***الجريمة المعلوماتية في التشريع الجزائري***"، مجلة القانون، كلية الحقوق والعلوم السياسية، المركز الجامعي، غليزان، الجزائر، المجلد01، العدد02 ، جويلية 2010.

11) صالح بن محمد المسند ،عبد الرحمان بن راشد المهيني، "***جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات***"، المجلة العربية للدراسات الأمنية والتدريب ، جامعة نايف العربية ، السعودية ، المجلد 15، العدد 29، أفريل 2000،

12) صالح شنين، " ***إجراءات التحري والتحقيق في جرائم تكنولوجيات الإعلام والاتصال في التشريع الجزائري (قانون 09-04)***"، مجلة الدراسات الحقوقية، كلية الحقوق والعلوم السياسية، جامعة الدكتور الطاهر مولاي سعيدة ،الجزائر ، العدد الأول، 2014.

13) عادل عبد العال إبراهيم خراشي، ***إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها***"، مجلة كلية الشريعة والقانون، دقهلية، مصر، المجلد 01 ، العدد 2014،16.

14) عائشة بن قارة مصطفى، ***آليات حماية المعطيات ذات الطابع الشخصي في التشريع الجزائري وفقا لأحكام القانون رقم 07/***18"، مجلة العلوم القانونية والسياسية، جامعة الوادي ، الجزائر، المجلد10، العدد01، أفريل 2019.

15) عبد الرحيم بوبرقيق ،" ***مفهوم أنظمة المعالجة الآلية للمعطيات في الجرائم المحددة في المواد 394 مكرر إلى 394 مكرر 2 من قانون العقوبات الجزائري***"، مجلة الدراسات والبحوث القانونية، جامعة المسيلة، الجزائر، المجلد04، العدد01، جوان2019.

16) عز الدين عثماني،" ***اجراءات التحقيق والتفتيش في الجرائم الماسة بأنظمة الاتصال والمعلوماتية***"، مجلة دائرة البحوث والدراسات القانونية والسياسية، مخبر المؤسسات الدستورية والنظم السياسية، المركز الجامعي مرسلي عبد الله ، تيبازة ، الجزائر، العدد04، 2018.

17) علاوة هوام، ***التسرب كآلية للكشف عن في جرائم القانون الجزائري***"، مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر ، 2012.

18) فريدة سعيدي ،هشام معزوز ، ***"دراسة سوسيو قانونية لمهام الشرطة العلمية في التحقيقات الجنائية"*** ، مجلة الدراسات القانونية ،جامعة يحي فارس المدية، الجزائر المجلد08 ، العدد02 ،جوان 2022.

19) فوزي عمارة، ***"اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية"***، مجلة العلوم الإنسانية، جامعة الإخوة منتوري، قسنطينة، الجزائر ، العدد 33، جوان 2010.

20) محمد أحمد سليمان عيسى،" ***التعاون الدولي لمواجهة الجرائم الالكترونية"***، المجلة الأكاديمية للبحث القانوني، جامعة المجمعة ،المملكة العربية السعودية، المجلد 14، العدد02، 2016.

21) محمد بن محمد ، ***"تنازع الاختصاص في الجرائم الالكترونية"***، مجلة الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر ، العدد02، 2010.

22) محمد قدري حسن عبد الرحمن، "***جرائم الاحتيال الالكتروني***"، مجلة الفكر الشرطي، صادر عن مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات العربية المتحدة، العدد 79، أكتوبر 2011.

23) مريم عراب، ***"الاختصاص القضائي في الجرائم المعلوماتية"***، مجلة Annales de facute de droit كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد وهران ، الجزائر، المجلد 07، العدد03، ديسمبر2015.

24) المعيني سرحان حسن،" ***التحقيق في جرائم تقنية المعلومات***"، مجلة الفكر الشرطي، مركز بحوث الشرطة، القيادة العامة لشرطة الشارقة، الإمارات، المجلد 20، العدد79، أكتوبر 2011.

25) مليكة درياد ، ***"المساس بأنظمة المعالجة الآلية للمعطيات"***، حوليات جامعة الجزائر، العدد33، مارس 2019.

26) مليكة عطوي،" ***الجريمة المعلوماتية"***، حوليات جامعة الجزائر، العدد 21، جوان 2012.

27) نادية بوراس، ***"الاستراتيجيات الوطنية لمواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات"***، مجلة الحقوق والحريات، سطيف، الجزائر المجلد10، العدد 03 ،2023.

28) ناصر حمودي ، ***"الحماية الجنائية لنظم المعالجة الآلية للمعطيات في التشريع الجزائري"***، المجلة الأكاديمية للبحث القانوني ، جامعة عبد الرحمان ميرة ، بجاية ، الجزائر، المجلد14، العدد02 ، 2016 .

29) هدى زورو ،" ***التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري***"، مجلة دفاتر السياسة والقانون، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، الجزائر، العدد11، 2014.

30) وردة شرف الدين ؛ سامية بلجراف ، ***الجوانب الموضوعية والإجرائية لمكافحة جرائم المعلوماتية في التشريع الجزائري***"، مجلة المنار للبحوث والدراسات القانونية والسياسية، جامعة يحي فارس ،المدية الجزائر،العدد 03، ديسمبر 2017.

خامسا – الملتقيات والمداخلات:

1) بحرية هارون، **دور الدليل الرقمي في أثبات الجريمة المعلوماتية في التشريع الجزائري**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق جامعة محمد خيضر، بسكرة ، الجزائر يومي 16-17 نوفمبر 2015.

2) سامية بلجراف، **سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي**، بحث مقدم إلى أعمال الملتقى الوطني حول-الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة بسكرة، الجزائر ، يومي 16-17 نوفمبر 2015.

3) عبد الرحمان حملاوي، **دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة، الجزائر ، يومي 16-17 نوفمبر 2015.

4) عبد الكريم بلعزوق، **دراسة في ماهية الاجرام الإلكتروني ومجرم الأنترنت**، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، بعنوان: "الاجرام السيبراني المفاهيم والتحديات، برج بوعريرج ، الجزائر ، يومي 11 و12 أفريل 2017.

5) عبد الله حسين محمود، **إجراءات جمع الأدلة في الأدلة في الجريمة المعلوماتية**، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، الإمارات، 2003.

6) عبد المومن بن صغير، **الطبيعة الخاصة للجريمة المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن**، مداخلة مقدمة ضمن فعآليات الملتقى الوطني الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة محمد خيضر بسكرة، بعنوان: الجريمة المعلوماتية بين الوقاية والمكافحة، بسكرة، الجزائر يومي 15 و16 نوفمبر 2015.

7) عبد الناصر محمد محمود فررلي؛ محمد عبيد اسيا سعيد المسماري، **الاثبات الجنائي بالأدلة الرقمية**، المؤتمر العربي، الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايا للعلوم الأمنية، الرياض، السعودية، 2007.

8) عطاء الدين فشار، **مواجهة الجريمة المعلوماتية في التشريع الجزائري**، الملتقى المغاربي حول القانون والمعلوماتية، اكاديمية الدراسات العليا، ليبيا، أكتوبر 2009.

9) عومرية حساين، **أثر التكنولوجيا في استفحال الجريمة المعلوماتية وسبل مكافحتها في ظل التشريع الجزائري**، كتاب الملتقى الدولي حول القانون الجنائي في ظل التطور التكنولوجي – اشكالات ومعالجات بيت الأفكار، الجزائر، 2023.

10) ليلى بومدين، **دور المؤسسات و الادارات في مكافحة التزوير – الجريمة السيبرانية** –، مداخلة ألقيت خلال اليوم الدراسي بعنوان "القانون 24-02 المؤرخ في 2024/02/26 المتعلق بمكافحة التزوير واستعمال المزور " مجلس قضاء عين تموشنت ، الجزائر، يوم 15ماي2024.

11) موسى مسعود أرحومة، **الإشكاليات الاجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية**، مداخلة مقدمة ضمن فعاليات، المؤتمر المغاربي الأول الذي نظمته أكاديمية الدراسات العليا ، بعنوان المعلوماتية والقانون ، طرابلس ، ليبيا، يومي 28-29 أكتوبر 2010.

12) نبيلة بن عائشة، **الجريمة الالكترونية**، مداخلة في إطار ندوة وطنية منظمة بكلية الحقوق لدى جامعة الجزائر1، بتاريخ 2019/11/19، تحت رئاسة كوثر مازوني، منشورة بمجلة الندوة الوطنية، الطبعة الأولى، دار الخلدونية للنشر والتوزيع، الجزائر، 2022.

13) هشام عبد الكريم، **التمييز العنصري وصور الاستخدامات الجديدة للانترنت**، مداخلة مقدمة ضمن فعاليات الملتقى الدولي الذي نظمته كلية الحقوق والعلوم السياسية قسم الحقوق جامعة برج بوعريريج، بعنوان الإجرام السيبراني المفاهيم والتحديات، برج بوعريريج، الجزائر، يومي 11 و12 أفريل 2017.

14) هواري عياش، **المعهد الوطني للأدلة الجنائية وعلم الإجرام مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية**، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة بسكرة الجزائر، يومي 16-17 نوفمبر 2015.

15) المركز العربي للبحوث القانونية والقضائية، **ضرورة التعاون الإقليمي والدولي في مكافحة جرائم المعلوماتية**، ورقة عمل مقدمة إلى الاجتماع السادس للمختصين بتقنية المعلوماتية في النيابات العامة في الدول العربية، بيروت، لبنان، 2018.

سادسا- المصادر القانونية :

أ-الدستور:

- التعديل الدستوري الجزائري 2020، المرسوم الرئاسي رقم 442/20 المؤرخ في 2020/12/30 يتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر 2020 ،جريدة رسمية رقم 22 مؤرخة في 2020/12/30 .

ب- الصكوك الدولية :

1) اتفاقية بودابست للإجرام المعلوماتي 2001

2) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، المصادق عليها بموجب المرسوم الرئاسي رقم 14-252، الصادر في 2014/09/08، ، جريدة رسمية 57، المؤرخة في 2014/09/20.

3) الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية المصادق عليها بموجب المرسوم الرئاسي رقم14-251 بتاريخ 2014/09/08، جريدة رسمية 56، الصادرة بتاريخ 2014/09/25.

4) القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات، اعتمده مجلس وزراء العرب في دورته التاسعة عشر بالقرار رقم 495 د19في 2003/10/08و مجلس وزراء الداخلية العرب في دورته الحادية و العشرون بالقرار رقم417- د21-2004

ج-القوانين و الأوامر :

1) الأمر رقم 66-155 المؤرخ في 08جوان 1966 المتضمن قانون الإجراءات الجزائية ، المنشور بالجريدة الرسمية، العدد 48 ، المؤرخة في 10 جوان 1966 ، المعدل والمتمم.
2) الأمر رقم 66-156 المؤرخ في 08جوان 1966 المتضمن قانون العقوبات ، المنشور بالجريدة الرسمية، العدد 49 ، المؤرخة في 11 جوان 1966 ، المعدل والمتمم.
3) قانون رقم 2000-03 المؤرخ في 2000/08/05، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، المنشور بالجريدة الرسمية، العدد 48، المؤرخة في 2000/08/06.
4) قانون رقم 03-05، المؤرخ في 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، المنشور بالجريدة الرسمية، العدد 44، المؤرخة في 23 يوليو 2003.
5) قانون رقم 08-01 المؤرخ في 23 جانفي 2008 يتمم القانون 83-11 المؤرخ في 02 جوان 1983 يتعلق بالتأمينات الاجتماعية، المنشور بالجريدة الرسمية، العدد 04، المؤرخة في 27 جانفي 2008.
6) القانون 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور بالجريدة الرسمية، العدد 47، المؤرخة في 16 أوت 2009 .
7) قانون رقم 15-03 المؤرخ في 2015/02/01، يتعلق بعصرنة قطاع العدالة، المنشور بالجريدة الرسمية، العدد 06، المؤرخة في 2015/02/10.
8) قانون رقم 15-04 المؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، المنشور بالجريدة الرسمية، العدد 06، المؤرخة في 10 فبراير 2015.

9) قانون رقم 18-04 المؤرخ في 2018/05/10، يتعلق بالبريد والاتصالات الالكترونية، المنشور بالجريدة الرسمية، العدد 27، المؤرخة في 2018/05/13.

10) قانون رقم 18-07 المؤرخ في 2018/06/10، المتعلق بحماية الأشخاص الطبيعية في مجال معالجة المعطيات ذات الطابع الشخصي المنشور بالجريدة الرسمية، العدد 34، المؤرخة في 2018/06/10.

11) أمر رقم 21-01، المؤرخ في 2021/03/10، المتضمن القانون المتعلق بنظام الانتخابات المنشور بالجريدة الرسمية، العدد 17، المؤرخة في 2021/03/10

د-المراسيـــــم:

- **المراسيم الرئاسية :**

1) المرسوم الرئاسي رقم 04-23، الصادر في 2004/02/07، المتضمن التصديق على الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجمهورية الجزائرية الديمقراطية الشعبية ومملكة إسبانيا الموقعة بمدريد في 2002/10/07، ، منشور بالجريدة الرسمية، العدد 08، المؤرخة في 2004/02/08.

2) المرسوم الرئاسي رقم 04-183، مؤرخ في 2004/06/26، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانون الأساسي، منشور بالجريدة الرسمية، العدد 41، المؤرخة في 27جوان 2004.

3) المرسوم الرئاسي رقم14-251 بتاريخ 2014/09/08، المتضمن التصديق على الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية ، منشور بالجريدة الرسمية، العدد 56، الصادرة بتاريخ 2014/09/25.

4) المرسوم الرئاسي رقم 14-252، الصادر في 2014/09/08، المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، ، منشور بالجريدة الرسمية، العدد 57، المؤرخة في 2014/09/20

5) المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال ومكافحتها. ، منشور بالجريدة الرسمية، العدد 53.الصادرة بتاريخ: 08 أكتوبر 2015.

6) المرسوم الرئاسي رقم 20-05، المؤرخ في 2020/01/02، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، المنشور بالجريدة الرسمية، العدد 04 الصادر في 2020/01/26.

➢ **المراسيم التنفيذية :**

1) المرسوم التنفيذي رقم 06-348 المؤرخ في 2006/10/05، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، منشور بالجريدة الرسمية، العدد 63، المؤرخة في 2006/10/08.

سابعا : المعاجم:

-الكفوي أبو البقاء أيوب موسى الحسني، معجم في المصطلحات والفروق اللغوية، ط2، مؤسسة الرسالة، بيروت، لبنان، 1998.

2-المراجع باللغة الأجنبية :

Les ouvragés:

1- Bokhari NAMRATA Agrawal, Dharmendra SAINI, Cyber Security Proceedings of CSI 2015 Springer Nature Singapore Pte Ltd, 2018.
2- Freyssinet E**, La cybercriminalité en mouvement**, Lavoisier, 2012, France**.**
3- Lazetik G B, Koshevaliska O, **Digital Evidence in Criminal Procedures(A comparative approach)**, Balkan Social Science Review, 2 (1), 2013.
4- Myriam QUÉMÉNER et Joel Ferry, **Cybercriminalité Défi mondial**, Economica, France, 2eme édition 2009.
5- Myriam QUÉMÉNER. **Cybercriminalité**. Droit pénal appliqué. 1e Edition, Economica. Paris, France , 2010.
6- Olivier BEAUVALLET , **Les investigations judiciaires internationales**, 1er édition, Berger-levrault, 2014.

Législations:

1- Loi n°88-19 du 05 janvier 1988, relative à la fraude l'informatique , journal officiel de la république française du 06 janvier 1988 , (LOI GODFRAIN).

مواقع الانترنيت:

https://

- www.arablegalnet.org.
- www.coe.int/fr/web/cybercrime/the-budapestconvention.
- http://conventions.coe.int/Treaty/fr/Reports/Html/185.htm .
- www.mdn.dz/site cgn.

الفـــهـــرس

محتويات البحث	الصفحة
الشكر والتقدير	
الإهداء	
مقدمة	01
الفصل الأول: الأحكام الموضوعية لمواجهة جرائم المساس بأنظمة المعالجة الآلية	
المبحث الأول: المساس بأنظمة المعالجة الآلية للمعطيات خصوصية المفاهيم وتأصيل قواعد التجريم	08
المطلب الأول: الإطار المفاهيمي لجرائم المساس بأنظمة المعالجة الآلية للمعطيات	08
الفرع الأول: تعريف نظام المعالجة الآلية للمعطيات وتحديد طبيعته القانونية	09
البند الاول: التعريف الفقهي والقانوني لأنظمة المعالجة الآلية للمعطيات	09
البند الثاني: الطبيعة القانونية الخاصة لأنظمة المعالجة الآلية للمعطيات	11
الفرع الثاني: خصوصية جرائم المساس بأنظمة المعالجة الآلية للمعطيات	12
البند الأول: خصائص الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات	13
البند الثاني: المجرم المعلوماتي في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات	16
الفرع الثالث: عناصر المعطيات المعالجة آليا محل المساس وتقنيات الاعتداء عليها	18
البند الاول: عناصر المعطيات المعالجة آليا محل المساس	19
البند الثاني: تقنيات الاعتداء على الأنظمة المعالجة آليا	20
الفرع الرابع: علاقة الحماية التقنية لأنظمة المعالجة الآلية للمعطيات بالمسؤولية الجزائية	22
البند الاول: أهمية الحماية التقنية لأنظمة المعالجة الآلية للمعطيات	22
البند الثاني: أهمية الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات	24
المطلب الثاني: إرساء قواعد تجريم الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات	25
الفرع الأول: مبررات الحماية الجزائية لأنظمة المعالجة الآلية للمعطيات	26
البند الأول: الأسباب المتعلقة بحداثة الظاهرة الإجرامية	26
البند الثاني: الأسباب المتعلقة بخصوصية المفاهيم وحاجتها لحلول مبتكرة	27
البند الثالث: الأسباب المتعلقة بأهمية المعطيات المدرجة ضمن النظم المعلوماتية	27
البند الرابع: الأسباب المتعلقة بإلزامية مواكبة الفكر القانوني لتطور الفكر الاجرامي	28
الفرع الثاني: إرساء قواعد الحماية من خلال تبني بنود اتفاقية بودابست	29
البند الأول: مضمون اتفاقية بودابست	29
البند الثاني: مدى توافق نظام بودابست مع التشريع الجزائري	30

الفرع الثالث: ارساء قواعد الحماية من خلال التعاون العربي	31
البند الأول: القانون العربي النموذجي الاسترشادي	31
البند الثاني: الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية	32
البند الثالث: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات	33
الفرع الرابع: ارساء قواعد الحماية ضمن التشريع الداخلي	34
البند الاول: أحكام تقنين العقوبات	35
البند الثاني: احكام قانون الاجراءات الجزائية	36
البند الثالث: ارساء قواعد الحماية ضمن نصوص القوانين المكملة	36
المبحث الثاني: أوجه الاعتداء على أنظمة المعالجة الآلية للمعطيات وجزاءات المساس بها	40
المطلب الأول: أوجه الاعتداء على أنظمة المعالجة الآلية للمعطيات	41
الفرع الأول: الدخول والبقاء غير المصرح به	41
البند الأول: الركن الشرعي لجريمتي الدخول او البقاء في النظام المعلوماتي	42
البند الثاني: الركن المادي لجريمتي الدخول والبقاء في النظام المعلوماتي	44
البند الثالث: الركن المعنوي في جريمة الدخول والبقاء	45
الفرع الثاني: الإتلاف غير العمدي للمعطيات	46
البند الأول: الركن الشرعي لجريمة الإتلاف الغير العمدي للمعطيات	46
البند الثاني: الركن المادي لجريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات وإتلاف المعلومات	47
البند الثالث: الركن المعنوي لجريمة إتلاف المعلومات	48
الفرع الثالث: التلاعب بالمعطيات	49
البند الأول: الركن الشرعي لجريمة التلاعب بالمعطيات	49
البند الثاني: الركن المادي لجريمة التلاعب بالمعطيات	50
البند الثالث: الركن المعنوي لجريمة التلاعب بالمعطيات	52
الفرع الرابع: التعامل في المعطيات غير المشروعة	53
البند الأول: الركن الشرعي لجريمة التعامل في معطيات غير مشروعة	54
البند الثاني: الركن المادي لجريمة التعامل في معطيات غير مشروعة	56
البند الثالث: الركن المعنوي لجريمة التعامل في معطيات غير مشروعة	58
المطلب الثاني: الجزاءات المترتبة على المساس بأنظمة المعالجة الآلية للمعطيات	60
الفرع الأول: الأحكام المتعلقة بالشروع والاتفاق الجنائي في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات	60

البند الأول: الشروع في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات ، وموقف المشرع الجزائري منه	61
البند الثاني: الاتفاق الجنائي في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات ، وموقف المشرع الجزائري منه	62
الفرع الثاني: العقوبات المطبقة على الشخص الطبيعي	64
البند الأول: العقوبات الأصلية المطبقة على كل جريمة من جرائم المعطيات	64
البند الثاني: العقوبات التكميلية	65
البند الثالث: الظروف المشددة	66
الفرع الثالث: العقوبات المطبقة على الشخص المعنوي	66
البند الأول: العقوبات الأصلية	67
البند الثاني: العقوبات التكميلية	68
الفصل الثاني: الأحكام الإجرائية لمواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات	
المبحث الأول: المساس بأنظمة المعالجة الآلية للمعطيات خصوصية الإجراءات وإرساء أجهزة الحماية	71
المطلب الأول: خصوصية آليات البحث والتحري عن الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات	71
الفرع الأول: تفتيش المنظومة المعلوماتية	72
البند الأول: تعريف التفتيش في البيئة التقنية	72
البند الثاني: الشروط الشكلية والموضوعية للإذن بالتفتيش في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات	73
البند الثالث: إجراءات التفتيش في الجرائم الماسة بالمعطيات الرقمية	74
الفرع الثاني: إجراء الضبط في الجريمة المتصلة بتكنولوجيا المعلوماتية	76
البند الأول: الحجز عن طريق نسخ المعطيات المعلوماتية	76
البند الثاني: الحجز عن طريق منع الوصول إلى المعطيات	77
البند الثالث: التعامل مع المحجوزات في الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات	78
الفرع الثالث: إجراء التسرب الالكتروني	78
البند الأول: شروط التسرب الالكتروني	79
البند الثاني: طرق التسرب الالكتروني	80
الفرع الرابع: الوسائل الأخرى للبحث والتحري الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات	81

البند الأول: اعتراض المراسلات	81
البند الثاني: مراقبة الاتصالات الإلكترونية	82
البند الثالث: التقاط الصور	83
البند الرابع: تسجيل الأصوات	84
المطلب الثاني: أجهزة وهيئات الحماية من الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات	84
الفرع الأول: الأجهزة الأمنية لمكافحة الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات	85
البند الأول: الأجهزة التابعة لسلك الأمن الوطني	85
البند الثاني: الأجهزة التابعة للدرك الوطني	87
الفرع الثاني: الهيئات القضائية الجزائية المتخصصة	90
البند الأول: الاقطاب الجزائية المتخصصة	90
البند الثاني: القطب الجزائي الوطني المستحدث	91
الفرع الثالث: الهيئات الشبه القضائية	93
البند الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها	93
البند الثاني: السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي	94
البند الثالث: المجلس الوطني لأمن الأنظمة المعلوماتية	96
الفرع الرابع: أجهزة التعاون الدولي في مجال الجرائم المعلوماتية	98
البند الأول: المنظمة الدولية للشرطة الجنائية "الانتربول"	98
البند الثاني: الأجهزة الأمنية الدولية الأخرى	100
المبحث الثاني: الدعوى العمومية للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وتحدياتها الإجرائية	102
المطلب الأول: مراحل سير دعوى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات	103
الفرع الأول: مرحلة التحري وجمع الاستدلالات في الجرائم الماسة بالأنظمة المعلوماتية	103
البند الأول: اختصاص ضباط الشرطة القضائية في الجرائم المعلوماتية	104
البند الثاني: آليات اتصال الضبطية القضائية بالجريمة الماسة بالنظام المعلوماتي	104
البند الثالث: قواعد التحقيق الابتدائي في الجرام الماسة بأنظمة المعالجة الآلية للمعطيات	106
الفرع الثاني: دور النيابة العامة في تحريك الدعوى جرائم المعطيات المعلوماتية	108
البند الأول: الاختصاص الاقليمي والنوعي لوكيل الجمهورية	108
البند الثاني: دور النيابة العامة في مباشرة الدعوى العمومية	108
البند الثالث: السلطات المخولة لوكيل الجمهورية	109
الفرع الثالث: مرحلة التحقيق القضائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات	111

البند الأول: اختصاص قاضي التحقيق	111
البند الثاني: آليات اتصال قاضي التحقيق بملف الدعوى الخاص بجرائم المعطيات المعلوماتية	112
البند الثالث: سلطات قاضي التحقيق المختص في جرائم المعطيات المعلوماتية	113
الفرع الرابع: دور القاضي الجزائي في الفصل في دعوى المساس بأنظمة المعالجة الآلية للمعطيات	115
البند الأول: تشكيلة المحكمة في الجرائم الماسة بـأنظمة المعالجة الآلية للمعطيات	115
البند الثاني: القواعد العامة لإجراءات المحاكمة في جرائم المساس بأنظمة المعالجة الآلية للمعطيات	116
البند الثالث: إجراءات سير جلسة المحاكمة	117
المطلب الثاني: التحديات الاجرائية في مواجهة جرائم المساس بأنظمة المعالجة الآلية للمعطيات	118
الفرع الأول: التحديات الإجرائية ذات الصلة بإجراءات التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات	119
البند الأول: الصعوبات ذات الصلة بشخص المحقق	119
البند الثاني: صعوبات تتعلق بطبيعة الجريمة والجهات المتضررة منها	120
الفرع الثاني: التحديات الاجرائية ذات الصلة بالاختصاص القضائي في جرائم المساس بأنظمة المعالجة الآلية للمعطيات	122
البند الأول: المبادئ العامة للاختصاص القضائي الدولي في مكافحة الجريمة	122
البند الثاني: موقف المشرع الجزائري من مسالة الاختصاص الدولي والمحلي	124
الفرع الثالث: التحديات الإجرائية ذات الصلة بتقدير الدليل الرقمي	126
البند الأول: مفهوم الدليل الرقمي	126
البند الثاني: شروط صحة الدليل الالكتروني	128
البند الثالث: ضمانات حرية القاضي في الأخذ بالدليل التقني	129
الفرع الرابع: التحديات ذات الصلة بالتعاون الدولي لمكافحة جرائم المساس بأنظمة المعالجة الآلية للمعطيات	130
البند الأول: المساعدة القضائية الدولية وتحدياتها	130
البند الثاني: تسليم المجرمين المعلوماتيين	132
الخاتمة	136
قائمة المصادر والمراجع	

ملخص

مست الثورة المعلوماتية كافة أوجه النشاط الإنساني، وقد نتج عن إساءة استخدامها العديد من الجرائم المستحدثة ، يذكر منها الجريمة الماسة بأنظمة المعالجة الآلية للمعطيات، الأمر الذي حتم على المشرع الجزائري – أسوة بالتشريعات المقارنة– العمل على تبني حماية جزائية لدرء هذه المخاطر وهذا في الشقين الموضوعي والاجرائي، وتجلى ذلك باستحداث مجموعة من القوانين العقابية الردعية وكذا إرساء جملة من التدابير الاجرائية المستحدثة غبر المألوفة في القوانين التقليدية لتتلاءم مع خصوصية هذه الجريمة التي خلقت عديد التحديات في سبيل مكافحتها، و جعلت التشريع في حالة تأهب دائم.

وهذا ما عالجته هذه المذكرة .

الكلمات المفتاحية :معالجة الية ، معطيات، نظم معلوماتية ،اجرام سيبراني ، دليل رقمي .

Absract

The information revolution has impacted all aspects of human activity, but its misuse has led to new crimes, such as cybercrime involving data processing systems. In response, Algerian legislation, following comparative laws, has adopted criminal protection measures to deter these risks. This includes punitive laws and unconventional procedural measures tailored to the unique nature of these crimes, posing significant challenges for enforcement. Legislation remains vigilant and prepared to address these evolving challenges.

Keywords: automated processing, data, information systems, cybercrime, digital evidence

Résumé

La révolution de l'information a touché tous les domaines de l'activité humaine. Cependant, son mauvais usage a conduit à l'émergence de nombreux crimes innovants, notamment les crimes liés aux systèmes automatisés de traitement des données. En réponse, le législateur algérien, à l'instar des législations comparatives, a œuvré pour adopter une protection pénale afin de prévenir ces risques, tant sur le plan substantiel que procédural. Cela s'est concrétisé par l'introduction de lois répressives dissuasives et la mise en place de mesures procédurales innovantes, non conventionnelles dans le droit traditionnel, afin de s'adapter à la spécificité de ces crimes. Ces défis ont créé une nécessité constante d'ajustement législatif pour lutter efficacement contre ces formes de criminalité. C'est ce que cette note a traité.

Mots-clés : traitement automatisé, données, systèmes informatiques, cybercriminalité, preuves numériques