جامعة عمار ثليجي بالأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

عنوان المذكرة

الحماية الجزائية لأمن المعلومات

مذكرة تخرج ضمن مقتضيات نيل شهادة الماستر

تخصص قانون جنائي والعلوم الجنائية

من اعداد الطلبة :

- سنوسي عبد القادر
- صيافة كريمة

تحت اشراف الاستاذ :

- أ.د بوقرين عبد الحليم

اعضاء لجنة المناقشة:

أ.د تركي محمد السعيد	رئيسا
أ.د بوقرين عبد الحليم	مشرفا و مقررا
أ.د سي الناصر محمد	ممتحنا

السنة الجامعية : 2023-2024

جامعة عمار ثليجي بالأغواط

كلية الحقوق والعلوم السياسية

قسم الحقوق

عنوان المذكرة

الحماية الجزائية لأمن المعلومات

مذكرة تخرج ضمن مقتضيات نيل شهادة الماستر

تخصص قانون جنائي والعلوم الجنائية

من اعداد الطلبة :

- سنوسي عبد القادر
- صيافة كريمة

تحت اشراف الاستاذ :

- أ.د بوقرين عبد الحليم

اعضاء لجنة المناقشة:

أ.د تركي محمد السعيد	رئيسا
أ.د بوقرين عبد الحليم	مشرفا و مقررا
أ.د سي الناصر محمد	ممتحنا

السنة الجامعية : 2023-2024

الاهـــــداء

الحمد لله والصلاة على الحبيب المصطفى وأهله

ومن وفى أما بعد الحمد لله الذي وفقنا لتثمين

هذه الخطوة في مسيرتنا بمذكرتنا هذه ثمرة

الجهد والنجاح بفضله تعالى مهداة إلى الوالدات

الكريمات حفظهما الله

لكل من العائلتين الكريمتين سنوسي و صيافة

التي ساندتنا ولا تزال من الأخوال والخالات

والعموم وإخوة وأخوات ولا ننسى الأبناء ، و

إلى رفقاء المشوار ، إلى دفعة 2024

شكر وتقدير

الحمد لله رب العالمين، والصلاة والسلام على أشرف المرسلين أما بعد: أتقدم بالشكر الجزيل إلى الأستاذ الدكتور بوقرين عبد الحليم المشرف الذي لم يبخل علينا بنصائحه وتوجيهاته، وإلى أعضاء اللجنة المناقشة المحترمين جزاهم الله كل خير

وإلى كافة الزملاء الكرام وإلى كافة الأساتذة

و إلى كافة الطاقم الإداري وإلى كل من شجعنا.

قائمة المختصرات

المختصرات	تعريفها
د . م . ج	ديوان المطبوعات الجامعية
ج . ر . ج . ج	جريدة رسمية للجمهورية الجزائرية
ج	الجزء
ع	العدد
د . ط	دون طبعة
د . س . ن	دون سنة نشر
د . ب . ن	دون بلد نشر
س . ج	السنة الجامعية
ص ص	من صفحة الى صفحة
ق . ا . ج . ج	قانون الإجراءات الجزائية الجزائري
ق . ع . ج	قانون العقوبات الجزائري

مقدمـــة

مقدمـــة:

بظهور شبكة الأنترنت كوسيلة اتصالات عالمية ساهمت في تقارب الشعوب و الثقافات و ما زاد من قيمتها هو ظهور الهاتف المحمول و ما صاحبه من تطور حتى أصبح متعدد الاستعمالات بما في ذلك مميزات الحاسوب خاصة ان كان مرتبطا بشبكة الأنترنت ، و هو بهذا يقدم خدمة جليلة للبشرية ، فيكفي أنه يقدم خدمة اتصالية تواصلية بأي شخص و في أي وقت أيا كان مكانه و على مدار الساعة.

و بالرغم من المزايا المكتسبة بفضل التطور في تقنية المعلومات في شتى المجالات و الميادين إلا أن هذا التطور في ذات الوقت حمل معه بذورا للشر ،المتمثل في المجرم المتميز بخصائص جد خاصة تميزه عن غيره من المجرمين العاديين و هو ما يطلق عليه تسمية المجرم المعلوماتي ، هذا الأخير الذي وجد ضالته التي كان يبحث عنها في تلك التقنية الحديثة للمعلومات التي أتاحت له فرصة إرتكاب الجريمة و الحصول من ورائها على أكبر قدر ممكن من النتائج الإجرامية التي يهدف إليها بأقل قدر ممكن من الخسارة والمخاطرة ، معتمدا على ما يمتلكه من مهارة فنية أو تقنية في هذا الصدد.

إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، استدعى تدخلاً تشريعياً صريحاً سواء على المستوى الدولي أو الداخلي، فدوليا وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي، أما على المستوى الوطني، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال تعديل قانون العقوبات بموجب القانون 15/04 باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه المساس بأنظمة المعالجة الآلية للمعطيات ،ويشمل المواد من (394) مكرر إلى (394) مكرر (7) ، وكذلك تقررت عقوبات.

هذه الاعتداءات تتطلب وجود نظام المعالجة الآلية للمعطيات كشرط مسبق بخلاف الاعتداءات على منتجات النظام، وتكشف عن أهم التحديات القانونية التي تفرضها جرائم المساس بأنظمة الكومبيوتر على النظام المعلوماتي الجزائري بشكل خاص والعالمي بشكل عام، ولتحقيق هذا الهدف يحاول هذا البحث بشكل مجمل تقديم صورة عامة لأبرز التحديات المصاحبة لشبكة الإنترنت، من هذا المنطلق ، سنحاول عمل دراسة عن الحماية الجزائية لأمن المعلومات في هذه المذكرة.

وتتجلى أهمية هذا الموضوع في كونه من المواضيع الحديثة المفروضة على المستوى الوطني والدولي على حد سواء ;

- معرفة تلك المشكلات القانونية التي تواجه دراسة أمن المعلومات ;
- تحليل النصوص القانونية المتضمنة لتجريم الاعتداءات الواقعة على النظام المعلوماتي ;
- تتضح أيضا في مطلب أساسي لدى مستخدمي تكنولوجيا المعلومات وهو ضمان سرية معلوماتهم التي تحتويها النظم المعلوماتية ;
- تناول الجوانب الإجرائية خاصة فيما تعلق بالدليل التقني ومختلف الإجراءات التقليدية والمستحدثة الخاصة بالبحث عن أدلة.

تتمثل أسباب الاختيار في طابعين موضوعي وذاتي :

- الأسباب الموضوعية:

يتمثل في الاهمية العلمية البالغة لموضوع جرائم المعطيات المعلوماتية ، ومحاربة هذه النوع من الجرائم من طرف كل الدول .

- الأسباب الذاتي:

يكمن في الميول الشخصي لدراسة مثل هذه المواضيع، بالإضافة إلى أنو يندرج ضمن تخصصنا.

يمكن تلخيص الاهداف في مجموعة من النقاط أهمها:

- تحديد المقصود بالمعطيات المعلوماتية وذكر مختلف الجرائم المتعلقة بجرائم المعطيات المعلوماتية ;
- معرفة مدى توفيق المشرع الجزائري في إقرار الحماية الجنائية للمعطيات المعلوماتية .

لقد كانت صعوبات الدراسة متمثلة في قلة الوقت، ونقص المصادر الجزائرية دفعني إلى الانتقال إلى جامعات أخرى للحصول على المعلومات ولتكثيف الجهد وإعطاء الأحسن بالإضافة الى رأي استاذ المشرف، والذي في الحقيقة كان حافزا .

- أحمد مسعود ، اليات مكافحة جرائم تكنولوجيات الاعلام والاتصال على ضوء قانون04/09 رسالة ماجستير، بجامعة قاصدي مرباح ورقلة، كلية الحقوق والعلوم السياسية قسم الحقوق سنة 2013 تناول فيها الباحث الجرائم المتصلة بالتكنولوجيات الاعلام والاتصال وآليات مكافحتها.

- نسيمة جدي ، جرائم الماسة بالأنظمة المعالجة الالية للمعطيات، رسالة ماجستير، بجامعة وهران ، كلية الحقوق ، سنة 2014 ، التي تناول الباحث الجرائم الماسة بالأنظمة المعالجة للمعطيات الواردة في القانون العقوبات.

موضوع الحماية الجزائية لأمن المعلومات له جوانب عديدة للدراسة ومن خلال دراستنا هذه بالإضافة إلى تطرقنا إلى انماط الجرائم المعلوماتية، ومعرفة طرق المساس بالأنظمة المعلوماتية والأجهزة المختصة لمكافحتها في هذا الموضوع.

- **الحدود المكانية**

تتمثل في تطرقنا إلى دراسة الحماية الجزائية لأمن المعلومات.

- **الحدود الزمنية**

تم التركيز على الحماية الجزائية لأمن المعلومات حيث أجريت هذه الدراسة في الفترة الممتدة من فيفري إلى جوان 2024.

وبناءا على ما تقدم بعد تحديدنا للاطار المكاني بالجزائر من خلال الاشكالية التالية :

- ما هي التدابير القانونية المتخذة من قبل المشرع الجزائري لحماية الجزائية لأمن المعلومات ؟

وبعبارات اكثر تفصيلا:

- ما هي أبرز الأنماط الإجرامية في مجال المساس بأنظمة الكومبيوتر والإنترنت ؟
- ما هي جرائم وعقوبات الاعتداء على المعطيات الشخصية ؟
- ما دور الاجهزة الخاصة الموضوعة لمكافحة جرائم الأمن المعلوماتي ؟
- وما هي آليات البحث والتحري في جرائم المعلوماتية ؟

اعتمدنا على المنهج الوصفي التحليلي لموضوع البحث، حيث تم إجراء دراسة مكتبية استعرضنا فيها أهم ما يمكن الحصول عليه من دراسات سابقة حول موضوع الحماية الجزائية لأمن المعلومات ويظهر ذلك في التعرض للآراء الفقهية والنصوص القانونية والكتب في المكتبات الافتراضية والاستعانة بالكتب والمجلات وشبكة الانترنت والمعلومات الثانوية، كما قمنا بجمع المعلومات المطلوبة عن أهم ما تطرق اليه المشرع الجزائري.

قسمت الدراسة الى فصلين تناولنا في الفصل الاول الحماية الموضوعية لأمن المعلومات وينقسم هذا الفصل الى تجريم الدخول والبقاء في نظام المعالجة الآلية للمعطيات في المبحث الاول ، ثم

تجريم المساس بالمعلومات في المعالجة الآلية للمعطيات في المبحث الثاني ، ثم في الفصل الثاني الحماية الاجرائية لأمن المعلومات ، حيث تناول هذا الفصل دراسة الأجهزة الخاصة بجرائم الأمن المعلوماتي في المبحث الاول ، ثم آليات التحري في الجرائم المعلوماتية في المبحث الثاني.

الفصل الأول

الحماية الموضوعية لأمن المعلومات

المبحث الأول : تجريم الدخول والبقاء في نظام المعالجة الآلية للمعطيات

المبحث الثاني : تجريم المساس بالمعلومات في المعالجة الآلية للمعطيات

تمهيد

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال جاء القانون رقم 15/04 الصادر في 10 نوفمبر 2004 ، المتضمن قانون العقوبات بتجريم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394 مكرر إلى 394 مكرر 7 ، وتأخذ صور الإعداء صورتين وهما: الدخول والبقاء في منظومة معلوماتية المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش، وهذا ما سنتناوله في المبحث الأول.

إن صور الاعتداء على البيانات الشخصية كثيرة و متعددة و يرجع ذلك إلى التطور الحاصل في مجال تكنولوجيات الإعلام و الاتصال ، لذلك يعمل المشرع على مواكبة هذا التطور من خلال إصدار قوانين تجرم كل سلوك يهدد البيانات و المعلومات الشخصية للفرد وتعاقب على ارتكابه ، فنجده جرم لنا سلوكات بموجب قانون العقوبات. ثم بعد هذا أصدر لنا قانون جديد في 2009 وهو القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من جرائم تكنولوجيات الإعلام و الاتصال و مكافحتها وجرم بموجبه نفس السلوكات المجرمة سابقا و أضاف فيه تجريم سلوكات أخرى ، وصولا بآخر قانون أصدره في هذا الشأن سنة 2018 قانون 07/18 [1] يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي الذي جرم بموجبه كل سلوك من شأنه المساس بسرية وسلامة البيانات الشخصية وهذا ما سنتناوله في المبحث الثاني.

[1] قانون رقم 07/18 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018.

المبحث الأول : تجريم الدخول والبقاء في نظام المعالجة الآلية للمعطيات

تعتبر جريمة الدخول أو البقاء غير المصرح به جريمة عمدية، حيث استعمل المشرع الجزائري عبارة " عن طريق الغش"، واشتراط أن تكون هذه الجريمة عمدية أمر بديهي، كون الواقع اليومي يكشف أن الكثير من عمليات الدخول لنظم المعالجة الآلية للمعطيات والبقاء فيها عمليات روتينية تتكرر بشكل كبير في اليوم الواحد.

المطلب الأول : تجريم الدخول لنظام المعالجة الآلية للمعطيات

جريمة الدخول غير المشروع لنظم المعالجة الآلية للمعلومات ، من أهم الظواهر الإجرامية التي أسفرت عنها التطورات التكنولوجية ،وهي وإن كانت جريمة شكلية، غير أنه في الغالب ما يرتبط بالدخول ارتكاب جرائم أخرى مادية لذا عاقب المشرع على مجرد الدخول لنظم المعالجة الآلية للمعطيات تفاديا للتمادي في الاعتداءات على النظم وما تحتويه من معلومات . وشدد العقوبات في حالة ما إذا ترتب على فعل الاختراق نتيجة مادية ما تتمثل في الإضرار بالمعلومات أو بنظم معالجتها، وذلك بموجب نص المادة 394 [1] مكرر المقابلة لنص المادة 1/313 من قانون العقوبات الفرنسي والمادة 2 من اتفاقية بودابست[2] وسنحاول تفصيل أركان هذه الجريمة من خلال المطالب.

الفرع الأول : مفهوم الدخول الغير مصرح به

يستمد عدم مشروعيته من كونه غير مصرح به وتم دون رضاء من صاحب هذا النظام أو رغما عنه سواء كان الدخول لكل النظام أو لجزء منه فقط، وفي كلتا الحالتين نكون بصدد دخول معنوي لا يتم بالطرق التقليدية ، لذا نجد تعدد محاولات الفقه في تحديد معناه، وهي محاولات ركزت جميعها على أنه ولوج بالطرق المعلوماتية ذو مدلول معنوي يشبه الدخول في ذاكرة الإنسان، ومدلول آخر مادي يتمثل في أن الشخص يكون قد حاول الدخول أو دخل بالفعل إلى النظام المعلوماتي . له

---

[1] المادة 394 مكرر من القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 ، المتعلق بقانون العقوبات والنصوص القانونية الخاصة المتعلقة بالحماية السيبرانية.

[2] شكلت الاتفاقية بودابست لمكافحة الجريمة السيبرانية، خطوة رائدة على مستوى التعاون بين الدول، وهي الوحيدة حتى اليوم، من حيث حجم الدول المنظمة اليها، وترتكز أهمية هذه الاتفاقية بفعاليتها على إقرارها إجراءات عملية، تلتزم الدول المنظمة بإدراجها في قوانينها الوطنية، مثل تلك الخاصة بجمع بيانات الاتصال وحفظها، بما يتيح تحديد مصدرها، وصلاحية الجهات القضائية المعنية، والمساعدة المتبادلة وتسليم المجرمين. والمشرع الجزائري على غرار هذه الدول رغم عدم المصادقة عليها، إلا أنه نهج نهجها وألتزم بتشريعها خاصة بالجانب الموضوعي لمواجهة الجريمة السيبرانية.

دلالتان دلالة المكان وهو التسلل الداخل النظام المعلوماتي ودلالة زمانية وتتمثل في تجاوز وقت وحدود التصريح أو الترخيص بالدخول إن وجد مثل هذا التصريح[1].

ونجد المشرع الجزائري أسوة بالمشرع الفرنسي، قد صاغ النص بطريقة تشمل جميع طرق الدخول الممكنة، دون تحديد طريقة أو وسيلة بعينها. مما يمكن من مواجهة جميع اشكال الاختراق غير المشروع للنظم المعلوماتية مع الإشارة أن هذه الجريمة تعد جريمة وقتية لها آثارا مستمرة، وفي ذات الوقت جريمة شكلية لا يتطلب فيها تحقق ضرر معين، كما لا يشترط فيها صفة معينة في الشخص الذي قام بهذا الدخول[2].

الفرع الثاني : مفهوم عدم التصريح بالدخول

التصريح بالدخول يثير مسألة هامة عن إعطاء التصريح. فإن التصريح يجب أن يمنحه الشخص المسؤول أو المسيطر أو المالك لتنظيم النظام المعلوماتي وإن كان للنظام أكثر من مسؤول واحد، فهنا يكون لكل منهم الحق في منح التصريح لذا فالجريمة التي نحن بصدد دراستها، تقوم في الحالة التي لا يكون هناك فيها تصريح بالدخول بتاتا، أو أن يوجد تصريح بالدخول، ولكن المصرح له يقوم يتجاوز الحدود التي رسمت له في هذا التصريح سواء من حيث الوقت المخصص له أو من حيث تجاوز الغرض الذي لأجله منح الترخيص[3].

الفرع الثالث : منظور المشرع الجزائري للدخول

تنص المادة 394 [4] مكرر من قانون العقوبات على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الألية للمعطيات أو يحاول ذلك، وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فإن العقوبة تضاعف، فالصورة البسيطة للجريمة

[1] خالد ممدوح إبراهيم ، أمن الجريمة الالكترونية ، الدار الجامعية، الإسكندرية ، مصر، 2008 ، ص84.

[2] محمد حماد مرهج الهيتي ، جرائم الحاسوب ماهيتها موضوعها وموقف التشريعات الجنائية منها، دار المناهج للنشر والتوزيع، عمان، الأردن، ط 1 ، 2006 ، ص 182.

[3] جلال الزعبي ، صايل فاضل الهواوشة ، جرائم الحاسب الآلي والإنترنت ، دار وائل للنشر، عمان ، الأردن ، ص231.

[4] المادة 394 مكرر من القانون رقم 15/04.

تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام[1].

فيجب على الجاني أن يدرك أنه يدخل بصورة غير مشروعة إلى نظام معالجة يخص الغير أو جزء منه، وأنه لا يحق له الدخول إلى هذا النظام، أي معرفته بأنه ولج أو دخل في نظام المعالجة الآلية ضد رغبة صاحب النظام وأيا كان الدافع إلى ذلك، مع انصراف إرادته إلى ارتكاب ذلك الفعل الإجرامي.

لقد جرم المشرع فعل الدخول بطريق غير شرعية إلى أي منظومة معلوماتية دخولا غير شرعي وذلك حين عبر عنه بطريق الغش ، كما أن المشرع لم يفرق بين الدخول إلى جزء من المنظومة أوكلها[2].

وهنا سيتخلص من نص المادة ما يلي:

- التسليم بتوفير القصد الجنائي بمجرد الدخول إلى نظام معلوماتي عن طريق الغش.
- عدم الاعتداد بنتائج هذا الدخول حتى ولو يسبب أي تخريب أو إضرار بالبيانات، لكون اعتبارها جريمة وقتية.
- مجرد المحاولة يعتبر في حد ذاته جريمة حتى وان لم يتحقق فعلا[3].

يفهم من نص المادة أيضا ، أن الجزاء عن مثل هذه المخالفات يكون بمجرد تحقق الركن المادي للجريمة، والذي يكمن في فعل الدخول، وطبعا هنا يكون الدخول باستعمال الوسائل الفنية والتقنية للنظام المعلوماتي، وبغض النظر إن كان الدخول إلى النظام بأكمله أو إلى جزء منه فقط.

كما يفهم من البند نفسه أن المشرع لا يعاقب على الفعل الكامل، أي على الجريمة التامة، وانما يوقع العقاب حتى على مجرد المحاولة أي الشروع في الجريمة بغض النظر عن تحقيق النتيجة الإجرامية، وهو ما أدى بالبعض إلى الإقرار أن هذه الجرائم من قبيل الجرائم الشكلية، التي لا تشترط لقيامها تحقق النتيجة الإجرامية، والشرط الوحيد في البند هو أن يكون الدخول إلى نظام المعالجة الآلية

---

[1] حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب ، جامعة باتنة، 2012 ، ص 46.

[2] أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، ط 2 ، الجزائر، 2007 ، ص10.

[3] سعيدة بكرة ، الجريمة الإلكترونية في التشريع الجزائري دراسة مقارنة مذكرة مكملة مقدمة لنيل شهادة الماجستير في الحقوق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016 ، ص52 .

للمعطيات عن طريق الغش، أي لن يكون مشروعا، كالدخول من دون وجه حق أو من دون ترخيص مسبق، بمعنى ألا يكون الدخول صدفة أو خطأ[1].

وتجدر الإشارة هنا، إلى أن المشرع الجزائري لم يشترط في البند أعلاه، طبيعة خاصة لهذا النظام أي أن المادة 394 مكرر[2] لم تشترط لتحقق جريمة الدخول غير المرخص به إلى نظام المعالجة أن يكون هذا النظام محاطا بحماية فنية تمنع الاختراق، بل جاءت عامة ومطلقة وتحمي كل الأنظمة المعلوماتية، وبدون أي استثناء.

وبذلك يكون مشرعنا قد أصاب بشكل كبير في تنظيمه لهذه المسألة، حيث وبتمييز المشرع بين تجريم الدخول غير المرخص به إلى نظام معلوماتية محاط بحماية فنية وعدم التجريم للدخول غير المرخص به إلى نظام غير محاط بحماية فنية، سيؤدي حتما إلى فتح المجال للمجرمين من التهرب من المسؤولية الجزائية عن فعل الاعتداء، بحجة أن النظام المعتدى عليه غير محاط بحماية فنية وبذلك، فيكون المشرع قد أحسن فعلا عندما لم يفصل بين النظام المحاط بالحماية الفنية، وذلك النظام غير المحاط بها[3].

[1] نسمة بطيحي ، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي ، مجلة الفقه القانوني والسياسي، م 1، ع 01 ، جامعة سطيف، 2015، ص 07.

[2] المادة 394 مكرر من القانون رقم 15/04.

[3] أمال قارة ، المرجع السابق ، ص 31.

المطلب الثاني : تجريم البقاء لنظام المعالجة الآلية للمعطيات

الصورة الثانية من صور السلوك الإجرامي للجريمة التي نحن بصدد دراستها في البقاء غير المصرح به في النظام ، لذا ستحاول تناول المقصود بالبقاء غير المصرح به، ومن ثم النظر ما إن كان البناء متلازما مع الدخول ، أم أن كل منهما جريمة مستقلة.

الفرع الأول : البقاء غير المصرح به

بالرجوع إلى المادة 394 [1]وفي الفقرة 1 فان المشرع قد فرق بين فعل الدخول غير الشرعي والبقاء فيه ، وذلك باعتبار كل فعل يعتبر مجرما ، فالبقاء قرينة على توفر القصد الجنائي كما تعتبر جريمة مستمرة ، على عكس الجريمة الأولى، غير أن المشرع لم يفرق بين البقاء غير الشرعي أو مجرد المحاولة على غرار الجريمة الأولى.

فالمقصود بالبقاء غير المصرح به لم يتطرق المشرع الجزائري ولا المشرع الفرنسي المعنى البقاء لذا نجد الفقه قد تصدى لبحث هذه المسألة، وتعددت تعريفاته ، غير أنها في مجملها تركز على أن البناء هو أن يكون الجاني قد دخل النظام عن طريق الصدقة أو الخطأ ، ومن بعدها يقرر البقاء داخله وعدم قطع الاتصال به ، وبالتالي هي جريمة سلوك إيجابي يتحقق بالترك أو الامتناع، كما أنها جريمة مستمرة.

الفرع الثاني : ضرورة التلازم بين فعلي البقاء والدخول

البقاء يتكون أصلا من فعلين أن يكون هناك دخول والفعل الثاني وهو البقاء بعد هذا الدخول، أي أن تتجه إرادة الجاني إلى عدم قطع الاتصال بالرغم من علمه أنه داخل نظام ممنوع عليه الدخول إليه لكن استعمال المشرع المصطلحي الدخول والبقاء معا يعني أن كل دخول غير مصرح به يترتب عليه بناء غير مشروع لكننا نرى أن كل جريمة مستقلة عن الأخرى، ولكل منهما سلوكيا الخاص، خاصة وأنه سبق القول أن إحداهما جريمة مؤقتة والأخرى جريمة مستمرة، وبالتالي فيما من طبيعتين مختلفتين[2].

---

[1] المادة 394 من القانون رقم 15/04.

[2] بوكر رشيدة ، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن ، رسالة انيل شهادة ماجستير في الحقوق، دمشق، سوريا، 2010، ص 94.

ويقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول في النظام وقد يجتمعان، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ، وهنا يجب على المتدخل أن يقتطع وجوده داخل النظام وينسحب، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع، ويكون البقاء جريمة في الحالة التي يطبع ، الشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الاطلاع فقط، ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية والتي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على مدة أطول من المدة التي دفع مقابلها، ففعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد، وذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية[1].

الفرع الثالث : الركن المادي في جريمة البقاء

ويتحقق في النظام كذلك إذا اتخذ صورة البقاء داخل النظام، ويقصد بفعل البقاء : "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام"[2] ، ومما لا شك فيه أن البقاء داخل نظام الكمبيوتر بعد دخوله عن طريق الخطأ لا يختلف عن الدخول غير المصرح به من حيث وجوب التجريم، فاتجاه إرادة الفاعل إلى البقاء داخل هذا النظام على الرغم من معرفته أنه غير مصرح له بالدخول، لا يختلف في جوهره عن الدخول غير المصرح به إلى نظام الكمبيوتر فالنتيجة الإجرامية في الحالتين واحدة وهي الوصول إلى نظام غير مصرح للدخول إليه، فالمصلحة التي يحميها القانون هي حماية نظام الكمبيوتر في الحالتين[3]، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا ، وذلك في الفرض الذي لا يكون فيه الجاني له الحق في الدخول إلى النظام ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك ، ويتحقق في هذا الفرض الاجتماع المادي لجريمتي الدخول والبقاء غير المشروع في النظام[4].

---

[1] حمزة بن عقون، المرجع السابق ، ص 184.

[2] علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية ، القاهرة ، 2009 ، ص 133.

[3] نائلة محمد فريد قروة ، جرائم الكمبيوتر الاقتصادية ، منشورات حلبي ، ط 1، بيروت، 2005، ص346 .

[4] علي عبد القادر القهوجي، المرجع السابق ، ص 134.

المبحث الثاني : تجريم المساس بالمعلومات في المعالجة الآلية للمعطيات

إن تفاقم الاعتداءات على الأنظمة المعلوماتية خاصة مع ضعف الحماية الفنية، استدعى تدخلا تشريعيا صريحا سواء على المستوى الدولي أو الداخلي، فدوليا وضعت أول اتفاقية حول الإجرام المعلوماتي بتاريخ 2001/11/08 تضمنت مختلف أشكال الإجرام المعلوماتي، أما على المستوى الوطني، فقد استدرك المشرع الجزائري الفراغ القانوني من خلال تعديل قانون العقوبات بموجب القانون 15/04 الصادر في 10 نوفمبر2004 باستحداث القسم السابع مكرر ضمن الفصل الثالث من الباب الثاني من الكتاب الثالث عنوانه المساس بأنظمة المعالجة الآلية للمعطيات، ويشمل المواد من 394 مكرر إلى 394 مكرر 7.

المطلب الأول : تجريم المساس بنظام المعالجة الآلية في قانون العقوبات

الحماية الجنائية للمعطيات الإلكترونية في إطار قانون العقوبات، الجرائم الماسة بالأنظمة المعلوماتية وإن كانت تختلف في أركانها وعقوباتها، إلا أن ما يجمعها أنها تحقق حماية جزائية تنظم المعالجة الآلية للمعطيات أي أن القاسم المشترك بينهما هو نظام المعالجة الآلية.

الفرع الأول : جريمة حذف أو تغيير في معطيات المنظومة

تنص المادة 394 مكرر في فقرتها الثانية على أنه " تضاعف العقوبة إذا ترتب على ذلك حذف أوتغيير لمعطيات المنظومة " وعليه فان المشرع الجزائري فرق بين عملية حذف البيانات وعملية تغييرها اللذين يعتبرهما كنتيجة لفعل الدخول غير الشرعي أو البقاء كما اعتبرهما جريمة مضاعفتين وذلك نتيجة لخطورة النتائج المترتبة عنهما.

الفرع الثاني : جريمة تخريب نظام الاشتغال

نصت المادة 394 مكرر 3 [1] على أنه " وإذا ترتب على الأفعال المذكورة أعلاه تخريب اشتغال المنظومة تكون العقوبة الحبس من 6 أشهر إلى سنتين والغرامة من 50.000 دج إلى 150.000 دج "وعلى أساس ذلك لم يعتبر المشرع الجزائري جريمة تخريب نظام الاشتغال جريمة مستقلة بذاتها على غرار الدخول غير الشرعي أو البقاء ، بل باعتبارها نتيجة للجرائم السابقة، وذلك يرجع إلى أنه من الممكن حدوث تخريب لهذا النظام ابتداء دون توفر القصد الجنائي إلا عندما يكون كنتيجة لجريمة سابقة.

[1] المادة 394 مكرر 3 من القانون رقم 15/04.

الفرع الثالث : جريمة إدخال معطيات في نظام المعالجة الآلية أو إزالتها أو تعديلها عن طريق الغش

نصت المادة 394 مكرر 01 من قانون رقم 15/04 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش .هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط لكي يتوافر الركن المادي، و أفعال الإدخال والإزالة و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل كما أن هذا السلوك يجسد فعل التخريب و إفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها[1].

نصت المادة 394 مكرر 1 [2]على أنه "يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 500.000 إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أوأزال أو عدل " ومنه فان المشرع قد اعتبر أن إدخال معطيات مغشوشة في نظام المعالجة الآلية جريمة معلوماتية تستوجب عقوبة ، والتي ضاعفها إذا ما قورنت بالعقوبات السابقة ، واذا كان قد ربط فعل الحذف بالنتيجة المترتبة عن الدخول غير الشرعي أو البقاء ، فقد اعتبر جريمة الإزالة جريمة مستقلة في حد ذاتها تستوجب نفس العقوبة السابقة بالرغم من اتفاقية بودابست وكذا المشرع الفرنسي استعمل مصطلح "الحذف " لاستخدامه ضمن نفس المعنى.

وان ذهبنا إلى المعنى اللغوي فان معنى الحذف هو الإسقاط بينما يعني مصطلح الإزالة هو الإبعاد من المكان ، ومنه فان المشرع قد يكون فرق في الآثار بين الفعلين ، فحذف بيانات الكترونية معينة بكون بإسقاطها من موقعها في النظام المستهدف ، ولو كان بصفة مؤقتة ، مما يعني ظرفيتها وبذلك تكون قابلة للاسترجاع عن طريق برامج خاصة Logiciel de récupération de données électroniques بالرغم من صعوبتها، ولكن إزالة البرامج تهدف إلى التخلص نهائيا منها وبشكل

[1] حمزة بن عقون، مرجع سابق، ص184 .

[2] المادة 394 مكرر 1 من القانون رقم 15/04.

كامل ، لذلك يكون المشرع قد فرق بين الفعلين الإجراميين واعتبر الفعل الأخير أشد وطأة ، لذا فرق بين عقوبة كل فعل مجرم منهما.

الفرع الرابع : جريمة تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات عمدا وعن طريق الغش

جرمت المادة 394 مكرر 02 [1] من قانون العقوبات الأعمال الأتية : تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب إحدى جرائم الغش المعلوماتي ، ويقصد بتصميم المعطيات هنا الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية، أو المعطيات المعلوماتية في حد ذاتها [2]، كما جرم المشرع كذلك أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لأي غرض[3].

عن طريق الغش ،تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أومعالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم " ، وعليه فإننا نكون أمام توفر عدة شروط لقيام هذه الجريمة المعلوماتية ، وهي:

1. توفر القصد الجنائي لدى الجاني :

في هذه الحالة ابتداء لأقر المشرع كشرط أساسي لإقرار هذا الفعل المجرم توفر القصد الجنائي لارتكابه، لان علمية تصميم برنامج معين أو بحث في برنامج معين آخر أو نشره وحتى الاتجار فيه لا يعتبر جرما في حد ذاته ، إذا لم يسبقها توفر نية مسبقة لارتكاب جريمة معلوماتية تعتمد بالأساس على توفر علم مسبق لدى الجاني بان هذا البرنامج مغشوش.

2. أن يكون هذا الجرم مرتبطا بأفعال محددة وهي :

تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في المعطيات، وعليه فان أي فعل آخر يمس هذه المعطيات لا يندرج ضمن هذا الإطار.

---

[1] المادة 394 مكرر 2 من القانون رقم 15/04.

[2] دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منثوري، قسنطينة، 2013، ص 55.

[3] حمزة بن عقون، مرجع سابق، ص184 .

3. أن تكون المعطيات محل الجرم مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية :

وهنا يكون المشرع قد اعترف ضمنا بضرورة أن تكون المعطيات تتوفر على قدر كاف من الحماية لأن المساس بالمعطيات المتاحة والمتوفرة للجمهور لا يمكن أن تكون محل متابعة جزائية ، وبذلك يكون المشرع قد تأثر بالاتفاقيات والقانون المقارن الذي سعى إلى هذا الاتجاه لاسيما اتفاقية بودابست.

كما يمكن إن يكون هذه الجرائم سببا غير مباشرا في ارتكاب الجرائم المعلوماتية السابقة، وعليه فان المشرع قد قرر لها نفس العقوبة السابقة.

يتضح بأن لهذا النمط من الجرائم طبيعة خاصة ومتميزة، وهي جريمة ناعمة حال ارتكابها، تتجاوز حد الخشونة في نتائجها، إذ بمجرد ملامسة الجاني لزر أو أكثر من لوحة المفاتيح، قد ترتكب أخطر الجرائم في بضعة ثواني، ودون التقاء بين الجاني والمجني عليه، وهذا ما يؤدي إلى صعوبة في مكافحتها.

الفرع الخامس : جريمة حيازة أو إفشاء أو نشر أو استعمال معطيات المتحصل عليها من الجرائم المذكورة سابقا عمدا وعن طريق الغش

المادة 394 مكرر 2 [1] الفقرة الثانية أقرّ المشرع جرمية الافعال المذكورة سابقا ، فان حيازة معطيات أو إفشائها أو نشرها أو استعمالها يعتبر جريمة يعاقب عليها القانون.

يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000دج كل من يقوم عمدا وعن طريق الغش بما يأتي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

[1] المادة 394 مكرر 2/2 القانون رقم 15/04.

المطلب الثاني : تجريم المساس بنظام المعالجة الآلية للمعطيات في قانون حماية المعطيات ذات الطابع الشخصي

سارعت التشريعات الحديثة إلى إعادة النظر في أنظمتها القانونية بإصدار نصوص خاصة بتنظيم عمليات المعالجة لتلك المعطيات و معاقبة مخالفيها بل تعدى الأمر لإعادة النظر حتى في المفهوم العام لحرمة الحياة الخاصة كمبدأ دستوري ، بحيث تم إدراج المعطيات الشخصية كجزء لا يتجزأ من مقوماتها إذ أشارت إليها الفقرة الأخيرة من المادة 46 من التعديل الدستوري لسنة 2016[1].

الفرع الأول : جريمة معالجة المعطيات ذات ط ش رغم عدم موافقة الشخص المعني

من بين أهم مظاهر احترام حق الإنسان في إبداء الرأي وحريته في التعبير، لذلك فإن أي عملية معالجة للمعطيات ذات الطابع الشخصي يجب أن تسبقها موافقة صريحة تصدر عن أصحاب العلّقة وبذلك فإن أي تجاوز لهذا الالتزام جريمة تقع بالمخالفة لأحكام المادة 07 و 36 من القانون 07/18 إذ ألزمتنا المادة الأولى على ضرورة الحصول على الموافقة الصريحة من طرف الشخص المعني للقيام بمعالجة معطياته الشخصية، أي أخضعت معالجة المعطيات الشخصية إلى ضرورة الحصول على الموافقة الصريحة للشخص المعني ، أما المادة الثانية فقد منحت للشخص المعني حق الاعتراض على ذلك إذا ما توفرت أسباب مشروعة، ولممارسة هذا الحق فقد ألزم المشرع الجزائري في المادة 32 [2] بضرورة اعلام الشخص المعني بكل عملية تجميع للمعطيات تخصه، سواء كان الجمع لديه أو لدى الغير[3].

---

[1] القانون رقم 01/16 المؤرخ في 06 مارس 2016 ، الجريدة الرسمية رقم 14 المؤرخة في 7 مارس 2016.

المادة 46 : لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون.

-سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

-لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا الحكم.

-حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه.

[2] المادة 07 و 32 و 36 من قانون 07/18، المصدر السابق.

[3] طباش عز الدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل قانون 07/18 المتعلق بحماية الاشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، ع 02 ، 2018 ، ص 38.

أما إذا تعلق الأمر بمعالجة المعطيات الحساسة ، القاعدة العامة أنه لا يجوز معالجتها وذلك وفق لنص المادة 18 فقرة أولى[1]، لكن نجد أن نفس المادة قد نصت على استثناء على القاعدة العامة القائلة بعدم جواز معالجة المعطيات الحساسة إذ يمكن معالجتها إذا وافق الشخص المعني، وفي الحالة الحكمية فإن ذلك سيؤدي إلى قيام الجريمة المنصوص عليها في المادة 57 [2]، إلا أن المشرع نص في نفس المادة على استثناء في حالات كما سبق بيانه يمكن بسببها معالجة المعطيات الحساسة دون الحصول على الموافقة بشرط أن ترخص بذلك السلطة الوطنية لحماية المعطيات الشخصية[3].

هذه الحالات وردت في المادة 18 عندما يتعلق الأمر بالمصلحة العامة وتكون ضرورية لضمان ممارسة المهام القانونية أو النظامية للمسؤول عن المعالجة، كما يمكن منح الترخيص أيضا إذا كانت المعالجة ضرورية لحماية المصالح الحيوية للشخص المعني أو لشخص آخر وعندما يكون في حالة عجز بدني أو قانوني يمنعه من تقديم موافقته ، كما يمكن أيضا إذا كانت المعالجة ضرورية للّاعتراف بحق أو ممارسته أو الدفاع عنه أمام القضاء ، بالإضافة إلى ذلك كانت المعالجة تخص المعطيات الجينية ، باستثناء تلك التي يقوم بها أطباء وبيولوجيون والتي تعد ضرورية لممارسة الطب الوقائي والقيام بتشخيصات طبية وفحوصات أو علّاجات ، ومن أجل ضمان عدم الاعتداء على حق الشخص المعني بالموافقة على معالجة معطياته الشخصية فقد جرم المشرع الجزائري فعل القيام بالمعالجة دون الحصول على موافقته، وكذا في حالة رفضه الصريح عندما يقدم اعتراضا على تلك المعالجة[4].

1. الركن الشرعي لجريمة رغم عدم موافقة الشخص المعني أو اعتراضه :

لقد جرم المشرع الجزائري فعل معالجة المعطيات الشخصية دون موافقة الشخص المعني أو رغم اعتراضه، ضمن نصوص المادتين 55 و 57 من القانون 07/18 إذ جاء في نص المادة 55 منه ما يلي:

"يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من 100.000 ألف دج إلى300.000 دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 7 من هذا القانون" .

---

[1] المادة 18 القانون رقم 15/04.

[2] المادة 57 القانون رقم 07/18.

[3] طباش عز الدين ، مرجع سابق، ص 36.

[4] انظر الفقرة 08 من المادة 03 من القانون 07/18.

ويعاقب بنفس العقوبة كل من يقوم بمعالجة المعطيات ذات الطابع الشخصي رغم اعتراض الشخص المعني، عندما تستهدف هذه المعالجة، لاسيما الإشهار التجاري أو عندما يكون الاعتراض مبنيا على أسباب شرعية."

2. الركن المادي لجريمة رغم عدم موافقة الشخص المعني أو اعتراضه :

السلوك الإجرامي في هذه الجريمة يتمثل في مخالفة أحكام نص المادتين 07 والمادة 36 من القانون 07/18 حيث ألزمت الأولى على ضرورة الحصول على الموافقة الصريحة من طرف الشخص المعني للقيام بمعالجة معطياته الشخصية، وقد اخرج المشرع الجزائري حسب نص المادة سالفة الذكر من دائرة التجريم حالات معينة تتم المعالجة دون موافقة المعني بالأمر، وتتمثل هذه الحالات في احترام التزام قانوني يخضع له المعني بالأمر والمسؤول عن المعالجة، ويعد من هذا القبيل بصفة خاصة ما يفرض من التزامات على صاحب العمل في المجال الضريبي والاجتماعي، لحماية حياة الشخص المعني ، وإذا تعلق الأمر بالمعطيات الحساسة فالمبدأ أنه لا يجوز معالجتها بحسب نص المادة 18 فقره 01 لكن استثناء يمكن ذلك إذا وافق الشخص، وفي الحالة العكسية فإن ذلك سيؤدي إلى قيام الجريمة المنصوص عليها في المادة 57 إلا أن المشرع نص على معالجة هذه المعطيات دون موافقة الشخص المعني إذ صدر ترخيص من السلطة الوطنية وهذه الحالة نصت عليها المادة 18 من القانون 07/18 ، وعليه تتحقق هذه الجريمة بأحد الأفعال التالية:

إجراء معالجة المعطيات ذات الطابع الشخصي بأن يقوم الجاني بأحد الأفعال المكونة لعملية أو أكثر من العمليات المشكلة للمعالجة، والمحدد في المادة 04 [1] والتي تنجز بمساعدة طرق آلية أو بدونها وتطبق على معطيات ذات الطابع الشخصي.

القيام بالمعالجة دون رضا الشخص المعني، يجب أن يكون هذا الرضى معبرا عنه بما لا يترك مجالا للشك عن رضاه عن العملية.

أن لا تتعلق المعالجة بالحالات المنصوص عليها في المادة 12 [2] لا يلزم فيها موافقة الشخص المعني، كما أشارت الفقرة الثانية من المادة 55 من القانون 07/18 جريمة المعالجة للمعطيات الشخصية مع اعتراض صاحبها حيث تتحقق هذه الجريمة حين يستمر المسؤول عن معالجة في

[1] المادة 04 القانون رقم 07/18.

[2] المادة 12 القانون رقم 07/18.

معالجة المعطيات الشخصية التي تخص الشخص المعني على الرغم من اعتراض هذا الأخير، فهو يشكل نوعا من ممارسة الحق في النسيان على شبكة الأنترنت[1].

3. العقوبة المقررة لجريمة رغم عدم موافقة الشخص المعني أو اعتراضه :

لقد وضع المشرع الجزائري لجريمة معالجة المعطيات ذات الطابع الشخصي رغم عدم موافقة الشخص المعني واعتراضه ، عقوبة الحبس من سنة إلى 03 سنوات وغرامة من 100.000 دج إلى 300.000 دج[2] كما قرر عقوبة الحبس من سنتين إلى 05 سنوات وغرامة من 200.000 دج إلى 500.000 دج بالنسبة لجريمة معالجة المعطيات الشخصية الحساسة ، دون إمكانية الاختيار بين عقوبة الحبس وعقوبة الغرامة، نلّحظ هنا أن المشرع الجزائري قد قيد القاضي الجنائي ولم يترك له سلطة تقديرية في توقيع احدى العقوبتين على الجاني بل جمع بين نوعين من العقوبة تمثلت في عقوبة الحبس وعقوبة الغرامة.

كما وضع أيضا المشرع الجزائري إضافة إلى العقوبة الأصلية المقررة لهذه الجريمة عقوبات تكميلية والتي نص عليها ضمن قانون العقوبات [3] ففي مادته التاسعة وتتمثل هذه العقوبات التكميلية في :

- الحجر القانوني.
- الحرمان من ممارسة الحقوق الوطنية والمدنية والعائلية.
- تحديد الإقامة.
- المصادرة الجزئية للأموال.
- منع مؤقت من ممارسة مهنة أو نشاط.
- إغلاّق المؤسسة.
- الإقصاء من الصفقات العمومية.
- الحظر من إصدار الشيكات أو استعمال بطاقات الدفع.
- تعليق أو سحب جواز السفر، نشر أو تعليق حكم أو قرار الإدانة.

[1] انظر الفقرة 08 من المادة 03 من القانون رقم 07/18.

[2] انظر الفقرة 08 من المادة 3 من القانون 07/18.

[3] الأمر رقم 156/66، المؤرخ في 08 يوليو 1966 ، المتضمن قانون العقوبات، جريدة رسمية ع 49 ، المؤرخة في 11 يوليو 1966 ، المعدل والمتمم.

الفرع الثاني : جريمة معالجة المعطيات ذات الطابع الشخصي دون إجرائي التصريح والترخيص المسبق

أخضعت عملية القيام بمعالجة المعطيات الشخصية إلى ضرورة الحصول على التصريح والترخيص من قبل السلطة المخولة لها هذه الصلّاحية وهي السلطة الوطنية لحماية المعطيات الشخصية وقد اعتبرت كذلك المادة 2/56 ، جريمة كل من يقوم بإعطاء تصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له.

1. الركن الشرعي لجريمة معالجة المعطيات دون إجرائي التصريح والترخيص المسبق :

لقد جرم المشرع الجزائري فعل إنجاز معالجة المعطيات التي تحمل الطابع الشخصي غير مصرح بها أو غير مرخص بها، أي دون تصريح ولا ترخيص مسبقين ، وذلك بموجب نص المادة 56 [1] يعاقب بالحبس من سنتين إلى خمس سنوات ، وبغرامة من 200.000 دج إلى 500.000 دج كل من ينجز أو يأمر بإنجاز معالجة معطيات ذات الطابع الشخصي دون احترام الشروط المنصوص عليها في المادة 12 [2] من هذا القانون ، ويعاقب بنفس العقوبات كل من قام بتصريحات كاذبة أو واصل نشاط معالجة المعطيات رغم سحب وصل التصريح أو الترخيص الممنوح له.

وجاء في نص المادة 51 من القانون 07/18:

دون الإخلال بالعقوبات الجنائية، يمكن للجنة الوطنية حسب الحالات وبدون أجل سحب توصيل التصريح أو الإذن إذا تبين بعد إجراء المعالجة موضوع التصريح أو الإذن المنصوص عليهما في المادة 12 من هذا القانون، أن هذه المعالجة تمس بالأمن أو النظام العام أو منافية للأخلاق أو الآداب العامة.

2. الركن المادي لجريمة معالجة المعطيات دون إجرائي التصريح والترخيص المسبق :

يتمثل الركن المادي لهذه الجريمة طبقا لنص المادة 56 من القانون 07/18 في السلوك الإجرامي لكل من قام بإنجاز معالجة للمعطيات الشخصية أو أمر بذلك، أي القيام بناء أو إنشاء معالجة

[1] المادة 56 من القانون رقم 07/18.

[2] المادة 12 من القانون رقم 07/18.

بالمخالفة لشروط المادة 12 من القانون 07/18 سواء كانت المعالجة آلية أو يدوية وسوى كان مرتكب الجريمة شخصا طبيعيا أو معنويا أو خاصا[1].

اذا نصت المادة 70 من القانون 07/18 بأن عقابه يتم وفق القواعد العامة لقانون العقوبات والقاعدة في المادة 51 مكرر من هذا القانون أن الأشخاص المعنوية العامة تستثني من تحمل المسؤولية الجزائية، لذلك يجب أن يقع على الموظف مباشرة كشخص طبيعي الذي قام بالمعالجة أو المسؤول عن الإدارة التابعة لشخص المعنوي العام، خاصة إذا كان هو الآمر بالمعالجة، فاذا تعلق الأمر بوزارة معينة، وزارة العدل مثلّ فإن الوزير هو الذي يتحمل المسؤولية الجزائية باعتباره الآمر بالمعالجة بدرجة أولى من جهة، وباعتباره المسؤول عن أعمال تابعيه وفق مبدأ افتراض أن يكون حريصا على كل ما يجري في الإدارة التي ترأسها.

3. الركن المعنوي لجريمة معالجة المعطيات دون إجرائي التصريح والترخيص المسبق :

إن جريمة معالجة المعطيات الشخصية دون إجرائي التصريح والترخيص من الجرائم العمدية التي تشترط لقيامها القصد الجنائي العام بعنصريه العلم والإدارة.

فمن خلّال نص المادة 56 من القانون رقم 07/18 فإن هذه الجريمة يكفي لثبوتها انعدام التصريح أو الترخيص أو استعمال تصريح أو ترخيص مسحوب وبالتالي فهي جريمة مادية يفترض فيها العلم والإرادة.

4. العقوبة المقررة لجريمة معالجة المعطيات دون إجرائي التصريح والترخيص المسبق :

على الرغم من الخطورة التي تحملها هذه الجريمة على حقوق حريات الأشخاص معالجة معطياتهم الشخصية دون تصريح أو إذن يأذن بذلك.

المشرع الجزائري فقد وضع لهذه الجريمة طبقا لنص المادة 56 من القانون 07/18 فقد وضع عقوبة الحبس التي تتراوح بين سنتين إلى 05 سنوات ، بالإضافة إلى عقوبة الغرامة التي تتراوح بين 200.000 دج إلى 500.000 دج.

[1] طباش عز الدين ، مرجع سابق ، ص 42.

خلاصة الفصل

لقد حاولنا من خلال الفصل الأول من هذا البحث التطرق إلى الحماية الموضوعية لأمن المعلومات من تجريم الدخول والبقاء في نظام المعالجة و تجريم المساس بالمعلومات في المعالجة الآلية للمعطيات وفي الشق الثاني الأحكام الموضوعية للحماية الجزائية للمعطيات الشخصية.

وخلصنا إلى أنه بالرغم من ما للثورة المعلوماتية من ايجابياتها وقدرتها على تغيير أوجه الحياة إلى الأحسن والأفضل، إلا أن هذه الثورة المعلوماتية ذاتها تحمل في طياتها أيضا العديد من السلبيات التي تتمثل في الاستخدام غير المشروع لنظم الحاسب الآلي، ومن هذا المنطلق استطاع الجناة تطوير طرق الإجرام على نحو عال من التقنية في بيئة تكنولوجيا المعلومات، رأينا كيف أن المشرع الجزائري لا يتوفر على آليات قادرة على الاضطلاع بالآثار الخطيرة التي ترتبها جرائم المساس بأنظمة المعالجة الآلية للمعطيات سواء على مستوى النصوص التشريعية أو على مستوى طبيعة الكوادر والأجهزة المتخصصة لمواجهة هذا النوع من الإجرام.

الفصل الثاني

الحماية الاجرائية لأمن المعلومات

المبحث الأول : الأجهزة الخاصة بجرائم الأمن المعلوماتي

المبحث الثاني : آليات التحري في الجرائم المعلوماتية

تمهيد

الجريمة المعلوماتية يرتكبها جناة ذوي صفات معينة أهمها الدراية الفنية بعمل الحاسب الآلي وكلها تقدم الجاني في فهم تكتيك العمل في الحسابات الآلية، وكيفية تصميم البرامج كلما استطاع أن يرتكب جريمته دون أن يتم الاهتداء إليه، لأنه لا يترك أي آثار يمكن أن يستدل عليه من خلالها، هذا ما يصعب على المحققين الكشف عن هاته الجرائم والقاء القبض على مرتكبيها وللتعرف أكثر على الأجهزة الخاصة بجرائم الأمن المعلوماتي و الآليات والإجراءات التي تتخذ للكشف عن هذه الجريمة تم التطرق في المبحث الأول الى الأجهزة الخاصة بجرائم الأمن المعلوماتي وفي المبحث الثاني آليات التحري في الجرائم المعلوماتية.

المبحث الأول : الأجهزة الخاصة بجرائم الأمن المعلوماتي

تعتبر الأجهزة الخاصة بجرائم الأمن المعلوماتي وعلى رأسها جهاز الضبطية القضائية صاحب الولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها واشكالها، غير أن ذلك لا يمنع أن تعهد بعض القوانين الخاصة بهذا الدور على سبيل الاستثناء الى بعض الجهات والهيئات الخاصة بحكم خبرتها في مجال معين وباعتبارها الأقدر من غيرها على كشف الجرائم الواقعة ضمن حدود اختصاصها الفني أو التقني، والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال الضبط القضائي.

المطلب الأول : الضبطية الخاصة بجرائم الأمن المعلوماتي

إن مقتضيات تطبيق مبدأ الشرعية تقتضي إرساء مجموعة قواعد إجرائية تخضع لها السلطة القضائية وأعوانها حتى يستطيع رجال الضبط القضائي ممارسة إجراءات خاصة تتوافق وطبيعة الجرائم المعلوماتية التي لا يمكن بأي حال من الأحوال البحث والتحري فيها بالأساليب التقليدية.

أشارت المادة 50 من القانون 07/18 إلى أن للسلطة الوطنية الاستعانة بضباط وأعوان الضبطية القضائية بغية المعاينة والتحري، تحت إشراف وكيل الجمهورية المختص إقليميا.

ومن أجل إشراك مزودي خدمات الأنترنت والاتصالات الثابتة والمتنقلة في محاربة الجرائم الالكترونية يلزم القانون[1] 04/09 هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها.

الفرع الأول : تشكيل الضبطية القضائية

إن أعضاء الضبطية موظفون منحهم القانون صفة الضبطية القضائية مكلفون خلال مرحلة التحقيق التمهيدي بالكشف عن وقوع الجريمة وجمع الاستدلالات عنها وعن المساهمين فيها باعتبارهم فاعلين أصليين وشركاء فيها ليتم تحرير محاضر بشأنها وتقديمها أمام الأجهزة المختصة.

[1] قانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

ويقصد بهم جميع الموظفين الذين خولهم القانون مباشرة إجراءات التحري وهؤلاء الموظفون يستمدون صفتهم واختصاصهم من نص القانون ومن ثم كان بيان المشرع لهم بيانا واردا على سبيل الحصر[1].

وقد حدد لنا القانون الإجراءات الجزائية الجزائري أهداف الضبطية القضائية وتتمثل في[2]:

- ضباط الشرطة القضائية.
- الموظفون والأعوان المنوط بهم قانون بعض مهام الضبط القضائي.

1. ضباط الشرطة القضائية :

يتمتع بصفة ضابط الشرطة القضائية حسب القانون الإجراءات الجزائية الجزائري.

- رؤساء المجالس الشعبية البلدية.
- ضباط الدرك الوطني.
- الموظفون التابعين للأسلاك الخاصة والمراقبين ومحافظي وضباط الشرطة للأمن الوطني.
- ذو الرتب في الدرك، ورجال الدرك الذين أمضوا في سلك الدرك 03 سنوات على الأقل والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني بعد موافقة لجنة خاصة[3].
- مفتشو الأمن الوطني الذين قضوا في خدمتهم بهذه الصفة 03 سنوات على الأقل وعينوا بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية بعد موافقة خاصة.

ويتبين من خلال نص المادة أن هناك 03 فئات ممن يتمتعون بصفة ضباط الشرطة القضائية وهي:

- **الفئة الأولى:**

هي الفئة التي تتمتع بصفة ضباط الشرطة القضائية بحكم القانون وهم رؤساء المجالس الشعبية البلدية وضباط الدرك الوطني ومحافظو وضباط الشرطة القضائية.

[1] خراشي عادل عبد العالي، ضوابط التحري والاستدلال عن الجرائم، دار الجامعة الجديدة للنشر، الاسكندرية، 2006 ، ص 107.

[2] المادة 14 من قانون إجراءات الجزائية المعدل والمتمم بموجب الأمر 02/15 ج ر، ج.ج.د.ش، العدد 40 .

[3] المادة 15 من قانون إجراءات الجزائية المعدل والمتمم بموجب الأمر 02/15 .

- **الفئة الثانية:**

هي الفئة التي يجب لكي تتمتع بصفة ضباط الشرطة القضائية تعيينهم بقرار مشترك من وزير الدفاع ووزير العدل لمصالح الأمن العسكري في الملفات.

- **الفئة الثالثة:**

وهي الفئة التي لا تخول لها صفة الضبطية إلا بعد تجاوز امتحان وموافقة لجنة خاصة وتعيينهم بقرار مشترك أما وزير الدفاع ووزير العدل (ذوي الرتب في الدرك والدركيين الذين قضوا في الخدمة 03 سنوات) أو وزير الداخلية ووزير العدل (مفتشي الأمن الوطني) والضباط التابعين للقطاع العسكري الذين تم تعيينهم بموجب قرار مشترك بين وزير العدل.

2. أعوان الضبط القضائي :

وقد حددهم قانون الإجراءات الجزائية في المادة 19:

موظفي مصالح الشرطة وذو الرتب في الدرك الوطني والدركيين ومستخدمو مصالح الأمن العسكري (الملفات) الذين بيس لهم ضباط شرطة قضائية.

والموظفون والأعوان المكلفون ببعضهم مهام الضبط القضائي وقد حددتهم المادة 21 **و** 27[1] وهم:

- المهندسون والأعوان، الفنيون، التقنيون، المختصون في الغابات وحماية الأراضي واستصلاحها.
- رؤساء الأقسام والأعوان التقنيون في الغابات وحماية الأراضي الذين حددتهم المادة 23 يجوز أثناء ممارستهم مهامهم أو يطلبوا مساعدة القوة العمومية.
- موظفون وأعوان الإدارات والمصالح العمومية الذين يباشرون بعض مهام الضبط الفضائي.
- الولاية (المادة 28 من قانون الإجراءات الجزائية)

الفرع الثاني : تحديات عمل الضبطية القضائية في حماية البيانات

إن جهاز الضبطية لم يسلم هو الآخر من تحديات هذه المرحلة وما تتطلبه من تمرس واحاطة شاملة بالتقنية العالية الآخذة في التطور، ذلك أن المعالجة غير مرتبطة بحيز جغرافي محدد، حيث يمكن أن تقع في زمن معين دون الارتباط بإقليم دولة معينة ودون اعتبار لتقارب المسافات أوتباعدها

[1] المادة 21 و27 من قانون إجراءات الجزائية.

مادامت تتم عبر شبكة الانترنت العالمية[1] ، ولذلك ينبغي التنسيق بين الدول لحد من امتدادها بتبني تشريعات دولية بإشراف الأمم المتحدة وعقد مؤتمرات دولية في هذا لا شأن.

ينبغي مراعاة جوانب شخصية تتمثل فيما يجب أن يتميز به المحقق بمناسبة قيامه بهذه المهمة الدقيقة، حيث ينبغي أن يكون من أهل الاختصاص المتعلق بالمعلوماتية، وبالرغم من أن سلك الضبطية القضائية يضم مثل هؤلاء إلا أنهم ليسوا مدربين على الفهم العميق للقصد الجنائي للفاعل حيث قد يتم الحصول على دليل حول الجريمة المعلوماتية غير أن ذلك ليس مثمرا في إقامة الدعوى العمومية، في مقابل ذلك أن المحققين ذوي الخلفية القانونية لديهم الدرية على استنتاج ما يلزم في إقامة الدليل ويفتقرون للشق التقني من المعلوماتية، وهو ما يفرض ضرورة تكوينهم المستمر بما يتماشى والتقنية الآخذة في التطور[2].

الفرع الثالث : ضوابط عمل الضبطية القضائية في حماية البيانات الشخصية

يتولى هذه المهمة عناصر الضبطية القضائية، على أن تتسم بالمعرفة الشاملة بما يتعلق بالأنترنت وتفاصيل الإعلام الآلي، لأن ذلك قد يكون حجر عثرة أمام الحفاظ على الدليل بل وتدميره من غير قصد، بسبب عدم الدراية الكافية بهذا المجال الواسع والمتطور بطريقة سريعة للغاية تستدعي تحيينا وتكوينا مستمرا لأفراد الضبطية القضائية، وضرورة الحرص على اتباع الإجراءات السليمة والمشروعة من أجل سرعة المحافظة على المعطيات الالكترونية المستخدمة في الجريمة، وعدم تعريض وسائط تخزينها إلى كل ما من شأنه المساس بها كالقوى الكهرومغناطيسية وموجات الميكرويف[3] ، مع الأخذ بعين الاعتبار ضرورة التمييز بين مختلف الأنظمة التشغيلية للوسائط الرقمية وخصائص كل نوع من الملفات، فضلا على الإحاطة بمعطيات الحاسوب والأساليب المتبعة في القيام بالعمل الجنائي ووسائل الحماية المتوفرة ومدى أمانها ، وهو ما يجعل من التكوين المستمر للجانب البشري الساهر على التحقيق أمرا ضروريا وأن يواكب ما يطرأ من تقدم في مجال الرقمنة[4].

---

[1] عاد خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، المجلد 22 ، العدد 86 ، 2012 ، ص252.

[2] خالد ممدوح إبراهيم، الجرائم المعلوماتية ، دار الفكر الجامعي، ط 1 ، الإسكندرية، مصر، 2009، ص135 .

[3] إبراهيم محمود اللبيدي، السلوك الإجرامي في جرائم الانترنت ، مركز الإعلام الأمني ، القاهرة، مصر، 2013 ، ص69.

[4] أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، ط 1 ، الاسكندرية، مصر، 2008 ، ص 271.

المطلب الثاني: هيئة مكافحة الجرائم المعلوماتية

لضمان فعالية هذه الأحكام أحدث المشرع الجزائري من خلال القانون 04/09 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، ونظمها بالمرسوم الرئاسي 261/15[1]، كما جاء القانون بمجموعة من الإجراءات لمكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

عرفيا المشرع الجزائري بموجب المادة 02 [2] ، على أنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي ، توضع لدى الوزير المكلف بالعدل.

وفيما يخص مقر الهيئة الوطنية فقد حددت ذلك المادة 03 [3] والتي تنص على ما يلي:

"يحدد مقر الهيئة بمدينة الجزائر".

الفرع الأول : تشكيلة الهيئة و تنظيمها

تضم التشكيلة البشرية للهيئة 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 للمراقبة الوقائية واليقظة الإلكترونية مديرية التنسيق التقني مركز للعمليات التقنية وملحقات جهوية.

نصت على تشكيلة الهيئة المادة 06 [4] والتي جاء فيها ما يلي:

1. اللجنة المديرة :

- مديرية عامة.
- مديرية للمراقبة الوقائية و اليقظة الإلكترونية.
- مديرية للتنسيق التقني.
- مركز للعمليات التقنية.
- ملحقات جهوية.

---

[1] القانون 261/15 المؤرخ في 2015 ، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، الجريدة الرسمية عدد 53 مؤرخة في 08 أكتوبر 2015.

[2] المادة 02 من القانون 261/15.

[3] المادة 03 من القانون 261/15.

[4] المادة 06 من القانون 261/15.

وتنص المادة 07 [1] على ما يلي :

يرأس المجنة المديرة الوزير المكلف بالعدل و تتشكل من الأعضاء الآتي ذكرهم :

- الوزير المكلف بالداخلية.
- الوزير المكلف بالبريد وتكنولوجيا الإعلام والاتصال.
- قائد الدرك الوطني.
- المدير العام للأمن الوطني.
- ممثل عن رئاسة الجمهورية.
- ممثل عن وزارة الدفاع الوطني.
- قاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وبخصوص ميام المجنة المديرة والتي تنص عليها المادة 08 [2]: تكلف المجنة المديرة على الخصوص بما يلي:

- توجيه عمل الهيئة والإشراف عليه ومراقبته، بالإضافة إلى دراسة كل مسألة تخضع المجال اختصاص الهيئة لا سيما فيما يتعلق بتوفير اللجوء إلى المراقبة الوقائية للاتصالات الإلكترونية وضبط برنامج الهيئة وتحديد شروط وكيفيات تنفيذه.
- قيام اللجنة بشكل دوري بتقييم حالة الخطر في مجال الإرهاب والتخريب والمساس بأمن الدولة للتمكن من تحديد مشتملات عمليات المراقبة الواجب القيام بها والأهداف المنشودة بدقة، تتولى عملية اقتراح كل نشاط يتصل بالبحث وتقييم الأعمال المباشرة في مجال.
- الوقاية من الجرائم الماسة بتكنولوجيات الإعلام والاتصال ومكافحتها،
- دراسة مشروع النظام الداخلي للهيئة وميزانيتها والموافقة عليه، مع تقديم كل اقتراح مفيد يتصل بمجال اختصاصها[3].

[1] المادة 07 من القانون 261/15.

[2] المادة 08 من القانون 261/15.

[3] أمال بن صويلح ، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خطوة هامة مكافحة الإرهاب الإلكتروني في الجزائر ، الملتقى الدولي حول الإجرام السيبيراني المفاهيم والتحديات، جامعة محمد البشير الابراهيمي برج بوعريريج، الجزائر، يومي 11 ، 12 أفريل 2017 ، ص 06.

كانت هذه تشكيلة الهيئة ، المتكونة من عدة هياكل تم ذكرها وكانت أيضا تشكيلة المجنة المديرة والمهام الموكلة إليها ، أما عن المهام الموكلة لباقي الهياكل التابعة للهيئة فهي منصوص عليها في المواد 09 وما بعدها.

وبالرجوع إلى نص المادة 15 [1] من نفس المرسوم نجدها تنص على أنه يحدد التنظيم الداخلي لهياكل الهيئة بموجب قرار وزاري مشترك بين الوزراء المكلفين بالعدل و الدفاع و الداخلية.

2. المديرية العامة :

حسب المادة 09 من المرسوم الرئاسي 261/15 يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي، ويتولى المدير العام الصلاحيات التالية:

- السهر على حسن سير الهيئة.
- السهر على تنفيذ برنامج عمل الهيئة.
- تنشيط نشاطات هياكل الهيئة وتنسيقها ومتابعتها و مراقبتها.
- تمثيل الهيئة لدى السلطات والمؤسسات الوطنية و الدولية.
- تمثيل الهيئة لدى القضاء وفي جميع أعمال الحياة المدنية.
- السهر على القيام بإجراءات التأهيل و أداء اليمين.
- إعداد التقرير السنوي لنشاطات الهيئة وعرضه على اللجنة المديرة للمصادقة عليه.
- ضمان التسيير الإداري والمالي للهيئة[2].

3. مديرية المراقبة الوقائية واليقظة الإلكترونية :

يتم تعيين مديرها بموجب مرسوم رئاسي موقع من رئيس الجمهورية، كما يتم إنهاء مهامه بنفس الطريقة[3] ، وهي تتكفل بالمهام التالية[4]:

- تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية بناء على السلطة المختصة.
- إرسال المعلومات المحصل عليها إلى السلطات القضائية ومصالح الشرطة.
- القضائية، تنفيذ طلبات المساعدة القضائية الأجنبية في مجال تدخل الهيئة.

[1] المادة 15 من القانون 261/15.

[2] المادة 10 من القانون 261/15.

[3] أمال بن صويلح، مرجع سابق ، ص 06.

[4] المادة 11 من القانون 261/15.

- تنظيم و/أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والاتصال وحول المخاطر المتصلة بها.
- تنفيذ توجيهات اللجنة المديرة.
- تزويد السلطات القضائية ومصالح الشرطة القضائية تلقائيا أو بناء على طلبها بالمعلومات والمعطيات المتعلقة بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- وضع مركز العمليات التقنية والملحقات الجهوية قيد الخدمة والسهر على حسن سيرها وكذا الحفاظ على الحالة الجيد لمنشآتها وتجهيزاتها ووسائلها التقنية.

4. مديرية التنسيق التقني :

حسب المادة 12 من المرسوم الرئاسي 261/15 تكلف مديرة التنسيق التقني بالمهام التالية:

- انجاز الخبرات القضائية في مجال اختصاص الهيئة.
- تكوين قاعدة معطيات تحليلية للإجرام المتصل بتكنولوجيات الإعلام والاتصال واستغلالها.
- إعداد الإحصائيات الوطنية المتعلقة بالجرائم المتعلقة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال،
- القيام بمبادرة منها أو بناء على طلب اللجنة المديرة، بكل دراسة أو تحليل أو تقييم .
- يتعلق بصلاحياتها.
- تسيير منظومة الإعلام الآلي للهيئة وادارتها.

5. مركز العمليات التقنية :

يزود المركز بالمنشآت والتجهيزات والوسائل المادية وكذا بالمستخدمين التقنيين الضروريين لتنفيذ لعمليات التقنية لمراقبة الاتصالات الإلكترونية، ويتبع هذا المركز مديرية المراقبة الوقائية واليقظة الإلكترونية ويتم تشغيله من طرفها[1].

[1] المادة 13 من القانون 261/15.

الفرع الثاني : مهام الهيئة

تتمثل مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته في نوعين المهام الأولى الوقاية من هذه الجرائم و الثانية مكافحة هذه الجرائم.

1. الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال :

يظهر الدور الوقائي للهيئة من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال من خلال مختلف الإجراءات الوقائية التي تنص عليها المادة 04 [1] وهي كالآتي:

- اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
- تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مصدرها و مسارها من أجل استعمالها في الإجراءات القضائية.
- السير على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية و تطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
- تطوير التعاون مع المؤسسات و الهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيات الإعلام و الاتصال.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

2. مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال :

يظهر دور الهيئة في مكافحة هذا النوع من الجرائم من خلال مختلف الإجراءات الردعية الممنوحة إليها بموجب المادة 14 [2] إضافة إلى بعض المهام الردعية الأخرى وهي كالآتي:

- مساعدة السلطات القضائية و مصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ، بما في ذلك جمع المعلومات و التزويد بها من خلال الخبرات القضائية.

[1] المادة 04 من القانون 261/15.

[2] المادة 14 من القانون رقم 04/09.

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعمقة بالأعمال الإرهابية و التخريبية و المساس بأمن الدولة ، تحت سلطة القاضي المختص وبإستثناء أي هيئة وطنية[1].

المبحث الثاني : آليات التحري في الجرائم المعلوماتية

يعد التشريع اللبنة الأولى والأساسية التي يمكن من خلالها مكافحة الجريمة مهما كانت، فلا جريمة ولا عقوبة إلا بنص، حيث أن قاضي التحقيق هو صاحب الاختصاص الأصيل في ذلك ولكن لكل قاعدة استثناء وهو الحال بالنسبة لجرائم الأنترنت، حيث خول القانون بعض السلطات لفئات مختصة لهذه الظاهرة الإجرامية، إلا أن النصوص القانونية مهما كثرت تبقى غير كافية في ظل غياب القواعد الإجرائية والمؤسساتية، فهذه القواعد مجتمعة هي التي يمكن من خلالها تجسيد القانون على أرض الواقع واعطائه الديناميكية التي يحتاجها لمكافحة الجريمة والقبض على مرتكبيها، حيث في هذا المبحث سوف نتناول فيه آليات التحري في الجرائم في ظل قانون الإجراءات الجزائية الحديثة وفي ظل قانون 04/09 التقليدية.

المطلب الأول : إجراءات المتابعة والتحقيق في الجرائم المعلوماتية

بالنسبة للجرائم الالكترونية فتختلف عن الجرائم الأخرى فيما تعلق بالتحري وجمع الأدلة، مما يوجب على السلطة المختصة بالتحقيق الإلمام الواسع بمعطيات الحاسوب وطبيعته وتشغيله ويتعين على المحقق معرفة بيئة الحاسوب والأنترنت والمعرفة الكافية بمسائل الضبط والتفتيش وكشف الأدلة والتحفظ عليها.

الفرع الأول : التفتيش والحجز في الجريمة الالكترونية

يهدف التفتيش الى البحث عن الأدلة التي تفيد في كشف الحقيقة وهو من بين الإجراءات التي ثمنها المشرع الجزائري من خلال القانون 04/09 ، اما الضبط أو الحجز كما أطلق عليه المشرع في إطار القانون 04/09 إجراء جديد خاص بالمعطيات والذي يتناسب مع طبيعة اللامادية واللامحسوسة لجرائم الأنترنت.

1. التفتيش في جرائم الأنترنت :

يعرف التفتيش على أنه البحث في مستودع السر عن اشياء تفيد في الكشف عن الجريمة وقعت ونسبتها الى مرتكبيها، وهو إجراء من إجراءات التحقيق التي تهدف الى البحث عن أدلة مادية لجناية

[1] المادة 04 من القانون 261/15.

أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص. وذلك بهدف إثبات ارتكابها أو نسبتها الى المتهم وفقا لإجراءات قانونية محددة ، وعرفه البعض الآخر بأنه: " البحث عن الأشياء المتعلقة بالجريمة لضبطها وضبط كل ما يفيد في كشف حقيقتها ويجب أن يكون التفتيش سند من القانون" من خلال هذه التعريفات يتضح بأن التفتيش ينطبق على الجرائم التي تترك آثار مادية وبالتالي فلا توجد مشكلات تعيق إجراؤه لأن من خلاله سيتم البحث عن الأدلة المادية الملموسة[1].

- **نطاق تفتيش مكونات النظام المعلوماتي في جرائم الأنترنت :**

يتكون النظام المعلوماتي من مكونات مادية وغير مادية أي معنوية، بالإضافة الى الشبكات المحلية والإقليمية والدولية التي تكون محل للتفتيش من أجل الحصول على الدليل الجنائي الالكتروني وهو المعلومات المخزنة في أجهزة الحاسوب ولواحقها وغيرها من الوسائل التقنية الأخرى وكذا شبكات الاتصال والتي يتم تجميعها باستخدام برامج وتطبيقات وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها الى مرتكبيها[2].

- **تفتيش مكونات النظام المعلوماتي المادية والمعنوية :**

يتكون النظام المعلوماتي من مكونات مادية ومعنوية :

أ. تفتيش مكونات النظام المعلوماتي المادية :

ليس هناك خلاف حول تفتيش المكونات المادية للنظام المعلوماتي بحثا عن شيء يتصل بالجريمة وقعت، يفيد في كشف الحقيقة عنها وعن مرتكبيها يخضع للإجراءات القانونية الخاصة بالتفتيش بمعنى أن حكم تفتيش تلك المكونات المادية يتوقف على طبيعة المكان الموجودة فيه تلك المكونات حيث أن لصفة المكان أهمية وطبيعته أهمية قصوى، فإذا كانت موجودة في مكان خاص كمسكن المتهم وأحد ملحقاته كان لها حكمه فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات والإجراءات المقررة قانونا[3].

فالتشريع الإجرائي الجزائري، يتضمن نصوص قانونية تنطبق من حيث الأصل على تفتيش المكونات المادية للنظام المعلوماتي ، ومن النصوص القانونية التي يمكن تطبيقها في هذا المجال نص المادة 64 من ق .إ .ج .ج والمواد 37 و 40 و 42 من المواد 44 الى 47 من ق .إ .ج .ج.

---

[1] دلال مولاي ملياني ، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، أطروحة دكتوراه تخصص قانون خاص ، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر،2017 ، ص 214.

[2] المادة 16 من القانون 04/09.

[3] خالد ممدوح ابرهيم ، الجرائم المعلوماتية، ط2 ، دار الفكر الجامعي، الاسكندرية، مصر،2019 .

ب. تفتيش مكونات النظام المعلوماتي المعنوية :

قد يرد التفتيش على مكونات النظام المعلوماتي المتمثل في المعلومات المعالجة آليا، ولعل الصورة المعتادة والمثال العملي الذي يمكن تقريره هو فحص البرمجيات، الذي يعد من الوسائل الرئيسية في الكشف عن أكثر جرائم الاعتداء على نظم المعالجة الآلية لوجود برمجيات غير مصنفة تعمل في بيئة الاختراق أو تساعد عليه، كما هو الشأن في برمجيات المسح للكشف عن الأبواب المفتوحة يمكن أن يشكل منطقة استفهام ودلالة كافية أيضا على ارتكاب الشخص لجريمة الدخول غير المشروع لنظام المعالجة الآلية إذا استتبع ذلك اعترافا شفويا بارتكاب الجريمة.

حيث أجاز المشرع الجزائري تفتيش المعطيات المعلوماتية وذلك بموجب المادة 05[1] السالف الذكر وقد أجازت هذه المادة للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 من نفس القانون التي من بينها توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الاقتصاد الوطني وللوقاية من هذه الجرائم، الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها وكذا منظومة تخزين المعطيات[2].

ج. تفتيش المنظومة المعلوماتية عن بعد في الجرائم الإلكترونية :

التفتيش في نطاق الجرائم الالكترونية لا يخرج عن إحدى الفرضيتين:

- **حالة جهاز متصل بجهاز المتهم داخل الدولة :**

تتمثل المشكلة في هذه الحالة عندما تقوم سلطة التحقيق بتفتيش جهاز متصل بجهاز المتهم ويقع داخل الدولة وكذا تجاوز الاختصاص المكاني لسلطة التحقيق من ناحية والاعتداء على خصوصيات الغير من ناحية أخرى ، ونظرا لوجود قصور في نصوص قانون إ .ج .ج لسنة 2006 تم مواجهة هذا القصور بأن سمح للسلطات القضائية المختصة تمديد التفتيش عن المعطيات المبحوث عنها بسرعة الى أي منظومة معلوماتية أو جزء منها تقع داخل الإقليم الوطني وهذا ما نصت عليه الفقرة الثانية من المادة 05 [3] وما يدخل ضمن نطاق الاستعجال في تمديد الاختصاص خوفا من العبث بالأدلة الرقمية[4].

---

[1] المادة 04 من القانون 04/09.

[2] دلال مولاي ملياني ، مرجع سابق ، ص 218.

[3] المادة 05 من القانون 04/09.

[4] دلال مولاي ملياني ، مرجع سابق ، ص 219.

- **حالة جهاز متصل بجهاز المتهم خارج الدولة :**

في هذه الحالة فإن الإشكالية تثار بصورة أكبر في حالة أن يكون الجهاز المطلوب تفتيشه والمتصل بجهاز المتهم بنهاية طرفيه يقع خارج الدولة ففي الغالب يعمد مرتكبي الجرائم الإلكترونية الى تخزين البيانات الخاصة بهم والتي تعد أدلة لإدانتهم في جرائم تم ارتكابها من قبلهم خارج الدولة وبالنسبة للقانون الجزائري فقد تلافى مشكلة التفتيش عن بعد خارج الإقليم الوطني بموجب الفقرة الثالثة من المادة 05 من القانون 04/09 التي نصت على أنه إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[1].

- **شروط التفتيش الجرائم الالكترونية :**

يمكن تقسيمهم الى نوعين:

أ. **القواعد الموضوعية للتفتيش :**

وتتضمن عدة شروط وهي:

- وقوع جريمة معلوماتية وهي كل فعل غير مشروع مرتبط باستخدام الحاسوب لتحقيق أغراض غير مشروعة.
- تورط شخص أو اشخاص معينين في ارتكاب الجريمة الالكترونية أو الاشتراك فيها.
- توافر إمارات قوية أو قرائن على وجود اشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة.
- أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به.

ب. القواعد الشكلية للتفتيش:

وتتضمن عدة شروط منها:

- أن يتم التفتيش بأسلوب آلي الكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة.
- أن يكون أمر التفتيش مسببا أي يجب أن يتضمن الاسباب التي أدت الى إجراءه.

[1] المادة 05 الفقرة الثالثة من القانون 04/09.

- تكوين فريق التفتيش يجب أن يتضمن خبراء مسرح الجريمة من الفنيين والمختصين بشكل ممتاز بالحاسوب والأنظمة الالكترونية وبالإضافة الى رجال الشرطة وأن يتكون الفريق من: المشرف على التحقيق، فريق التفتيش العملي من خبراء الحاسوب، فريق الأمن والحماية من رجال الشرطة[1].

2. الضبط في الجرائم الالكترونية في إطار قانون 04/09 :

لما أقر المشرع الجزائري تفتيش المنظومة المعلوماتية كما سبق وأن فصلنا فبالضرورة كان لابد له أن يقر ضبط الاشياء المستخلصة من تفتيش البيئة الافتراضية بما يناسبها وهو الحجز بأنواعه والحجز هنا هو كل ما يتعلق بإجراءات التحقيق أي التفتيش عن بعد والضبط هنا يعد من إجراءات التحقيق حيث أن الضبط يعد في الأصل من إجراءات الاستدلال.

حيث نظم المشرع الجزائري الضبط في المادة 06 من القانون 04/09 والتي تتمكن من خلالها السلطة التي تباشر التفتيش من ضبط أو حجز المعطيات تكون مفيدة في كشف الجرائم أو مرتكبيها.

والضبط يعني وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبيها[2].

- إجراءات الضبط في الجريمة الالكترونية :

نص المشرع الجزائري على حجز المعطيات في المواد 06 الى 09 من القانون 04/09 فوفقا للمادة 06 عندما تكتشف السلطة التي تباشر التفتيش معطيات تفيد في كشف الجرائم أو مرتكبيها يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون قابلة للحجز والوضع وفقا للقواعد المقررة في قانون إ. ج. ج واذا استحال الحجز لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول الى المعطيات أو نسخها ويجب عليها السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية[3].

---

[1] خالد حياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط1 ، عمان ، 2011 ، ص 154 .

[2] شنتير خضرة ، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة أحمد دراية، أدرار، 2020 ، ص 101.

[3] صالح شنين، إجراءات التحري والتحقيق في جرائم تكنولوجيا الاعلام والاتصال في التشريع الجزائري، مجلة الدراسات القانونية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، ع 01 ، ص 283.

- صعوبات عملية حجز البيانات المعالجة الكترونيا :

- حجم الشبكة التي تحتوي على المعلومات المعالجة الكترونيا والمطلوب ضبطها من ذلك البحث في نظام الكتروني لشركة متعددة الجنسيات.
- وجود هذه البيانات في شبكات أو أجهزة تابعة لدولة أجنبية مما يستدعي تعاونها مع جهات الشرطة والتحقيق في عملية التفتيش والضبط والتحفظ.
- يمثل التفتيش والضبط أحيانا اعتداء على حقوق الغير أو على حرمة حياته الخاصة فيجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق وتلك الحريات[1].

الفرع الثاني : المعاينة والمراقبة الإلكترونية

بالإضافة الى التفتيش والضبط تأتي إجراءات تتعلق بالمعاينة والمراقبة:

1. المعاينة في الجريمة الالكترونية :

المعاينة هي إجراء ينتقل بمقتضاه المحقق أو القاضي لمكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة ويعرف كيف وقعت ويقوم بجمع الأشياء التي تفيد في كشف الحقيقة ، حيث أن جوهر المعاينة هو ملاحظة وفحص حسي مباشر لمكان أو شخص أو شيء له علاقة بالج ريمة لإثبات حالته والكشف والتحفظ على كل ما قد يفيد من الاشياء في كشف الحقيقة ، ويعد مسرح الجريمة بمثابة الشاهد الصامت الذي إذ أحسن المحقق استنطاقه حصل على معلومات مؤكدة[2].

- معاينة مسرح الجريمة

يقع مسرح الجريمة داخل بيئة الحاسوب والبيانات الرقمية التي تتواجد وتنتقل داخل بيئته وشبكاته وفي ذاكرته وفي الأقراص الصلبة الموجودة بداخله والمقصود بمعاينة مسرح الجريمة الالكترونية هو معاينة الآثار والبصمات الالكترونية التي يتركها مستخدم الشبكة المعلوماتية، والتي تشمل الرسائل المرسلة منه والواردة إليه وكافة الاتصالات الالكترونية كما تتم داخل شبكة الأنترنت نفسها عن طريق بيانات المتهم كالولوج الى بريده الالكتروني أو معاينة حسابه على مواقع التواصل الاجتماعي، كما

[1] منير محمد الجنبيهي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات، ط 1 ، دار الفكر الجامعي، الاسكندرية، 2018 ، ص 116.

[2] نفس المرجع ، ص 116.

يمكننا من خلال معاينة الحاسب الآلي للمتهم معرفة المواقع الالكترونية التي زارها أو الملفات التي حملها[1].

فالمعاينة في الجريمة الإلكترونية ليست مسألة مرتبطة بالضرورة بالانتقال عبر العالم المادي بل قد تتم عبر العالم الافتراضي وهناك عدة طرق يستطيع بها عضو سلطة التحقيق أن ينتقل الى العالم الافتراضي للمعاينة ومن ذلك:

- من مكتبه بالمحكمة من خلال الحاسب الآلي الخاص به .
- كما يمكنه اللجوء الى مقهى الأنترنت وأيضا يمكنه اللجوء الى مزود خدمة الأنترنت الذي يعتبر أفضل مكان يمكن إجراء المعاينة فيه.
- ويستطيع المحقق المعاينة في المسرح التقليدي ويقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة كالبصمات وغيرها وربما ترك متعلقات شخصية[2].

- **الضوابط الواجب مراعاتها عند معاينة مسرح الجريمة**

عند إجراء المعاينة بعد وقوع الجريمة في المجال الالكتروني فيجب مراعاة الضوابط التالية:

- ضبط أو سحب أو جمع أو التحفظ على البيانات والمعلومات أو أنظمة المعلومات أو تتبعها في أي مكان أو نظام ويتم تسليم أدلتها الرقمية للجهة مصدرة الأمر على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتضى.
- البحث والتفتيش والدخول والنفاذ الى برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقا لغرض الضبط .
- تصوير الحاسب والأجهزة الطرفية المتصلة به على أن يتم تسجيل وقت وتاريخ ومكان التقاط الصورة.
- إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كاف حتى يستعد من الناحية الفنية والعلمية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.
- إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها.
- أن تتم هذه الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليه القوانين الجنائية.

---

[1] شنتير خضرة ، مرجع سابق، ص 116.

[2] خالد ممدوح ابرهيم ، مرجع سابق، ص 157.

والمعاينة وان آنت في الجرائم إلا أن أهميتها تتضاءل في بعض الجرائم مثل جريمة السب[1].

2. المراقبة الالكترونية للاتصالات :

تتمثل المراقبة في كشف الجرائم قبل وقوعها وتلعب دورا كبيرا في الكشف عن الجرائم الالكترونية وهي وسيلة هامة من وسائل الإرشاد الجنائي، ويقصد به المراقبة الأمنية التي محلها الاتصالات الالكترونية التي عرفها المشرع الجزائري في إطار القانون 04/09 وهي التي تراسل أو إرسال أواستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية .

وقد استعمل المشرع الجزائري مصطلح مراقبة الاتصالات الالكترونية بالرغم أن معظم أحكام قانون 04/09 هي مستمدة من اتفاقية بودابست والتي استخدمت مصطلح اعتراض معطيات المحتوى[2].

- محل مراقبة الاتصالات الالكترونية :

إن محل المراقبة هو ذلك الهدف الذي تتم مراقبته وتتبع حكاته وتصرفاته في نطاق المراقبة الالكترونية محل المراقبة هو الحاسوب الرقمي أو الموقع عبر شبكة الأنترنت أو البريد الالكتروني بما يحتويه من مراسلات الكرتونية وحلقات نقاش وغرفة أو اللوح الرقمي، إذن محل المراقبة يشمل الاتصالات الالكترونية الخاصة والتي عرفتها المادة الثانية من القانون 04/09 ، قد ميز المشرع بين نوعين من المعطيات المعالجة، المراقبة، النوع الأول المراقبة المتعلقة بحركة سير معطيات المرور أما النوع الثاني المعطيات المتعلقة بمحتوى الاتصال فبالنسبة للنوع الأول عرفت المادة 02 من القانون 04/09 أما النوع الثاني والمتعلقة بالمحتوى فلم يرد تعريف لذلك ولو أنه بمفهوم المخالفة هي كل المعطيات المعالجة باستثناء ما تعلق بمعطيات المرور، فمعطيات المحتوى هي محل المراقبة الالكترونية ذلك بأن أدرجها المشرع في المادة الرابعة من القانون 04/09 أما معطيات المرور فقد خصها المشرع بإجراء حفظ المعطيات المتعلقة بحركة السير المادة 11 من القانون 04/09. [3]

[1] خضرة شنتير ، مرجع سابق، ص 68.

[2] دلال مولاي ملياني ، مرجع سابق، ص 209.

[3] دلال مولاي ملياني ، مرجع سابق، ص 209.

الفرع الثاني : أساليب التحري الحديثة

لقد استحدث المشرع الجزائر قواعد إجرائية حديثة بموجب قانون 22/06 المعدل والمتمم لقانون اجراءات الجزائية وتضمن التسرب واعتراض المراسلات كما أضاف قانون 04/09 المتعلق بالقواعد الخاصة بالوقاية ومكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها إجرائيين آخرين وما المراقبة الالكترونية وحفظ المعطيات المتعلقة بحركة السير.

1. اعتراض المراسلات وتسجيل الأصوات والتقط الصور :

جعل المشرع الجزائري من اعتراض المراسلات وتسجيل الأصوات والتقاط الصور أهم الأساليب المستحدثة للكشف عن الجرائم الالكترونية وهي جرائم ترتكب بشكل خفي وذلك تماشيا مع التقدم العلمي والتكنولوجي المعاصر لاسيما في مجال الاتصالات الإلكترونية، مما أفرز أساليب عملية جديدة عالية الكفاءة والفعالية أحدثت ثورة في مجال التحريات ، حيث سنقوم بتسليط الضوء على هاته الإجراءات باعتبار كل منها بشكل إجراء مستقلا[1].

- اعتراض المراسلات السلكية واللاسلكية :

استحدث المشرع الجزائري بموجب القانون رقم 22/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية من خلال الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وقد ضمنه ستة مواد من المادة 65 مكرر الى المادة 65 مكرر 10 وتناول من خلالها المقصود بهذا الإجراء وضمانات استخدامه.

لذلك وعلى هذا الأساس جمع المشرع كل الاتصالات في خندق واحد بموجب المادة 5 من المرسوم رقم 261/15.

وطبقا للمادة 65 مكرر 5 من قانون الإجراءات الجنائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء الى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية هذا الإجراء.

ومن نص المادة 65 مكرر 7 التي نصت على أنه يجب أن يتضمن الإذن باعتراض المراسلات كل العناصر التي تسمح بالتعرف على الاتصالات أو المراسلات المطلوب اعتراضها، كما أن المشرع

[1] بومدين كعيبش، أساليب التحري الخاصة في جرائم الفساد، مجلة القانون، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ع 7، 2016 ، ص30 .

قد استوجب أن لا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدره الإذن وفقا لمقتضيات التحري والتحقيق.

2. التسرب :

أدرج المشرع الجزائري عملية التسرب بموجب قانون 22/06 المتضمن قانون الاجراءات الجزائية والذي أفرد الفصل الخامس منه تحت عنوان "في التسرب"، والذي تضمن 8 مواد، من المادة 65 مكرر 11 حتى المادة 65 مكرر 18 ، وتناول من خلالها تحديد مفهوم هذه العملية وشروط إجرائها العمليات المبررة وأخيرا الحماية الجنائية للقائم بعملية التسرب، والتي تعني قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية الكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك[1].

ويمكن تجسيد عملية التسرب في الجرائم الإلكترونية كاشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة مثلا، فيتخذ المتسرب أسماء مستعارة ويحاول الاستفادة حول كيفية اقتحام الهاكر لموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم وتصح عملية التسرب إذا توفرت الشروط التالية:

- صدور أذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية.
- أن يكون الإذن مكتوبا ومسببا.
- يحدد مدة التسرب التي لا يمكن أن تتجاوز أشهر غير أنه يمكن أن تحدد[2].

3. الشهادة :

تعرف الشهادة بصفة عامة أنها: الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أوالقضاء بشأن جريمة وقعت سواء تتعلق بثبوت الجريمة وظروف ارتكابها واسنادها إلى المتهم أو براءته منها[3].

ويقصد بالشاهد في الجريمة الإلكترونية هو الشخص الفني صاحب الخبرة والتخصص في تقنية المعلومات، والذي يمكنه الدخول إلى نظام المعالجة الآلية للبيانات متى كانت مصلحة التحقيق تتطلب ذلك، لذلك يطلق عليه بالشاهد المعلوماتي تمييزا له عن الشاهد التقليدي وينحصر في مشغلي الحاسب

[1] آمنة أمحمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية دراسة تحليلية، الملتقى الوطني حول آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر، يوم 03/29/ 2018 ، ص57.

[2] فاطمة بوعناد، مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانوني، ع 01 ، الجزائر، ص70.

[3] عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي دراسة مقارنة، رسالة مقدمة للحصول على درجة الماجستير في الحقوق، كلية الحقوق جامعة الإسكندرية، مصر، 2009 ، ص77.

الآلي، المحللون، خبراء البرمجة، مهندسو الصيانة والاتصال ومديرو النظم، أما الشهادة الإلكترونية فتفترض هذه النوعية من الشهادة حصولها أمام قاضي الموضوع حيث يكون الشاهد غير حاضر جسديا في جلسة المحاكمة إلا أنه يظهر بشكل سمعي ومرئي[1].

4. الخبرة التقنية :

تكتسي عملية ندب الخبير خلال التحقيق في الجرائم الإلكترونية أهمية بالغة، نظرا لطبيعتها الفنية والتقنية التي تتميز بها، وكذلك التنوع الأجهزة في هذا المجال وسرعة تطورها، وندب الخبير من سلطات المحقق وليس هناك في القانون ما يلزم بذلك، ويحدد المحقق للخبير المهمة التي كلف بها وميعاد تسليمه لتقريره كما يجب عليه أن يؤدي اليمين القانونية بهذا الخصوص[2].

وتخضع الخبرة التقنية في أغلب التشريعات المقارنة إلى نفس أحكام الخبرة القضائية من حيث القواعد التي تحكم عمل الخبير واجراءاته، فبالنسبة للمشرع الجزائري تناول أحكام الخبرة في المواد من 143 إلى 155 من قانون الإجراءات الجزائية .وتكمن أهمية الخبرة التقنية أن جهات التحري والتحقيق كثيرا ما تفشل في جمع الأدلة الرقمية، بل إن المحقق في كثير من الأحيان ما يتسبب في تدمير الدليل الرقمي إما نتيجة خطأ أو إهمال أو جهل في التعامل معه، وعموما يراعي في الخبير أن تتوافر لديه القدرات الفنية والإمكانيات العلمية في مسألة موضوع الخبرة[3].

5. اعتراض المراسلات وتسجيل الأصوات والتقاط الصور :

لقد أشار المشرع الجزائري إلى ظروف وكيفية اللجوء في المادة 65 [4]مكرر 5 من قانون الإجراءات الجزائية : إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو في الجرائم المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من

---

[1] محمد بن فردية، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، تخصص القانون الجنائي، كلية الحقوق جامعة الجزائر،2015 ، ص159.

[2] المادة 143 من قانون رقم 22/06.

[3] محمد بن فردية، مرجع سابق، ص 164.

[4] المادة 65 من قانون رقم 22/06.

طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية، أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص.

المطلب الثاني: تدابير وعقوبات المساس بنظام المعالجة الآلية للمعطيات

قد حدد المشروع الجزائري كل صور الاعتداء الواقعة عل المعطيات حيث وقعها بعقوبات رادعة لمرتكبها خصصها في مواد 394 مكرر إل 394 مكرر 7 لهذا الاجرام الحديث، وتماشيا ما نص المادة 13 من الاتفاقية الدولية للإجرام المعلوماتي، فان العقوبات المقررة للجرائم المعلوماتية يجب أن تكون رادعة وتتضمن عقوبات سالبة للحرية، والمتمثلة في عقوبات أصلية وعقوبات تكميلية تطبق عل الشخص الطبيعي هما توجد عقوبات تطبق عل الشخص المعنوي بناء عل تبني مبدأ مساءلة الشخص المعنوي الواردة في المادة 12 من الاتفاقية.

الفرع الاول : العقوبات المقرر لشخص الطبيعي

لقد خصص المشرع الجزائر العقوبات المقررة للشخص الطبيعي عن كل جريمة من الجرائم الاعتداء على المعطيات :

وعند التطرق للنصوص العقابية المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية يتبين لنا وجود تدرج داخل النظام العقابي، حيذ أن وهذا التصاعد في تشديد العقوبات يحدد الخطورة الاجرامية التي قدرها المشرع لهذ التصرفات[1].

1. جريمة الدخول أو البقاء بغش :

تعاقب المادة 394 مكرر على هذا الفعل بالحبس من ثلاثة اشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الالية للمعطيات أو يحاول ذلك، تضاعف العقوبة إذا ترتب عل ذلك حذف آو تغيير لمعطيات المنظومة.

نصت المادة 394 [2] مكرر 2 و 3 من قانون العقوبات على أنه : 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 ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000دج.

---

[1] أمال قارة ، المرجع السابق ، ص127.

[2] المادة 394 مكرر 2 3 القانون رقم 15/04.

وباستقراء نص المادة 394 مكرر 2 و 3 من قانون العقوبات ، نجد أنها قد نصت على ظرفين مشددين تشدد بهما عقوبة الدخول أو البقاء داخل النظام ، ويتمثل هذان الظرفان في حالة ما إذا نتج عن الدخول أو البقاء غير المشروع محو أو تعديل البيانات التي يحتويها النظام أو عدم قدرة النظام على تأدية وظيفته ويكفي لتوافر هذا الظرف المشدد أن تكون هناك علاقة سببية بين الدخول أو البقاء غير المشروع وبين النتيجة التي تحققت وهي محو النظام أو عدم قدرته على أداء وظيفته أو تعديل البيانات ، وبذلك فالهدف الأساسي من هذا النص هو التعرض لكل محاولة لإعاقة أو تحريف قد تلحق بهذا النظام[1].

2. جريمة المساس بسلامة المعطيات :

تعاقب المادة 394 مكرر 1 على هذا الفعل بالحبس من 06 اشهر إلى ثلاثة سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج.

3. جريمة تخريب أو تعطيل نظام التشغيل :

تعاقب المادة 394 مكرر 1 على هذا الفعل في فقرتها الثالثة بالحبس من ستة أشهر إلى سنتين وغرامة من 50.000 دج إلى 150.000 دج .

4. جريمة إساءة استخدام الاجهزة :

تعاقب المادة 394 مكرر 2 على هذا الفعل بالحبس من شهرين إلى ثلاثة سنوات و بغرامة من 1.000.000 دج إلى 5.000.000 دج.

5. الاتفاق الجنائي :

يعاقب المشرع على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها ، فإذا تعددت الجرائم التي يتم التحضير لها، تكون العقوبة هي عقوبة الجريمة الاشد[2].

لقد نص علي المشرع في المادة 394 مكرر 5 حيث:

تعاقب على هذا الفعل بنفس العقوبات المقررة للجريمة ذاتها للجرائم المنصوص عليها في جرائم الماسة بأنظمة المعالجة الالية للمعطيات.

---

[1] ختير مسعود ، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى ، عين مليلة ، الجزائر، ص 119.

[2] فيصل بدري ، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتورا في علوم تخصص كلية الحقوق بن يوسف ، 2018، ص 181.

وما تجدر اليه اشارة هنا ان المشرع لم يخضع هذه الجريمة لأحكام المادة 176 من قانون العقوبات[1].

كما يمكن استنتاج مجموعة من الشروط من المادة 394 مكرر5 كالاتي[2] :

- مجموعة أو اتفاق.
- بهدف التحضير لجريمة من الجرائم الماسة بأنظمة المعلوماتية.
- تطبيق هذا التحضير بفعل مادي.
- فعل المشارك في هذا الاتفاق.
- القصد الجنائي.

بعد الاطلاع عل جزئيات المادة 394 مكرر5 نجد ان المشرع لم يخرج عن النطاق العام في عقاب الشريك فنجد قد ألزم بنفس عقوبة الفاعل الاصلي، كما أن أكثرية جرائم الاعتداء الماسة بأنظمة المعالجة الآلية للمعطيات تكون بشكل اتفاق جماعات، حتى وان لم يكن وهنالك اتفاق ضمني بينهم.

6. الشروع :

لقد خص المشرع الجزائر الشروع في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بنص المادة 394 مكرر 07 ، بقوله " يعاقب عل الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها "[3].

ويتضح من خلال نص المادة 394 مكرر 7 رغبة المشروع في توسيع نطاق العقوبة لتتضمن أكبر قدر من افعال الماسة بأنظمة المعلوماتية، إذ جعل الشروع في إحدى الجرائم الماسة بأنظمة المعلوماتية معاقب عليه بنفس عقوبة الجريمة التامة.

الفرع الثاني : العقوبات المقررة للشخص المعنوي

لقد تبن المشرع مبدأ مسائل الشخص المعنوي في القانون 15/04 وذلك بموجب نص المادة 51 مكرر منه ، فحدد ثلاثة شروط لإمكانية مساءلة لشخص المعنوي جنائيا وهي كالتالي:

- أن ترتكب إحدى الجرائم المنصوص عليها قانونا.
- أن تكون بواسطة أحد أعضاء أو ممثلي الشخص المعنوي.

[1] أمال قارة ، مرجع سابق، ص 130.

[2] المادة 394 مكرر 5 القانون رقم 15/04.

[3] المادة 394 مكرر 7 القانون رقم 15/04.

- إن ترتكب الجريمة لحساب الشخص المعنوي.

كما حدد في المادة 18 [1]مكرر من نفس القانون، العقوبات المطبقة على الاشخاص المعنوية حيث تضمنت ما يلي: " العقوبات التي تطبق عل الشخص المعنوي في الجناية و الجنح هي :

الغرامة التي تساوي من مرة إلى خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة، واحدة أو أكثر من العقوبات الآتية :

- حل الشخص المعنوي .
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس سنوات .
- اقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية او اجتماعية بشكل مباشر، نهائيا لمدة لا تتجاوز خمس سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة او نتج عنها.
- نشر وتعليق حكم الادانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس سنوات وتوقيع الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته .

كما أن المسؤولية الجزائية للشخص المعنوي لا تغني عن مساءلة الاشخاص الطبيعية بصفتهم فاعلين أو شركاء في الجريمة .

لقد اخص المشرع الجزائر الجرائم المعلوماتية التي تستهدف الدفاع الوطني أو أي من المؤسسات الرسمية بمثابة ظرف تشديد يستخلص من نص المادة 394 مكرر 3 [2] بنصها " تضاعف العقوبات المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الاخلال بتطبيق عقوبات أشد".

وما تجدر إليه الاشارة هو حرص المشرع الجزائري عل حفظ ومواجهة كل الجرائم الماسة بأنظمة معالجة الآلية للمعطيات التي تمس بمؤسسات الدولة ولا غرابة في ذلك حيث إن كمبيوتراتها وما تحمل من معلومات ومعطيات ذات طابع خاص وسري ، ذات أهمية بالغة الخطورة لأنها مستهدف بالدرجة الاولى من طرف القراصنة ومجرمي الانترنت .

[1] المادة 18 مكرر القانون رقم 15/04.

[2] المادة 394 مكرر 3 القانون رقم 15/04.

وأضاف المشرع الجزائر عقوبات أخرى تكميلية منصوص عليها في المادة 394 مكرر 6 [1]من قانون العقوبات حيث تضمنت.

- **المصادرة :**

هي عقوبة ملحقة تتضمن الاجهزة والبرامج والادوات المستعملة في اقتراف جريمة من الجرائم الماسة بالأنظمة المعلوماتية مع احترام الحقوق المير الغير حسن النية.

- **اغلاق المواقع :**

يخص الامر هنا المواقع الالكترونية التي تكون محلا لجريمة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات .

- **اغلاق المحل أو مكان الاستغلال :**

يكون ذلك في حالة التي يكون صاحب المحل مشارك في الجريمة، وذلك في حالة ما إذا تعقدت الجريمة، وهو مدرك لها ولم يخبر عنها أو قام بمنع مرتكبها من قصد محله لارتكاب مثل هذه الجرائم.

[1] المادة 394 مكرر 6 القانون رقم 15/04.

خلاصة الفصل :

وفي خلاصة هذا الفصل ، يتأكد لدينا أن المشرع الجزائر استخدم لمكافحة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أساليب إجرائية تقليدية متعارف عليها ،كما ألحق بها أساليب جديدة منها مراقبة الاتصالات الالكترونية وحفظ المعطيات، ذلك أن الدليل في هذه الجرائم غير مرئي يصعب تعامل معه أثناء التحقيق.

كما أن هناك أساليب مؤسساتية لتصدي لهذا اجرام المستحدث، كهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الهيئة القضائية الجزائية المتخصصة، إضافة إلى المعهد الوطني للأدلة الجنائية وعلم الاجرام.

كما وضحنا الجزاءات المقررة لكل صورة من الصور التي نص عليها تعديل قانون العقوبات 15/04 من خلال استعرض العقوبات المقررة للشخص الطبيعي والعقوبات المقررة للشخص المعنوي.

الخاتمـــة

الخاتمة:

بالرغم من ما للثورة المعلوماتية من ايجابياتها وقدرتها على تغيير أوجه الحياة إلى الأحسن والأفضل، إلا أن هذه الثورة المعلوماتية ذاتها تحمل في طياتها أيضا العديد من السلبيات التي تتمثل في الاستخدام غير المشروع لنظم الحاسب الآلي، ومن هذا المنطلق استطاع الجناة تطوير طرق الإجرام على نحو عال من التقنية في بيئة تكنولوجيا المعلومات. رأينا كيف أن المشرع الجزائري لا يتوفر على آليات قادرة على الاضطلاع بالآثار الخطيرة التي ترتبها جرائم المساس بأنظمة المعالجة الآلية للمعطيات سواء على مستوى النصوص التشريعية أو على مستوى طبيعة الكوادر والأجهزة المتخصصة لمواجهة هذا النوع من الإجرام، ومن ثم كان لابد أن يبادر إلى تبني سياسة موسعة ومحكمة تستهدف إيقاف كل التحديات التي يطرحها هذا الإجرام وإيمانا بأهمية الوقوف أمام التحديات التي تفرضها هذه الجريمة،

اولا: النتائج

- إن الجرائم المعلوماتية جرائما خطيرة تشكل تهديدًا جسيمًا على الأمن الاجتماعي والاقتصادي والسياسي والعسكري لمجتمعاتنا، نظرا للقيمة العالية والطبيعة الحساسة للمعلومات.
- جرم فعل البقاء غير المصرح به داخل نظام المعالجة الآلية للمعطيات إلى جانب الدخول سواء كان دخول بناء على تصريح انتهت مدته أو اتصل صدفة بالنظام.
- يتمتع جهاز الضبطية القضائية بسلطات واسعة في سبيل جمع الاستدلالات عن الجرائم الواقعة على المعطيات ذات الطابع الشخصي.
- تجريم عدة أفعال قد تمس بسلامة ووفرة وتكامل المعطيات.
- نسجل تأخر المشرع الجزائري في إقرار منظومة قانونية لمعالجة المعطيات ذات الطابع الشخصي مقارنة الأخرى
- التحقيق في الجرائم المعلوماتية يتطلب تأهيلا تقنيا و فنيا عاليين.

ثانيا: الاقتراحات

- ضرورة التعاون بين الدول لمواجهة هذا النوع من الجرائم.
- تدريس مواد خاصة بالأنظمة المعلوماتية و بصفة خاصة الجرائم المعلوماتية و طرق الحماية الخاصة بها.
- ضرورة توضيح وإزالة اللبس عن بعض النصوص والتي تتداخل أحيانا مع بعضاها البعض، بحيث يصعب تحديد نطاق تطبيقها.

قائمة المصادر و

المراجع

قائمة المراجع:

1) الكتب

1. ختير مسعود ، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى ، عين مليلة ، الجزائر، 2017.
2. خالد ممدوح إبراهيم ،أمن الجريمة الالكترونية ، الدار الجامعية، الإسكندرية ، مصر، 2008.
3. محمد حماد مرهج الهيتي ، جرائم الحاسوب ماهيتها موضوعها وموقف التشريعات الجنائية منها، دار المناهج للنشر والتوزيع، عمان، الأردن، ط 1 ، 2006.
4. جلال الزعبي ، صايل فاضل الهواوشة ، جرائم الحاسب الآلي والإنترنت ، دار وائل للنشر، عمان ، الأردن.
5. أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، ط 2 ، الجزائر، 2007.
6. علي عبد القادر القهوجي ، الحماية الجنائية لبرامج الكمبيوتر، المكتبة القانونية ، القاهرة ، 2009.
7. نائلة محمد فريد قروة ، جرائم الكمبيوتر الاقتصادية ، منشورات حلبي ، ط 1، بيروت،2005.
8. خراشي عادل عبد العالي، ضوابط التحري والاستدلال عن الجرائم، دار الجامعة الجديدة للنشر، الاسكندرية، 2006 .
9. خالد ممدوح إبراهيم، الجرائم المعلوماتية ، دار الفكر الجامعي، ط 1، الإسكندرية، مصر،2009.
10. إبراهيم محمود اللبيدي، السلوك الإجرامي في جرائم الانترنت ، مركز الإعلام الأمني ، القاهرة، مصر، 2013.
11. أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، ط 1 ، الاسكندرية، مصر، 2008.
12. خالد ممدوح ابرهيم ، الجرائم المعلوماتية، ط 2، دار الفكر الجامعي، الاسكندرية، مصر، 2019.
13. خالد حياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة للنشر والتوزيع، ط 1، عمان ، 2011 .

14. منير محمد الجنبيهي، صعوبات التحقيق واستخراج الأدلة في جرائم المعلومات، ط 1 ، دار الفكر الجامعي، الاسكندرية، 2018.

2) المذكرات و الرسائل

1. دلال مولاي ملياني ، إشكالية الإثبات في جرائم الانترنت في التشريع الجزائري، أطروحة دكتوراه تخصص قانون خاص ، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2017.
2. شنتير خضرة ، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة أحمد دراية، أدرار، 2020.
3. محمد بن فردية، الإثبات الجنائي للجرائم المعلوماتية بالأدلة الرقمية، أطروحة لنيل شهادة الدكتوراه علوم، تخصص القانون الجنائي، كلية الحقوق جامعة الجزائر، 2015.
4. فيصل بدري ، مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتورا في علوم تخصص كلية الحقوق بن يوسف ، 2018.
5. دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منثوري، قسنطينة، 2013.
6. بوكر رشيدة ، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن ، رسالة لنيل شهادة ماجستير في الحقوق، دمشق، سوريا، 2010.
7. سعيدة بكرة ، الجريمة الإلكترونية في التشريع الجزائري دراسة مقارنة مذكرة مكملة مقدمة لنيل شهادة الماجستير في الحقوق، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2016.
8. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب ، جامعة باتنة، 2012.
9. عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي دراسة مقارنة، رسالة مقدمة للحصول على درجة الماجستير في الحقوق، كلية الحقوق جامعة الإسكندرية، مصر، 2009.

3) محاضرات وملتقيات

1. أمال بن صويلح ، الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال خطوة هامة مكافحة الإرهاب الإلكتروني في الجزائر ، الملتقى الدولي حول الإجرام السيبيراني المفاهيم والتحديات، جامعة محمد البشير الابراهيمي برج بوعريريج، الجزائر، يومي 11 ، 12أفريل2017 .
2. آمنة أمحمدي بوزينة، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية دراسة تحليلية، الملتقى الوطني حول آليات مكافحة الجريمة الإلكترونية في التشريع الجزائري، مركز جيل البحث العلمي، الجزائر، يوم 2018/03/29.

4) المجلات

1. طباش عز الدين، الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري دراسة في ظل قانون 07/18 المتعلق بحماية الاشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي، المجلة الأكاديمية للبحث القانوني، ع 02 ، 2018.
2. نسمة بطيحي ، جريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي ، مجلة الفقه القانوني والسياسي ، م1 ، ع 01 ، جامعة سطيف، 2015.
3. خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، م 22 ، ع 86، 2012.
4. بومدين كعيبش، أساليب التحري الخاصة في جرائم الفساد، مجلة القانون، جامعة أبو بكر بلقايد، تلمسان، الجزائر، ع7 ، 2016.
5. صالح شنين، إجراءات التحري والتحقيق في جرائم تكنولوجيا الاعلام والاتصال في التشريع الجزائري، مجلة الدراسات القانونية، جامعة عبد الرحمان ميرة، بجاية، الجزائر، ع 01.
6. فاطمة بوعناد، مكافحة الجريمة الإلكترونية في التشريع الجزائري"، مجلة الندوة للدراسات القانوني، ع 01 ، الجزائر.

5) النصوص القانونية

- **القوانين**

1. قانون رقم 07/18 مؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018.
2. القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004 ، المتعلق بقانون العقوبات والنصوص القانونية الخاصة المتعلقة بالحماية السيبرانية.
3. القانون رقم 01/16 المؤرخ في 06 مارس 2016 ، الجريدة الرسمية رقم 14 المؤرخة في 7مارس 2016.
4. قانون رقم 04/09 المؤرخ في 14 شعبان عام 1430 الموافق 05 غشت سنة 2009 ، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
5. القانون 261/15 المؤرخ في 2015 ، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته، الجريدة الرسمية عدد 53 مؤرخة في 08 أكتوبر 2015.

- **الأوامر والمراسيم**

1. الأمر رقم 156/66، المؤرخ في 08 يوليو 1966 ، المتضمن قانون العقوبات، جريدة رسمية ع49 ، المؤرخة في 11 يوليو 1966 ، المعدل والمتمم.

فهرس المحتويات

فهرس المحتويات :

ملخص الدراسة

ملخص الدراسة:

تطرح الجريمة المعلوماتية العديد من المشاكل من ناحية القانون الإجرائي، إذ يصعب على المحققين إجراء تحقيق وجمع الأدلة الرقمية، بإتباع الإجراءات التقليدية للتحقيق : كالمعاينة، التفتيش الضبط، ... الخ ، في هذا السياق ورغبة منها في مكافحة فعالة للجريمة المعلوماتية، تبنت الجزائر أساليب جديدة للتحري ، من خلال تعديل قانون العقوبات عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الآلية للمعطيات

وفي 2009 أصدر المشرع الجزائري القانون رقم المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، في هذا القانون خلق المشرع آليات جديدة خاصة للتحري من أجل مكافحة الجريمة المعلوماتية، إلا أن هذه الأساليب الحديثة للتحري أثارت مشكلة مدى مشروعيتها، خاصة وأنها تمس بالحقوق والحريات الأساسية للفرد والمعترف بها في الاتفاقيات الدولية ولحل هذا الإشكال فقد وضعت شروط وضمانات يقتضي على السلطات القضائية مراعاتها عند الإذن بهذه الأساليب.

الكلمات المفتاحية :

الجريمة المعلوماتية ، القانون الإجرائي ، الأدلة الرقمية ، المعاينة، التفتيش ، الضبط ، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، السلطات القضائية.

Summary:

Cybercrime poses many problems in terms of procedural law, as it is difficult for investigators to conduct an investigation and collect digital evidence, by following traditional investigation procedures : such as inspection, inspection, seizure, etc. In this context, and with a desire to effectively combat cybercrime, Algeria has adopted methods New investigation measures, by amending the Penal Code by adding new procedures applied to crimes of harming automated data processing systems.

In 2009, the Algerian legislator issued Law No. containing special rules for preventing and combating crimes related to information and communication technologies. In this law, the legislator created new mechanisms for investigation in order to combat information crime. However, these modern methods of investigation raised the problem of the extent of their legality, especially since they affect rights and freedoms. These methods are essential to the individual and recognized in international agreements. To solve this problem, conditions and guarantees have been set that judicial authorities must take into account when authorizing these methods.

key words :

Information crime, procedural law, digital evidence, inspection, inspection, seizure, crimes related to information and communication technologies and combating them, judicial authoritie.