جـــــــامعة غردايـــــة

كلية الحقوق والعلوم السياسية

قسم: الحقوق

الآليات المستحدثة للحد من الجريمة الإلكترونية في التشريع الجزائري

مذكرة مكملة لاستكمال متطلبات نيل شهادة ماستر أكاديمي حقوق

تخصص قانون جنائي

إعداد الطالبتين:

ابن الضب فاطنة

حبي فتيحة

إشراف الدكتور

لغلام عزوز

لجنة المناقشة

الاسم واللقب	الرتبة العلمية	الجامعة	الصفة
فروحات السعيد	أستاذ محاضر –أ –	جـامعة غرداية	رئيسا
لغلام عزوز	أستاذ محاضر –أ –	جـامعة غرداية	مشرفا ومقررا
سيد أعمر محمد	أستاذ محاضر — ب–	جـامعة غرداية	مناقشا

السنة الجامعية:

1439هـ-1440م/2018-2019هـ


بسم الله الرحمن الرحيم

﴿قَالُو سُبحَانَكَ لَا عِلْمَ لَنَا إِلاَّ مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ﴾.

الآية (32) من سورة البقرة.

﴿...وَمَا أُوتِيتُمْ مِنَ الْعِلْمِ إِلَّا قَلِيلًا﴾.

الآية (85) من سورة الإسراء.

كلمة الشكر

يسرنا أن نتقدم بجزيل الشكر والعرفان إلى الله ثم إلى الذي قدم لنا يد المساعدة ووقف وراء هذا العمل المتواضع بمجوداته ونصائحه القيّمة

أستاذنا المشرف الدكتور لغلام عزوز فلولا ما جدتم به علينا من توجيه رشيد ورأي سديد ونصح مفيد ما كان ليتهيأ لنا الأمر لإنجاز هذا العمل، فلا نملك عرفانا بما تفضلتم به علينا إلا أن نسدي لكم وافر الشكر ونتقدم لكم بعميق الإمتنان، وخالص التقدير عسى الله أن يديمكم في خدمة العلم، وينفع بكم البحث العلمي، فحياكم الله أستاذنا الفاضل وسدد خطاكم.

كما يسرنا أن نتقدم بجزيل الشكر إلى اللجنة الموقرة التي قبلت مناقشة هذا البحث المتواضع.

إهداء

أحمد الله عز وجل على منه وعونه لإتمام هذا البحث.

إلى التي قال في حقها صلوات الله عليه وسلامه أمك ثم أمك ثم أمك...

إلى نبع الحنان والحياة أمي رحمها الله وأسكنها فسيح جنانه.

إلى أبي الغالي أطال الله في عمره.

إلى سندي وقوتي وملاذي بعد الله.

إلى من آثروني على أنفسهم.

إلى من علموني علم الحياة.

إلى من أظهروا لي ما هو أجمل من إخوتي وأخواتي ربي يحفظهم ويخليهم إن شاء الله.

إلى الكتكوت الصغير ابن أختي "عبد الرزاق" أطال الله في عمره وحفظه الله ورعاه.

إلى كل عائلة "حبي" كبير وصغير.

إلى صديقتي العزيزة ورفيقة دربي "بوعلام سعيدة".

أهدي لكم عملي المتواضع وثمرة مشواري الجامعي.

وفي الأخير لكم مني جميعا كل المحبة والتقدير والشكر والعرفان.

-والله الموفق والمستعان-

فتيحة حبي
فتيحة حبي

إهداء

أحمد الله عز وجل على منه وعونه لإتمام هذا البحث.

إلى التي وهبت فلدة كبدها كل العطاء والحنان إلى التي صبرت على كل شيء ورعتني حق رعاية وكانت سندي في الشدائد وكانت دعواها لي بالتوفيق إلى نبع الحنان أعز ما أملك أمي الغالية جزاها الله عني خير الجزاء في الدارين وأطال الله في عمرها.

إلى الذي وهبني كل ما يملك حتى أحقق أماله، إلى من كان دوما يدفعني نحو الأمام قدما لنيل المبتغى، إلى الذي سهر على تعليمي بتضحيات جسام أبي الغالي على قلبي أطال الله في عمره وحفظه ورعاه، إليهما أهدي هذا العمل المتواضع لإسعادهما دوما؛

إلى من أسر بهم أزري إلى إخوتي عبد الحميد ومحمد والطاهر وزوجته وأولاده كل باسمه الى أخواتي وأزواجهم وأولادهم كل باسمه؛ إلى عائلة بن الضب صغيرا وكبيرا؛ إلى جميع الأصدقاء والزملاء الذين ساعدونا من قريب أو من بعيد واخص بالذكر ياسين أبي إسماعيل، كما أتقدم بالشكر إلى جميع الأساتذة الكرام على مدار السنة وبالأخص الدكتور لغلام عزوز.

اهدي ثمرة جهدي اليكم جميعا والله الموفق

قائمة المختصرات

ج ر.ج.ج:	الجريدة الرسمية للجمهورية الجزائرية.
د.ط:	دون طبعة.
ص:	صفحة.
ص ص:	من الصفحة إلى الصفحة.
ق.ع.ج:	قانون العقوبات الجزائري.
ق.إ.ج.ج:	قانون الإجراءات الجزائية الجزائري.
ق.ع.ف:	قانون العقوبات الفرنسي.

ملخص:

إن التطور الحاصل في تكنولوجيا الإعلام والاتصال وظهور شبكة الأنترنت بكل ما حملته من تقدم وخدمات لم يمر على العالم بسلام لأنه بقدر ما أحدث آثار إيجابية وغير نمط حياة المجتمعات وساهم في التطور والرقي في جميع المجالات ولا سيما المعاملات الإلكترونية، بقدر ما كان له أثر سلبي على حياة الناس ومصالح الدول، كل هذا تجلى في تطويع الأنترنت والوسائل الإلكترونية لتكون عالما من عوالم الجريمة وهكذا ظهرت إلى الوجود الجرائم الإلكترونية بشتى أنواعها، وسنحاول في بحثنا هذا التطرق إلى التعريف بماهية الجريمة الإلكترونية وماهي الآليات الكفيلة بمكافحتها.

الكلمات المفتاحية: شبكة الأنترنت ،الجريمة الالكترونية، آليات مكافحتها.

Abstract :

The évolution in the information and communication technologie. And the émergence of the internet with all what it carrid as Progress and services, this is not passed peacefully on the world, because as much as it affected positive us and it chanded in communities life style and cotritsuted to the développent and progresse in all fields particulary electronic transaction, as much as it had a négativeimpact on peoples lives and interests of the states.All of this was reflected in the adaptation of the internet and electronic meais to be a world from the worlds of crime and So come into being the electronic crime, and so come into being the electronic crime of varois kinds.And we Will try in our research that adresse the développent of electronic transaction and the définition of what the cyber crime and what the mechanisms to ensure combating it.

Key words:internet, cyber crime.

مقدمة

إن الثورة المعلوماتية التي يشهدها العالم في عصرنا هذا ساهمت وبشكل كبير في تطور معاملات الأفراد، وتسهيلها ذلك في شتى مجالات الحياة، لاسيما بعد ظهور الأنترنت التي وضعت العالم كله في قرية صغيرة، نظرا لما ميزها من سرعة في تبادل البيانات والمعلومات، فتطورت بها المعاملات بين الأفراد، وكان هذا التطور الهائل الذي شهده قطاعي تكنولوجيا المعلومات والاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد، هو المحور الأساسي الذي قامت عليه ثورة جديدة أطلق على تسميتها بالثورة المعلوماتية، والتي تعد طفرة علمية وتكنولوجية نشهدها اليوم، حتى بات يطلق على هذا العصر عصر المعلوماتية، والمعلومة هي من أهم ممتلكات الانسان التي اهتم بها على مر العصور فجمعها ودونها وسجلها على وسائط متدرجة، بدأً بجدران المعابد والمقابر إلى أن وصل بها المطاف إلى أقراص الكترونية ممغنطة، إلا أن هذه الأخيرة ورغم ما تركته من آثار إيجابية نتيجة للتقنيات العالية التي تقوم عليها بتوفيرها للراحة والمساهمة في رفع المستوى المعرفي والاقتصادي لمختلف شعوب العالم، فقد جرت معها عيوبا استفاق عليها العالم وأدرك خطورتها وبات أثرها ملموسا ومحسوسا، فهذه الإساءة لاستخدام شبكة الانترنت والحاسوب مهد الطريق لأصحاب النوايا الخبيثة من المجرمين باستخدام هذه التقنية وتطويعها لإشباع رغباتهم وتحقيق نواياهم الاجرامية.

ومن هنا ولدت جرائم جديدة اختلفت عن الجرائم التقليدية اتسمت بخطورتها الكبيرة نظرا لطابعها الخاص سواء ما ميز الجريمة أو مرتكبها وصعوبة اثباتها، وقبل ذلك تثار مشكلة الأمن المعلوماتي الذي يعد مهمة صعبة في ظل الجريمة المعلوماتية التي لا تعترف بالحدود والأوطان ويعيش محترفوها في عالم افتراضي، فتطور الأمن المعلوماتي بات أمرا حتميا وهاجسا أمام رجال القانون، فكان من الضرورة التصدي لبوادره كي لا يستفحل مع وتيرة النمو المتسارع الذي تشهده دول عربية عدة . ومن بينها الجزائر. في استخدام النظم المعلوماتية فضلا عن ظروف العولمة والتبعية التكنولوجية من مناخ ملائم لاختراق البيانات الشخصية والمساس بالأمن القومي لهذه الدول وسيادتها الوطنية.

ومن هنا تتجلى أهمية موضوع **"الجريمة الإلكترونية"**.

وتهدف هذه الدراسة إلى:

– حداثة الموضوع ومدى مساسه بالواقع وامتداد خطره، مما يستدعي ضرورة المعالجة القانونية السريعة والفورية. وبيان طرق وأساليب الحماية المعلوماتية أو ما عرف بالأمن المعلوماتي، ودوره في قمع الجريمة.

– كما تبرز الأهمية من خلال السيطرة على الوضع بواسطة قوانين حديثة، ولعله من اللازم الإشارة إلى أن نظام الحماية لم يعد مقتصرا على خصوصية الأفراد وحمايتهم، بل أنه امتد إلى الدول ذاتها.

– وبالتالي يمكن الاستفادة من هذه الدراسة في مواجهة جرائم الأنترنت والتعامل معها ومكافحتها، كما يمكن أن تساهم هذه الدراسة بطرح اقتراحات تصورية وتلقت انتباه الباحثين في العلوم الجنائية والاجتماعية والإنسانية بشكل عام إلى كثير من الظواهر السلوكية المتعلقة باستخدام الانترنت التي تتطلب البحث والدراسة فيها، ولفت انتباه كلا من الجهاز القضائي والقانوني والأمني إلى سلوكيات وأفعال جنائية ترتكب ضد الآخرين بواسطة الحاسب الآلي ومن خلال شبكة الأنترنت، لابد من مواجهتها بضوابط قانونية وقضائية وأمنية.

وإن اختيارنا لموضوع الجريمة الالكترونية في التشريع الجزائري يرجع في حقيقة الامر الى العديد من الاسباب منها شخصية وموضوعية.

فالشخصية تمثلت في الاهتمام بالاطلاع على هذا النوع من الجرائم المستحدثة بحيث لا يخفى على احد ما يشهده العالم من اعتداءات واقعة بسبب هذه الجريمة وما خلفه هذا التطور التكنولوجي وما جعله موضوع جديد ومواكب للتطورات الحاصلة في الجانب المعلوماتي، أما الموضوعية تكمن في ما يطرحه هذا الموضوع من اشكالات قانونية ومدى مسايرة المشرع الجزائري لهذا الموضوع نظرا لحداثته بتجريم الاعتداءات الماسة بنظام المعالجة الالية والقواعد الاجرائية الحديثة التي جاء بها قانون الاجراءات الجزائية وقانون 09/04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ومعرفة كيف تصدى المشرع الجزائري بالاعتداء على المعطيات في الجريمة الالكترونية وذلك بتعديل قانون العقوبات بإضافة القسم السابع مكرر وكذا قواعد اجرائية من خلال تعديل قانون الاجراءات الجزائية 09/04.

وقد واجهتنا صعوبات جمة ترجع إلى حداثة استخدام الحاسب الآلي وما يتسم به من صبغة علمية بحتة غريبة في تصورنا على رجال القانون نحن نسعى أساسا من خلال هذه الدراسة إلى تحقيق هدفين أساسيين:

* على المستوى النظري التركيز على تحديات القانون الجنائي في مواجهة الإعلام الآلي حيث أن ظهور المعلوماتية وتطبيقاتها المتعددة أدى إلى بروز مشاكل قانونية جديدة في نطاق القانون الجنائي يفرض حلها البحث في الأوضاع القانونية القائمة ومدى ملاءمتها لمواجهة هذه المشاكل؟

* على المستوى التطبيقي نهدف من هذه الدراسة إلى تغطية الفراغ القانوني الملحوظ في هذا المجال وتوجيه أنظار المشرع الجزائري إلى ضرورة مسايرة قانون العقوبات للتطورات التكنولوجية وما تطرحه من مشاكل قانونية.

وهذا برجوع إلى جملة من الدراسات السابقة في هذا المجال منها المذكرات والرسائل التالية:

1/ أمال قارة، الجريمة المعلوماتية مذكرة لنيل شهادة الماجستير.

2/ سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية جامعة الحاج لخضر باتنة.

3/ عبد اللطيف المعتوق، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجيستير والعلوم الجنائية.

4/ يوسف مناصرة، جرائم المساس بأنظمة المعالجة الألية للمعطيات، رسالة مقدمة لنيل شهادة الماجيستير في القانون الجنائي والعلوم الجنائية.

إلا أن ما ميز دراستنا هذه أنها تناولت الموضوع من زاوية مختلفة؛ إذ أنها تطرقت إلى إشكالية مغايرة وتقسيم مختلف، ومن خلال ما سبق ذكره يمكن أن نطرح الإشكالية:

– ماهي الآليات المستحدثة لمكافحة الجريمة الإلكترونية في ضل التشريع الجزائري؟

وتتفرع عن الإشكالية الرئيسية مجموعة من التساؤلات الفرعية:

– هل يمكننا إعطاء تعريف جامع للجريمة الالكترونية؟

– ماهي الجرائم المعلوماتية، وماهي أركانها وخصائصها وأنواعها وآليات مكافحتها؟

وللإجابة على الإشكالية المطروحة وبغيت التوصل إلى نتائج قانونية إخترنا **المنهج الوصفي التحليلي** وذلك من خلال التطرق إلى أهم التعاريف والمفاهيم الخاصة بالجريمة الإلكترونية وكذا الآليات المستحدثة للحد من هذه الجريمة وذلك من خلال التطرق إلى أهم النصوص القانونية ذات الصلة بموضوعنا هذا.

ولقد قسمنا دراستنا هذه على فصلين، خصصنا الفصل الأول إلى الإطار المفاهيمي للجريمة الالكترونية وقسمناه إلى مبحثين الأول مفهوم الجريمة الإلكترونية والثاني مفهوم الجريمة الالكترونية في التشريع الجزائري؛

أما الفصل الثاني فخصصناه إلى الجوانب العملية للحد من الجريمة الإلكترونية وقسمناه إلى مبحثين الأول الآليات التشريعية للحد من الجريمة الإلكترونية أما الثاني الآليات المؤسساتية لمواجهة الجريمة المعلوماتية.

الفصل الأول:
الإطار المفاهيمي للجريمة الإلكترونية

عرفت المعلوماتية تطورا مذهلا، كما ساعد اقترانها بتكنولوجيات أخرى، الالكترونيك، الرقمنة ...إلخ، على تعميم استعمالها وتعدد وظائفها، والحديث اليوم لم يعد عن الحاسوب وقدراته في اختزال الوقت وتخزين المعلومات وإنجاز عمليات معقدة بقدر ما هو عن تكنولوجيات الإعلام والاتصال، والفضاء الافتراضي الذي نشأ نتيجة ارتباط المعلوماتية بمختلف شبكات المواصلات السلكية واللاسلكية، ومع التغلغل المتزايد للمعلوماتية وتكنولوجيات الاتصال في مختلف مجالات النشاطات البشرية كان ولا بد من وضع أطر قانونية ملائمة لتحديد شروط استعمال هذه الوسائل الجديدة في مختلف المعاملات، كما ظهرت أيضا ضرورة وضع نصوص جزائية لحماية الأنظمة المعلوماتية وردع إساءة استعمالها.

فالجريمة الالكترونية باعتبارها جريمة مستحدثة أثارت ضجة في الأوساط الفقهية بخصوص تحديد ماهيتها والأفعال الإجرامية التي تدخل في نطاقها، وسوف نقسم الدراسة في هذا الفصل الى مبحثين نخصص المبحث الأول إلى ماهية الجريمة الالكترونية والمبحث الثاني فسنتطرق الى مفهوم الجريمة الالكترونية في التشريع الجزائري.

المبحث الأول: ماهية الجريمة الإلكترونية:

بداية وقبل التكلم عن الجريمة الإلكترونية لابد أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلومات واستخدامها فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الآخر يطلق عليها جريمة الاختلاس المعلوماتي أو الاحتلال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية، وحتى نتعرف على هذا النوع من الجرائم ارتأينا أن نقسم هذا المبحث إلى ثلاثة مطالب بداية تعرف الجريمة الالكترونية كمطلب أول ثم التطور التاريخي لها في مطلب ثاني أما المطلب الثالث خصصناه لأركان الجريمة الالكترونية.

المطلب الأول: تعريف الجريمة الالكترونية:

نتيجة للتطور المذهل في الاتصالات وتكنولوجيا المعلومات، وظهور الانترنت فالانتشار الواسع والسريع لها أدى إلى ظهور أشكال وأنماط جديدة من الجرائم لاسيما المتعلقة منها بشبكة الأنترنت، والتي باتت تشكل خطرا ليس على سرية النظم الحاسوبية أو سلامته فحسب، بل تعدت إلى أمن البنى الأساسية الحرجة[1].

فهناك من يرى أن هذه الجريمة القائمة أساسا على التقدم التكنولوجي المتطور والمتجدد بصفة دائمة ومستمرة خاصة في مجال تكنولوجيا المعلومات، ويفضل أن يطلق عليها اصطلاح جرائم التكنولوجيا الحديثة، كونها جرائم

[1] عادل عبد العالي إبراهيم خراشي، **إشكالية التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها**، دار الجامعة الجديدة، الإسكندرية، 2015، ص 07.

باعتبارها مرتبطة ارتباطا وثيقا بالتكنولوجيا التي تعتمد أساسا على الحواسيب وغيرها من أجهزة تقنية التي لازالت في تطور والتي قد تظهر في المستقبل، وهي كذلك جرائم حديثة نظرا لحداثتها النسبية من ناحية ولارتباطها الوثيق بما يظهر من أجهزة حديثة ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل.

ولكن يبقى اصطلاح الجريمة المعلوماتية على الجرائم المتعلقة بالحاسوب والانترنت اصطلاحا عام ويشمل التقنيات الحالية والمستقبلية كلها المستخدمة في التعامل مع المعلومات بما في ذلك الحاسوب وشبكة الانترنت[1].

وفي هذا الإطار آثر المشرع الإنجليزي في قانون إساءة استخدام الحاسوب عام 1990 عدم وضع تعريف محدد لجرائم الحاسوب، بغية عدم حصر القاعدة التجريمية في إطار أفعال معينة، تحسبا للتطور العلمي والتقني في المستقبل وحتى يسهل إعطاء تعريف للجريمة المعلوماتية فقد تراوحت التعريفات المقدمة بين المفهوم الواسع والضيق وجاءت التعريفات كالآتي:

الفرع الأول: المفهوم الواسع للجريمة الالكترونية:

هناك العديد من التعريفات الواسعة من بينها: أن الجريمة المعلوماتية تتمثل في كل عمل أو امتناع يأتيه إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به اعتبارا من المصالح والقيم المتطورة التي تمتد نصوص قانون العقوبات لحمايتها[2].

كما عرفها الفقيه الألماني (Tiedemann) الجريمة المعلوماتية بأنها تشمل كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسب.

وعرفها الفقيه (Ball.D.Leslie) بأنها فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية[3].

عرفها الفقيهان (Hardcastle et Totty) بأنها تلك الجرائم التي يكون قد وقع في مراحل ارتكبها بعض العمليات الفعلية داخل نظام الحاسب، وبعابرة أخرى هي تلك الجرائم التي يكون دور الحاسب فيها إيجابيا أكثر منه سلبيا.

ويوسع البعض مفهوم الجريمة المعلوماتية لتشمل أي فعل متعمد مرتبط بأي وجه بالحاسبات، يتسبب في تكبد أو إمكانية تكبد المجني عليه لخسارة أو حصول أو إمكانية حصول مرتكبه على مكسب.

---

[1] أمين فرج يوسف، **الجرائم على شبكة الانترنت**، دار المطبوعات الجامعية، كلية الحقوق، الاسكندرية، 2009، ص58.

[2] طعباش أمين، **الحماية الجنائية للمعلومات الإلكترونية**، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى 2015، ص 16.

[3] عبد الفتاح بيومي حجازي، **مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي النموذجي**، دار الفكر الجامعي، الإسكندرية، 2006، ص02.

ويوسع الخبير الأمريكي (Parker) في تعريفها بأنها "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ترتبت عنه خسارة تلحق بالمجني عليه أو مكسب يحققه الجاني.

ويتبين من خلال هذا التعريف أنه ربط الفعل الإجرامي بالخسارة أو الربح أيا كانت الصلة التي تربطه بالمعلوماتية.

كما ذهب الفقيهان (Credo-Michel) إلى أن جريمة الحاسوب تشمل استخدام الحاسب كأداة لارتكاب الجريمة هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على بطاقات الائتمان، وانتهاك ماكينات الحاسب الآلي بما تتضمنه من شيكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة الحاسب في حد ذاته وأي من مكوناته[1].

ومن أنصار هذا الاتجاه الموسع من عرفها بأنها كل سلوك إجرامي يتم بمساعدة الكمبيوتر أو كل جريمة تتم في محيط أجهزة الكمبيوتر.

ويذهب البعض إلى أنه عند وضع تعريف محدد للجريمة المعلوماتية يجب مراعاة عدة اعتبارات مهمة منها:

1-أن يكون هذا التعريف مقبول ومفهوم على مستوى العالمي.

2-أن يراعي هذا التعريف التطور السريع والمتلاحق في تكنولوجيا المعلومات.

3-أن يحدد التعريف الدور الذي يقوم به جهاز الكمبيوتر في إتمام النشاط الإجرامي.

4-أن يفرق هذا التعريف بين الجريمة العادية والجريمة المعلوماتية وذلك عن طريق إيضاح الخصائص المميزة للجريمة المعلوماتية[2].

ويمكن القول إن إعطاء هذا التعريف الواسع للجريمة المعلوماتية يدخل في نطاقها كل التصرفات غير المشروعة التي لها علاقة بالحاسوب أيا كانت هاته العلاقة وأيا كان دور الحاسوب فيها سواء كان وسيلة أو مناسبة لارتكاب التصرفات غير المشروعة أو كان موضوعا لها، ولذلك فهي كل فعل إجرامي متعمد أي كانت صلته بالمعلوماتية،

[1] نهلا عبد القادر المومني، **الجرائم المعلوماتية**، ماجستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع،2008، الطبعة الاولى، الاصدار الاول 2008، ص 49.

[2] طعباش امين، المرجع السابق ص 17.

ترتب عنه خسارة تلحق بالضحية أو مكسب يحققه الجاني[1].

ويمكن حصر هذه الحالات كالتالي:

*الحالات التي يكون فيها الإعلام الآلي كمناسبة لارتكاب الجريمة.

*الحالات التي تكون فيها المعلوماتية كأداة لارتكاب الجريمة.

*الحالات التي تكون فيها المعلوماتية كموضوع للجريمة.

إن الاعتماد في تعريف الجريمة المعلوماتية على الوسيلة المستخدمة في ارتكابها أو المناسبة التي ارتكبت في إطارها منتقد لأنه لتعريف الجريمة المعلوماتية وجب الرجوع إلى العامل الأساسي المكون لها، وليس فقط إلى الوسائل المستخدمة لارتكابها، أو لمجرد أن الحاسب قد استخدم في الجريمة أن نعتبرها من جرائم المعلوماتية وهذا ما أدى إلى ظهور التعريف الضيق[2].

الفرع الثاني: المفهوم الضيق للجريمة الالكترونية:

من بين التعريفات الضيقة للجريمة المعلوماتية بأنها تلك التي يكون الغرض منها موجه ضد الأموال المعلوماتية متى كانت مرتبطة باستخدام نظام المعالجة الآلية للمعطيات، مع إقصاء تلك الأفعال المتمثلة في استخدام الإعلام الآلي كوسيلة للاعتداء على الغير سواء الأشخاص أو الثقة.

وقد انطلق أنصار التعريف الضيق للجريمة المعلوماتية من النقطة المتعلقة بضرورة تحديد العلاقة بين المعلوماتية والأفعال غير المشروعة. أو بعبارة أخرى حتى تشكل الأفعال غير المشروعة جريمة معلوماتية يجب أن تكون موجهة ضد "الأموال المعلوماتية" مع إقصاء الأفعال المتمثلة في استخدام الإعلام الآلي كوسيلة للاعتداء على الغير سواء الأشخاص أو الأموال، ومن أهم التعريفات التي وردت فيه ما يلي:

تعريف الفقيه (Merwe) حيث يرى أن الجريمة المعلوماتية هي الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي، أو هو الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية.

فيما ذهب الفقيه (Ros Blat) بأنها كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي وإلى تحويل طريقه.

[1] المقدم عزالدين، **الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها**، بملتقى حول الجرائم المعلوماتية، بسكرة في 2016/11/16.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 5.

وعرفها كلاوس تايدومان بأنها كافة أشكال السلوك الغير المشروع الذي يرتكب باسم الحاسب الآلي[1].

ويرى البعض أن تعريف كلا من (Merwe) و (Ros Blat) جاء مقصورين على الإطاحة بأوجه المظاهرة الإجرامية، أما تعريف كلاوس تايدومان فيؤخذ عليه أنه بالغ في العمومية والاتساع، لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع.

وتبنى الفقه الفرنسي تعريفا أضيق من ذلك حيث عرفها بأنها كل الأفعال غير المشروعة الموجهة ضد نظام المعالجة الآلية للمعطيات.

في حين يرى الأستاذ (Massa) أن المقصود منها هو الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح.

ويدخل في نطاق تعريفات مفهوم الجريمة المعلوماتية الضيقة تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية حيث يعرف الجريمة المعلوماتية من خلال تحديد مفهوم جريمة الحاسب بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا.

الفرع الثالث: المفهوم القانوني للجريمة الالكترونية:

هي الانحرافات والتجاوز عن مختلف المعايير الجمعية التي تتصف بكم ضخم من الحرية والنوعية والكلية أي أن الجريمة لا توصف بذلك إلا في حال توفر القيمة التي تضعها الجماعة القانونية وتحترمها بالإضافة إلى الانعزال عن الصعيدين الحضاري والثقافي.

- ويمكن تعريف الجريمة بأنها الإتيان بفعل ينافي مع المعايير الجمعية والقانونية والدستورية أيضا وتتمثل بالتعدي على حقوق الآخرين وانتهاكها أيضا ويعاقب عليها القانون نظرا لتحريمه قانونا وشرعا[2].
- كما تعرف الجريمة على أنها فعل وامتناع يخالف قاعدة جنائية يقرر لها القانون جزاءا جنائيا.
- وفي تعريف هي تلك العلل التي تنتهك القانون الجنائي ويعاقب عليها من طرف السلطة السياسية في المجتمع.
- كما تعرف على أنها الفعل الذي يقع مخالف لقانون العقوبات أو أنها فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبير احترازيا، وهناك من يزيد على ذلك بأنها سلوك إنساني يعاقب عليه بوصفه خرقا أو تهديدا لقيم المجتمع أو لمصالح أفراده الإنسانية[3].

---

[1] مناصرة يوسف، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات**، رسالة مقدمة لنيل شهادة الماجيستير في القانون الجنائي والعلوم الجنائية، قسم العلوم القانونية، جامعة الجزائر، السنة الجامعية 2009/2008، ص 10.

[2] Https://mawdoor.com.(28/08/2019)

[3] Https://crimedz.blogspot.com.(28/08/2019)

- وهناك من يقول بأن الجريمة الالكترونية هي عبارة عن أنشطة غير مشروعة تستهدف المعلومات بطريقة تمكن الاطلاع عليها أو تزييفها أو حذفها وذلك بواسطة تقنية المعلومات، ومعلوم أنها تستخدم الكمبيوتر والآلات الذكية كأداة استخدام للجريمة[1].
- والجريمة من الناحية القانونية: هي عمل غير مشروع ناتج عن إرادة جنائية ويقرر القانون لها عقوبة أو تصرف قانوني.

المطلب الثاني: مراحل تطور الجرائم الإلكترونية:

عرفت الجرائم الإلكترونية تطورا لاستهان به، وهي كثيرة حيث لم يوضع لها معايير محددة من أجل تصنيفها مما أدى إلى صعوبة إثباتها، وهذا راجع إلى التطور المستمر للشبكة والخدمات التي تقدمها، وعليه خصصنا هذا المطلب لمراحل تطور الجرائم الإلكترونية.

مر تطور الجرائم الإلكترونية بثلاثة مراحل تبعا لتطور التقنية واستخدامات الحاسوب:

الفرع الأول: معالجة الجرائم الإلكترونية في شكل مقالات:

بظهور استخدام الكمبيوتر وربطه بالشبكة في الستينات إلى السبعينات، ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، وشكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة جرمية مستجدة؟ وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية؟ فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني ومع توسع الدراسات تدريجيا وخلال السبعينات بدأ الحديث عنها كظاهرة إجرامية جديدة[2].

الفرع الثاني: إرتباط الجرائم الإلكترونية بعمليات إقتحام نظام الكمبيوتر:

في بداية الثمانينات تأكد مفهوم جديد لجرائم الكمبيوتر والأنترنت حيث ارتبطت هذه الأخيرة بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدمير كلي للملفات أو البرامج، وشاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظم وكذا المجرم المعلوماتي المتفوق

[1] Https://makkahnewspaper.com.(28/08/2019)

[2] الملتقى الوطني، **آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري**، الجزائر العاصمة، 29 مارس 2017.

الفرع الثالث: النمو الهائل والسريع لشبكة الأنترنت:

حيث شهدت فترة التسعينات تناميا هائلا في حقل الجرائم الإلكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيلات لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط جديدة وخطيرة في ذات الوقت.

حيث نمت الانترنت بشكل مذهل خلال هذه الفترة بعد ما كانت مجرد شبكة أكاديمية صغيرة وتحولت إلى بيئة متكاملة للاستثمار والعمل والإنتاج والاعلام والحصول على المعلومات، وفي البداية لم يكن ثمة اهتمام بمسائل الأمن بقدر ما كان الاهتمام ببناء الشبكة وتوسيع نشاطها، دون مراعاة تحديات أمن المعلومات، فالاهتمام الأساسي تركز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة، وهذه الثغرة التي شجعت تنامي الجريمة الإلكترونية وتسببت في أضرار بالغة، وهو ما أدى إل لفت النظر إلى حاجة شبكة الأنترنت الى توفير معايير من الأمن، وبدأ التفكير مليا في الثغرات ونقاط الضعف.

وعليه قد يكون الكمبيوتر هدفا للجريمة، وغايته المعلومات المخزنة والسيطرة على النظام دون التصريح والسرقة والاعتداء على الملكية الفكرية ...الخ[1].

كما قد يكون الكمبيوتر محل للجريمة، كحالة استغلال الكمبيوتر للاستيلاء على أموال الغير بإجراء تحويلات غير شرعية، كما أن الكمبيوتر قد يعد أداة للجريمة، كحالة تخزين البرامج المنسوخة أو في حالة استخدامه لنشر المواد غير القانونية

خاصة بعد دخول الأنترنت إلى قطاع تقنية المعلومات، حيث لا يستطيع أحد أن ينكر أهمية الأنترنت لأنها أحد أهم دعائم تكنولوجيا الاتصال والمعلومات، إلا أن لديها آثار سلبية من بينها ظهور نوع جديد من الجرائم المستحدثة ونتيجة لحداثة هذا النوع من الجرائم، نجد أن التشريعات اختلفت في تعريف هذه الجريمة، بحيث خولت مسألة تعريفها للفقه وبالنسبة للمشرع الجزائري نجده اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، هذه الجريمة كأي نوع من الجرائم الأخرى لها خصائص وأركان خاصة بها.

من خلال استعراض تعريفات الفقهية، يتضح لنا أن هناك اختلاف في تعريف الجريمة المعلوماتية، إلا أنه في الحقيقة تعددت التعاريف إلا أنها كلها تدل على نفس الجريمة التي نحن بصدد دراستها.

[1] الملتقى الوطني، **آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري**، المرجع السابق.

المبحث الثاني: مفهوم الجريمة الالكترونية في التشريع الجزائري:

أدت الحداثة التي تتميز بها الجريمة الإلكترونية واختلاف النظم القانونية والثقافية بين الدول إلى عدم الاتفاق على مصطلح موحد للدلالة عليها مما انجر عنه عدم وضع تعريف موحد لهذه الظاهرة الإجرامية، وبالنسبة للمشرع الجزائري نجده للدلالة على الجريمة الالكترونية اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

المطلب الأول: تعريف الجريمة الالكترونية:

تبنى المشرع الجزائري للدلالة على مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث، ولم يختلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات حيث أنه عرف من خلال نص المادة 20 من قانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مسميا إياه: " المنظومة المعلوماتية" وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين.

وقد جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل[1].

وأدت الحداثة التي تتميز بها الجريمة الالكترونية، واختلاف النظم القانونية والثقافية بين الدول إلى عدم الاتفاق على مصطلح موحد لهذه الظاهرة الإجرامية. وبالنسبة للمشرع الجزائري نجده للدلالة على الجريمة الالكترونية اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال[2].معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية، محلا للجريمة، ويمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحققه حتى يمكن توافر أركان الجريمة، وبالرجوع إلى قانون العقوبات الجزائري نجده لم يعرف جرائم الأنترنت بل اكتفى بالعقاب على بعض الأفعال تحت عنوان **"الجرائم الماسة بنظام المعالجة الآلية للمعطيات"**، حيث نصت المادة 394 مكرر من قانون العقوبات الجزائري ما يلي: ((يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من 50.000 دج إلى 200.000دج، كل من يدخل أو يبقى عن طريق الغش في

[1] محمد علي العريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة، الإسكندرية، 2004، ص 44.

[2] أشرف عبد القنديل، المرجع السابق، ص 92.

كل أو جزء من منظومة المعالجة الآلية، وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين وبغرامة من 50.000دج إلى 300.000 دج))[1].

وبناء على ما سبق، نجد المشرع الجزائري اعتمد على عدة معايير للدلالة على الجريمة الالكترونية، وذلك باعتماده على معيار وسيلة الجريمة من جهة، وهو نظام الاتصالات الالكتروني، ومن جهة أخرى على معيار موضوع الجريمة ألا وهو المساس بأنظمة المعالجة الآلية للمعطيات، أما المعيار الثالث وهو قانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات[2].

كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة الالكترونية باعتبار أن الجريمة الالكترونية ترتكب في نظام معلوماتي أو نظام لاتصالات الالكترونية

وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية.

ويمكننا أن نستخلص من خلال هذا التعريف أن المشرع الجزائري اعتمد عدة معايير لتعريف الجريمة الالكترونية، منها معيار الوسيلة وهو نظام الاتصالات الالكترونية، وكذلك معيار موضوع الجريمة وهو المساس بأنظمة المعالجة الآلية للمعطيات، كما هو مبين في قانون العقوبات من المادة 394 مكرر إلى 394 مكرر7[3]، حيث نجد أن المشرع ترك المجال واسع لأي جريمة ترتكب أو يسهل ارتكابها عن طريق الحاسب الآلي أو نظام الاتصالات الالكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم حتى تلك الجرائم التي يكون للمنظومة المعلوماتية دورا فيها، وكذلك قد وسع في نطاق الجريمة كونها ترتكب في نظام معلوماتي[4].

الفرع الأول: موقف المشرع الجزائري من الجريمة الالكترونية:

وتجدر الإشارة إلى ان المشرع الجزائري قد اقر في التعديل الأخير لقانون العقوبات المسؤولية الجزائية للشخص المعنوي وذلك في نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات[5] الذي ينص على أن:

"العقوبات المطبقة على الشخص المعنوي في مواد الجنايات والجنح هي:

أ/ الغرامة التي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقدرة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

---

[1] المادة 02 من قانون رقم 04/09 المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر عدد 47 سنة 2009.

[2] قانون رقم 04/ 15 مؤرخ في 10 نوفمبر 2004، المتضمن قانون العقوبات ج ر عدد 71، الصادرة في 10 نوفمبر 2004.

[3] لجريدة الرسمية للجمهورية الجزائرية، العدد 71 المؤرخة في 2004/11/10.

[4] مندیلي رحيمة، المرجع السابق، ص06.

[5] قانون رقم 15/04 المتضمن قانون العقوبات ج ر عدد 71 الصادر في 10 نوفمبر 2004.

ب/ واحدة أو أكثر من العقوبات الآتية:

- حل الشخص المعنوي.
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز 5 سنوات.
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز 5 سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو إجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز 5 سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر او تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز 5 سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكب الجريمة بمناسبته.

بالنسبة لعقوبات الغرامة المطبقة على الشخص المعنوي عند ارتكابه أحد الجرائم الماسة بالأنظمة المعلوماتية فهي تعادل طبقا للمادة 394 مكرر 4 قانون العقوبات 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.

د/ عقوبة الاتفاق الجنائي:

نصت عليه المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي[1] وقد تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5، بغرض التحريض للجرائم الماسة بالأنظمة المعلوماتية ولم يخضعها لأحكام المادة 176 من قانون العقوبات المتعلقة بجمعية أشرار، حيث تنص المادة 394 مكرر 5 من قانون العقوبات[2]: "كل من شارك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسد بفعل أو بعدة أفعال مادية، يعاقب بالعقوبات المقررة بالجريمة ذاتها".

إن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو في اتفاق بغرض الاعداد لجريمة من الجرائم الماسة بالأنظمة المعلوماتية هو أن مثل هذه الجرائم تتم عادة في إطار مجموعات، كما أن المشرع ورغبته في توسيع نطاق العقوبة أخضع الأعمال التحضيرية التي تسبق البدء في التنفيذ للعقوبة إذا تمت في إتفاق جنائي، بمعنى أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.

ويعاقب المشرع الجزائري على الاشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم التي يتم التحضير لها تكون العقوبة هي عقوبة الجريمة الأشد.

---

[1] المادة 11 من الإتفاقية الدولية للامم المتحدة لمكافحة الجريمة المنظمة في15 تشرين الثاني نوفمبر 2000.

[2] المادة 394 مكرر 5 من قانون العقوبات رقم 15/04 مؤرخ في 10 نوفمبر 2004.

وشروط المعاقبة على الاتفاق الجنائي بمن استخلاصها من نص المادة394 مكرر5 من قانون العقوبات والتي هي:

- مجموعة أو اتفاق.
- بهدف تحضير جريمة من الجرائم الماسة بالأنظمة المعلوماتية.
- تجسيد هذا التحضير بفعل مادي.
- فعل المشاركة في هذا الاتفاق.
- القصد الجنائي.

فبالنسبة لمجموعة أو الاتفاق يستوي أن يكون أعضاء الاتفاق في صورة شركة أو مؤسسة أو شخص معنوي، كما يستوي أن يعرف أشخاص الاتفاق بعضهم بعضا كما في العصابة أم تكون مجرد مجموعة من الأشخاص، لا يعرف أحدهم الآخر من قبل لكن اتفقوا فيما بينهم على القيام بالنشاط الاجرامي، المهم أن يتم الاتفاق بين شخصين على الأقل، فإذا ارتكب الشخص العمل التحضيري المادي شخص واحد بمفرده أو بمنعزل عن غيره فلا يعاقب في هذه الحالة، فالعقاب لا يتقرر إلا في حالة اجتماع شخصين أو أكثر.

وتكاثف الجهود لا يكفي بل يجب أن يكون هذا التحضير جريمة من جرائم الماسة بالأنظمة المعلوماتية بمعنى أن الاتفاق يجب أن يكون له هدف إجرامي منذ البداية فعليه فإنشاء نادي للمعلوماتية بهدف التكوين أو التسلية العلمية يحول نشاطه لأهداف إجرامية لا يقع تحت طائلة المادة 394 مكرر 5 من قانون العقوبات[1].

الجنح التي يشكل تحضيرها هدف الاتفاق المنصوص عليه بالمادة 394 مكرر 5 قانون العقوبات هي الجنح الماسة بالأنظمة المعلوماتية وعليه لا يعاقب استنادا لهذا النص الاتفاق بهدف ارتكاب جنحة تقليد البرامج المعاقب عليها بنصوص حق المؤلف وحقوق المجاورة.

التحضير لا يكفي بل يتجسد بفعل مادي، الأمر يتعلق بأعمال تحضيرية مثل تبادل المعلومات الهامة لارتكاب الجريمة كالإعلان عن كلمة مرور mots de passe أو رمز الدخول code d'acces إلخ.

فعل المشاركة في الاتفاق إذ أن المجرم بنص المادة 394 مكرر 5 ليس الاتفاق وإنما المشاركة من طرف شخص طبيعي أو معنوي فبمجرد الانضمام إلى الاتفاق غير كافي بل يجب توفر فعل إيجابي للمشاركة.

توافر القصد الجنائي لدى أعضاء الجماعة والمتمثل في توافر العلم لدى كل منهم بأنه عضو في الجماعة الاجرامية وأن تتجه إدارة كل عضو أي تحقيق نشاط إجرامي معين هو العمل التحضيري.

[1] المادة 394 مكرر 5 من قانون رقم 15/04 مؤرخ في 10 نوفمبر 2004.

الفرع الثاني: عقوبة الشروع في الجريمة الالكترونية:

نصت المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي وتبناه المشرع الجزائري في المادة 394 مكرر 7 قانون العقوبات: "يعاقب على الشروع في ارتكاب جنح المنصوص عليها في هذا القسم بالعقوبة المقررة للجنحة ذاتها"[1].

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر ممكن من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص المادة 394 مكرر 5 من قانون العقوبات مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي.

بعض التشريعات المقارنة بما فيها التشريع الفرنسي أخرجت جنحة الاتفاق الجنائي لتحضير جرائم ماسة بالأنظمة المعلوماتية من نطاق الشروع لأنها تعتبر أن في ذلك مساس بالنظرية العامة في القانون الجنائي، لأن التحضير للجرائم الذي يتم في إطار اتفاق أو مجموعة تشكل في حد ذاتها محاولة أو عمل تحضيري مما يؤدي إلى تبني فكرة الشروع فيها[2].

كما أن للجريمة الالكترونية حقائق وأرقام: مع شيوع استخدام الكمبيوتر أواخر سبعينيات القرن الماضي برزت ظاهرة القرصنة الالكترونية، وسرعان ما تحول السلوك الذي بدا في بدايته انحراف لمراهقين شغوفين بالتكنولوجيا، حربا تشن بين الدول، وهي تهدد منشئات حيوية كالمفاعلات النووية ومحطات الكهرباء كما تدمر المخزونات النقدية لبنوك دول وتهتك اسرار لا يراد لها الخروج إلى العلن، وكشفت أرقام وبيانات عالمية تزايد الجرائم الالكترونية في مختلف انحاء العالم، مع التوسع المتزايد لاستخدام الأنترنيت والأجهزة الذكية، وأظهرت دراسة لموقع "أرقام ديجيتال" أن عدد ضحايا الهجمات والجرائم الالكترونية يبلغ 555مليون مستخدم سنويا، واكثر من 1,5 مليون ضحية يوميا، في حين تقع ضحية كل ثانية لهذه الهجمات، واكثر أنواع الجرائم سرقة هويات وعددها 224 مليون سرقة، واظهرت الدراسة أن مواقع التواصل الاجتماعي هي الكثر اختراقا، إذ بينت ان أكثر من 600 ألف حساب فيسبوك يتم اختراقها يوميا وبينت الدراسة أن الكلفة السنوية المخصصة للأمن المعلوماتي قدرت بـ 100 مليار دولار، بعدما كانت في حدود 23,1 مليار دولار سنة 2011، ومن المتوقع أن تتجاوز 120 مليار دولار بحلول سنة 2017[3]، وحسب تقرير نشرته شركة مشاريع المن السيبراني (CYBERSECURITY

[1] المادة 11 من الاتفاقية الدولية للأمم المتحدة لمكافحة الجريمة المنظمة في 15 تشرين الثاني، نوفمبر 2000.

[2] القرصنة الالكترونية سلاح العصر الرقمي، مقال منشور على موقع قناة الجزيرة الالكتروني بتاريخ 2015/01/05.

[3] إحصائيات صادمة وغريبة عن جرائم الأمن المعلوماتي، دراسة مقدمة من طرف موقع أرقام ديجيتال بتاريخ 2015/10/25.

VENTURES) بعنوان: Cyber Security Economy predictions 2017-2021، فإن العالم سينفق ما قيمته 1تريليون دولار خلال الفترة الممتدة من 2017 إلى غاية 2021 على منتجات وخدمات الأمن السيبراني لمكافحة الجريمة الالكترونية وفي هذا الإطار فقد سجل فتح حوالي مليون وظيفة خاصة بالأمن السيبراني خلال 2016، ومن المتوقع أن يكون هناك عجز بحوالي 1,5 مليون وظيفة خلال عام 2019[1].

والشكل الموالي يوضح تطور تكاليف الأمن السيبراني خلال الفترة الممتدة من 2011 إلى غاية 2021[2].

والشكل الموالي يبين أكثر المؤسسات أو الشركات تعرضا للإختراق خلال سنة 2015[3].

أما بالنسبة للدوافع الأساسية للإجرام المعلوماتي فقد تباينت ما بين جرائم من اجل السرقة، بدافع التجسس المعلوماتي، الحرب الالكترونية أو الاختراق من أجل قضية ما، والشكل الموالي يوضح النسب المئوية المقابلة لذلك[4].

ومن المتوقع أن تكبد الجرائم الالكترونية الاقتصاد العالمي حوالي 6 تريليون دولار بحلول سنة 2021 وهي ضعف الخسائر المسجلة سنة 2015 والمقدرة بحوالي 3 تريليون دولار[5]، وأكثر الخسائر تحدث إما بسبب فقدان بيانات ومعلومات هامة أو نتيجة لتكلفة صيانة عمليات الاختراق أو بسبب احتيال وسرقة أموال من الشركات، والشكل الموالي يوضح ذلك[6]:

ولقد عايشنا خلال سنتي 2015 و 2016 العديد من حوادث الاختراق والقرصنة ولعل أهمها ما يلي:

1/ في سبتمبر من سنة 2016 كشفت شركة ياهوو (Yahoo) عن أكبر عمليات قرصنة وسرقة لقاعدة بيانات مستخدميها، هذه العملية تعتبر من أكبر عمليات القرصنة في التاريخ لشركة تقنية، حيث حصل القراصنة على بيانات أكثر 500 مليون مستخدم، وفي ديسمبر من نفس السنة تعرضت الشركة نفسها، لصدمة أخرى حيث أعلنت بأن بيانات أكثر من مليار .....

والجزائر كغيرها من الدول لم تسلم هي الأخرى من ما يسمى الجريمة الالكترونية، حيث لم تسلم مواقع التواصل الاجتماعي وفضاءات تبادل المعلومات من عملية السطو على الصور والبيانات الشخصية، واستعمالها

[1] Cyber Security Economy predictions 2017-2021, cybersecurity ventures 2016.

[2] ينضر الملاحق الشكل رقم 1: تكاليف الأمن المعلوماتي خلال الفترة من 2011 إلى 2021

[3] ينظر الملاحق الشكل رقم 2: أكثر الشركات والمؤسسات اختراق خلال 2015.

[4] ينظر الملاحق الشكل رقم 3: الدافع الأساسي لجرائم المن المعلوماتي.

[5] Cyber Security Economy predictions 2017-2021, Op. Cit.

[6] ينظر الملاحق الشكل رقم 4: أسباب خسائر الجرائم الالكترونية.

كوسيلة للابتزاز والمساومة والتشهير، ناهيك عن استغلال بيانات الحسابات الشخصية بالإضافة إلى الاعتداء على أنظمة المعلومات، وحسب مصدر عليم لجريدة الفجر، فقد تم تسجيل أكثر من 500 جريمة إلكترونية[1] خلال سنة 2016، علما أن هذا يخص عدد الحالات التي قامت بالتبليغ فقط، والكيد ان البعض يرفض إيداع شكوى لاعتبارات اجتماعية وثقافية، وهو المر الذي جعل مصالح الدرك الوطني تتجند لحماية مستعملي الأنترنيت مثل مستخدمي مواقع التواصل الاجتماعي الذين يشكلون حيزا كبيرا من طبيعة استعمال هذه التكنولوجيا، كما تمت معالجة 385 جريمة إلكترونية من قبل الفرق المتخصصة في مكافحة الجريمة الالكترونية التابعة للأمن الوطني، إلى جانب تسجيل 57 قضية في مجال جرائم الاعتداء على سلامة الأنظمة المعلوماتية[2].

فقد سعت الدول والحكومات بشكل جدي للحد من الجرائم الإلكترونية وآثارها عبر طرق كثيرة منها:

- فرض سياسات دولية وعقوبات كبيرة على مرتكبي هذه الجرائم.
- تفعيل أحدث التقنيات والوسائل للكشف عن هوية مرتكبي هذه الجرائم.
- نشر التوعية في المجتمعات حول الجرائم الإلكترونية ومخاطرها وتعريف الأفراد بكيفية الحفاظ على معلوماتهم وخصوصياتهم كحساباتهم البنكية وبطاقاتهم الائتمانية.
- إنشاء خطوط هاتفية ومؤسسات معينة تابعة للدولة للإبلاغ عن الحالات التي تتعرض لمثل هذا النوع من الجرائم.
- توجيه التشريعات والقوانين وتحديثها بما يتماشى مع التطورات التكنولوجية لفرض قوانين جديدة فيما يُستجد من هذه الجرائم[3].

وللجرائم الإلكترونية أهداف تتمثل في:

- النيل من سمعة الضحية والتشهير بها بدافع الإنتقام وذلك من خلال الحصول على معلومات وبيانات الضحية من صور ومقاطع فيديو وأشياء أخرى تخص الضحية.
- إبتزاز الضحية وتهديده وذلك من أجل الحصول على مكسب مادي أو معنوي.
- إنتهاك فكر الضحية وخطفه ذهنيا وذلك من أجل إيقاع الضحية فريسة فكر يتعارض مع عقيدة المسلم الصافية مستغلا بذلك الضحية بالتيارات الفكرية الموجودة على الساحة العالمية وطبيعة توجهها وأهدافها.

---

[1] المؤتمر الوطني آليات مكافحة الجريمة الالكترونية في التشريع الجزائري، جزائر العاصمة، مارس 2017.

[2] أزيد من 500 جريمة إلكترونية في الجزائر سنة 2016، مقال منشور على الموقع الالكتروني لجريدة الفجر بتاريخ 2017/02/10، http://www.alfadjr.com/ar/realite/352178.html، تاريخ الاطلاع 2017/02/11.

[3] https://mawdoo3.com>

- التمكن من الوصول إلى المعلومات بشكل غير شرعي كسرقة المعلومات أو الإطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.
- الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالمؤسسات والبنوك والجهات الحكومية والأفراد وابتزازهم بواسطتها.
- تجنب نشر أي صور شخصية أو معلومات شخصية على مواقع التواصل الاجتماعي أو أي مواقع أخرى وذلك حتى لا تتعرض للسرقة ومن ثم الابتزاز من قبل مرتكبي الجرائم الالكترونية.
- عدم كشف كلمات المرور لأي حساب.
- وضع قوانين عقوبات ردعية لمرتكبي الجرائم المعلوماتية وذلك للحد من انتشارها.

كما لها أدوات تتمثل في:

وحتى يتمكن القراصنة (hackers) من تنفيذ جريمتهم الالكترونية يستلزم ذلك توفر أدوات لذلك من أبرزها:

- الاتصال بشبكة الأنترانت وتعتبر أداة رئيسية لتنفيذ الجريمة.
- توفير برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب.
- وسائل التجسس ومنها ربط الكاميرات بخطوط الاتصال الهاتفي.
- الباركورد وهي عبارة عن أدوات تستخدم لنسخ الترميز الرقمي وفك شيفرة الرمز.
- طابعات وهواتف نقالة.
- برامج ضبارة تتمثل وظيفتها بخداع الضحية وتشجيعه على تشغيله فيلحق الضرر الشامل بالحاسوب والملفات الموجودة عليه[1].

الفرع الثالث: خصائص الجريمة الالكترونية في التشريع الجزائري:

تختلف الجريمة الالكترونية عن غيرها من الجرائم العادية أو التقليدية لأن هذا النوع من الجرائم يرتبط بالحاسب الآلي أو تقنية المعلومات، وعليه سوف نتطرق أولا إلى أهم سمات هذه الجريمة، وثانيا السمات الخاصة بالمجرم[2].

أولا: سمات الجريمة الالكترونية في التشريع الجزائري:

وتتميز الجريمة الالكترونية بعدة خصائص أهمها:

[1] https//democratic.(26/08/2019)

[2] -بوحفص راوية ،الجريمة الالكترونية في التشريع الجزائري، مذكرة ماستر حقوق جامعة محمد خيضر بسكرة،2017-2018 ص 10.

أ/ عالمية الجريمة الإلكترونية:

مع ظهور شبكة الأنترنت أو الشبكة المعلوماتية كما يطلق عليها البعض أدى إلى تخطي كل الفواصل والحدود الجغرافية وظهور ما يسمى بالفضاء لا منتهي أو العالم الافتراضي، وجعل العالم ككل قرية صغيرة، وهذا بدوره ما ساعد على إضفاء صفة العالمية على الجريمة الالكترونية وتميزها بالطابع الدولي في أغلب الأحيان حيث تكون آثار هذه الأخيرة بتخطي حدود الدولة الواحدة،[1] فنقل المعطيات أو البيانات التي تتم عن طريق الحاسب الآلي عبر شبكة الأنترنت فيمكن نقل كم هائل منها في بضع دقائق من دولة إلى أخرى، أو عدة دول في آن واحد، وهذا ما سهل سرعة تنفيذ هذا النوع من الجرائم من جاني إلى مجني عليه تفصل بينهم مئات الكيلومترات، وخاصة في المعاملات الالكترونية التي تتم بين الأشخاص[2].

ب/ صعوبة إثبات واكتشاف الجريمة الالكترونية:

تتسم الجريمة الالكترونية بصعوبة اكتشافها، لأن معظمها تتم في الخفاء ولا يلاحظها المجني عليه ولا يدري حتى بوقوعها، حتى أنها لا تترك أثرا في مسرح الجريمة وإن وجد فمن الصعب إثباته، فليس هناك شيء ملموس أو مادي فهي عبارة عن مجموعة من البيانات والمعطيات يتم التلاعب بها في عالم غير مرئي ونقل المعلومات عبر نبضات إلكترونية، وما يزيد من صعوبات إثبات هذا النوع من الجرائم هي عدم إبلاغ الضحية أو المجني عليه[3].

ج/ جريمة ناعمة ومغرية:

الجريمة الالكترونية على عكس الجرائم الأخرى لا تتطلب جهد عضلي في تنفيذها، فهذه الأخيرة لا تكلف الجاني جهدا ابدا بل بضع دقائق وسوى أنامله لإتمامها، وإنما تحتاج منه توفر المعرفة بتقنية الحاسب الآلي أو الكمبيوتر، والتعامل السليم مع شبكة الانترنت ويتميز المجرم في هذه الجريمة بالتوافق مع المجتمع وأسلوبه الراقي في ارتكاب هذا النوع من الجرائم وتوفر لديه ثقافة عالية بهذه التقنية، ويرتكب الشخص هذه الجريمة بدافع اللهو أو القرصنة أو تفوقه على الكمبيوتر، أو لأجل مصلحة معينة ككسب الربح أو دافع الانتقام[4].

---

[1] هرة سعيدة، الجريمة الالكترونية في التشريع الجزائري، مذكرة مكملة لمتطلبات نيل شهادة الماستر، 2015-2016، ص 20.

[2] سوير سفيان، **جرائم المعلومات**، مذكرة ماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبوبكر بالقايد تلمسان، سنة 2010، ص20.

[3] مزيود سليم، **الجريمة المعلوماتية وواقعها في الجزائر وآليات مكافحتها**، المجلة الجزائرية للاقتصاد والمالية، جامعة المدية، العدد الأول، أفريل 2014، ص 120.

[4] فضيلة عاقلي، المرجع السابق، ص 08.

د/ جرائم فادحة الأضرار:

أكدت دراسات الشركة العالمية المتخصصة في تقنيات حماية وأمن المعلومات "إنتل سكيور يتي" أن الخسائر التي كبدتها الجرائم الالكترونية ضخمو، لاسيما أن الاعتماد على الحاسب الآلي في مختلف مجالات الحياة، وبالأخص المجال الاقتصادي وإدارة المؤسسات المالية والبنوك والشركات التجارية قد تؤدي إلى خسارة مبالغ مالية كبيرة بسبب هجوم الكتروني واحد مقارنة مع الجرائم التقليدية[1].

هـ/ قلة الإبلاغ عن وقوع الجريمة الالكترونية:

لا يتم في الغالب الإبلاغ عن الجرائم الالكترونية أو جرائم الأنترنت كما يطلق عليها البعض إما لعدم اكتشاف الضحية لها وإما خشية من التشهير، ويعتبر هذا السبب هو الغالب، حيث أن أغلب الجرائم الالكترونية تم اكتشافها بصدفة، بل وبعد وقت طويل من ارتكابها، فرد على ذلك أن الجرائم التي اكتشفت كبيرة جدا إلا أن التي لم تكتشف أكبر وهو رقم خطير بالضرورة، وبعبارة أخرى أن الفرق بين عدد الجرائم الحقيقية وبين ما تم اكتشافه فرق كبير[2].

المطلب الثاني: أنواع الجريمة الالكترونية:

ومن خلال هذا المطلب سوف نتطرق إلى أنواع الجرائم الالكترونية الأكثر انتشارا منها الجرائم الواقعة على الأشخاص وذلك في الفرع الأول والجرائم الواقعة على أمن الدولة في الفرع الثاني، والجرائم الواقعة على الملكية في الفرع الثالث والفرع الرابع الجرائم الواقعة على الأشخاص.

الفرع الأول: الجرائم الواقعة على الأشخاص:

لقد حمت مختلف التشريعات في قواعدها الدستورية الحياة الخاصة للفرد، حيث أنه من الطبيعي لكل شخص حياة خاصة به وأسراره الشخصية التي لا يجوز الاطلاع عليها من غيره بحيث يمكنه أن يحتفظ بها في أي مكان شاء، وتكون الاعتداء عليها عن طريق الحاسب الآلي في الجريمة الإلكترونية تلك المعلومات والأسرار الموجودة في حاسب الشخص وهو جريمة قائمة في حد ذاتها بمجرد الدخول إلى نظام المعالج للمعلومات والاطلاع الغير المشروع على أسرار الشخص.

ويكون كذلك الاعتداء على الأشخاص بالسب والقذف والتشهير والتحقير أو التهديد بالشخص عبر شبكة الأنترنت، حيث يتم نشر أخبار أو معلومات صحيحة أو غير صحيحة أو مشوهة هذه إلى أشخاص آخرين

[1] محمد خليفة، المرجع السابق، ص 38.

[2] خالد ممدوح إبراهيم، **أمن الجريمة الإلكترونية**، الدار الجامعية، 2008، ص 51.

بحيث يمكنهم الجاني بالاطلاع على المعلومات الخاصة بالمجني عليه على مواقع التواصل الاجتماعي أو البريد الالكتروني[1].

وكذلك يمكن أن تكون عن طريق نشر الإباحة والجنس سواء البالغين أو أطفال خاصة، وبحيث أن أكثر فئة معرضة للاستغلال الجنسي هي فئة الأطفال عن طريق الصور وتسجيلات الفيديوهات الجنسية التي يستمر نشرها ونقلها من شخص إلى آخر عبر الأنترنت[2].

الفرع الثاني: الجرائم الواقعة على الأموال:

مع تزايد المعاملات الالكترونية عبر شبكة الأنترنت أصبح البيع والشراء وكذا الإجار عبر هذه الأخيرة، والذي كان من نتاجه تطور وسائل الدفع والوفاء فوجدت وسائل السطو على المال بطريقة غير مشروعة التحويل الالكتروني، السرقة، القرصنة حيث يتم سرقة المال من خلال اختلاس البيانات والمعلومات الشخصية للمجني عليهم، كدخول إلى حسابات مصرفية خاصة بالعملاء في البنوك من قبل أحد الموظفين، وتحويل المال إلى حسابه، ولذلك باستخدام الجاني الحاسب الآلي والأنترنت للوصول إلى المصارف والبنوك[3].

وكذلك يدخل ضمن جرائم الاعتداء على الأموال في الجريمة الالكترونية تجارة المخدرات عبر الأنترنت، قرصنة البرمجيات وهي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية، وأيضا جريمة القمار عبر شبكة الأنترنت حيث وجدت لها كازينوهات افتراضية أو اندية القمار الافتراضي التي أصبحت فيها بعد مسرحا كذلك لجريمة غسيل الأموال[4].

الفرع الثالث: جرائم ضد الملكية:

يمكن أن يكون النشاط المعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية والأدبية مثال ذلك استخدام النظام المعلوماتي في السطو علة بنوك المعلومات التي تتضمنها برامج نظام معلوماتي أخرى أو حالة تخزين واستخدام هذه المعلومات أو التفريط فيها دون إذن من صاحبها، وذلك لأن استخدام معلومة معينة دون إذن من صاحبها يتضمن اعتداء على حقوق المعنوية بالإضافة إلى كونه اعتداء على قيمتها المالية كون أن المعلومة لمالها

[1] خالد عيادي الحلبي، **إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت**، دار الثقافة، عمان، 2011، ص 61.

[2] منديلي رحيمة، المرجع السابق، ص 09.

[3] سورية ديش، **أنواع الجريمة الالكترونية وإجراءات مكافحتها**، مجلة العلوم السياسية والقانون، جامعة جيلالي ليابس، سيدي بلعباس، العدد الأول 2017، ص 149.

[4] منديلي رحيمة، المرجع السابق، ص 09.

إضافة إلى قيمتها المادية كما يندرج أيضا ضمن الحقوق الفكرية لذلك، براءة الاختراع باعتبارها تمثل فكرة المخترع تحتوي على حق معنوي وآخر مالي للمخترع[1].

الفرع الرابع: جرائم ضد أمن الدولة:

تعهد هذه الجرائم من أخطر الجرائم الالكترونية خاصة الإرهاب المعلوماتي، والجريمة المنظمة المعلوماتية، حيث تاحت الانترنت للكثير من المنظمات الإرهابية الترويج لأفكارها ومعتقداتها، وأدت إلى ظهور جريمة أخرى أخطر منها التجسس الالكتروني على الدول بالاطلاع على مختلف الأسرار العسكرية والاقتصادية بين الدول المتصارعة، كما تعطي الشبكة العنكبوتية فرصة للتأثير على المعتقدات الدينية وتقاليد المجتمعات مما يسهل خلق الفوضى داخل الدولة والمساس بأمنها الداخلي وبنظامها العام[2].

لكن هناك حالات ضئيلة أين يتم الإبلاغ فيها عن الجرائم الالكترونية نسبة إلى شخصية المجني التي تلعب دور مهم في عملية الإبلاغ[3].

ثانيا: صفات المجرم المعلوماتي:

لا شك أن الشخص الذي يرتكب الفعل غير المشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع، يعد مجرما في نظر القانون ويتعرض للعقاب إذا ما اقترف جريمته وتكون العقوبة هدفها تحقيق الردع العام أو الخاص أما الجريمة الالكترونية تتطلب مقدرة ذهنية لدى الجاني.

فلا بد أن يكون الجاني ذو كفاءة عالية في مجال التقنية، يحتاج إلى جهاز حاسوب موصول بالشبكة العنكبوتية إلى جانب درايته بمختلف الأنظمة المستعملة في هذا المجال، ويمكن حصر هذه الصفات في عدة جوانب[4].

---

[1] أحمد خليفة الملط، **الجرائم المعلوماتية**، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، مصر، 2006، ص 184.

[2] منديلي رحيمة، المرجع السابق، ص09.

[3] شهدت الجزائر في السنوات الأخيرة تضاعف مخيف للجرائم الالكترونية، التي باتت تهدد كيان المجتمع، حيث تقول زهرة فاسي أستاذة في علم الاجتماع أن أكثر عرضة لهذا النوع من الجرائم هن النساء الاتي لا يبلغن عن الفاعل خوفا من الفضيحة، مشيرة إلى أن العديد من الفتيات رضخن للابتزاز وسلمن مبالغ مالية ضخمة مقابل عدم نشر صورهن على سبيل المثال، ومنهم من هربت من بيوت الأهل خوفا من الفضيحة. / أنظر: مقال صحفي باسم خديجة بودومي، الجزائر، www.dw.com، يوم 2019/08/26.

[4] عائشة بن قارة، **حجة الدليل الإلكتروني في مجال الاثبات الجنائي في القانون الجزائري والقانون المقارن**، د.ط، دار الجامعة الجديدة، الإسكندرية، مصر، 2010، ص 41.

أولا: السمات الشخصية للمجرم المعلوماتي:

يختلف المجرم ألمعلوماتي كثيرا عن المجرم في الجرائم التقليدية، ذلك أن له سمات خاصة تميزه عن غيره إلا أن هذه الصفات تقترب في كثير من الأحيان من سمات المجرمين ذوي الياقات البيضاء.

فكلاهما قد يكونوا من ذوي المناصب الرفيعة المستوى ويتمتعون بالاحترام والثقة والقدرة على التكيف الاجتماعي، بالإضافة إلى ذلك يمتلك هذا المجرم المعلوماتي المعرفة على كافة الظروف التي تحيط بالجريمة وتنفيذها، وإمكانية نجاحها، فيتمتع هذا الأخير بقدر لا يستهان من المهارة بتقنيات الحاسوب والأنترنت[1].

فيعتبر إجرام الانترنت إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، مجرم الانترنت يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها أحد سواه، وذلك من أجل اختراق الحواجز الأمنية في البيئة الالكترونية ثم نيل مبتغاه.

كما يتصف مجرمو الانترنت بالخوف من كشف جرائمهم، فتساعد طبيعة الأنظمة المعلوماتية نفسها مجرمي الانترنت على الحفاظ على سرية أفعالهم، ذلك أن الكثير ما يعرض المجرم إلى اكتشاف أمرع هو أن يطرأ في أثناء تنفيذه لجريمته عوامل غير متوقعة لا يمكن التنبؤ بها.

نجد أن أغلب الجرائم التي ترتكب مكونة من مجموعة أشخاص يحدد لكل شخص دور معين، ويتم العمل فيها لتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمن فيها متخصص في الجانب التقني من المشروع الإجرامي، وشخص آخر من المحيط الخارجي لتغطية التلاعب ولتحويل المكاسب إليه[2].

ثانيا: الدافع إلى ارتكاب الجريمة:

تتباين دوافع ارتكاب الجريمة الالكترونية تبعا لطبيعة المجرم ومدى خبرته في مجال الحاسب الآلي، ومما لا شك فيه أن وراء كل فعل سواء كان يحمل في طياته جانب الخير أم الشر إلا وخلفه دافع غرض أو غاية من ذلك. وبالنسبة لجرائم الكمبيوتر والانترنت دوافع عديد تحرك الجناة لارتكاب أفعال الاعتداء الغير المشروعة، وبالتالي نتطرق إلى بعض الدوافع كالآتي:

1/ السعي إلى تحقيق الكسب المالي:

يعد هذا الدافع من بين أهم الدوافع تحريكا للجناة لاقتراف جرائم الالكترونية، ذلك أن خصائص هذه الجرائم وحجم الربح الممكن تحقيقه من بعضها، لا سيما غش الحاسوب أو الاحتيال المرتبط بالحاسوب يتيح تعزيز هذا الدافع.

[1] خليفة محمد، المرجع السابق، ص 33.

[2] عائشة بن قارة، المرجع السابق، ص 41.

إذا ما انتقلنا للدراسات الحديثة نجد أن هذا الدافع يعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية، وفي مقدمة هذه الدراسات والتقارير الإحصائية نجد التقارير الصادرة عن مركز احتيال المعلومات الوطني للولايات المتحدة الأمريكية[1].

2/ الانتقام من رب العمل وإلحاق الضرر به:

لقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق الأعمال الأخرى، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل، والمشكلات المالية، هذه الأمور قد تدفع إلى النزعة إلى تحقيق الربح، لكنها في حالات عديدة، مثلث قوة حركة لبعض العاملين لارتكاب جرائم الكترونية، باعثا للانتقام من المنشأة أو رب العمل.

3/ الرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية:

يرى البعض أن الدافع إلى ارتكاب الجرائم الالكترونية، يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ومع أن الدراسات لا تظهر هذه الحقيقة، إذ يظهر في قهر النظام نسبة معتبرة من جرائم الحاسوب، كما هو الحال بالنسبة إلى ما يعرف أنشطة الهاكر، حيث يميل مرتكبو هذه الجرائم إلى تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجاد سبل لتحطيمها، ويتزايد شيوع هذا الدافع لدى صغار السن، الذين لديهم شغف المغامر، محاولين بذلك كسر حواجز أمن أنظمة الحواسيب وشبكات المعلوماتية، ولإظهار تفوقهم على وسائل التقنية[2].

ثالثا: أنماط مجرمي المعلوماتية:

يمكن تصنيف مرتكبي الجرائم على أساس أغراض الاعتداء إلى الفئات التالية:

1/ الفئة الأولى: تضم نوعين من المتطفلين، الهاكر والكراكز.

أ-الهاكر:

الهاكر هم الأشخاص الشغوفين والذين لديهم ميل لفهم واستعمال التقنية والبرامج، ويصنف على أنهم الأشخاص الذين يدخلون إلى المواقع المعلوماتية بدون استخدام العنف، حيث يعرف الأستاذ Vivant الهاكر بأنه: "كل شخص يدخل إلى النظام لإرضاء رغبته بدون تخريب للمعطيات الموجودة داخل النظام"، وهناك من يطلق على الهواة أو Hacker بصغار نوابغ المعلوماتية.

---

[1] جعفر حسن الطائي، **جرائم تكنولوجيا المعلومات**، رواية جديدة للجريمة الحديثة، ط1، جامعة عمر المختار، 2007، ص 168.

[2] المرجع نفسه، ص 169.

وتستعمل هذه الطائفة أجهزة خاصة بهم، وغالبا ما يرتكبون هذه الجرائم بمحض الصدفة فيصلون إلى نظام المعلوماتية سواء خاصة بالوزارات أو الشركات التجارية، وعليه فإن الدافع الاجرامي لديهم غير موجود عند اتصالهم[1].

ولا يمكن تصنيفهم من بين الطوائف الاجرامية لأن نادرا ما تكون غير شريفة، بل تميل إلى المغامرة والاكتشاف ويمكن لهؤلاء أن تتطور أعمالهم وتتغير شخصيتهم ليدخلوا في نطاق Crackers.

ب–الكراكز:

تعرف الكراكز هذه الطائفة بالمجرمين البالغين، الذين يتمتعون بالمهارات والمعارف الفنية في مجال الأنظمة الالكترونية، وتدل الاعتداءات التي يقترفها أفراد هذه الطائفة إلى جانب كبير من الخطورة الإجرامية[2]، على أساس أن الهاكر ومن يقوم بتحريف وتحويل التقنيات المطورة من طرف الهاكر لأغراض مادية ويطلق عليهم بـ Spiders لأنهم يعملون في الخفاء، ولا يتركون آثار مادية لأفعالهم، لذلك فهم أشد خطورة، إذا ما تم تبادل تقنياتهم فيما بينهم وشكلوا ما يعرف بالجماعات أو الفرق المتخصصة [3].

2/ الفئة الثانية:

تشمل فئة المحترفين التي تعد أخطر من بين مجرمي التقنية العالية تتميز هذه الطائفة بالتقنية العالية والمهارات التقنية، وبالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها، حيث تهدف اعتداءاتهم من جهة إلى تحقيق الكسب المادي لهم، أو لجهات التي كفلتهم وسخرتهم لارتكاب هذا النوع المستحدث من الجرائم، ومن جهة أخرى قد تهدف إلى تحقيق أغراض سياسية، أو التعبير عن موقف فكري، ويمكن تقسيم هذه الطائفة إلى مجموعات متعددة تبعا لتخصصهم بنوع معين من الجرائم، أو طبقا للوسيلة المعتمدة في ارتكاب الجرائم على سبيل المثال، طائفة محترفي التجسس الصناعي أو طائفة مجرمي الاحتيال والتزوير[4].

---

[1] نذكر على سبيل المثال، عصابة 414 من أمريكا نسب إليها 60 فعلا، أنظر إلى باطلي غنية، المرجع السابق، ص 38.

[2] محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 186.

[3] عائشة قارة، المرجع السابق، ص 42.

[4] نذكر على سبيل المثال ما حدث أثناء محادثات السلام في كامب ديفيد الثانية بين الفلسطينيين والاحتلال الإسرائيلي تحت رعاية الولايات المتحدة الأمريكية، فقد أرسل القراصنة فيروسا جديد غير معروف إلى مجموعة من الموظفين والصحفيين ترتب عليه عدم إمكانية تحميل صور الرؤساء المجتمعين حيث كانت الرسائل مرسلة إلى عنوان الوزارة الخارجية تحمل عنوان الظرف الضاحكة "fanny jokers" وبمجرد فتح الرسالة فإن فيروسا غير معروف يبدأ بتدمير القرص الصلب ثم يرسل تلقائيا نسخة من البريد الالكتروني الحامل للفيروس إلى كل عنوان بريدي موجود في الجهاز. / أنظر: محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 186.

3/ الفئة الثالثة:

يقصد بها طائفة الحاذقون، يغلب على هذه الطائفة عدم وجود اهداف وأغراض إجرامية لدى أفرادها، فهم لا يسعون لإثبات مقدراتهم التقنية، ولا إلى تحقيق مكاسب مادية أو سياسية، إنما يحركهم الثأر والرغبة بالانتقام كأثر لتصرف صاحب العمل معهم، أو لتصرف منشأة ما سبق لهم التعامل معها، ولذلك فهم ينقسمون إلى مستخدمين للنظام بوصفهم موظفين أو علاقة ما بالنظام محل الجريمة، وإلى غرباء عن النظام ولا يتصف أعضاء هذه الطائفة بالضرورة بالمعرفة التقنية الاحترافية، كما تغلب على أنشطتهم من الناحية التقنية استخدام الفيروسات والبرامج الضارة[1]، الهادفة لتخريب واتلاف الأنظمة المعلوماتية سواء كان الاتلاف كلي أو جزئي، ليس هناك ضوابط محددة بشأن أعمارهم وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها، لتوفر ظروف وعوامل تساعد ذلك.

وبالتالي فإن سمات هذه الطائفة تضعها في مؤخرة الطوائف السابقة الذكر على أساس أنهم أقل خطورة من غيرهم من مجرمي التقنية، لكن ذلك لا يمنع أن تكون الأضرار التي نجمت عن الأنشطة بعضهم جسيمة ألحقت خسائر فادحة بالمؤسسات المستهدفة سواء تلك التي يعملون فيها، أو التي تم استهدافها لإلحاق الضرر بها[2].

4/الفئة الرابعة:

تعتبر طائفة ظهرت حديثا يطلق عليها تسمية صغار نوابغ المعلوماتية أو طائفة صغار السن، ولقد ثار جدل فقهي حول تصنيف هذه الطائفة ضمن مجرمي المعلوماتية كغيرهم دون تمييز وانقسم هؤلاء الفقهاء بصدد ذلك إلى ثلاثة اتجاهات اولها:

وهو الاتجاه الذي يرى أنه من غير الملائم تصنيف هؤلاء الشباب ضمن الطوائف الإجرامية لأن لديهم ببساطة ميلا للمغامرة والتحدي والرغبة في الاكتشاف.

وثانيها يؤيد هذا الاتجاه هذه الفئة على أساس أن لها الفضل في كشف الثغرات الأمنية في تكنولوجيا المعلومات.

اما الثالث يصنف هذه الطائفة ضمن مجرمي الإنترنت وذلك باعتبار أن العبث في الحواسب قد يؤدي إلى ارتكاب جرائم والتي قد ينزلق أفرادها في طوائف محترفي الإجرام ألمعلوماتي.

[1] محمد طارق عبد الرؤوف الخن، المرجع السابق، ص ص 187،188.

[2] جعفر حسن الطائي، المرجع السابق، ص 38.

المطلب الثالث: أركان الجريمة الإلكترونية:

سبق وأن أشرنا في معرض حديثنا عن مفهوم الجريمة الإلكترونية بالتعرض إلى الجدل الواقع في تسميتها بين التشريعات المقارنة والتشريع الجزائري، فرغم اختلاف التشريعات في تعريفها إلا أنها تنصب في نفس المجرى، كذلك تضمن حديثنا خصائص هذه الجريمة من جهة وسمات التي يتصف بها المجرم الالكتروني من جهة أخرى[1].

أما في هذا المطلب نتطرق إلى تبيان أركان الجريمة المعلوماتية من الركن المادي المتمثل في السلوكيات المجرمة والتي تختلف من جريمة إلى أخرى (الفرع الأول) والركن المعنوي الذي يعبر عن إرادة المجرم المعلوماتي (الفرع الثاني).

الفرع الأول: الركن المادي للجريمة الالكترونية:

يعتبر الركن المادي في الجريمة التقليدية فعل أو السلوك المجرم الذي يقوم به الجاني ملامسا لأرض الواقع حتى يمكن التحقق منه وإثباته كما يجب أن يرتبط السلوك الإجرامي والنتيجة الضارة والعلاقة السببية.

بمعنى حتى يعاقب المجرم على سلوكه الإجرامي لابد أن يتطابق هذا الفعل المجرم مع النموذج الإجرامي المنصوص عليه في قانون العقوبات[2].

أما الركن المادي في الجريمة الإلكترونية فيتطلب قيام السلوك الإجرامي والنتيجة والعلاقة السببية، مع العلم أنه يمكن تحقق الركن المادي دون حدوث النتيجة كالتبليغ عن الجريمة قبل تحقق نتيجتها.

ويتخذ الركن المادي عدة صور بحسب نوع الجريمة وهو ما نقوم بتبيانه في ثلاث عناصر أساسية، السلوك الإجرامي، النتيجة الضارة، العلاقة السببية.

أولا: السلوك الإجرامي:

ما يميز الجرائم الإلكترونية بشكل عام، هو وجود حاسب آلي وشبكة معلوماتية، حيث لا يمكننا تصور وجود جريمة الكترونية من دون الحاسب الآلي وشبكة الأنترنت، التي يعتبر استخدامها كشروع كأصل عام ولكن الخلاف يثور من حيث استخدام هذه الوسائل الحديثة لغايات غير مشروعة، ولذلك تعد الوسيلة الإلكترونية من أهم مقومات السلوك الإجرامي في الجرائم الإلكترونية،[3] فالسلوك هذا يتطلب بينة رقمية من حيث الجهاز الالكتروني والاتصال بالأنترنت، لارتكاب الجرائم الإلكترونية بشكل خاص، كما ويتطلب الأمر المعرفة بكيفية استخدام هذه التقنية مثل كيفية تحميل صور مخلة بالآداب العامة على الجهاز، وإعداد برنامج "فيروس" تجهيزا لنشره على الأنترنت، إن المنطق التقني الذي ذكرناه يمثل سلوكا ماديا إيجابيا للجرائم الالكترونية، فهذا يجعل الجرائم الالكترونية

[1] مذكرة لنيل شهادة الماجيستير في الحقوق تخصص القانون الخاص والعلوم الجنائية، جامعة عبد الرحمن ميرة، بجاية.

[2] معتوق عبد اللطيف، المرجع السابق، ص25.

[3] الحسيناوي علي جبار، **جرائم الحاسوب والانترنت**، د.ط، دار الباروزي للنشر والتوزيع، عمان 2009، ص37.

ذات طابع موحد يتمثل في السلوك والنشاط المادي كعنصر أساسي للجرائم الالكترونية، ونلمس ذلك من خلال ما عبر عليه المشرع الجزائري في الفصل السابع من ق.ع.ج باستخدام عبارة المساس بأنظمة المعالجة الآلية للمعطيات، حيث قام بتجريم بعض الأفعال المساهمة في حدوث الجريمة الالكترونية[1]، ويتخذ السلوك الإجرامي في الجرائم الالكترونية صورتين:

*الصورة الأولى تتمثل في السلوك الإيجابي والذي يتطلب مجهود بدني يتمثل في العالم الخارجي من حركات عضوية يأتيها الجاني بهدف الاعتداء على المصلحة التي يحميها المشرع، ومثال ذلك: كل الأفعال التي يرتكبها الجاني، كفعل الدخول والبقاء عن طريق الغش في كل أو جزء من نظام المعالجة الآلية للمعطيات، نص المشرع الفرنسي على فعل الدخول والبقاء في مادة 1/323-1 من قانون العقوبات الفرنسي، والتي تنص كالآتي: "فعل الدخول أو البقاء –بطريق الغش- داخل كل أو جزئ من نظام المعالجة الآلية للمعطيات، يعاقب عليه بالحبس لمدة سنتين وبغرامة مقدارها 60000 أورو"[2].

كما قام المشرع السعودي بنص في مادة الثالثة من نظام مكافحة الجرائم الالكترونية، على بعض الأفعال التي تعتبر السلوك الإجرامي المكونة للركن المادي لهذه الجريمة، نذكر البعض منها:

الدخول غير المشروع لتهديد شخص أو ابتزازه، أو الدخول غير المشروع إلى المواقع الالكترونية بهدف تغيير تصاميم الموقع أو إتلافه أو تعديله أو تغيير عنوانه. فعل التصنت إلى ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي ...الخ.

بينما يكون السلوك الإجرامي في جريمة السرقة المعلوماتية[3]، والإتلاف العمدي للمعلومات والبرامج أو جريمة القرصنة والاحتيال المعلوماتي، سلوكا إجراميا متعددا يبدأ من الدخول إلى نظام الحاسب الآلي أو إلى موقع ما على

---

[1] الحسيناوي علي جبار، المرجع نفسه، ص 252.

[2] قانون العقوبات الفرنسي رقم 1159/97 المؤرخ في 19 ديسمبر 1997 المتضمن قانون العقوبات الفرنسي.

[3] السرقة هي نزع المال من حيازة صاحبه دون رضاه وعلمه وإدخاله في حيازة السارق، أما بالنسبة لمن يقوم بسرقة البيانات بأخذ نسخة من البيانات أو المعلومات أو برامج معينة وأدخلها في حيازته لكن لم يخرج المعلومات من حيازة مالكها بل أبقاها في حيازته بناء على هذا فإن السرقة لهذا المعنى تعارض تعريف السرقة المنصوص عليها في قانون العقوبات وإمكانية أن تكون البيانات أو البرامج محلا للسرقة لأنها أشياء غير محسوسة وغير مادية يمكن أن تقع السرقة على البرامج والمعلومات وبالتالي تخضع لذات أحكام جريمة السرقة ولأركانها وهما الركن المادي والركن المعنوي في أن الركن المادي يتمثل في السرقة أخذ نسخة عن المعلومات أو البرامج دون إذن صاحبها وعلمه، أما الركن المعنوي يتمثل في القصد الجرمي القائم على العلم والإرادة وذلك لتحقيق مصلحته الشخصية./ أنظر: وسيم طعمة، **السرقة المعلوماتية "دراسة مقارنة"**، مجلة جامعة البحث، جامعة دمشق، العدد 68، سوريا 2017، ص 167-168.

شبكة الأنترنت بوجه غير شرعي ثم القيام بالتلاعب بمحتوياته،[1] ينطوي هذا التلاعب على عدة أنشطة إجرامية من إدخال البيانات غير صحيحة أو محو أو تدمير محتويات هذا النظام، أو نشر لمواد مخلة بالنظام والآداب العامة.

قد يكون النشاط الإجرامي في الجرائم الالكترونية وقتيا، أي يبدأ وينتهي بمجرد تمامه، مثل السرقة المعلوماتية أو الاعتداء على معطيات الحاسب الآلي بإتلافها، وقد يكون مستمر مثل إنشاء مواقع لتحريض القصر على الفسق أو الانتحار[2].

* أما الصورة الثانية وهي السلوك السلبي، وهو الامتناع عن إتيان أمر يوجبه المشرع، فمن الممكن التوقف عن عمل معين كان من الواجب مباشرته، وهذا الامتناع عن قاعدة فرضها المشرع مثل امتناع المنفذ البحري من إنقاذ غريق كان بإمكان إنقاذه، أما الامتناع في الجرائم الالكترونية يكون مثل، امتناع موظف أمن عن حماية بيانات ومعلومات الشركة التي يعمل بها، أو عدم إبلاغ عن الجريمة لحفاظ على حقوق الغير وخصوصيتهم.

وبالتالي فالسلوك الإجرامي في الجريمة الالكترونية يتم عن طريق الجهاز الالكتروني أيا كان نوعه أو شكله، متصلا بشبكة الأنترنت، وبدون هذه الوسيلة لا يمكن مباشرة السلوك الإجرامي، وقد يكون سلوك إيجابي، بمباشرة الفعل من الجاني باستخدام الوسائل الالكترونية، وقد يكون سلوك سلبي بامتناع عن الفعل كان من الواجب اتيانه وهو نادر الحدوث، وفي الغالب يرتكب من قبل موظفين مختصين[3].

ثانيا: النتيجة الإجرامية:

تعتبر النتيجة الإجرامية العنصر الثاني للركن المادي للجريمة، وهي عبارة عن الضرر الذي نتج عن السلوك الإجرامي سواء كان فعلا أو تركا، وهو الأثر الخارجي الذي يتولد عن السلوك ويحدث تغييرا يعتد به القانون، وذلك طبقا للتصور المادي للجريمة، أما التصور الشرعي أو القانوني فهو الاعتداء على المصلحة التي يحميها القانون.

---

[1] لقد تعددت التعاريف بشأن جريمة الاحتيال عبر الأنترنت، نذكر منها على سبيل المثال: أنها سلوك احتيالي يستخدم فيه الحاسوب الآلي والأنترنت كوسيلة للحصول على امتياز مالي. / أنظر: محمد طارق عبد الرؤوف الخن، المرجع السابق، ص37.

[2] معتوق عبد اللطيف، المرجع السابق، ص 23.

[3] كلعبة الحوت الأزرق Blue whale أو تحدي الحوت الأزرق، وهي لعبة على شبكة الانترنت، حيث قام فيليب بودكين بابتكار هذه اللعبة وكان هدفه منها تنظيف المجتمع من خلال دفع الناس على الانتحار الذي اعتبر أنه ليس له قيمة، تتكون اللعبة من تحديات لمدة 50 يوما وفي التحدي النهائي يطلب من اللاعب الانتحار، بدأت اللعبة بالانتشار الواسع في روسيا ونجم عنها العديد من الضحايا وخلق موجة منن الذعر في روسيا، لتنتشر بعد ذلك في مختلف مناطق العالم تعتمد هذه اللعبة على غسل لدماغ المراهقين الضعفاء، وأمرهم بالقيام بأعمال معينة مثل مشاهدة أفلام الرعب و الاستيقاظ في ساعات متأخرة من الليل، وإيذاء للنفس وبعد أن يتم استنفاذ قواهم في النهاية يتم أمرهم بالانتحار. / انظر: الموقع الالكتروني: www.albawaba.com

وبالتالي تعتبر الأثر المباشر للسلوك الجرمي غير المشروع، يعرف من الفقه النتيجة الإجرامية على أنها ذلك التغيير الذي يحدث كأثر للسلوك أو الفعل غير المشروع الذي قام به الجاني، ويطلق على هذا التغيير الذي يحدث في العالم الخارجي بالمدلول المادي للنتيجة الإجرامية[1].

أما المدلول القانوني للنتيجة الإجرامية فو ذلك الاعتداء على الحق الذي يحميه القانون وهو يمثل التكييف القانوني للنتيجة المادية التي خلفها الفعل الغير المشروع، وتعتبر الجريمة الالكترونية كغيرها من الجرائم والتي يفترض وجود النتيجة الإجرامية فيها، وتختلف النتيجة الضارة في الجريمة المعلوماتية حسب نوع الجريمة المرتكبة.

ففي جريمة تزوير المعلومات أو البيانات والتي تدخل ضمن جرائم المعلوماتية، فإن النتيجة الإجرامية فيها تحريف الحقيقة في البيانات والمعلومات الموجودة في جهاز الكمبيوتر أو في الموقع الالكتروني، إذا النتيجة هي الأثر المادي المترتب على القيام بالفعل الغير المشروع، وهي أيضا الأثر القانوني الذي يمثل الاعتداء على خصوصيات الناس ومعلوماتهم بتعديلها أو حذفها أو تحريفها بما يخالف القانون.

أما في جريمة التلاعب غير المصرح به بالمعلومات تكون النتيجة الضارة، هي وقوع ضرر فعلي على هذه المعلومات ويكون ذلك بتغيير حالتها عن طريق الإزالة أو التعديل أو المحو.

مما تقدم نستخلص أن الجريمة الالكترونية هي كغيرها من الجرائم يفترض فيها وجود النتيجة الإجرامية كأساس لقيام الركن المادي لهذا النوع المستحدث من الجرائم، حيث تعتبر من العناصر المكونة للركن المادي، والذي يعد من أهم أركان الجريمة والذي لا تقوم الجريمة بدونه[2].

بصدد دراستنا لنتيجة الجريمة المعلوماتية بصفة عامة دون الحديث بالتفصيل عن النتيجة الإجرامية لكل جريمة معلوماتية بالتالي تثير النتيجة الإجرامية في الجرائم الإلكترونية مشاكل عديدة على سبيل المثال، مكان وزمان تحقق النتيجة، فلو قام أحد المجرمين في أمريكا باختراق جهاز حاسب آلي رئيسي وهو ما يعرف باسم الخادم Server في أحد البنوك في فرنسا، وهذا الجهاز الخادم موجود في الصين، ومعرفة وقت حدوث الجريمة، إما بالنظر إلى توقيت بلد المجرم أو توقيت بلد البنك المسروق، أم توقيت الخادم في الصين، وهذا ما يثير إشكالا بالنسبة إلى وقت حدوث الجريمة بالإضافة إلى القانون الواجب التطبيق في هذا الشأن.

كما يواجه الخطر أو الضرر بوصفه نتيجة إجرامية مشاكل أخرى، كالمتعلقة بجرائم العدوان الفيروسي، إذ تثير هذه النوعية من الجرائم مشكلة تحديد الضرر وهي من الصعوبات التي تواجه الفكر القانوني المعاصر في هذا المجال

[1] خيرت علي محرز، **التحقيق في جرائم الحاسب الآلي**، دار الكتاب الحديث، الإسكندرية، مصر، 2012، ص 123.

[2] لورنس سعيد الحوامدة، **الجرائم المعلوماتية أركانها وآلية مكافحتها**، دراسة تحليلية مقارنة، مجلة الميزان للدراسات الإسلامية والقانونية، كلية الحقوق، المملكة العربية السعودية، 2016، ص 20،19.

خاصة إذا اشترط المشرع تحقق نتيجة معينة أما أثر النتيجة الإجرامية ذا البعد الدولي، سواء في شكل امتداد الضرر أو الخطر إلى ما يتجاوز الحدود الإقليمية التي وقع فيها السلوك والنتيجة، يأخذ هذا الامتداد شكل العدوان المحدد على مصلحة قائمة ومشروعة في دولة أو دول متعددة.

ثالثا: العلاقة السببية:

يقصد بالعلاقة السببية هي العلاقة بين السلوك الإجرامي فعلا أو تركا وبين النتيجة الإجرامية، بمعنى السلوك الإجرامي هو السبب في إحداث النتيجة الإجرامية، ولولا هذا السلوك ما كانت لتحدث النتيجة الإجرامية، وتبرز الأهمية القانونية لعلاقة السببية من حيث أنها من العناصر الأساسية المكونة للركن المادي للجريمة، وتحققها يعد شرطا جوهريا من شروط المسؤولية الجزائية، فإذا أسندنا النتيجة الإجرامية إلى السلوك وكانت هناك إرادة حرة واعية، توفرت أسباب قيام المسؤولية الجزائية، أما إذا لم يكن هناك علاقة بين النتيجة الإجرامية والسلوك انتفت المسؤولية الجزائية[1].

ولكي تكتمل علاقة السببية في جريمة التعدي على الحق في الخصوصية، يجب أن يكون هناك اتصال بالأنترنت من خلا جهاز الكتروني، ومن ثم اختراق جهاز ما أو موقع للوصول إلى بياناته الخاصة، وبعدها يتم نشر هذه البيانات من معلومات أو صور عبر موقع معد مسبقا لذلك، أو عن طريق الواقع الالكترونية كمواقع التواصل الاجتماعي، وتثبت كذلك علاقة السببية في جريمة حيازة صور إباحية لأطفال في حاسوب بمجرد ثبوت الضرر من خلال بث هذه الصور، فتظهر العلاقة السببية بين حيازة الصور وبين ترويجها أو عرضها أو تداولها.

فتعد العلاقة السببية عنصر مهم من عناصر الركن المادي للجريمة، حيث تعتبر حلقة وصل بين السلوك الإجرامي والنتيجة الإجرامية، ذلك بإثبات أن هذا السلوك هو سبب في حدوث النتيجة الضارة[2].

أما في نطاق الجرائم الالكترونية تعتبر العلاقة السببية أساسية لقيام هذا النوع المستجد من الجرائم، والمبدأ العام الذي يحكم العلاقة السببية أن الإنسان لا يسأل إلا عن النتائج التي يكون لنشاطه دخلا في إحداثها فاستحقاق العقاب في القانون هو رهن قيام الرابطة السببية بين نشاط الجاني وبين الواقعة الإجرامية، وبالتالي ينبغي لمسائلته أن تكون هناك رابطة بين ماديات الفعل وبين النتيجة الإجرامية.

---

[1] خيرت علي محرز، **التحقيق في جرائم الحاسب الآلي**، دار الكتاب الحديث، الإسكندرية، مصر، 2012 ، ص 32.

[2] خيرت علي محرز، المرجع نفسه، ص ص 124، 125.

ففي جريمة انتهاك الحق في الخصوصية عبر شبكة الأنترنت يجب أن يكون هناك دخول غير مصرح به باستخدام الحاسوب والقيام باختراق الخوادم المختلفة في مسارها، ثم بعد ذلك التعدي على الخصوصية لموقع ما، وتكون العلاقة السببية قائمة بمجرد ثبوت الضرر الناتج عن السلوك الغير المشروع[1].

ومنه فقد برزت عدة اتجاهات فقهية حول المعيار المناسب لقيام العلاقة السببية وهي كالتالي:

أ/ نظرية تعادل الأسباب:

وقد قال بها الفقيه الألماني (فون بوري)، ومضمونها مساواة جميع العوامل التي تساهم في إحداث النتيجة الإجرامية، فهي كلها متعادلة ومتساوية من حيث قوة أثرها في حصول النتيجة ولما كان سلوك الجاني إحدى هذه الأسباب، فإن يسأل عن النتيجة الإجرامية حتى ولو كانت الأسباب الأخرى مرادها فعل الطبيعة، ومثال ذلك أن يطلق أحدهم النار على آخر ليقتله[2]، ويتم نقله بسيارة الإسعاف التي ترتطم بشجرة سقطت على الطريق فتضاعف من إصابة المجني عليه ثم ينقل إلى المستشفى حتى يتلوث جرحه من العلاج الغير المناسب فيموت، فالجاني وسقوط الشجرة بفعل الطبيعة وتلوث الجرح من المستشفى كلها عوامل ساهمت في وفاة المجني بقدر متساوي، ولذلك تتوافر السببية في سلوك الجاني وبين النتيجة الإجرامية في هذه الجريمة[3].

ويؤخذ على هذه النظرية أنها قررت تعادل الأسباب من حيث أثرها في حصول النتيجة ثم اختص رجع نفت إحداها فقط وهو سلوك الجاني للمسؤولية عن هذه النتيجة، فضلا عن التوسع غير المبرر في إثبات السببية حتى أن الجاني بات مسؤولا عن العوامل النادرة التي تساهم في حصول النتيجة.

ب/ نظرية السبب الأقوى أو السبب المباشر:

ومضمون هذه النظرية أنها لا تسلم بتساوي العوامل المساهمة في حصول النتيجة الإجرامية، بل يختار من بينها أقوى هذه الأسباب، سواء كان سلوك الجاني أو غيره، وبالتالي يكون ذلك السبب الأقوى هو المسؤول عن النتيجة التي وقعت مع ملاحظة أنه لكي يسأل الجاني لا يشترط أن يكون سلوكه أقوى من بقة الأسباب الأخرى المجتمعة، ولكن يكفي أن يكون أقوى هذه العوامل على حدى[4]. (باطلي غنية، الجريمة الالكترونية، دراسة مقارنة

ففي المثال السابق، لو كان إطلاق الرصاص أقوى من أثر سقوط الشجرة وارتطام سيارة الإسعاف بها، وكذلك أقوى من أثر التلوث العلاجي للجرح فيكون الجاني مسؤولا عن وفاة المجني عليه، ولو كان التلوث أقوى في أثره

[1] الحسيناوي علي جبار، المرجع السابق، ص 39.

[2] خيرت علي محرز، المرجع السابق، ص 127.

[3] المرجع نفسه، ص 128، 129.

[4] عائشة بن قارة، المرجع السابق، ص 85.

بالنسبة للوفاة فلا يسأل الجاني عن القتل، ولو كان سقوط الشجرة هو العامل الأقوى ما سئل الجاني أو المستشفى.

ويأخذ على هذه النظرية أنها حصرت النتيجة في عامل واحد يؤدي إليها وهو أقوى الأسباب، وهو أمر قد يؤدي بالجاني إلى الإفلات من العقاب[1].

ج/ السببية الملائمة:

ومضمون هذه النظرية أن الجاني يسأل عن النتائج المحتملة أو المتوقعة لفعله، أي تلك التي تقع حسب المجرى العادي من الأمور، ولو لم يكن وصفها بأنها مباشرة أو محققة لهذا الفعل، ويعد فعل الجاني مناسبا أو ملائما للنتيجة التي وقعت متى كان كافيا بذاته في حصول هذه النتيجة وفقا للمجرى العادي من الأمور، ومادامت ظروف الحال تنبئ بأنه قد توقعها أو كان من الممكن له أن يتوقعها بصرف النظر عن العوامل الأجنبية التي تدخلت بين سلوك الفاعل والنتيجة، وسواء كانت هذه العوامل سابقة أو لاحقة أم معاصرة لسلوك الجاني.

وقد قال الفقيه الألماني بهذه النظرية، والعبرة عنده أن تكون النتيجة ممكنة وعادية وفقا للظروف والعوامل التي حدثت، وعلى ذلك فلو تداخلت عوامل شاذة في حصول النتيجة لأدى ذلك إلى قطع علاقة السببية بين السلوك الإجرامي والنتيجة الإجرامية، كأن يموت المصاب بطلق ناري في المستشفى على إثر حريق فيه، أو تنقلب سيارة الإسعاف التي تنقله فيصاب بارتجاج في المخ يؤدي بحياته، والمعول عليه أن يتعين تقدير الوقائع في كل حالة على حدة.

ويرى جانب من الفقه أن هذه النظرية لا تخلو من التحكم، فكون النتيجة ممكنة أو ليست ممكنة مع مراعاة الظروف التي حدثت فيها، مسألة تقديرية يختلف فيها تقدير الناس، ولا يصح أن تبنى أحكام القانون الجنائي على أسس تحكمية كهذه.

ولذلك يميل الفقه إلى الأخذ بمعيار موضوعي في التوقع أو الاحتمال حتى يتفادى بعض الحلول التحكيمية التي ينتهي إليها المعيار الشخصي، ولذلك لا يعتمد على ما يتوقعه الجاني شخصيا، وإنما ما يتوقعه الشخص العادي – إن وجد–في مثل ظروفه[2].

الفرع الثاني: الركن المعنوي للجريمة الإلكترونية:

الركن المعنوي هو النصف الآخر للجريمة، ويمكن التعبير عنه بأنه الحالة النفسية للجاني وقت ارتكاب جريمته، حيث لا تقوم الجريمة قانونا بدونه، فلابد من توفر الإرادة الآثمة لدى الجاني عند إقدامه على السلوك الإجرامي،

[1] أمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستير، جامعة الجزائر، 2002، ص 17.

[2] خيرت علي محرز، المرجع السابق، ص 129، 130.

كما يجب أن تكون الأفعال ارادية، وإلا انتفى الركن المعنوي للجريمة، وأن تكون هذه الأفعال متجهة نحو مخالة القواعد القانونية، لترتب على مخالفتها الجزاء الجنائي المناسب.

فمن المتصور غالبا ألا تقع الجريمة الالكترونية إلا بصورة عمدية سبقها التفكير في الحصول على المعلومة أو اختراق الشبكة، والأصل في الجرائم هو العمدية إلا ما استثني بنص[1].

يتخذ الركن المعنوي في هذا النوع المستجد من الجرائم صورة القصد الجنائي العام بعنصريه العلم والإرادة، إذ يجب أن تتجه إرادة الجاني إلى فعل الاعتداء، كما يجب أن يعلم بأن نشاطه الإجرامي يؤدي إلى ارتكاب سلوك يعاقب عليه القانون[2].

ولقد ثار جدل فقهي حول مدى ضرورة توافر القصد الجنائي الخاص في بعض الجرائم الالكترونية فهناك من يرى بضرورة توافر هذا القصد، في حين يرى البعض الآخر أن القصد الجنائي العام كاف لوحده لقيام الركن المعنوي للجريمة المعلوماتية، وبالتالي لا يتطلب وجود القصد الجنائي الخاص لاكتمال الركن المعنوي، ويختلف الركن المعنوي باختلاف النشاط الغير المشروع المقترف من طرف المجرم المعلوماتي لذا نقوم بالعرض القصد الجنائي العام (أولا)، القصد الجنائي الخاص (ثانيا).

أولا: القصد الجنائي العام:

يراد بالقصد العام، القصد العادي الذي يتعين توافره في كافة الجرائم العمدية ويكتفي به القانون في أغلب الجرائم، وهو إرادة السلوك الإجرامي ونتيجته والعلم بهما.

بمعنى أن للقصد الجنائي العام صورتين العلم والإرادة، أي تكون من إرادة الفاعل التي تهدف إلى تحقيق عمل يجرمه القانون مع علمه بكل عناصره التي يحددها القانون[3].

ويختلف القصد الجنائي العام باختلاف السلوك المؤدي لارتكاب الجريمة، فهناك بعض من الجرائم المعلوماتية بحكم طبيعتها لا يشترط لقيامها وقيام الركن المعنوي فيها وجود قصد خاص، كالجريمة الدخول غير المصرح بها إلى نظام المعالجة الألية للمعطيات تتطلب قصدا جنائيا عاما يتمثل في العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار أن المشرع الجزائري سعى لحماية محل الحق وهو جاز الحاسب الآلي بما يتضمنه من معلومات وبرامج[4].

---

[1] باطلي غنية، المرجع السابق، ص 48.

[2] معتوق عبد اللطيف، المرجع السابق، ص 25.

[3] حمدي ناصر، المرجع نفسه، 78.

[4] معتوق عبد اللطيف، المرجع نفسه، ص 24.

كما اشترط المشرع توافر القصد الجنائي العام في جريمة اتلاف المعلومات، حيث يكفي علم الجاني بأنه يقوم بأعمال من شأنها أن تؤدي إلى تغيير الحالة التي كانت عليها المعلومات أو المعطيات بمحوها أو اتلافها وأن تتجه إرادته إلى تحقيق ذلك[1].

وبالتالي نجد أن معظم الجرائم المعلوماتية اشترط فيها المشرع القصد الجنائي العام، حيث اكتفى بالضرورة توافر القصد الجنائي العام لوحده لقيام الركن المعنوي لهذا النوع من الجرائم المستحدثة على غرار التشريعات الأخرى التي دعت إلى توافر القصد الجنائي الخاص إلى جانب القصد الجنائي العام، في بعض الجرائم الالكترونية وهو ما نقوم بتبيانه في الفرع الثاني.

ثانيا: مدى توافر القصد الجنائي الخاص:

إن أغلب الجرائم ترتكب بصورة قصدية، بالتالي يعد القصد الجنائي من بين أكثر عناصر الركن المعنوي تصورا.

لقد اختلفت التشريعات حول مدى ضرورة توافر القصد الجنائي الخاص في البعض من الجرائم المعلوماتية، فنجد أن القضاء الأمريكي لم يقم بالتحديد في بعض الجرائم ما إذا كانت تتطلب قصد جنائي خاص من جهة، ولا يمانع من جهة أخرى في توافر قصد جنائي خاص في جريمة التهديد بالبريد الالكتروني[2].

أما القانون العقوبات الفرنسي اشترط سوء النية في منطق القصد الخاص حين وجود عدوان على البريد الالكتروني، وفي جريمة سرقة المعلومات وهي من جرائم المعلوماتية يتطلب فيها لقيام الركن المعنوي قصد جنائي عام وخاص فالقصد العام ينصب في علم الجاني على أن فعل سرقة المعلومات من الحاسب الآلي أو البريد الالكتروني يعد فعل غير مشروع، ويجب أن يرتبط هذا العلم مع الإرادة، وهي الحالة النفسية التي تعكس قيام الجاني بالسلوك المحظور، وقصد جنائي خاص الذي يتمثل في نية التملك للمعلومة التي تم سرقتها وتطبيقا لذلك قضت محكمة النقض الفرنسية بتوافر نية التملك الوقتية في سرقة المعلومات من جهاز الحاسوب، وتتحقق هذه النية من سلب وحيازة المستندات خلال الوقت الازم لإعادة نسخها دون إرادة صاحبها، وهو الأمر الذي يستدعي تدخل التشريعات لمواجهتها بالنصوص خاصة، ويرى اتجاه من الفقه أن نية التملك في جريمة سرقة المعلومات تبدأ بقيام الجاني بالدخول على أدوات الحاسب الآلي من وحدات الإدخال والإخراج والتخزين والمعالجة أو البرامج والبيانات والمعلومات والنظم المخزنة داخل ملفات الحاسب الآلي أو في ذاكرته، كل هذا من أجل الاستيلاء على المعلومات الموجودة بقصد نية التملك والإضرار بالمجني عليه[3].

---

[1] الشوابكة محمد أمين أحمد، المرجع السابق، ص 221.

[2] الحسيناوي على جبار، المرجع السابق، ص 42، 43.

[3] لورنس سعيد الحوامدة، المرجع السابق، ص 24، 25.

كما يرى جانب من الفقه أن جريمة التعامل في معلومات غير مشروعة تشترط قصد جنائي عام بالإضافة إلى قصد جنائي خاص سواء في صورة الجريمة الأولى وهي التعامل في معلومات صالحة لارتكاب الجريمة أو في صورتها الثانية المتمثلة في التعامل في معلومات متحصلة من جريمة[1].

* بخصوص الصورة الأولى ذهب هذا الاتجاه إلى القول بوجوب توفر قصد خاص إلى جانب القصد العام حتى تقوم جريمة التعامل في معلومات صالحة لارتكاب جريمة ويتمثل القصد الخاص في اتجاه إرادة الجاني إلى الإعداد والتمهيد لاستعمال هذه المعلومات في ارتكاب جريمة من جرائم الاعتداء على نظم المعالجة الآلية للمعلومات غير أن المشرع الجزائري لم يشترط القصد الجنائي الخاص.

* أما الصورة الثانية لهذه الجريمة فقد اشترطت فيها اتفاقية بودابست[2] قصدا خاصا، وهو نية استخدام المعلومات في جريمة من الجرائم طبقا للفقرة (ب) من المادة 06 حيث أشارت المذكرة التفسيرية لهذه الاتفاقية لأهمية تطلب القصد الخاص، بأنه: " من أجل تجنب خطر العقاب المبالغ فيه، حيث يتم إنتاج الأجهزة وعرضها في السوق لأغراض شرعية من أجل التصدي لاعتداءات على أجهزة الحاسب الآلي، فإنه يجب إضافة عناصر أخرى من اجل تضييق نطاق الجريمة، وبالإضافة إلى اشتراط القصد العام فإنه يجب توافر نية خاصة أو قصد خاص لاستخدام الجهاز من أجل ارتكاب الجريمة من الجرائم المشار إليها في المواد من 2 إلى 5 من الاتفاقية"[3].

نجد أن المشرع الجزائري لم يشترط قصد جنائي خاص في الصورة الثانية من الجريمة التعامل في معلومات غير مشروعة وذات الوضع بالنسبة للمشرع الفرنسي.

وبالتالي المشرع الجزائري لم يشترط توافر القصد الجنائي الخاص في هذه الجريمة بصورتيها وبالنسبة للجرائم الأخرى المتعلقة بالاعتداء على الأنظمة المعالجة الآلية للمعطيات، بل اكتفى بالضرورة توافر القصد الجنائي العام لقيام الركن المعنوي لهذا النوع المستحدث من الجرائم[4].

لقد اكتسبت المعلومات في عصرنا الحاضر أبعاد جديدة وأهمية خاصة نتيجة للعولمة وتطور وسائل الاتصال وارتفاع حدة التنافس بين الدول، فالدول أصبحت تعد المعلومات ثروة يجب المحافظة عليها وهذه المكانة التي تحتلها المعلومات اليوم، جعلت التهافت للحصول عليها بشتى الطرق، وجعلها عرضة للسرقة والسطو والقرصنة

[1] خليفة محمد، المرجع السابق، ص 212، 213.

[2] إتفاقية بودابست في 2001/11/23 تم التوقيع عليها وهي اتفاقية خاصة فقط لدول الاتحاد الأوروبي لمكافحة الجرائم الالكترونية.

[3] حمدي ناصر، المرجع السابق، ص 85.

[4] خليفة محمد، المرجع نفسه، ص ص 213، 215.

خاصة بعد دخول الأنترنت إلى قطاع تقنية المعلومات، حيث لا يستطيع أحد أن ينكر أهمية الأنترنت لأنها أحد أهم دعائم تكنولوجيا الاتصال والمعلومات، إلا أن لديها آثار سلبية من بينها ظهور نوع جديد من الجرائم المستحدثة ونتيجة لحداثة هذا النوع من الجرائم، نجد أن التشريعات اختلفت في تعريف هذه الجريمة، بحيث خولت مسألة تعريفها للفقه وبالنسبة للمشرع الجزائري نجده اصطلح على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، هذه الجريمة كأي نوع من الجرائم الأخرى لها خصائص وأركان خاصة بها.

من خلال استعراض تعريفات الفقهية، يتضح لنا أن هناك اختلاف في تعريف الجريمة الالكترونية، إلا أنه في الحقيقة تعددت التعاريف إلا أنها كلها تدل على نفس الجريمة التي نحن بصدد دراستها.

خاتمة الفصل الأول:

وعليه لقد تناولنا في هذا الفصل تعاريف الجريمة الالكترونية وأبرز المعايير التي اعتمدت على مفاهيمها وكذلك موقف المشرع الجزائري حيث انه لم يعرفها بل إكتفى بالدلالة عليها بتسميتها بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال، ثم تطرقنا إلى مراحلها بالإضافة إلى خصائص الجرائم الالكترونية، ثم تطرقنا إلى أنواعها واركانها.

ونظرا لأهميتها البالغة نتيجة العولمة وتطور وسائل الإتصال فهي بمثابة ثروة يجب المحافظة عليها وقد جعلت التهافت للحصول عليها بشتى الطرق وجعلها عرضة للسرقة والسطو والقرصنة خاصة بعد دخول الانترنت إلى قطاع تقنية المعلومات حيث لا يستطيع أحد أن ينكر أهمية الأنترنت لأنها أحد دعائم تكنولوجيا الاعلام والاتصال.

الفصل الثاني:
الجوانب العملية للحد من الجريمة الإلكترونية

المبحث الأول: الأليات التشريعية للحد من الجريمة الإلكترونية:

تمهيد:

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الالكتروني، وما يصاحبها من أضرار من جهة، ومحاولة منه تدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى، قام من خلال ذلك إلى إصدار قوانين عامة وخاصة. وتنقسم الدراسة في هذا المبحث الى مطلبين المطلب الأول القوانين العامة المنظمة للجريمة الاكترونية والمطلب الثاني القوانين الخاصة المنظمة لها.

المطلب الاول: القوانين العامة المنظمة للجريمة الالكترونية:

سعى المشرع الجزائري إلى تنظيم الجريمة الالكترونية بقوانين عامة هادفا بذلك إلى ردع هذا النوع المستحدث من الجرائم.

الفرع الأول: الدستور الجزائري:

كفل الدستور الجزائري حماية الحقوق الأساسية والحريات الفردية والسهر على أن تضمن الدولة عدم انتهاك حرمة الإنسان، وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجزائية وقوانين خاصة أخرى تحذر كل مساس بهذه الحقوق، ومن بين المبادئ الدستورية نجد بحسب المواد التالية[1]:

* المادة 38 التي تنص على ما يلي: " الحريات الأساسية وحقوق الإنسان والمواطن مضمونة"، بالتالي المشرع الجزائري سعى لحماية الحقوق من جميع أشكال الانتهاكات.

* بينما نصت المادة 44 على ما يلي: "حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن، حقوق المؤلف يحميها القانون، لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي، الحريات الأكاديمية وحرية البحث العلمي مضمونة، وتمارس في إطار القانون تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة.

لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمه وشرفه ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"[2].

---

[1] قانون رقم 08-19 المؤرخ في 15 نوفمبر2008 يتضمن تعديلات الدستور، جريدة الرسمية عدد 63 الصادرة في 16نوفمبر 2008.

[2] قانون رقم 16-01 المؤرخ في 6 مارس 2016 يتضمن تعديل لدستور 1696، جريدة الرسمية عدد 14 الصادرة في 07 مارس 2016.

يفهم من سياق نص المادة أن المشرع سعى لحماية حق المؤلف من جانونه لا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام، إلا بمقتضى أمر قضائي، وحماية الحياة الخاصة من كل أشكال الاعتداءات.

الفرع الثاني: قانون العقوبات الجزائري:

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته التورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل ق.ع.ج بموجب قانون 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات،[1] الذي أفرد القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات الذي تضمن 8 مواد من المادة 394 مكرر إلى 394 مكرر7 ونص على عدة جرائم وهي كالآتي:

*الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

* إدخال أو إزالة أو تعديل –عن طريق الغش–معطيات في نظام المعالجة الآلية.

*تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة معلومات 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 احدى الجرائم المنصوص عليها في هذا القسم[2].

وقد ضاعف المشرع العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات العمومية، بالإضافة إلى ذلك نجد أن المشرع الجزائري اتبع نفس نهج المشرع الفرنسي من خلال إقراره لمسؤولية الشخص المعنوي بموجب المادتين 18 مكرر و18 مكرر1 من قانون 04-15، وشدد عقوبة الغرامة على الشخص المعنوي إلى خمس مرات للحد الأقصى للعقوبة المقررة للشخص الطبيعي.

كما تم التطرق لعقوبة الاشتراك في مجموعة أو اتفاق بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم.

[1] قانون العقوبات معدل ومتمم الامر 156/66 المؤرخ في1966/06/08 المتضمن قانون العقوبات.

[2] المادة 394 مكرر2 من قانون رقم 06-23 مؤرخ في 20/12/2006 يعدل ويتمم الأمر 66/156 مؤرخ في 18 صفر 1386 الموافق لـ 8 يونيو 1966 والمتضمن قانون العقوبات.

ونص هذا التعديل على عقوبة مصادرة وسائل ارتكاب الجريمة – الأجهزة والبرامج–وإغلاق المواقع التي تكون محلا لها، علاوة على إغلاق المحل أو المكان الذي ارتكبت فيه الجريمة[1].

طبقا لنص المادة 394 مكرر 6 والآتي نصها: "مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القيم علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها"[2].

أدخل المشرع الجزائري تعديل آخر على ق.ع.ج بموجب قانون رقم 06-23 المؤرخ في 20 ديسمبر 2004، ومس هذا التعديل القسم السابع مكرر الخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، حيث تم تشديد العقوبات بالحبس والغرامة المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم، من القانون رقم 04-15[3].

الفرع الثالث: قانون الإجراءات الجزائية:

لقد قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية لمواكبة التطور ألمعلوماتي الذي لحق بالجريمة المعلوماتية، محاولة منه تطوقها والقضاء عليها، أو على الأقل الحد من انتشارها، حيث وضع قواعد وأحكام خاصة لسلطة التحري والمتابعة، الغرض منها هو مواجهتها وقد وردت هذه الأساليب في قانون الإجراءات الجزائية.

متابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة والضبط...الخ.

كما قام باستحداث أساليب أخرى خاصة كاعتراض المراسلات، المراقبة الالكترونية، التسرب، تسجيل الأصوات، التقاط الصور[4]، لنتطرق إليها في الفرع الثاني، من المطلب الثاني، وبالتالي نجد أن القانون إ ج ساهم في متابعة الجريمة الالكترونية من خلال نصه لقواعد الإجرائية في التحقيق في هذه الجريمة والمساهمة في كشف الحقيقة بإزالة الغموض ومعاقبة مرتكبيها.

---

[1] بن بورنان كاتية، **الجريمة المعلوماتية في التشريع الجزائري**، مذكرة تخرج لنيل شهادة الماستر في الحقوق، قسم القانون الخاص، تخصص القانون الخاص والعلوم الجنائية، كلية العقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية، 2014، ص 37، 39.

[2] المادة 394 مكرر6 من الأمر 66/156 مؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات، الجردة الرسمية عدد 71 معدل ومتمم، راجع موقع الأمانة العامة للحكومة: www.jordp.dz.

[3] بن بورنان كاتية، المرجع نفسه، ص 41.

[4] المرجع انفسه، ص 35.

المطلب الثاني: القوانين الخاصة للحد من الجريمة الالكترونية:

ونظرا لاتساع نطاق الجريمة الالكترونية التي أصبحت لا تقتصر على جريمة واحدة وإنما استعت إلى عدة جرائم، وعلى أساس أن القانون الجنائي التقليدي غير قادر على استيعاب الجرائم الالكترونية الحديثة مما دفع بالمشرع الجزائري الى استحداث قوانين خاصة لمواكبة هذا النوع المستحدث من الجرائم.

الفرع الاول: قانون البريد والمواصلات السلكية واللاسلكية:

سعى قانون البريد والمواصلات لمواجهة هذه الظاهرة الإجرامية من خلال المواد التي تضمنها لهذا الغرض، بات من السهولة إجراء التحويلات المالية عن الطريق الالكتروني نظرا لتطور تكنولوجيا الإعلام والاتصال.

كما نص القانون السالف الذكر إلى استخدام حوالات دفع عادية أو الكترونية أو برقية.

بينما نصت المادة 23 منه على ما يلي: "يجوز إنشاء و/أو استغلال شبكات المواصلات السلكية واللاسلكية مهما كان نوع الخدمات المقدمة، وفق الشروط المحددة في هذا القانون وفي النصوص التنظيمية المتخذة لتطبيقه.

لا تشمل أحكام هذه المادة منشآت الدولة المعدة لتلبية حاجات الدفاع الوطني أو الأمن العمومي"[1].

بحسب هذه المادة يجوز كأصل عام إنشاء استخدام شبكات الاتصال السلكية واللاسلكية، باختلاف نوع الخدمة المقدمة، لكن وفقا للشروط المحددة قانونا، باستثناء منشآت الدولة المعدة لتلبية حاجات الدفاع الوطني أو الأمن العمومي.

كما نصت المادة 93 الفقرة الأخيرة كما يلي: " لا يمكن بأي حال من الأحوال انتهاك سرية المراسلات"، بمعنى أنه يجب احترام سرية المراسلات[2].

تطرق أيضا القانون السالف الذكر إلى معاقبة كل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه، يعاقب فيه الجاني بالحرمان من ممارسة كل نشاط أو مهنة في قطاع المواصلات السلكية واللاسلكية، أو في قطاع ذي صلة بهاذين القطاعين لمدة تتراوح بين سنة إلى خمس سنوات.

الفرع الثاني: قانون التأمينات:

تطرق هذا القانون إلى تنظيم الجريمة من خلال هيئات الضمان الاجتماعي، في نصوص قانوني عديدة تخص البطاقة الالكترونية، التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني.

[1] قانون البريد والمواصلات السلكية واللاسلكية، رقم 03-2000 مؤرخ في 05/08/200 ج.ر.ج.ج. العدد 48، معدل ومتمم.

[2] أعمال مؤتمر الجرائم الالكترونية المنعقد في طرابلس، يومي 24-2017/03/25، ص 131.

حدد هذا القانون الجزاءات المقررة في حالة الاستعمال الغير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة للبطاقة الالكترونية وفقا لنص المواد التالية: ففي المادة 93 مكرر2 من ق ت إ نصت على ما يلي: "دون الاخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة مالية من 100000دج إلى 200000دج، كل من يسلم أو يستلم بهدف الاستعمال الغير المشروع البطاقة الالكترونية للمؤمن له اجتماعيا أو مفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهني الصحة"[1].

طبقا لنص المادة، نجد المشرع الجزائري يعاقب كل من يستخدم البطاقة الالكترونية، أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهني الصحة، لأغراض غير شرعية، كما قام أيضا المشرع وفقا لهذا القانون بتجريم مجموعة الأفعال الغير مشروعة من القيام عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية التي تتضمنها البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهني الصحة[2].

كما عاقب كل من أعد أو عدل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستخدام المعطيات التي تتضمنها البطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو لمهني الصحة.

الفرع الثالث: قانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

نص هذا القانون على مراقبة الاتصالات الالكترونية وذلك بتحديد الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، حيث نصت المادة 4 منه على الحالات التي يسمح فيها للسلطات الأمنية باللجوء إلى المراقبة الالكترونية وهي: الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

حالة توفر معلومات عن احتمال اعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

---

[1] المادة 93 مكرر 2 من قانون رقم 01/18 المؤرخ في 23 يناير 2008، يتمم القانون رقم 83-11 المؤرخ في 2 يونيو 1983 المتعلق بالتأمينات الاجتماعية.

[2] أعمال مؤتمر الجرائم الالكترونية، المرجع السابق، ص 130، 131.

في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، اشترط المشرع إجراء عمليات المراقبة بإذن مكتوب من السلطة القضائية المختصة[1].

كما نص كذلك هذا القانون على قواعد إجرائية تساهم بدورها في كسف الجريمة ومعالمها، من تفتيش وحجز للمعطيات المعلوماتية وحفظ المعلومات المتعلقة بحركة السير.

فيما يخص التفتيش فقد أجازت المادة 5 من القانون 04-09 الذي يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى:

* منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

* منظومة معلوماتية.

يلاحظ بأن التفتيش في الوضعيات المشار إليها لها يأخذ مجالين إما أن يكون في مجال أعمال التحقيق تقوم به السلطان القضائية المختصة وإما في مجال أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطات المختصة، وفي كلتا الحالتين يكون جهاز الكمبيوتر هو المستهدف بمختلف مكوناته.

كما أجاز هذا القانون تسخير كل شخص له دراية بعمل المنظومة المعلوماتية التي تتضمنها، وذلك قصد مساعدة السلطات المكلفة بالتفتيش من خلال تزويدها بكل المعلومات الضرورية لإتمام مهمتها.

يسمح هذا القانون للسلطات التي تباشر التفتيش في منظومة معلوماتية، بنسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في ق.إ.ج[2].

يعتبر قانون 04/09 كخطوة أولى للجزائر في مجال مواجهة الجريمة الالكترونية من ناحية وسد للفراغ التشريعي الذي كان يعتري القانون الجزائري من ناحية أخرى، لكن هذا لا يكفي لردع الجرائم الالكترونية بمختلف أنواعها.

[1] زبيحة زيدان، المرجع السابق، ص 129.

[2] نفس المرجع، ص 131.

المبحث الثاني: الآليات المؤسساتية لمواجهة الجريمة الالكترونية:

نتطرق من خلال هذا المبحث إلى الآليات المؤسساتية التي واجهة الجريمة الإلكترونية وهي الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال كهيئة وطنية مستحدثة في مطلب أول والهيئات القضائية الجزائية المختصة في مطلب ثاني أما المطلب الثالث فيكون التطرق فيه للمعهد الوطني للأدلة الجنائية وعلم الإجرام أما المطلب الرابع فيكون الحديث فيه عن المديرية العامة للأمن الوطني.

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

تم استحداث هيئة وطنية مهمتها متابعة كل منشورات الانترنت ومراقبة اتصالات الهاتف الثابت والنقال، في الجزائر من أجل ضمان المراقبة الوقائية للاتصالات الالكترونية والكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدول.

واعتمدت الجزائر رسميا الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والتي تأتي كلبنة جديدة في مسار الإصلاحات التي باشرها رئيس الجمهورية من أجل تعزيز دولة القانون، والتأكيد أكثر على سيادة القانون في كل الأحوال في مرسوم رئاسي رقم 15-261 مؤرخ في 08 أكتوبر2015[1]، وذلك في خطوة جديدة نحو مراقبة كل المحتويات المنشورة عبر شبكة الأنترنت، حيث تم وضع هذه الهيئة تحت تصرف وزير العدل وتتكون لجنتها المديرة من وزير الداخلية ووزير تكنولوجيا البريد والاتصال وقائد الدرك الوطني والمدير العام للأمن الوطني، وممثلين عن وزارة الدفاع الوطني ورئاسة الجمهورية، إضافة إلى قاضيين من المحكمة العليا، وذلك بهدف مكافحة الجرائم الإلكترونية وحسب هذا المرسوم فإن هذه الهيئة تعمل على مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومن خلال جمع المعلومات

والتزويد بها عبر الخبرات القضائية، وتهدف هذه الهيئة الجديدة تحت سلطة القاضي المختص، إلى تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصادرها ومسارها من أجل استعمالها في الإجراءات القضائية، كما تسهر الهيئة أيضا على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها، موضحا أن هذه الهيئة التي تعد سلطة إدارية مستقلة لدى وزير العدل، ستعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتضم أساسا أعضاء من الحكومة معنيين بالموضوع، ومسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا يعينها المجلس الأعلى للقضاء، وستضم الهيئة قضاة وضباطا وأعوانا

[1] الجريدة الرسمية للجمهورية الجزائرية، العدد 47، المرجع السابق، ص14.

من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين وفقا لأحكام قانون الإجراءات الجزائية، فيما تكلف بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

كما تعني الهيئة الجديدة بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الاعلام والاتصال، وضمان مراقبة الاتصالات الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة، وذلك تحت سلطة القاضي المتخصص.

ومن بين الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تلك التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الالكترونية[1].

حيث تمت الإشارة في هذا المجال إلى أنه: "وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون ومع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية، وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية، وينص القانون على الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، كما يحدد قوانين الإجراءات المتعلقة بتفتيش المنظومة القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها".

ويتطرق كذلك لالتزامات مانحي خدمات الأنترنت وبخصوص التعاون والمساعدة القضائية الدولية، أشار القانون إلى أن " المحاكم الجزائرية تختص بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني"، ويعتبر هذا المسار قد مكن بالفعل من تزويد العدالة بالمزيد من الموارد البشرية المؤهلة، ولمراجعة الترسانة التشريعية بما في ذلك المجال الجزائي، من أجل تحسين حماية حقوق وحريات المواطنين، وتشديد العقوبات على أي تقصير في هذا المجال. "كما جاء القانون الذي تم تنفيذه الفعلي بفضل سلسلة من تعليمات الرئاسية ذات الصلة لتحديد صلاحيات السلطة القضائية، ومنها على وجه الخصوص التعليمة الصادرة في 28 ماي 2014 التي تحظر بدون أي استثناء، كل قرار بالمنع من مغادرة التراب الوطني ما لم يسلم من طرف قاضي التحقيق أو نيابة الجمهورية، كما ذكر في بيان الرئاسة في هذا السياق بحركة الإصلاحات الأمنية والسياسية

[1] سالم عبد الرزاق، **ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية**، محكمة سيدي محمد، ص11.

الواسعة التي شرع في تجسيدها منذ سنة 2011 برفع حالة الطوارئ، وتنفيذ عدة قوانين ذات بعد سياسي، مؤكدا بالمناسبة هذا المسار سيتوج لاحقا بمشروع مراجعة الدستور[1].

المطلب الثاني: الهيئات القضائية الجزائية المختصة:

سنتطرق في هذا المطلب إلى الهيئات القضائية الجزائية المختصة في ردع الجريمة الإلكترونية والمتمثلة في كلا من الضبطية القضائية وقاضي التحقيق والمحكمة ودورها في توفير الأمن المعلوماتي.

الفرع الأول: الضبطية القضائية

ويأتي دور الشرطة القضائية في الحماية من الجريمة الإلكترونية من خلال مرحلة جمع الاستدلالات وضباط الشرطة القضائية نوعان:

*النوع الأول: وهم ضباط يتمتعون باختصاص عام ويختصون بإجراءات الاستدلال شأن الجرائم المنصوص عليها في قانون العقوبات.

*أما النوع الثاني: فهم ذوو النوعي المحدود بخصوص نوع معين من جرائم حددها القانون على سبيل الحصر، هؤلاء المشار إليهم في المادة 21 من قانون الإجراءات الجزائية وسلطتهم كذلك محددة لا تمتد إلى مرحلة التفتيش ودخول المنازل والمعامل والمباني أو الأماكن المحاطة بأسوار إلا بحضور أحد ضباط الشرطة القضائية ومن بين هؤلاء: رؤساء الأقسام، المهندسون، وأعوان الغابات وحماية الأراضي، وتعد محاضرهم ذات حجية وقوة إثبات كما استقر عليه القضاء الوطني وما يهمنا في هذه الدراسة هو دور الضبطية القضائية ومجال اختصاصها فيما يتعلق بالجريمة المعلوماتية[2].

أولا: الإجراءات التقليدية لجمع الدليل

سنتطرق في هذا الفرع إلى إجراءين الإجراءات المادية والإجراءات الشخصية.

1/ **الإجراءات المادية:** تتمثل هذه الإجراءات في المعاينة والتفتيش والضبط

أ/ **المعاينة:** والمقصود بالمعاينة هي الرؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة.

وتعتبر المعاينة إجراءً من إجراءات التحقيق التي يقوم بها سلطة التحقيق بنفسها أو تندب ضباط الشرطة القضائية للقيام بها، كما يمكن للمحكمة أن تقوم بإجراءات معاينة إذا رأت ذلك يستدعي لكشف الحقيقة سواء

[1] نفس المرجع السابق، ص 12.

[2] زبيخة زيدان، المرجع السابق، ص 116، 117.

كان ذلك من تلقاء نفسها أو بناء على طلب من الشخص المعني بعد موافقة القاضي المختص بناء على طلب عريضة.

-كيفية إجراء المعاينة التقنية لمسرح الجريمة الالكترونية:

عند العلم بوقوع الجريمة فإن أول خطوة يقوم بها مأمور الضبط القضائي إلى مسرح الجريمة، لأن هذا الأخير حجر الزاوية في التحقيق الجنائي ومكمن الآثار والأدلة المادية، وينبغي التعامل في الإطار مع مسرح الجريمة الالكترونية على أنه مسرحان هما:

***المسرح التقليدي:**

يقع خارج البيئة الالكترونية لأنه يتكون من المكونات المادية للمكان الذي وقعت فيه الجريمة وهو أقرب إلى مسرح الجريمة التقليدية ويترك فيها الجاني عدة آثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.

***المسرح الافتراضي:**

يقع داخل البيئة الالكترونية لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الأنترنت في ذاكرة الأقراص الصلبة الموجودة بداخله[1]. ونظرا لاختلاف مسرح الجريمة عن غيره من الجرائم الأخرى فينبغي التعامل الخاص مع هذه الجريمة وذلك باتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة الالكترونية والمتمثل:

1/ ضرورة وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوب معاينتها وشبكاتها.

2/ وجود خريطة توضح الموقع الذي سيتم معاينته وتفاصيل المبنى أو الطابق موضوع البلاغ، وعدد الأجهزة والخزائن والملفات ويحدد ذلك من خلال مصادر سرية لجهات الأمن.

3/ تحديد الأجهزة المحتمل تورطها في الجريمة الإلكترونية حتى يتم تحديد كيفية التعاون معها قبل المعاينة.

4/ تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج.

5/ إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.

6/ تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حدة، وذلك حتى لا تتداخل الاختصاصات.

7/ إعداد خطة المعاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل.

8/ أن تتم هذه المعاينة وفق مبدأ المشروعة وفي إطار ما تنص عليه القوانين الجنائية.

[1] عائشة بن قارة مصطفى، المرجع السابق، ص 79، 80.

9/ تأمين عدم انقطاع التيار الكهربائي لأن معاينة الأجهزة وما بها من برامج وشبكات وأنظمة تشغيل لا جدوى منها في ظل عدم وجود التيار الكهربائي[1].

ب/ تفتيش في البيئة الالكترونية:

التفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات الجزائية رغم اختلاف المحل الذي يقع عليه التفتيش، ويقصد به إجراء من الإجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبتها إلى المتهم بارتكابها.

كما تتفق التشريعات العربية على تعريف التفتيش بأنه إجراء من إجراءات التحقيق غايته ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد الحقيقة في شأنها.

يثير موضوع التفتيش الذي يقع على نظم الحاسب الآلي مسائل عديدة للبحث كمدى صلاحية الكيانات المعنوية في هذه الوسائل كمحل يرد عليه التفتيش، وحكم تفتيش الوسائل التي تتصل مع بعضها البعض وتقع في أماكن عامة أو خاصة، وضوابط هذا التفتيش.

1/ مدى صلاحية الكيانات المعنوية كمحل يرد عليه التفتيش.

إذا كان التفتيش كوسيلة إجرائية يستهدف الحصول على دليل مادي يساعد في إثبات الجريمة فإن البعض قد شك في مدى صلاحيته للبحث عن ادلة الجريمة في الكيانات المعنوية للحاسب الآلي وهو ما حذا ببعض التشريعات بأن تنص صراحة على أن تفتيش يتم بالنسبة لأنظمة الحاسب الآلي مثل ذلك قانون إساءة استخدام الحاسب الآلي في إنجلترا الصادر في سنة 1990 حيث نص على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلي[2].

وهناك تشريعات أخرى قد أجازت التفتيش أي "شيء" له علاقة بالأفعال الإجرامية مثلما هو الحال بالمشرع الجزائري، وعلى ضوء ذلك فإن تفتيش المكونات المعنوية للحاسبات الآلية يدخل في عداد الأشياء التي جاء النص عليها عاما دون تقييد.

---

[1] عائشة بن قارة مصطفي، **حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن**، دار الجامع الجديد، كلية الحقوق، جامعة الإسكندرية، مصر، د ط، 2006، ص 85، 86.

[2] هلالي عبد الله أحمد، **تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي**، دار النهضة العربية، القاهرة، ط1، 1997، ص 73

وعلى ضوء هذه الآراء الفقهية، وعلى النحو الذي قننه المشرع الجزائري صراحة في إمكانية وقوع التفتيش على مساكن أشخاص يظهر أنهم يحوزون على أشياء لها علاقة بالأفعال الجنائية فإن التفتيش يرد على الكيانات المعنوية في حاسبات الآلية، بحسب أن هذه الكيانات المعنوية وإن كانت غير مادية إلا أنها في نطاق الأشياء المادية[1].

ويترتب على ذلك أنه يمكن تفتيش نظام معلومات الحاسب الآلي ووسائط أو أوعية حفظ وتخزين البيانات المعالجة آليا كالأسطوانات والأقراص والأشرطة الممغنطة ومخرجات الحاسب، ويدخل في هذا التفتيش أيضا محتويات المخزنة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته.

2/ ضوابط التفتيش الذي يقع على نظم ومكونات الحاسب الآلي

لقد تطورت طرق التفتيش بحيث أنها أصبحت لا تقف –فقط–عند ضبط الأدوات المادية المستخدمة في ارتكاب الجريمة أو ضبط جسم الجريمة الذي يحقق نموذجها القانوني، وإنما يمكن لهذه الطرق كذلك أن تتعامل مع الجرائم التي ترتكب بالوسائل الإلكترونية وخاصة الحاسب الآلي، أو تقع عليه، فيمكن تبعا لذلك تسجيل البيانات المعالجة أليا بعد تحويلها من نبضات أو ذبذبات أو إشارات أو موجات كهرومغناطيسية إلى أشياء محسوسة تسجل وتخزن على وسائل معينة، وعلى هذه الوسائل يرد التفتيش أو الضبط[2].

ويخضع التفتيش لشروط مقيدة يجب مراعاتها تحت طائلة البطلان. إذ تنص المادة 44 من قانون الإجراءات الجزائية بعد تعديله بالقانون رقم 06-22 على عدم جواز إجراء التفتيش من قبل ضباط الشرطة القضائية إلا بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش.

ثم تنص المادة 45 على القيود الذي يتعين على ضباط الشرطة القضائية احترامها أثناء فترة التفتيش بصفة عامة لكن أضاف التعديل وتمم نص المادة 45 بأن رفع القيود الواردة فيها فيما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إلا ما تعلق منها بالحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات[3].

كما أجاز في نص المادة 47 إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل دون احترام الأوقات المذكورة في الفقرة الأولى في المادة 47 من قانون الإجراءات الجزائية، إذ تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات غير أنه يشترط أن يكون مصحوبا بإذن مسبق من وكيل الجمهورية المختص أو قاضي التحقيق.

---

[1] زبيخة زيدان، المرجع السابق، ص 130، 131.

[2] هلالي عبد الله أحمد، المرجع السابق، ص 89.

[3] هشام رستم، الجوانب الإجرائية، المرجع السابق، ص 69.

غير أن المشرع لم يتطرق إلى المحل الذي يقع عليه التفتيش بصفة مدققة من الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، ذلك أن التفتيش هنا يقع على نظام معلومات الحاسب أو الوسائط أو أوعية حفظ وتخزين البيانات المعالجة إلكترونيا كالأسطوانات والأقراص والأشرطة الممغنطة ومخرجات الحاسب.

ويدخل في هذا التفتيش أيضا المحتويات المخزنة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته، والملاحظ أن المشرع الجزائري عندما عدل نصوص المواد المتعلقة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات قد خص الحاسبات الآلية داخل الدولة حتى لو اتصلت مع بعضها البعض فيكون ذلك عن طريق شبكة محلية.

لكن يطرح التساؤل هنا في حالة ما إذا اتصلت بحاسبات أخرى خارج الدولة عن طريق الربط الشبكي بين أجزاء العالم المختلفة، ومنها شبكة الأنترنت[1].

ففي حالة وقوع جريمة في نظم الحاسب الآلي داخل الدولة الجزائرية فيجوز هنا لوكيل الجمهورية أو قاضي التحقيق إصدار الإذن بالتفتيش.

لكن هذا الإذن بالتفتيش لا ينفذ إلا على الحاسب الآلي الذي صدر من اجله، ويترتب على ذلك أنه إذا كان الحاسب المراد تفتيشه يتصل بحاسب آخر لم يصدر بالنسبة له إذن بالتفتيش لا يمكن أن يمتد إليه التفتيش حتى لو كان يحتوي على جريمة.

إلا إذا أمر قاضي التحقيق هنا في إذنه بالتفتيش أن يمتد على مستوى التراب الوطني بكامله حسب الفقرة الأخيرة من نص المادة 47.

لكن في حالة الإذن بالتفتيش على حاسب واحد معين يتعين استصدار إذن جديد بالتفتيش للحاسب الثاني إذا تبين أنه تبين أنه متصل عن طريق شبكة داخلية بالحاسب الذي التفتيش فيه.

لكن هناك حالة أخرى أكثر تعقيدا تواجه التفتيش على الحاسب الآلي وذلك عندما يقوم بعض الجناة بتخزين بياناتهم في أنظمة حاسبات آلية تقع خارج الدولة الجزائرية مستخدمين في ذلك الاتصالات البعدية أو مواقع خارج الجزائر مستهدفين عدم إمكان الوصول إليها وفي هذه الحالة فإن تفتيش هذه الحسابات التي تقع خارج حدود الدولة لضبط جريمة تتصل بحاسبات آلية داخل الدولة أمر قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها، غير أنه يمكن اتخاذ هذا الإجراء عن طريق اتفاقيات خاصة تعقد بين الدول المعنية[2].

[1] هشام رستم، المرجع السابق، ص 69.

[2] المرسوم التنفيذي رقم 348/06 المؤرخ في اكتوبر 2006 المتضمن تحديد الاختصاص المحلي لبعض وكلاء الجمهورية وقضاة التحقيق جر عدد 63.

وكتطبيق لهذا الإجراء فقد حدث في ألمانيا أثناء إجراءات التحقيق عن جريمة غش وقعت في بيانات حاسب آلي، ذلك أنه قد تبين وجود اتصال بين حاسب الآلي المتواجد في ألمانيا وبين شبكة الاتصالات في سويسرا حيث تم تخزين بيانات المشروعات فيها وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات فلم تتمكن من ذلك إلا عن طريق التماس المساعدة الذي تتم بالتبادل بين الدولتين ولقد أدرك المجلس الأوربي مشكلة التفتيش التي قد تثار بالنسبة للجرائم التي ترتكب بالوسائل الالكترونية في أكثر من دولة فأصدر التوصية رقم R9513 التي أكد فيها على وجود قصور على مستوى التعاون الدولي بالنسبة لإجراء التفتيش عبر الحدود Perquisition transfrontière.

لكن الجزائر لحد الآن لم تنضم إلى أي من المعاهدات أو الاتفاقيات الخاصة بجريمة المعلوماتية[1].

ثانيا/ الإجراءات الشخصية:

سنتطرق في هذه المجموعة التي هي ذات طبيعة شخصية لأنه غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على دليل تتمثل هذه الإجراءات في: عملية التسرب، الشهادة، والخبرة التقنية، واستجواب المتهم.

أ/ التسرب:

المادة 65 مكرر 12 قانون الإجراءات الجزائية الجزائري عرفت التسرب بأنه يقصد بالتسرب قيام ضباط أعوان الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف يسمح لضابط الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه ولا يجوز تحت طائلة البطلان أن تشكل هذه الأفعال تحريض على ارتكاب الجرائم[2].

أما بالنسبة لمواصفات الآخرين وطبيعته حددتها المادة 65 مكرر من قانون الإجراءات الجزائية وهي:

1/ أن يسلم فقط للضرورة التحري أو التحقيق القضائي.

2/ أن يكون مكتوبا.

3/ أن يكون مسببا.

4/ أن يذكر في الإذن طبيعة الجريمة التي ينص عليها الإذن.

5/ يذكر فيه هوية ضابط الشرطة القضائية المعني أو الذي تتم العملية تحت مسؤوليته.

[1] عائشة بن قارة مصطفي، المرجع السابق، ص 201.

[2] بوكثير خالد، المرجع السابق، ص 26.

6/ يحدد فيه المدة المقررة للعملية والمحددة بأربعة أشهر وهي قابلة للتجديد لمدة أربعة أشهر أخرى كل ما دعت الضرورة ذلك.

7/ أن تودع الرخصة أي الإذن في ملف الإجراءات بالانتهاء من عملية التسرب[1].

* وملاحظة على ذلك أنه إذا أغفل شرط من هذه الشروط يؤدي إلى بطلان الإذن خرج المشرع الجزائري عن الأصل العام في التحقيق القائم بالفصل بين سلطتي الاتهام والتحقيق وأوكل لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية مهمة إصدار الإذن بالتسرب[2].

ب/ الشهادة في الجريمة الإلكترونية:

تعريف الشاهد في الجريمة الإلكترونية: يطلق عليه اسم الشاهد المعلوماتي لأنه هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي والذي يكون لديه معلومات جوهرية لأزمة الدخول إلى نظام المعالجة الآلية للبيانات فلذلك نجد أن الشاهد المعلوماتي ينحصر في إحدى الطوائف التالية: مشغلة الحاسب الآلي، خبراء البرمجة، المحللون، مهندسو الصيانة والاتصالات، ومديرو النظم[3].

وللشاهد التزامات لابد من التقيد بها مثل: طبع ملفات البيانات المخزنة في ذاكرة الحاسوب الآلي أو الدعامة الأخرى على أن يقوم بطباعتها وتسليمها إلى سلطات التحقيق والإفصاح عن كلمات المرور السرية والكشف عن الشفرات المدونة بها والأوامر الخاصة بتنفيذ البرامج المختلفة[4].

ج/ الخبرة في الجريمة الإلكترونية:

الخبرة هي الوسيلة لتحديد التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا عن الدليل المادي وإنما هي تقييم لهذا الدليل.

وقد أجاز المشرع للمحقق الاستعانة بخبير متخصص في المسألة موضوع الخبرة فقد نصت المادة 143 قانون الإجراءات الجزائية في فقرتها الأولى على أنه يجوز لكل جه قضائية تتولى: التحقيق او تجلس للحكم إذا تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة أو الخصوم أو من تلقاء نفسها.

[1] مولود ديدان، قانون الإجراءات الجزائية، المرجع السابق، ص 42.

[2] زبيخة زيدان، المرجع السابق، ص 169.

[3] مولود ديدان، قانون الإجراءات الجزائية، من نفس القانون، ص 43.

[4] زبيخة زيدان، المرجع السابق، ص 169.

وبالنظر إلى الطبيعة الخاصة بالجرائم الإلكترونية فإن إماطة اللثام عنها قد يحتاج إلى خبرة فنية تظهر الحاجة إليها منذ بدء التحري عن هذه الجرائم، ثم تستمر هذه الحاجة في مرحلتي التحقيق والمحاكمة نظرا للطابع الفني الخاص بأساليب ارتكابها والطبيعة المعنوية لمحل الاعتداء[1].

وبالعودة لنص المادة 146 نجد أن المشرع يفرض على الجهة القضائية الآمرة بندب الخبير تحديد مهمة الخبير بدقة وهذا يعود بنا إلى ضرورة تأهيل سلطات التحقيق أو الحكم في الجرائم الإلكترونية لنجاح الهدف المتوخى من التحقيق في هذا النوع المستحدث من الجرائم.

كما تجدر الإشارة على أنه يجب على القاضي اختيار الخبراء ذوي الإمكانيات العلمية والمقدرة الفنية الحالية فلا يكفي مجرد الحصول على شهادة علمية، إذ يجب مراعاة الخبرة العلمية فالوسائل الالكترونية متعددة وشبكات الاتصال بينها متنوعة فطبيعتها الفنية تجعلها موزعة على تخصصات فنية وعلمية دقيقة.

وعلى القاضي أن يتناول في أمر ندب الخبير المسائل التالية:

1/ تركيب الحاسب الآلي، طرازه، نوعه، نظام تشغيله، الأنظمة الفرعية التي يستخدمها.

2/ بيئة الحاسب أو الشبكة من حيث طبيعتها، تركيزها وتوزيعها، وكذلك نمط ووسائط الاتصالات.

3/ المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.

4/ الآثار الاقتصادية والمالية المترتبة عن الجريمة الإلكترونية.

5/ كيفية عزل النظام المعلوماتي دون اتلاف الأدلة أو الأجهزة أو تدميرها.

6/ إمكانية نقل أدلة الإثبات لأوعية أو وسائط مادية كالأوراق أو الأسطوانات على أن تكون مطابقة لما هو مسجل في الحاسب الآلي أو النظام أو الشبكة[2].

د/ الاستجواب:

وهو مناقشة المتهم مناقشة تفصيلية في التهمة المنسوبة إليه من طرف جهة التحقيق ومطالبته بإبداء رأيه في الأدلة القائمة ضده إما تنفيذا أو تسليما، وذلك قصد محاولة كشف الحقيقة واستظهارها بالطرق القانونية.

أحالت التشريعات استجواب المتهم بضمانات خاصة وذلك في القسم الخامس من الباب الثالث الكتاب الأول من قانون الإجراءات الجزائية وتتمثل في حق الاستعانة بمحام أثناء الاستجواب[3].

- الإجراءات الحديثة لجمل الدليل الالكتروني:

[1] بوكثير خالد، المرجع السابق، ص 23.

[2] زبيخة زيدان، المرجع السابق، ص 170.

[3] مولود ديدان، قانون الإجراءات الجزائية، المرجع السابق، ص 35.

أولا: الإجراءات المتعلقة بالبيانات الساكنة:

1/ التحفظ المعجل على البيانات المخزنة:

في المادة 16 من اتفاقية بودابست نصت على ضرورة كل طرف السماح لسلطاته المختصة أن تأمر أو تفرض بطريقة أخرى مزود الخدمة التحفظ العاجل على البيانات الإلكترونية المخزنة بما في ذلك البيانات المتعلقة بالأمور المخزنة بواسطة نظام المعلوماتي[1].

وذلك عندما تكون هناك أسباب تدعوا للاعتقاد بأن هذه البيانات على وجه الخصوص معرضة للفقد أو التغيير، وهذا خلال مدة 90 يوم كحد أقصى وتكون هذه المدة قابلة للتمديد.

-المقصود بمزودي الخدمات:

مزود الخدمات هو من تقدم خدمته إلى الجمهور بوجه عام في مجال الاتصالات الالكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود.

- مفهوم التحفظ المعجل على البيانات المخزنة:

يقصد به توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته، في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية.

ثانيا: الإجراءات المتعلقة بالبيانات المتحركة: ونجد فيها:

-اعتراض الاتصالات الالكترونية.

-اعتراض المراسلات السلكية واللاسلكية والمراقبة الالكترونية.

تجدر الإشارة إلى أن تأثير التطور العلمي لا يقف عند مضمون الدليل وإنما يمتد هذا التأثير كذلك إلى الإجراءات التي يترتب عليها الحصول على هذا الدليل، ولذلك فإنه يجب أن تكون هذه الإجراءات المتطورة ذات طبيعة مشروعة لكي تحافظ على شرعية الأدلة المتولدة منها[2].

وانطلاقا من أهمية حماية الحياة الخاصة نجد الدستور ينص في المادة 39 منه " لا يجوز انتهاك حرمة حياة المواطن المختصة وحرمة شرفه يحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"، وتبعا لذلك نظم سبل الرقابة عليها وحدد السلطة التي تملك ذلك والإجراءات التي يتم اتباعها حيال هذه المراقبة[3].

---

[1] هشام رستم، المرجع السابق، ص 134.

[2] خالد بوكثيرة، **الجرائم المعلوماتية**، مذكرة نهاية التدريب، المنظمة الجهوية للمحامين ناحية سطيف، الدفعة 2005-2006، ص 24.

[3] عائشة بن قارة مصطفى، المرجع السابق، ص 154.

وإذا كانت شبكات الحاسب الآلي تستخدم خطوط الهاتف وتستعين بجهاز معدل الموجات "modem" والذي يستطيع تحويل الإشارات الرقمية المستحدثة بواسطة الحاسب على موجات تناظرية تنقل مع موجات الصوتية خلال خطوط الهاتف، وبذلك فإنه يتبين وجود علاقة بين المراسلات التي تتم بالطرق التقليدية وتلك تتم بالوسائل الالكترونية بحيث يمكن القول إن هناك تنصتا ومراقبة إلكترونية تتم على شبكات الحاسب الآلي[1].

ومن ثمة لا يجوز التنصت عليها أو الاطلاع على الأسرار التي تحتويها إلا بذات الطرق التي عليها قانون الإجراءات الجزائية، فلا يستطيع الشخص اختراق صندوق البريد الالكتروني أو الدخول إلى أنظمة الحاسب الآلي المخزنة به الرسائل البريدية الإلكترونية وضبطها إلا عن طريق اتباع إجراءات قانونية محددة في القانون ومن قبل أشخاص مخولين قانونا بذلك.

وقد اختلف الفقه في تكييف إجراء اعتراض المراسلات السلكية واللاسلكية، فذهب رأي إلى أنها تعد تفتيشا وبالتالي تخضع لقيوده، واستند في ذلك إلى أن هذه المراقبة تتفق مع التفتيش في أن الهدف منها هو البحث وضبط ما يفيد الوصول إلى الحقيقة.

ولا أهمية لأن يكون الشيء المضبوط ماديا أم معنويا، وهي ذات الغاية من المراقبة والتصنت فهي البحث عن دليل معين[2].

في حين ذهب رأي آخر إلى التفرقة بين التفتيش والمراقبة، واعتبر الأول إجراء غايته العثور على الأدلة المادية وضبطها بوضع اليد عليها لمصلحة العدالة أما الثانية فليس لها كيان مادي ملموس والقول بأن الرسائل الالكترونية أو الحديث في التلفون يندمج في كيان مادي يمكن ضبطه، فأسلاك التلفون أو التسجيل ليس دليلا في حد ذاته وإنما هي وسيلة أو أداة لسماع الحديث ولا تتأثر طبيعته بوسيلة أو أداة الحصول عليه[3].

والرأي السديد أن التفتيش واعتراض المراسلات إجراءان مختلفان ذلك أن المشرع الإجرائي قد أفرد أحكاما خاصة لكل واحد منها نظرا لاختلاف المحل الذي يقع على كل منهما، فالأخير يقع على حرمة الحياة الخاصة بمطلق القول، أما الأول فقد يمس مصادفة هذه الحياة الخاصة حتى وإن تمت على كيانات معنوية فليس معنى أنه يتصور وقوع التفتيش على كيان معنوي وأن المراقبة تتم دائما على كيانات معنوية أن نسوي بينهما من حيث تأثيرهما على حرمة الحياة الخاصة بما قد لا يتوافر بالنسبة للتفتيش.

---

[1] هلالي عبد الله، المرجع السابق، ص 22.

[2] رؤوف عبيد، **مبادئ الإجراءات الجنائية في القانون المصري**، دار الجيل للطباعة، الطبعة 16، 1985، ص 385.

[3] أحمد فتحي سرور، المرجع السابق، ص 147.

وقد تدخل المشرع الفرنسي في 10 جويلية 1991 بإصدار قانون يفرض الرقابة على الاتصالات عن بعد بما في ذلك شبكات تبادل المعلومات بعد اختلاف الفقه بشأن ضبط الأشياء المعنوية من مكونات الحاسب الآلي عن طريق التنصت أو اعتراض المراسلات إذا اعتبر جانب من الفقه أن قانون الإجراءات الجزائية عندما نص على إصدار إذن بضبط أي شيء: فإنه يشمل بذلك بيانات الحاسب المعنوية، أما الجانب الآخر للفقه فاقترح مواجهة هذا القصور التشريعي بالنص صراحة على اعتراض المراسلات ويجب أن تشمل المواد المعالجة عن طريق الحاسب الآلي.

وعلى ضوء هذا القانون فإن المشرع الإجرائي الفرنسي خص إصدار قرار المراقبة بقاضي التحقيق (المادة 1/110) وله أن يندب مأمور الضبط القضائي للقيام به، ولا يأذن بالمراقبة إلا إذا كانت هناك ضرورة تستوجبها ظروف كشف الحقيقة وكانت هناك استحالة في الوصول إلها بطرق البحث والتنقيب العادية م (1/100) وتطلب هذا القانون كذلك في الجريمة المراد ضبطها بهذه الوسيلة أن تكون جناية أو جنحة معاقب عليها بالحبس الذي يزيد عن سنتين، م(2/100) وكذلك حدد ميعادا زمنيا للمراقبة مدته أربعة أشهر في حدها الأقصى وتكون قابلة للتجديد، وأنه يتعين أن يتم التسجيل وتفريع التسجيل تحت سلطة قاضي التحقيق ورقابته (م100).

وقد خاض المشرع الجزائري في تعديله الأخير لقانون الإجراءات الجزائية بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 في نص المادة 14 المتممة للباب الثاني من الكتاب الأول من الأمر رقم 66-155 بالفصل الرابع تحت عنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" بالمواد 65 مكرر 5 إلى المادة 65 مكرر 10[1].

وقد خول المشرع لوكيل الجمهورية أن يأذن باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم محددة على سبيل الحصر في نص المادة 65 مكرر5 ومن بين هذه الجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

فيسمح الإذن بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المنصوص عليها في المادة 47 من القانون الإجراءات الجزائية بغير رضا أو حتى علم الأشخاص الذين لهم حق على تلك الأماكن وتنفيذ عمليات المراقبة هنا تكون تحت المراقبة المباشرة لوكيل الجمهورية[2].

والإذن بالمراقبة أو التنصت أو اعتراض المراسلات محددة بميعاد 4 أشهر كحد أقصى قابلة للتجديد المادة 65 مكرر7.

[1] بوكثيرة خالد، المرجع السابق، ص 24.

[2] عائشة قارة مصطفى، المرجع السابق، ص 176، 177.

كما خول لقاضي التحقيق الإذن أيضا بوضع هذه الترتيبات في حالة فتح تحقيق قضائي وتتم العمليات تحت مراقبته المباشرة.

كما أجاز المشرع في نص المادة 65 مكرر8 تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات السابقة المذكورة في نص المادة 65 مكرر5، وفي الأخير على ضباط الشرطة القضائية تحرير محضر عن أي عملية اعتراض أو تسجيل أو وضع ترتيبات تقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، ويذكر تاريخ بداية هذه العمليات والانتهاء منها، وكما يودع أي تسجيل أو اعتراض أو نسخ تم أثناء عملية المراقبة ويودعها بالملف.

الفرع الثاني: دور قاضي التحقيق في توفير الأمن الإلكترونية:

ويبرز دور قاضي التحقيق من خلال المرحلة الثاني بعد مرحلة جمع الاستدلالات وهي مرحلة التحقيق

أولا: تعيين قاضي التحقيق:

في الجزائر يتعين قاضي التحقيق بمقتضى قرار من وزارة العدل، ثم عدل المشرع عن ذلك بموجب القانون 01-08 المؤرخ في 26 جوان 2001 وأصبح التعيين بموجب مرسوم رئاسي، وفقا لنص المادة 39 قانون الإجراءات الجزائية، إلا أنه حتى هذه الأخيرة تم إلغاؤها بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 ليرجع من جديد للتعيين[1].

بموجب قرار من وزير العدل بعد استشارة المجلس الأعلى للقضاء من بين قضاة الجمهورية وهذا رجوعا إلى نص المادة 50 من القانون الأساسي للقضاة، وتكون مدة التعيين ثلاث سنوات، وتنتهي مهام قاضي التحقيق بنفس الأشكال التي يتعين فيها، أي بقرار من وزير العدل[2].

ثانيا: اختصاص قاضي التحقيق:

سنتناول في هذا العنصر قواعد الاختصاص الشخصي ثم النوعي وأخيرا المحلي لقاضي التحقيق.

أ/ الاختصاص الشخصي:

الأصل أن قاضي التحقيق يحقق مع جميع الأشخاص دون تمييز، إلا أن المشرع الجزائري استثنى بعض الفئات:

-الأحداث.

-العسكريين.

[1] عبد الرحمان خلفي، **الإجراءات الجزائية في التشريع الجزائري**، دراسة مقارنة، دار بلقيس للنشر، د ط، 2015، ص223، 224.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص 177.

-ضباط الشرطة القضائية.

-قضاة الحكم والتحقيق ومساعدي وكيل الجمهورية.

-قضاة المجالس القضائية ورؤساء المحاكم ووكلاء الجمهورية.

-أعضاء الحكومة والولاة ويختص كذلك بالتحقيق في جميع جرائم القانون العام سواء كانت جناية أو جنحة او مخالفة التي من خلالها تقدم النيابة العامة طلب افتتاحي أو الجنايات أو الجنح التي من خلالها يقدم الطرف المدني ادعاء مدنيا[1].

ب/ الاختصاص النوعي:

يختص قاضي التحقيق بالتحقيق في جميع الجرائم ويكون ذلك وجوبي في الجنايات وجوازي في الجنح إذا كان هناك نص واختياري في المخالفات طبقا لنص المادة 66 من قانون الإجراءات الجزائية: التحقيق الابتدائي وجوبي في مواد الجنايات أما في مواد الجنح فيكون اختياري ما لم يكن ثمة نصوص خاصة، كما يجوز إجرائه في مواد المخالفات إذا طلبه وكيل الجمهورية ويختص كذلك قاضي التحقيق على مستوى المحاكم الجهوية في جرائم: المخدرات، الجريمة المنظمة، والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال، والإرهاب وجرائم الصرف طبقا للمرسوم التنفيذي رقم 348 المؤرخ في 2006/10/06.

ج/ الاختصاص المحلي:

تنص المادة 40 من 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 ولو كان القبض قد حصل لسبب آخر...[2].

-كذلك يجوز أن يمتد اختصاص قاضي التحقيق إلى أكثر من محكمة طبقا لنص المادة 40 من قانون الإجراءات الجزائية.

ثالثا: سلطات قاضي التحقيق وحدود الدعوى الجنائية أمامه:

القيام باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة وبالتحري عن أدلة الاتهام وأدلة النفي المادة 68 قانون الإجراءات الجزائية يجوز قاضي التحقيق أن يأمر بإجراء فحص طبي كما له أن يعهد إلى الطبيب بإجراء فحص نفساني أو يأمر باتخاذ أي إجراء يراه مفيدا المادة 68 قانون الإجراءات الجزائية.

[1] عبد الفتاح بيومي حجازي، **التوقيع الالكتروني في النظم القانونية**، دار الفكر الجامعي، الإسكندرية 2005، ص 519.

[2] عبد الرحمان خلفي، المرجع السابق، ص 228.

ينسق القاضي المكلف بالتحقيق سير إجراءات التحقيق وله وحده الصفة في مسائل الرقابة القضائية والحبس المؤقت واتخاذ أوامر التصرف في القضية طبقا لنص المادة 70 من قانون الإجراءات الجزائية[1].

يستطيع القاضي سماع أقوال كل من يشير إليهم في كل الشكوى باعتبارهم شهودا طبقا لنص المادة 73 من قانون الإجراءات الجزائية.

كما يستطيع قاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جمع المعاينات اللازمة أو القيام بتفتيشها طبقا لنص المادة 79 قانون الإجراءات الجزائية.

استدعاء كل شخص يرى فائدة من سماع شهادته بواسطة أحد أعوان القوة العمومية طبقا لنص المادة 88 قانون الإجراءات الجزائية. كما يجوز للقاضي استدعاء مترجم طبقا لنص المادة 91 قانون الإجراءات الجزائية.

رابعا: السمات التي تتميز بها قاضي التحقيق بالنسبة للجريمة الإلكترونية:

إن الجريمة الإلكترونية تختلف عن الجريمة التقليدية فلذلك لا يمكن أن يحقق فيها أي قاضي تحقيق وإنما لا بد أن يكون له صفات خاصة وهذه الصفات هي:

كأن يكون لديه معرفة بلغات البرمجة وأنظمة التشغيل الجديدة وأن يميل إلى تصميم وتحليل البرامج أو أنظمة التشغيل بسرعة وأن يؤمن بوجود أشخاص آخرين مثله لديهم القدرة على الاختراق والشبكة وكل هذه الأمور لا تتوافر إلا لمن كان لديه إمكانيات عقلية تزيد على متوسط العام المألوف.

خامسا: اتصال قاضي التحقيق بملف الدعوى الخاص بالجريمة الإلكترونية:

يتصل قاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي للطلب الافتتاحي لإجراء تحقيق، وإما عن طريق شكوى مصحوبة بادعاء مدني ضمن الشروط المنصوص عليها في المادتين 67 و73[2].

أ/ الطلب الافتتاحي لإجراء التحقيق:

يتصل وكيل الجمهورية بملف ضباط الشرطة القضائية فيمكن لوكيل الجمهورية أن يطلب فتح التحقيق ما لم ينص القانون على وجوب التحقيق في بعض الجنح، ويمكن لوكيل الجمهورية أن يقدم طلبا إضافيا لقاضي التحقيق إذا ظهرت وقائع جديدة طبقا للمادة 3/67 من قانون الإجراءات الجزائية الجزائري على أنه: " لا يجوز لقاضي

[1] مولود ديدان، قانون الإجراءات الجزائية، ص 38، 40.

[2] المادة 73/67 من قانون رقم 04/14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للامر 156/66 المتضمن قانون الاجراءات الجزائية، جريدة عدد 71.

التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية لإجراء التحقيق حتى ولو كان ذلك بصدد جناية أو جنحة متلبس بها.

ويجوز أن يوجه الطلب ضد شخص مسمى او غير مسمى، ولقاضي التحقيق سلطة اتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المحال تحقيقها إليه.

فإذا وصلت لعلم قاضي التحقيق وقائع لم يشر إليها في طلب إجراء التحقيق يتعين عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع.

ب/ الشكوى المصحوبة بالادعاء المدني:

تنص المادة 72 من قانون الإجراءات الجزائية " يجوز لكل شخص تضرر من جناية أن يدعي مدنيا بأن يتقدم بشكواه امام قاضي التحقيق المختص[1].

إن إحدى طرق تحريك الدعوى من طرف الأفراد، وهي في نفس الوقت إحدى طرق اتصال قاضي التحقيق بملف الدعوى، ويلجأ عادة المتضرر من الجريمة إلى هذه الطريقة تجنبا لطول الإجراءات وتقليصا للوقت، وحرصا منه على أن يكون الإشراف على الملف من طرف قاضي التحقيق، كما أن يستفيد من تتبع مجريات الدعوى العمومية بنفسه طالما كان هو من حركها.

إلا ان أخطر سلبيات الادعاء المدني المتمثل في سوء استعمال هذا الطريق لأن من شأنه أن يعرض الطرف المدني إلى متابعة جزائية بتهمة الوشاية الكاذبة إذا ما خسر دعواه ولهذا عليه يتأكد من أن اتهامه كان مبنيا على دليل قوي في الدعوى[2].

سادسا: استئناف أوامر قاضي التحقيق: الجهات التي تستأنف أوامر قاضي التحقيق هي:

أ/ النيابة العامة:

لوكيل الجمهورية أو أحد مساعديه استئناف جميع أوامر قاضي التحقيق دون استثناء وذلك طبقا لنص المادة 170 من قانون الإجراءات الجزائية الجزائري: " لوكيل الجمهورية الحق في أن يستأنف أمام غرفة الاتهام جميع أوامر قاضي التحقيق".

ويكون هذا الاستئناف بتقرير قلم مكتب المحكمة ويجب أن يرفع في ثلاثة (3) أيام من تاريخ صدور الأمر. يجوز للنائب العام الطعن في أوامر قاضي التحقيق في ظرف 20 يوما على ألا يكون لهذا الطعن أثر موقف في حالة استئناف أمر الإفراج ويفرج على المتهم رغم استئناف النائب العام ما لم يكن وكيل الجمهورية قد استأنفه

[1] عبد الرحمان خلفي، المرجع السابق، ص 296.

[2] مولود ديدان، قانون الإجراءات الجزائية، ص 42، 49.

بالطبع ويجب أن يبلغ النائب العام عند استئناف الخصوم في الدعوى، وذلك خلال العشرين يوما التالية لصدور الأمر حتى يكونوا على بينة من أمرهم لا يفاجؤوا بقرار من غرفة الاتهام في غير صالحهم.

طبقا لنص المادة 171 من قانون الإجراءات الجزائية الجزائري " يحق الاستئناف أيضا للنائب العام في جميع الأحوال ويجب أن يبلغ استئنافه للخصوم خلال العشرين يوما التالية لصدور أمر قاضي التحقيق ولا يوقف هذا الميعاد ولا رفع الاستئناف بتنفيذ الأمر بالإفراج المؤقت[1].

ب/ استئناف المتهم:

إن المتهم لا يجوز له استئناف جميع أوامر قاضي التحقيق ويرفع الاستئناف بعريضة تودع لدى قلم مكتب المحكمة في ظرف ثلاثة أيام من تبليغ الأمر على المتهم طبقا للمادة 168 من قانون الإجراءات الجزائية.

ج/ استئناف المدعي المدني:

كما أجاز المشرع الجزائري للمدعي المدني الحق في استئناف أوامر قاضي التحقيق التي لها علاقة بحقوقه المدنية، وبمفهوم المخالفة لا يجوز له استئناف الأوامر المتعلقة بالجانب الجزائي مثل الحبس المؤقت والإفراج والرقابة القضائية.

ويرفع الاستئناف خلال ثلاثة أيام من تاريخ تبليغ الأمر المراد استئنافه إلى المدعي المدني، وذلك بتقديم عريضة لدى قلم كاتب الضبط قاضي التحقيق طبقا لنص المادة 173 الإجراءات الجزائية[2].

الفرع الثالث: المحكمة:

أولا: الاختصاص المحلي في الجريمة الإلكترونية:

طبقا لنص المادة 37 من قانون الإجراءات الجزائية يتحدد الاختصاص المحلي للجريمة في ثلاث ضوابط أو مكان إقامة المتهم أو مكان الضبط[3].

كما نصت أحكام المرسوم التنفيذي رقم 348-06 المؤرخ في 5 أكتوبر 2006 على تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق إلى دائرة اختصاص محاكم أخرى، ويتعلق الأمر بكل من محكمة وهران وفي نطاق الجرائم الإلكترونية فإن السلوك الإجرامي قد يتم في مكان معين مثل جريمة الاتلاف عن طريق بث الفيروس وتتحقق النتيجة بتدمير المعلومات في مكان آخر، فإن الاختصاص ينعقد إما في مكان السلوك أو مكان تحقق النتيجة، تعد الجريمة الإلكترونية إذا تمت عن طريق شبكة الانترنت جريمة مستمرة حيث تعتبر أنها ارتكبت في جميع الأماكن التي امتدت الجريمة فيها، ومتى كانت الجريمة الإلكترونية، أيا كان نوعها فقد وسع المشرع

[1] مولود ديدان، قانون الإجراءات الجزائية، ص 106.

[2] عبد الرحمان خلفي، المرجع السابق، ص 298.

[3] نفس القانون، ص 79.

الجزائري من اختصاص المحاكم الجزائية بالنظر في الجرائم الإلكترونية أو المتصلة بتكنولوجيا الإعلام والاتصال إذا ارتكبت خارج الإقليم الوطني، أو إذا كان مرتكبيها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاقتصادية الاستراتيجية للدولة وذلك في إطار التعاون الدولي[1].

ثانيا: الاختصاص النوعي في الجريمة الإلكترونية:

يتحدد الاختصاص النوعي للمحكمة الفصل في القضية المعروضة عليها تبعا لنوع الجريمة التي ينظر فيها، حيث تختص محكمة الجنايات في الفصل في الجنايات والجرائم الموصوفة بأفعال إرهابية أو تخريبية المحالة إليها بقرار نهائي من غرفة الاتهام حسب نص المادة 248 من قانون الإجراءات الجزائية الجزائري[2].

كما تختص المحاكم في النظر في الجنح والمخالفات فيما عدا الاستثناءات المنصوص عليها في قوانين خاصة حسب المادة 01 من المرسوم التنفيذي رقم 348-06 المؤرخ في 28 أكتوبر 2006 المتضمن تحديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق[3].

ولأن الطبيعة التقنية المعقدة للجرائم الإلكترونية تفرض على رجال القضاء لتكوين يمكنهم من متابعة هذه الجرائم فقد خصها المشرع مع بعض أنواع الجرائم المتعلقة بالمتاجرة بالمخدرات والجريمة المنظمة العابرة للحدود وجرائم تبييض الأموال والإرهاب، والجرائم المتعلقة بالتشريع الخاص بالصرف بإجراءات خاصة إذ جعل الاختصاص ينعقد إلى دائرة اختصاص أخرى وهذا ما نصت عليه المواد 37، 40 والمادة 329 من قانون الإجراءات الجزائية إثر تعديل الذي جاء به القانون 04-14 المؤرخ 10 نوفمبر 2004 والذي حددت أحكامه في المرسوم التنفيذي رقم 06-348 والمتعلق بالتنظيم القضائي حيث نص على إنشاء أقطاب قضائية متخصصة ذات إقليم موسع لدى المحاكم بكل من: الجزائر العاصمة، قسنطينة، وهران، ورقلة[4].

[1] المرجع نفسه، ص 17.

[2] جميل عبد الباقي صغير، **القانون الجنائي والتكنولوجي الحديث**، دار النهضة العربية، القاهرة، 2009، 63.

[3] الجريدة الرسمية للجمهورية الجزائرية، العدد 63، المرجع السابق، ص 29.

[4] القانون رقم 14-04، المرجع السابق، ص 4.

المطلب الثالث: المعهد الوطني للأدلة الجنائية وعلم الإجرام:

المعهد الوطني للأدلة الجنائية وعلم الإجرام مقره ببوشاوي بالعاصمة ويتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن التكوين والتعليم وتقديم المساعدات التقنية، الدراسات والتحاليل في علم الجريمة وإنجاز الخبرة، والبحوث.

دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي وتمثالي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة، أفراد الدائرة يسهرون على تأمين اليقظة التكنولوجية من أجل تحسين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية لإنجاز المهام المنوطة بها.

الفرع الأول: تشكيلته:

كما سبق وأشرنا أن المعهد الوطني للأدلة الجنائية وعلم الإجرام يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة وتنقسم الدائرة إلى ثلاث مخابر وذلك حسب نوع المعلومات سمعية، بصرية، والإعلام الآلي.

كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل وهذه المخابر هي:

1/ مخبر الإعلام الآلي، 2/ مخبر الفيديو، 3/ مخبر الصوت.

أولا: مخبر الإعلام الآلي:

يختص مخبر الإعلام الآلي بتحليل ومعالجة حوامل المعطيات الرقمية، الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش، وتحديد التزوير الرقمي للبطاقات البنكية.

يتوفر على وجود محطة ترميم وتصليح الأجهزة والحوامل المعطلة وكذلك الشبكات الإعلامية، خبرات الإعلام الآلي والتجهيزات البيانية.

كما يضم الشبكات الإعلامية خبرات الإعلام الآلي والتجهيزات البيانية وجهاز اقتناء معلومات الهواتف والحواسيب والقاعات التي يحتوي عليها هي 7 قاعات: مكتب التوجيه، فصيلة الأنظمة المشحونة، فصيلة تحليل المعطيات، فصيلة الهواتف، فصيلة اقتناء المعطيات، قاعة موزع وقاعات تخزين[1].

[1] هواري عياش، **مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام**، جامعة محمد خيضر بسكرة، كلية الحقوق 2016، ص 03.

ثانيا: مخبر الفيديو:

من مهام مخبر الفيديو مقارنة الأوجه وشرعية الصورة والفيديو وإعادة بناء مسرح الجريمة بالتشكيل ثلاثي الأبعاد وتحسين نوعية الصورة الفيديو – صورة بمختلف التقنيات.

وتضم الأجهزة التالية: جهاز فيديو بوكس وحوامل الفيديو الرقمية والممغنطة وحبكات إعلامية، كونيتك ستوديو، ماكس ثلاثي الأبعاد وموزع لحفظ شرائح الفيديو. أما بالنسبة للقاعات يحتوي مخبر الفيديو على 4 قاعات، قاعتان للتحليل، قاعة التخزين وقاعة موزع.

ثالثا: مخبر الصوت:

يعمل على تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة ومعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية.

ومن أجهزته أجهزة الازدواجية والسماع وحبكات إعلامية معالجة وتحسين التسجيلات الصوتية، نسخ الأقراص المضغوطة وأجهزة التصليح والتعبير. أما بالنسبة للقاعات فإنه يحتوي مخبر الصوة على 05 قاعات: 3 قاعات للتحليل، قاعة تخزين، وقاعة موزع[1].

الفرع الثاني: مهام المعهد الوطني للأدلة الجنائية وعلم الإجرام:

على غرار الدول الأخرى لم تعد الجزائر بعيدة عن الإجرام الالكتروني حيث أضحى هذا النوع الجديد من الجريمة الخفية، والعابرة للأوطان يشكل تهديدا جديا وحقيقيا على الأفراد ومؤسسات الدولة الاقتصادية.

وبموجب النص الذي تم سنة 2004 والمتعلق بمكافحة الجريمة الإلكترونية تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية ومكافحتها من أجل القضاء أو الحد من هذه الآفة وذلك من خلال:

*مساعدة وحدات الدرك الوطني الممارسة لمهام الشرطة القضائية في البحث والتوصل إلى مرتكبي المخالفات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات وكذا المخالفات المتعلقة باستخدام الأنظمة المعلوماتية لتكنولوجيا الإعلام والاتصال.

*ومن أجل تحقيق ذلك يحوز أفرادها الذين يطاردون الجريمة المعلوماتية أحدث الأنظمة والبرمجيات المتطورة من أجل استخدامها في عمليات الوقاية من الإجرام الإلكترونية ومكافحتها وهذا ما يعد تحديا في حد ذاته حيث يتعلق الأمر بحماية المنظومة الوطنية للمعلومات من خلال تطبيق القانون وقد نجحت خلال السنوات الأخيرة في حل العديد من القضايا منها 65 في المائة متعلقة بالمخالفات المرتكبة ضد الأشخاص و8 بالمائة ضد الأمن العام وكذا

[1] مجلة الجيش حوار مع العقيد ابن رجم جمال، مدير مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، عدد 599، جوان 2013، ص 15/14.

27 في المائة متعلقة بمخالفات مرتكبة ضد المؤسسات في إطار ممارسة مهامه ونشاطه ويقوم المركز بالتعاون والتنسيق مع المصالح الأمنية الوطنية وعدد من متعاملي الخدمات الهاتفية من أجل الاستجابة للطلبات التي تأتيها من مختلف وحدات الدرك الوطني والمتعلقة بالتشخيص و التعرف على العناوين الالكترونية أو أرقام المرسلين محل التحقيق كما أن المركز يتعاون مع مختلف السلطات القانونية والتشريعية في مجال طلبات التعامل مع الهيئات القانونية الدولية[1].

أما فيما يخص أفاق المركز فيمكن القول إن المركز يسعى إلى:

-تعميم واستكمال نشر فرق المحققين في الجريمة الإلكترونية وتعميم نظام لليقظة على المستوى الوطني عبر كافة الوحدات التابعة للدرك الوطني.

-تكوين مجموعة مختصة في مهام أمن أنظمة المعلوماتية وحمايتها.

-تكوين المكونين في المجال وإعداد برامج المواد المتعلقة بالتكنولوجيات الجديدة ومكافحة الجريمة الإلكترونية على صعيد كافة مستويات التكوين.

المطلب الرابع: المديرية العامة للأمن الوطني:

لقد تنبهت المديرية العامة للأمن الوطني لخطر الإجرام الالكتروني في مطلع الألفية الثانية وكان ذلك من خلال مشاركة إطاراتها في الملتقيات الدولية التي كانت تنظمها الدول الأجنبية خاصة الأوربية حول الإجرام الإلكتروني، فمن خلال دق ناقوس الخطر في تلك الدول حول هذه الظاهرة الإجرامية المستحدثة، اتضح انتشار وتعميم استعمال تكنولوجيا الإعلام والاتصال في تلك المجتمعات كانت لها آثار جانبية سلبية، من جراء استغلال هذه التكنولوجيا من طرف المجرمين وهو ما جعل الجوانب السلبية لتكنولوجيا الإعلام والاتصال ستعرف لا محالة طريقها إلى مجتمعنا، بالموازاة مع تعميم واستعمال هذه التكنولوجيا في بلدنا[2].

ولقد واجهت هذه المديرية الجريمة المعلوماتية بمختلف الوسائل منها:

الفرع الأول: الوسائل القانونية:

أ/ القانون 22-06 المؤرخ في 2006/12/10 المعدل والمتمم لقانون الإجراءات الجزائية والذي صنف جرائم المساس بأنظمة المعالجة الآلية للمعطيات ضمن الجرائم الخطيرة ووضع لها تدابير إجرائية خاصة منها:

*تمديد الاختصاص المحلي لضباط الشرطة القضائية إلى كافة التراب الوطني.

[1] مجلة الجيش حوار مع العقيد ابن رجم جمال، المرجع السابق، ص 15.

[2] مصطفاوي عبد القادر محافظ الشرطة الوطنية ومكافحة الجريمة المعلوماتية، ملتقى دولي حول محاربة الجريمة المعلوماتية، الجزائر 5-6 ماي 2010، مركز البحوث القانونية والقضائية، ص 22.

*مراقبة الأشخاص والتسليم المراقب.

*إمكانية اللجوء إلى الأساليب الخاصة في التحري، لا سيما اعتراض المراسلات، التقاط وتسجيل الصور والأصوات، التسرب.

ب/ القانون 05-03 الخاص بحماية الملكية الفكرية الذي صنف برامج الحاسوب ضمن المصنفات المحمية واعتبر نشر المصنفات عبر أنظمة المعالجة الآلية للمعطيات كوسيلة من وسائل التقليد المعاقب عليها.

ج/ القانون المدني الذي أقر بأن المعطيات الرقمية يعتد بها كوسيلة إثبات مثلها مثل الوثائق المكتوبة.

د/ القانون 04-09 المؤرخ في 2009/08/05 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها والذي من أهم جاء فيه:

-المراقبة الالكترونية.

-تفتيش المنظومات المعلوماتية مع إمكانية تمديد التفتيش من منظومة إلى أخرى ولو خارج الوطن.

-حجز المعطيات المعلوماتية.

- إلزام مقدمي الخدمات بمساعدة السلطات وحفظ المعطيات.

-إلزام مقدمو خدمة الأنترنت بسحب المحتويات المخالفة للقوانين أو جعل الدخول إليها غير ممكن.

-وضع ترتيبات تقنية تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام وإخبار المشتركين لديهم بوجودها.

الفرع الثاني: الوسائل المعلوماتية:

تتركز استراتيجية المديرية العامة للأمن الوطني في مجال مكافحة الجريمة الإلكترونية على الأعمدة التالية[1]:

أ/ التكوين:

1/التكوين الأولي: في مجال التكوين الابتدائي تم إدراج موضوع الجريمة الإلكترونية ضمن البرامج التكوينية المخصصة لضباط الشرطة القضائية.

2/ التكوين المتواصل والمتخصص: أصبح موضوع الجريمة الإلكترونية من بين الجرائم المستحدثة والتي أدرجت في برامج التكوين المتخصص الموجه للإطارات والرتباء التابعين للشرطة القضائية.

[1] مصطفاوي عبد القادر، المرجع السابق، ص123.

ب/ إعادة تنظيم مصالح الشرطة القضائية:

في إطار سياسة التخصص في مجال الشرطة القضائية شرعت المديرية العامة للأمن الوطني في إدخال تعديلات على الهياكل التنظيمية الخاصة بمصالح الشرطة القضائية، وذلك من أجل جعل المصالح المكلفة بمكافحة الجريمة أكثر تناسبا مع الواقع وأكثر استعدادا لما تشير إليه التنبؤات المستقبلية ففي الجريمة الإلكترونية بات من الضروري وضع آليات عملياتية، لذا تم إنشاء مصالح مختصة في مكافحة هذه الجرائم.

1/ على مستوى مخابر الشرطة العلمية: إثر تفاقم ظاهرة استخدام التكنولوجيا في مختلف أشكال الإجرام تم سنة 2007 تدعيم مخابر الشرطة العلمية والتقنية بأقسام مختصة في الأدلة الرقمية على مستوى المخابر الثلاثة المتواجدة بكل من العاصمة، وهران، وقسنطينة، تكمن مهامها في استخراج المعطيات المخزنة بداخلها والتي من شأنها أن تساعد المحققين في التحقيق والتي تشكل في ذاتها أدلة إقناع.

2/أهم الأجهزة التي تتكفل باستغلالها هذه الأقسام: أجهزة الكمبيوتر ولواحقها، أدوات التخزين الرقمية مثل (أقراص مضغوطة، أقراص صلبة، أقراص وماضية، أجهزة الهواتف النقالة، أجهزة التصوير الرقمية) إلى جانب القضايا المتعلقة بالجرائم الإلكترونية تساعد الأقسام المختصة في الأدلة الرقمية[1].

[1] حملاوي عبد الرحمان، **مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية**، جامعة محمد خيضر بسكرة، كلية الحقوق، 2016، ص 5-6.

خاتمة الفصل الثاني:

وقد تناولنا فيه الجوانب العملية للحد من الجريمة الالكترونية في القوانين العامة المنظمة للجريمة الالكترونية، بالإضافة إلى القوانين الخاصة للحد منها في المبحث الأول، أما المبحث الثاني تناولنا فيه الآليات العضوية للحد من الجريمة الالكترونية.

ونظرا لأهمية مكافحة الجرائم الإلكترونية وخطورتها دفع بالدولة إلى خلق أجهزة ووضع مختلف الوسائل للتصدي لها كونها تتطلب آليات ووسائل حديثة تتماشى معها والحد منها حيث أصبحت في وقتنا الراهن تهدد أمن وسلامة الأفراد وهو ما يقتضي الإسراع في اتخاذ الإجراءات اللازمة والتي من شأنها التقليل من حدة هذا النوع من الجرائم.

خاتمـــــــة

نستخلص مما سبق أن العالم اليوم يعيش في زمن ساده تطور تكنولوجي أو ما يسمى بالثورة المعلوماتية حيث أصبحت حياتنا اليوم تستدعي اللجوء إليها فقد مكنت الوسائل الإلكترونية المجتمعات من تجاوز فكرة الحدود السياسية، نظرا للإمكانات المتاحة أمامها، لكن مع هذا التطور قد ارتبط به تطور هذا النوع من الجرائم وذلك نتيجة سوء استخدام هذه الوسائل.

ولقد حاولنا من خلال الفصل الأول الوقوف على الإطار المفاهيمي للجريمة الالكترونية وذلك بالتعريف على أهم التعريفات المختلفة، وآراء الفقهاء حول تحديد المعيار التعريف في الجريمة، ثم الخصائص التي تتميز بها الجريمة الالكترونية عن غيرها، وأهم أنواع هذه الجريمة، كذلك من هم الأشخاص الذين يرتكبون هذا النوع من الجرائم، والأسباب الدافعة لارتكابها.

أما في الفصل الثاني فقد تناولنا جل المواد المتعلقة بأحكام الموضوعية الخاصة، أشكال الاعتداء في الجريمة الالكترونية، وكذا العقوبات التي أوجدها أو وضعها المشرع الجزائري لكل جريمة على حدى، وأهم القواعد الإجرائية المتبعة في هذه الجريمة بحيث لا حظنا تشعب في الموضوع وصعوبته وخصوصا ما تعلق بالقواعد الإجرائية حيث أن هذه الجرائم حديثة نسبيا لتستلزم دراسة مستقبلية محاولة وضع مبادئ عامة بكل ما يتعلق بجرائم ترتبط بالتطور الالكتروني والمعلوماتي ووسائل الاتصال الحديثة وهذا ما يتطلب تدخلا تشريعيا من اجل وضع حماية قانونية متكاملة لسد جميع الثغرات في قانون العقوبات وبحيث تكون صالحة لمواكبة نظم المعلومات ولعل من أبرز النتائج التي أفرزتها هذه الجريمة تتمثل في:

أ/ النتائج:

أهم النتائج التي توصلت لها الدراسة:

* لم يتفق على تعريف جامعا مانعا للجريمة الالكترونية.

* تبين من خلال دراسة خصائص الجريمة الالكترونية أنها تتمتع بطبيعة قانونية مغايرة تماما للجريمة التقليدية.

* قصور القوانين التقليدية أمام هذه الجرائم المستحدثة.

* رغم اجتهاد المشرع الجزائري للتصدي لهذه الجريمة إلا انه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة.

* إن التطور التكنولوجي والتقني يحتم على المشرع تعديل القواعد القانوني، خاصة فيما يتعلق بحقوق الملكية الفكرية والحقوق المجاورة لم تعد قابلة للتطبيق في بيئة رقمية.

* أن النصوص الوضعية لحماية حقوق المؤلف والحقوق المجاورة تعتبر غير كافية لمواجهة لاعتداءات الواقعة عليها عبر الانترنت.

ب/ الاقتراحات:

- من واجب المشرع أن يوضع نصوصا قانونية واضحة وخالية من الغموض، بحث أنها ستؤطر ظواهر اجتماعية جديدو مستقبلا.
- عند وضع النصوص يجب أن يدقق في حماية المواطن، على أساس أن حماية الأمن الرقمي يمكن أن تحيل على مفاهيم متعددة تتراوح ما بين حماية الأشخاص وحماية المجموعات وغيرها
- ضرورة التعاون الدولي لمكافحة هذه الجرائم من خلال مجموعة تشريعات وطنية واتفاقيات دولية وإقليمية.
- عقد الدورات التدريبية التي تعتني بمكافحة الجرائم الالكتروني.

قائمة المراجع

قائمة المصادر والمراجع

أولا: قائمة المصادر

***القوانين:**

1/دستور الجمهورية الجزائرية الديموقراطية الشعبية الصادر بموجب المرسوم الرئاسي رقم 438/96 المؤرخ في 1996/12/07.

2/ قانون رقم 09-04 المؤرخ في شعبان عام 1430 الموافق لـ 05 غشت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ج ر ع 47 صادر بتاريخ 16 أوت 2009.

3/ قانون رقم 14/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 155/66 المتضمن قانون الإجراءات الجزائية، جريدة عدد 71.

4/ قانون رقم 2000-03 المؤرخ في 2000/08/05 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

5/ قانون العقوبات الفرنسي رقم 97-1159 المؤرخ في 19 ديسمبر 1997 المتضمن قانون العقوبات الفرنسي.

*** المراسيم:**

- المرسوم التنفيذي رقم 06-348 المؤرخ في أكتوبر 2006 المتضمن تحديد الاختصاص المحلي لبعض وكلاء الجمهورية وقضاة التحقيق جر عدد 63.

ثانيا: قائمة المراجع

*** الكتب:**

1/ أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، ط10،

2/ أمين طعباش، الحماية الجنائية للمقالات الالكترونية، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى 2015.

3/ أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة الجزائر، ط2، 2007.

4/ أمين فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، كلية الحقوق، الإسكندرية، 2009.

5/ جميل عبد الباقي، الجوانب الإجرائية للجرائم بالأنترنت، دار النهضة العربية القاهرة، 2001.

6/ جميل عبد الباقي صغير، القانون الجنائي والتكنولوجي الحديث دار النهضة العربية، القاهرة، 2009.

7/ خيثر مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات دار الهدى، عين مليلة الجزائر.

8/ رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجيل للطباعة، الطبعة 16، 1985.

9/ طارق إبراهيم الدعسوقي عطية، الأمن المعلوماتي، النظام القانوني لحماية المعلوماتية، دار الحاسمة الجديدة، الإسكندرية 2009.

10/ عائشة بن قارة مصطفي، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والقانون المقارن، دار الجامع الجديد، كلية الحقوق، جامعة الإسكندرية، د ط، 2006.

11/ عادل عبد العالي إبراهيم خراشي، إشكالية التعاون الدولي في مكافحة الجرائم المعلوماتية عليها، دار الجامعة الجديدة، الإسكندرية، مصر، 2015.

12/ عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2010.

13/ عمر أبو الفتوح عبد العظيم الحمامي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي الاسكندرية، مصر، 2008.

14/ عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، مصر، 2006.

15/ عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونية، دار الفكر الجامعي، الإسكندرية، مصر، 2005.

16/ علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعية للطباعة والنشر، بيروت، لبنان، د ط، دس.

17/ عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري، دراسة مقارنة، دار بلقيس للنشر، د ط، 2015.

18/ عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنت، منشورات الجلبي الحقوقية، بيروت، لبنان، دط،2007.

19/ محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة الإسكندرية، مصر، 2007.

20/ محمد زكي أبو عامر وعلي عبد القادر القهوجي، قانون العقوبات، القسم الخاص، دار النهضة العربية، القاهرة، 1993.

21/ محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، د ط، 2004.

22/ محمد أمين الرومي، جرائم الكمبيوتر والأنترنت، جار المطبوعات الجامعية، الإسكندرية، مصر، 2003.

23/مولود ديدان، دستور، تعديل نوفمبر، 2008، دار بلقيس، الجزائر.

24/ مولود ديدان، قانون العقوبات رقم 09-01 مؤرخ في 25 فبراير 2009.

25/ مولود ديدان، قانون الإجراءات الجزائية، رقم 11-02 د ط، ديسمبر 2014.

26/ نائلة عادل محمد فريد قورة، الجرائم الحاسب الآلي والاقتصادية، منشورات الحلبي الحقوقية، ط1، 2005.

27/ نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنت، في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي، الإسكندرية، مصر، د ط، 2013.

28/ نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، ط1، الإصدار الأول، 2008، 1429هـ/2008م.

29/ هشام فريد، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، ط1، 1994.

30/ هلالي عبد الله أحمد، تفتيش نظام الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، ط1، 1997.

31/ خيرت علي محرز، **التحقيق في جرائم الحاسب الآلي**، دار الكتاب الحديث، الإسكندرية، مصر، 2012.

***المجلات:**

1/ مجلة جامعة بابل، العلوم الإنسانية، المجلد 14، العدد 2، 2008.

2/ مجلة الجيش حوار مع العقيد ابن رجم جمال، مدير مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، عدد 599، جوان 2013.

***المداخلات:**

1/ المقدم عز الدين عز الدين، ملتقى حول الجرائم المعلوماتية، الإطار القانوني للوقاية من الجرائم بمكافحتها، جامعة محمد خيضر بسكرة، 10 نوفمبر 2016.

2/ حملاوي عبد الرحمان، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة محمد خيضر بسكرة، كلية الحقوق، 2016.

3/ سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية، محكمة سيدي محمد.

4/ هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، جامعة محمد خيضر بسكرة، كلية الحقوق 2016.

5/ مصطفاوي عبد القادر محافظ الشرطة الوطنية ومكافحة الجريمة المعلوماتية، ملتقى دولي حول محاربة الجريمة المعلوماتية، الجزائر 5-6 ماي 2010، مركز البحوث القانونية والقضائية.

6/ بورزام أحمد، وكيل الجمهورية لدى باتنة، الجرائم المعلوماتية المجلس القضائي باتنة.

7/ مشار عطا الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر، 2009.

8/ مجلة الأمن العام، نائلة محمد فريد، جريمة الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، بحث مقدم للمؤتمر التاسع لمنع الجريمة ومعاملة المجرمين، العدد 151، 1995.

*** المذكرات الجامعية:**

- رسائل الماجستير:

1/ أمال قارة، الجريمة المعلوماتية، مذكرة لنيل شهادة الماجيستير في القانون الجنائي، الجزائر، 2002.

2/ سعيد نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجيستير في العلوم القانوني، جامعة الحاج لخضر باتنة، 2013/2012.

3/ معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة لنيل شهادة الماجيستير في العلوم الجنائية، 2012/2011.

4/ يوسف مناصرة، جرائم المساس بأنظمة معالجة الآلية للمعطيات، رسالة مقدمة لنيل شهادة الماجيستير في القانون الجنائي والعلوم الجنائية، قسم العلوم القانونية، جامعة الجزائر، السنة الجامعية 2009/2008.

- رسائل الماستر:

1/خالد بوكثيرة، الجرائم المعلوماتية، مذكرة نهاية التدريب، المنظمة الجهوية للمحامين ناحية سطيف، الدفعة 2006-2005.

2/ مراد ماشوش، مكافحة جرائم المعلوماتية في التشريع الجزائري، مذكرة مقدمة لاستكمال نيل شهادة ماستر أكاديمي في مسار الحقوق تخصص قانون الجنائي، 2003.

ملاحق

1) إحصائيات الجرائم المالية بأنظمة المعالجة الآلية للمعطيات وفق القانون 15/04 في 10نوفمبر 2004 على مستوى مجموعة المحاكم خلال سنوات 2011-2012-2013

ملحق رقم 1 يتضمن:

إحصائيات الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفقا للقانون 04-15 المؤرخ في 10 نوفمبر 2004 على مستوى مجموع المحاكم خلال السنوات 2012-2013-2014

المجموع العام

نوع الجريمة	عدد الجرائم المرتكبة	العدد الإجمالي للأشخاص المتابعين					العدد الإجمالي للأشخاص المتابعين حسب فئة السن (الأشخاص الطبيعيين)								عدد الأشخاص المتابعين المعرفة بالمعلوماتية حسب كل جريمة		عدد الأشخاص المتابعين الذين لهم علاقة بالضحية		الدافع لإرتكاب هذه الجرائم من قبل إجمالي الأشخاص المتابعين						عدد الضحايا					
		الأشخاص المعنويين		الأشخاص الطبيعيين		المجموع	أقل من 18 سنة		من 18 إلى أقل من 25 سنة		من 25 سنة إلى 30 سنة		أكثر من 30 سنة		من جنسية جزائرية	من جنسية أجنبية	من جنسية جزائرية	من جنسية أجنبية	الكسب المادي	الانتقام	الفضول	التحدي	أسباب أخرى متنوعة	إدارات عمومية و مؤسسات ذات طابع صناعي و تجاري	شركات خاصة	شركات خاصة أجنبية	هيئات عمومية أجنبية	أشخاص معنوية أخرى غير الدولة	أشخاص طبيعيين
		من جنسية جزائرية	من جنسية أجنبية	من جنسية جزائرية	من جنسية أجنبية		من جنسية جزائرية	من جنسية أجنبية	من جنسية جزائرية	من جنسية أجنبية	من جنسية جزائرية	من جنسية أجنبية	من جنسية جزائرية	من جنسية أجنبية			من جنسية جزائرية	من جنسية أجنبية											
سنة 2012	12	1		18		19					1		17		19		9		1					2	4	1		3	2
سنة 2013	14			16		16	1		3		1		11		12		9		1	1		2	12	4	4	1		2	4
سنة 2014	29	2		35		37	2		11		11		11		24	2	18	2	9	3	2		19	5	2	2	1	2	24

ملحق رقم 2 يتضمن:

على المستوى الوطني

الإحصائيات المتعلقة بجرائم المساس بأنظمة المعالجة الآلية للمعطيات وفقا للمواد من 394 مكرر إلى 394 مكرر7 من قانون العقوبات

من 1 جانفي 2015 إلى 31 ديسمبر 2015

الجرائم	الجنسية	عدد الجرائم المرتكبة	العدد الإجمالي للأشخاص المتابعين (حسب فئة السن)						عدد الأشخاص المتابعين الذين لهم معرفة بالمعلوماتية	عدد الأشخاص المتابعين الذين لهم علاقة بالضحية	الدافع لإرتكاب هذه الجرائم من قبل إجمالي الأشخاص المتابعين						عدد الضحايا						
			أقل من 18	من 18 إلى 25	من 26 إلى 35	أكثر من 35	أشخاص معنوية	المجموع			الكسب المادي	الانتقام	الفضول	التحدي	أسباب أخرى متنوعة أذكرها		أشخاص طبيعيين	إدارات عمومية أو مؤسسات ذات طابع صناعي و تجاري	شركات خاصة	شركات خاصة أجنبية	هيئات عمومية أجنبية	أشخاص معنوية أخرى أذكرها
الدخول أو البقاء عن طريق الغش في منظومة المعالجة الآلية في المعطيات المادة 394 مكرر من ق ع	38	5	10	22	4	3	44	31	10	22	5	6	0	11	45		3	2	0	0	0	0
الإدخال أو الإزالة أو التعديل بطريق الغش للمعطيات في نظام المعالجة الآلية للمعطيات المادة 394 مكرر 1 من ق ع	7	0	4	5	3	0	12	8	5	5	0	2	0	5	3		4	0	0	0	0	0
التصميم أو البحث أو التجميع أو التوفير أو النشر أو الإتجار في المعطيات المخزنة أو المعالجة أو المرسلة عن طريق المنظومة	6	0	1	7	3	0	11	10	5	3	2	6	0	0	4		2	0	0	0	0	0
الحيازة أو الإفشاء أو النشر أو الإستعمال لأي غرض كان للمعطيات المتحصل عليها من إحدى جرائم المعالجة الآلية للمعطيات عمدا و عن	7	0	2	4	2	3	11	6	3	7	1	2	0	1	6		0	2	0	0	1	0
المشاركة في مجموعة أو إتفاق بغرض الإعداد لجريمة المساس بأنظمة المعالجة الآلية للمعطيات المادة 394 مكرر 5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0
جرائم المساس بأنظمة المعالجة الآلية للمعطيات المستهدفة للدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام المادة 394	1	0	2	0	0	0	2	0	0	0	0	0	0	2	0		0	0	0	0	1	0
المشاركة أو الإتفاق بغرض لإعداد لجريمة أو أكثر من جرائم المساس بأنظمة المعالجة الآلية للمعطيات المادة394 مكرر 5من ق ع	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0
المشروع في إرتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات المادة394 مكرر 7من ق ع	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		0	0	0	0	0	0
المجموع	59	5	19	38	12	6	80	55	23	37	8	16	0	19	58		9	4	0	0	2	0

ملحق رقم 3 يتضمن:

على المستوى الوطني

الإحصائيات المتعلقة بقضايا المساس بأنظمة المعالجة الآلية للمعطيات وفقا للمواد من 394 مكرر إلى 394 مكرر7 من قانون العقوبات على مستوى جهة الحكم

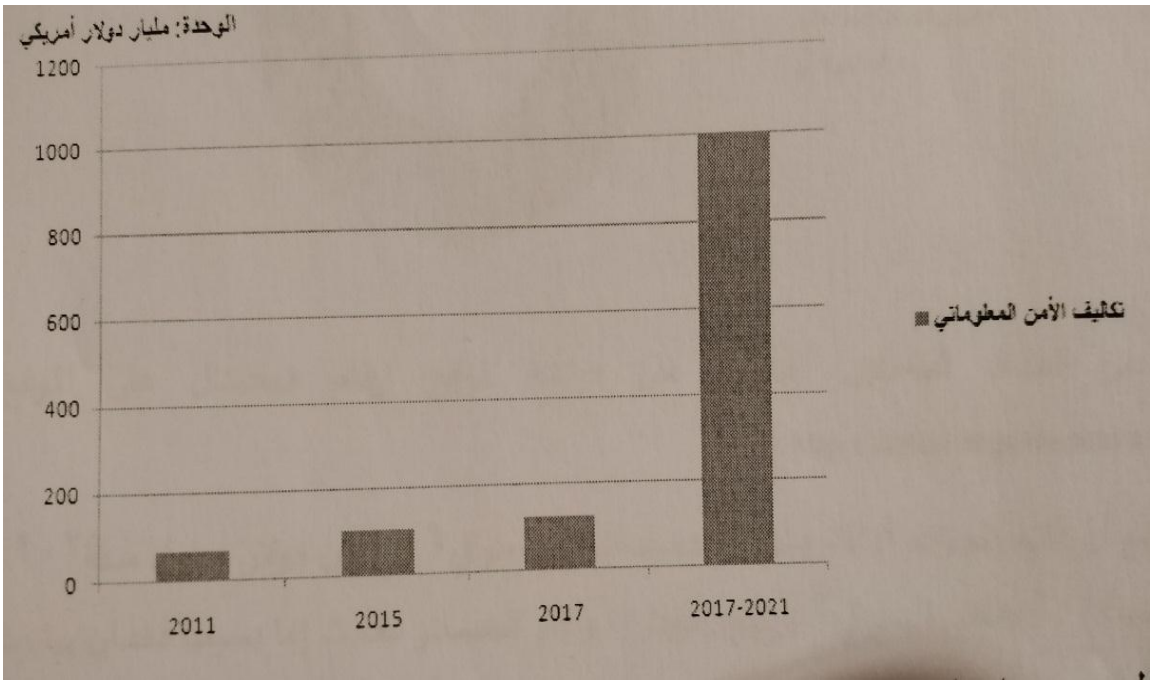
من 1 جانفي إلى 30 جوان 2016

الجدول رقم 1 (القضايا)

الجهة القضائية	عدد القضايا الباقية	عدد القضايا المسجلة	المجموع	عدد القضايا المفصولة	عدد القضايا الباقية	عدد الأشخاص المتهمين (في القضايا المجدولة)			نتيجة الفصل (حسب الأشخاص)				
						جزائريين	أجانب	أشخاص معنوية	عدد المحكوم عليهم بالبراءة	عدد المحكوم عليهم بالإدانة		عدد المحكوم عليهم بأحكام أخرى أذكرها	
										أشخاص طبيعية	أشخاص معنوية	العدد	ذكر الحكم
مجموع المجالس	2	11	13	13		44	0	0	31	12	0	1	
محاكم الجنايات الجزائي	0	1	1	0	1	4	0	0	0	0	0	0	
مجموع المحاكم	4	42	46	29	17	61	0	0	9	29	0	2	

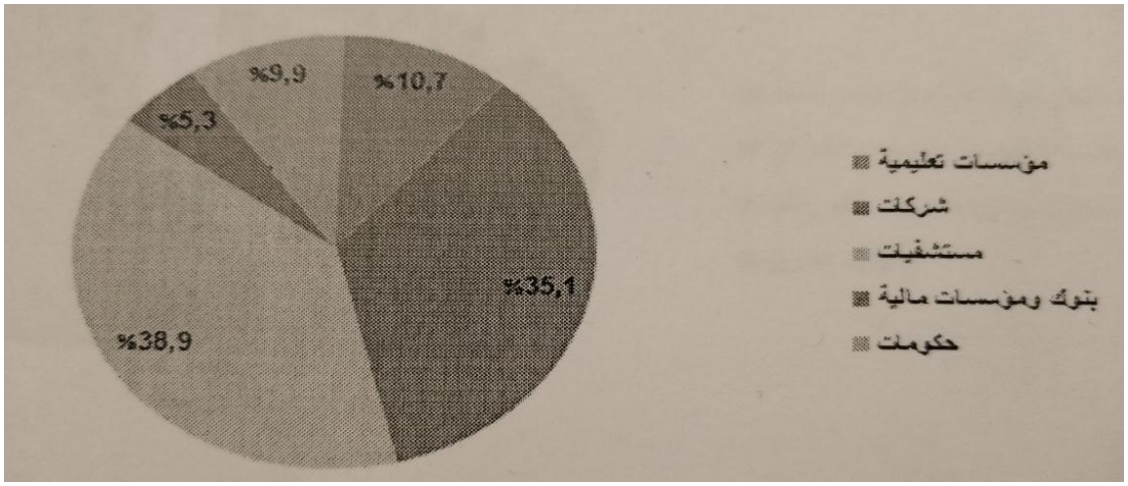
2) أسباب خسائر الجرائم الإلكترونية:

الشكل رقم 1: تكاليف الأمن المعلوماتي خلال الفترة من 2011 إلى 2021



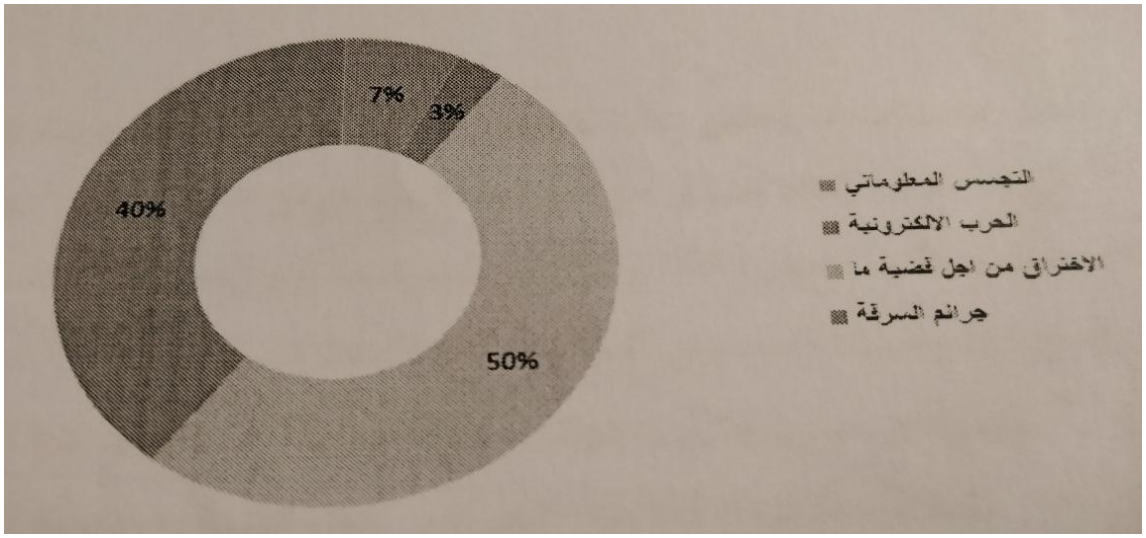
المصدر: من إعداد الباحثين اعتمادا على معطيات موقع ارقام ديجيتال cybersecurity ventures.

الشكل رقم 2: أكثر الشركات والمؤسسات اختراق خلال 2015.



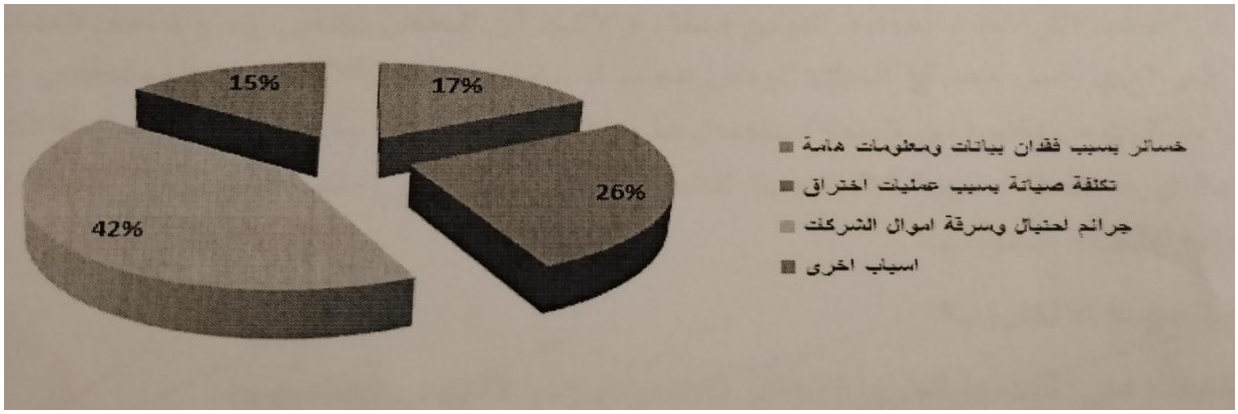
المصدر: من إعداد الباحثين اعتمادا على دراسة لموقع ارقام ديجيتال على الموقع التالي:
http://digital.argaam.com/article/detail/112326

الشكل رقم 3: الدافع الأساسي لجرائم المن المعلوماتي.



المصدر: المصدر: من إعداد الباحثين اعتمادا على دراسة لموقع ارقام ديجيتال على الموقع التالي: http://digital.argaam.com/article/detail/112326

الشكل رقم 4: أسباب خسائر الجرائم الالكترونية.



المصدر: المصدر: من إعداد الباحثين اعتمادا على دراسة لموقع ارقام ديجيتال على الموقع التالي: http://digital.argaam.com/article/detail/112326

فهـــــــرس

الفهـــــــــــرس