وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche Scientifique

جامعة عبد الحميد بن باديس بمستغانم
كلية الحقوق والعلوم السياسية

المرجع:.....

قسم: قانون عام

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجريمة الإلكترونية في التشريع الجزائري

مـن إعـداد الطالبة:
- بن داني رانيا.

تحت إشراف الأستاذ:
- بن عوالي علي

أعضاء لجنة المناقشة:

الأستاذ (ة):	بوسحبة جيلالي	**رئيسا**
الأستاذ (ة):	بن عوالي علي	**مشرفا ومقررا**
الأستاذ (ة):	زواتين خالد	**مناقشا**

السنة الجامعية: 2023/2022م

تاريخ المناقشة: 2023-06-08


بسم الله الرحمن الرحيم

شكر وعرفان

الحمدلله الذي أنار لنا طريق العلم ووفقنا لإتمام هذا العمل المتواضع، رغم كل الصعاب والمعوقات.

أتوجه بجزيل الشكر والامتنان إلى الأستاذ " بن عوالي علي" لقبوله الإشراف على هذه المذكرة، وعلى نصائحه وتوجيهاته القيمة النابعة من تجربته الطويلة في ميدان البحث العلمي، و متابعته المتواصلة لأطوار إنجاز هذا البحث.

وإلى الأساتذة "عثماني محمد" و "حساين محمد" على مساعدتهم لي في اختيار موضوع المذكرة.

كما أتقدم بالشكر الجزيل للسادة أعضاء لجنة المناقشة كل باسمه على قبولهم مناقشة هذه المذكرة.

وإلى أختي وحبيبتي " قنديل نور الهدى" على نصائحها وإرشاداتها وتوجيهاتها القيمة، والتي شجعتني ووقفت وراء هذا العمل.

إلى كل من ساهم في هذا العمل ولو بكلمة طيبة.

كما أتقدم بالشكر إلى طاقم مكتبة كلية الحقوق والعلوم السياسية ، كل إطارات و عمال الجامعة.

الإهداء

أهدي ثمرة جهدي إلى :

من فارقتني بجسدها و لم تفارقني بروحها، جدتي رحمها الله.

إلى أمي رفيقة دربي حفظها الله و أطال في عمرها.

إلى حبيبي و نصفي الثاني ، سندي و عوني أخي "شريف" حفظه الله تعالى و وفقه.

إلى كل من عرفتهم خلال المشوار الدراسي من زملاء و أساتذة.

إلى كل من دعمني و ساندني خلال الخمس سنوات الماضية.

قائمة المختصرات

1- باللغة العربية:

الرمز	المعنى
ط	الطبعة
ج	جزء
ص	صفحة
ع	العدد
ق ع	قانون العقوبات
ق إ ج	قانون الإجراءات الجزائية

المقدمة

مقدمة:

شهد العالم تطورا هائلا لم يسبق له مثيل، فإذا كان القانون هو وليد فكرة المجتمع يتطور بتطوره فإن ظاهرة الإجرام هي الأخرى تنمو وتتطور لتأخذ أبعادًا خطيرة لم تكن تخطر على البال، فهي لم تعد منحصرة في مفهومها التقليدي بل تعدت إلى أن تصبح تنظيما يولد من نسيج تخطيط وتدبير يجسد في النهاية بناءً تحكمه سلوكات وقواعد من الصعب التحكم فيها.

وهذا التنظيم أو ما يعرف بالجريمة المنظمة لم يعد محصورا في مكان أو إقليم معين، بل أصبح منتشرا وموزعا عبر العالم كله وعليه قد أُلحِقَ بمفهوم الجريمة المنظمة مفهوم آخر أكثر تطورا والذي اصطلح عليه بالجريمة العابرة للحدود أو العابرة للقارات، شهد هذا المصطلح العديد من الجرائم كجرائم المتاجرة بالمخدرات والأسلحة بشتَّى أنواعها، وتبييض الأموال والإرهاب، لتبرز أخيرا الجرائم الحديثة والمسماة بجرائم المعلومات أو الجرائم التي ترتكب بواسطة الانترنت والحاسوب[1].

فالجريمة الالكترونية تعد من أبرز وأخطر التحديات الأمنية التي تواجه كافة مجتمعات العالم في مجال استخدامات تقنية المعلومات والاتصالات على نطاق مؤسسات القطاع العام والخاص والأفراد[2] فهي تستهدف الاعتداء على البيانات والمعلومات والبرامج المعرفة التقنية أو الفنية، وتوجه للنيل من أجهزة الحواسيب وشبكة الاتصالات، وقواعد البيانات والبرمجيات ونظم التشغيل، مما يظهر مدى خطورة هذه الجرائم باعتبارها أنها تمس الحياة الخاصة للأفراد وتهدد الأعمال التجارية بخسائر فادحة كما قد تنال من الأمن القومي والسيادة الوطنية للدول وتشيع فقدان الثقة في التعاملات الالكترونية[3].

[1]– زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة، والنشر، الجزائر، 2010، صفحة 5.

[2]– سعيد بن سالم البادي وآخرون، مجمع البحوث والدراسات، الجريمة الالكترونية في المجتمع الخليجي وكيفية، مواجهتها أكاديمية السلطان قابوس للعلوم الشرطه نزوى، سلطنة عمان، 2016 ص 7.

[3]– خالد ممدوح إبراهيم ،جرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط 01، 2009 ، ص6.

كما أن الثورة المعلوماتية[4]، جاءت مصحوبة بفرص جديدة لارتكاب أشكال وصور مستحدثة في الجرائم الفنية، التي أثرت على حقوق الأشخاص الطبيعية والمعنوية، وحرياتهم نتيجة استغلال الأفراد للتقنيات المعلوماتية في غير الغرض الذي جاءت لأجله و أصبحت محلا للاعتداء وإساءة الاستخدام[5].

وفي الوقت الذي تطورت فيه الجريمة تطور كذلك المجرم، فلم يعد ذلك الرجل الذي يشهر سلاحا في وجه شخص آخر، بل أصبح رجلا ذا علم استخدم علمه ضد المؤسسة التي تعتبر أساس اقتصاد كل دولة ملتمسًا بذلك أمنها واستقرارها، ومن هنا بدأ يظهر نوع أخر من المجرمين نقلوا الجريمة من صورتها التقليدية إلى أخرى إلكترونية يصعب التعامل معها لارتباطها بالتكنولوجيا[6].

وقد تميز المجرم المعلوماتي بخصائص وصفات تختلف عن مرتكب الجرائم التقليدية وهذا مرده تميز شخصية مرتكبي الجرائم المعلوماتية بالتقدم في مجال استخدام الحاسب الآلي، وهذا بعكس المجرم العادي الذي غالبا ما يتميز بالقوة العضلية، ونادرا ما يتميز بعضهم بالذكاء[7].

نظرا لحداثة الجرائم الإلكترونية والتي لم يكن المجتمع البشري يتوقعها، لم يوضع لها المشرع عقابًا معينا، ولم يخصص لها حيز للردع والعقاب، ولكن إزاء هذا التطور التقني والتكنولوجي، كان لابد أن تجرم تلك السلوكيات وقد تم تجريمها فعلا، حيث سارعت الدول إلى سن قوانينها وتحديثها مع أنماط السلوكيات التي تدخل ضمن الجريمة المعلوماتية[8]؛ إذ وضعت أول اتفاقية حول الإجرام المعلوماتي وهي اتفاقية"بودابست" التي تضمنت مختلف أشكالا لإجرام

---

[4]– تعرف المعلوماتية بأنها المعالجة العقلية للمعلومات باستخدام الآلات تعمل ذاتيا، أنظر أحمد خليفه الملط ،الجريمة المعلوماتية، دار الفكر الجامعي، الاسكندريه، ص 81

[5]– بوهرين فتيحة، الجريمة الالكترونية في التشريع الجزائري، مجله الحقوق والعلوم الانسانية ،جامعه قسنطينة 2،الجزائر العدد04 ، المجلد 14 ،نوفمبر 2021 ، ص49.

[6]– بوهرين فتيحة، المرجع السابق، ص 49

[7]– خالد ممدوح ابراهيم ،المرجع السابق، ص 13

[8]–قنديل نور الهدى، جرائم افشاء الأسرار في مجال المعلوماتية ، مذكره لنيل شهادة الماستر في الحقوق، تخصص قانون عام، جامعة الجيلالي ليابس، سيدي بلعباس، الجزائر ،2018– 2019 ،ص 3.

المعلوماتي[9] إضافة إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنه 2010[10]، والتي صادقت عليها الجزائر سنه 2014 [11]، وبالطبع لم يقف المشرع الجزائري متفرجا بل سارع هو أيضا إلى سن قوانين تتلاءم وطبيعة الجرائم المستحدثة، فقد استدرك الفراغ القانوني من خلال القانون رقم 04- 15 [12]، الذي أدخل إلى قانون العقوبات بالقسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات" والذي تضمن تماثل ثمانية مواد.

كما أصدر المشرع الجزائري القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال،إضافة إلى الاتفاقيات الدولية التي أبرمتها الجزائر لمكافحة الجريمة الالكترونية. [13]

أهمية الموضوع

تعتبر الجريمة الإلكترونية من أهم المواضيع في الوقت الحالي، نظرا للاستعمال السيئ للإنترنت من طرف الأشخاص، فقط أصبحت هذه التقنية أي الإنترنت فضاء يمارس فيه المجرمون الإلكتروني وإن أعمالهم الإجرامية، مما يزيد من احتمال توسيع دائرة هذا النوع من الجرائم تطور الاستعمالات التقنية لشبكة الإنترنت لاسيما في المجالات المالية والتجارة الإلكترونية.

كما نجد بأن الجرائم الإلكترونية تعددت وتنوعت، بالإضافة إلى أن السلوك الإجرامي للمجرم الإلكتروني يختلف عن المجرم التقليدي، وهذا ما سنتناوله في هذه الدراسة.

أسباب اختيار الموضوع:

من بين الأسباب الدافعة لاختيار هذا الموضوع:

---

[9]- إتفاقية " بودابست" الاتفاقية الاوروبية المتعلقة بالجرائم المعلوماتية رقم 185 المصادق عليها في 2001/11/23.

[10]- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات ،القاهره ،2010.

[11]- المرسوم الرئاسي رقم 14- 252 المؤرخ في 08 سبتمبر 2014، ج.ر، العدد 57.

[12]- القانون رقم 04-15المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الامر رقم 66- 156 الصادر في 8 جوان 1966، المتضمن قانون العقوبات ،ج ر، العدد 71، ص 8.

[13]- القانون رقم 09 04- المؤرخ في 5 اوت 2009 المتضمن القواعد الخاصه للوقاية من جرائم المتصله بالتكنولوجيا الاعلام والاتصال ومكافحتها ،ج ر، العدد 47.

- اندراج الموضوع ضمن اهتماماتي الخاصة كوني طالبة للتعمق في دراسته.
- كون الجريمة الإلكترونية موضوع الساعة و انتشرت بكثرة في الآونة الأخيرة.
- حب الاطلاع والاستكشاف والبحث ومعرفة كل ما هو جديد على أساس أن هذا الموضوع من ضمن المواضيع المستحدثة.
- البحث و المعرفة الأساليب الحديثة المتبعة لمكافحة هذا النوع من الجرائم.

أهداف الموضوع :

يكمن الهدف من هذه الدراسة في :

- معرفة الجريمة الالكترونية بمفهومها و خصائصها وأركانها.
- التعرف على أطراف وأنواع الجريمة الالكترونية.
- معرفة أصناف المجرمين المعلوماتيين و دوافعهم لارتكاب هذه الجرائم.
- التعرف على الجزاءات المترتبة عن ارتكاب هذه الجرائم.
- تسليط الضوء على جهود المشرع الجزائري في محاولته لمواجهة هذه الظاهرة الإجرامية.

إشكالية موضوع البحث:

وعليه يمكن طرح الإشكال التالي: ماهية الجريمة الإلكترونية؟ وكيف واجهها المشرع الجزائري؟

ويمكننا طرح التساؤلات الفرعية الآتية:

ما هو مفهوم الجريمة الإلكترونية؟

ما هي خصائص وأركان الجريمة الإلكترونية؟

فيم تتمثل أطراف الجريمة الإلكترونية وما هي أنواعها وفقا للتشريع الجزائري؟

ما هي الإجراءات المتبعة لمكافحة هذه الجريمة في التشريع الجزائري؟

اعتمدنا في دراستنا هذه على منهجين هما المنهج الوصفي والتحليلي، حيث أنه اتبعنا المنهج الوصفي في محاولتنا لإعطاء وصف للجريمة الإلكترونية وعلى المنهج التحليلي من أجل بيان أنواع الجرائم الالكترونية وتحليل بعض النصوص القانونية.

ولمعالجة الإشكالية المطروحة والإجابة عليها قسمنا بحثنا إلى فصلين كل فصل إلى مبحثين كالأتي:

الفصل الأول:الإطار ألمفاهيمي للجريمة الالكترونية ويحتوي على مبحثين:

المبحث الأول: مفهوم الجريمة الإلكترونية.

المبحث الثاني: دوافع ارتكاب الجريمة الالكترونية وأنواعها في التشريع الجزائري

الفصل الثاني:الإطار القانوني للجريمة الالكترونية في التشريع الجزائري في المبحث الأول تطرقنا إلى مواجهة الجريمة الالكترونية في القوانين الجزائرية وفي المبحث الثاني إلى آليات التحقيق في الجريمة الالكترونية.

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية

المبحث الأول: مفهوم الجريمة الإلكترونية

المبحث الثاني: دوافع ارتكاب الجريمة الالكترونية وأنواعها في التشريع الجزائري

أدى التطور التكنولوجي الذي شهدته مختلف جوانب الحياة في الآونة الأخيرة إلى استعمال جهاز الحاسوب وشبكة الانترنت في مختلف الميادين؛ ولكن قد يتم استخدام هذه الوسائل بطرق غير مشروعة الأمر الذي ينتج عنه ارتكاب أفعالا إجرامية في هذا المجال وهو ما يطلق عليه بالجريمة الإلكترونية، ونظر لحداثة هذه الجريمة وارتباطها بتكنولوجيا متطورة، فقد اختلف الفقهاء والباحثون في وضع تعريف موحد لها، كما اتسمت بمجموعة من الخصائص وعرفت نوعا جديدا من المجرمين لهم عدة دوافع لارتكاب هذه الجريمة، وعليه سنتولى الدراسة في هذا الفصل بالتعرض إلى مفهوم الجريمة الإلكترونية في المبحث الأول، ثم بيان دوافع ارتكاب الجريمة الإلكترونية وأنواعها في التشريع الجزائري من خلال المبحث الثاني.

المبحث الأول:مفهوم الجريمة الإلكترونية.

الجريمة الإلكترونية جريمة حديثة نسبيا وذلك لارتباطها بتقنية حديثة وهي تكنولوجيا المعلومات، ونظر لهذا اختلفت الاتجاهات في تعريفها، كما أنها تميزت عن الجريمة التقليدية بمجموعة من الخصائص ولتفاصيل أكثر حول هذا الموضوع سنتطرق إلى تعريف الجريمة الإلكترونية وبيان الأركان التي ترتكز عليا في المطلب الأول أما المطلب الثاني فقد تناولنا خصائص وأطراف الجريمة الإلكترونية.

المطلب الأول: تعريف الجريمة الإلكترونية وأركانها.

بداية لابد أن نشير إلى أنه لا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال تقنية المعلمات واستخدامها، فالبعض يطلق عليها جريمة الغش المعلوماتي، والبعض الأحر يطلق عليها جريمة الاحتيال المعلوماتي، وآخرون يفضلون تسميتها بالجريمة المعلوماتية[1]. وتجدر الإشارة إلى أن هناك فارق بين ميدان جرائم الحاسب الآلي وميدان جرائم الانترنت، فبينما تتحقق الأولى بالاعتداء على مجموعة الأدوات المكونة للحاسب وبرامجه والمعلومات المخزنة به، فإن جرائم الانترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب عبر خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى اندماج الميدانيين(الحوسبة والاتصال)[2]. وظهور مصطلح (CYBERCRIMINALITÉ) وفي إطار تعريف الفقه للجريمة الإلكترونية نجد أن الاتجاهات تباينت في هذا السياق بين مضيق لمفهوم الجريمة وبين موسع لمفهومها كما أن لهذه الأخيرة أركان لا تقوم الجريمة إلا بتوافرها، وهذا ما سأحاول عرضه في الفرعين الآتيين.

---

[1]– نهلا عبد القدر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، الطبعة 02، 2010، ص46.

[2]– مفتاح أبوبكر المطرودي، الجريمة الإلكترونية والتغلب على تحدياتها ، ورقة مقدمة إلى المؤتمرات الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 23-2021/09/25، ص13.

الفرع الأول: تعريف الجريمة الإلكترونية.

لقد اختلفت الآراء حول وضع تعريف محدد للجريمة الإلكترونية ويعود هذا الاختلاف إلى اختلاف المصطلح المستخدم في تسميتها، فالبعض من الفقهاء ينظر إلى الجريمة الإلكترونية بمفهوم ضيق، والبعض الأخر ينظر إليها بمفهوم موسع.

أولا: الاتجاه المضيق لتعريف الجريمة الإلكترونية.

ومن التعريفات التي أخذ بها أنصار هذا الاتجاه أن الجريمة الإلكترونية هي:" كل فعل غير مشروع يكون العلم بتكنولوجيا الكومبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى".[1]

كذلك تعرف على أنها: " الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أوهي الفعل الإجرامي الذي يستخدم في اقترافه الحاسوب باعتباره أداة رئيسية ".[2]

وعرفت أيضا بأنها :" الجرائم التي تلعب فيها بيانات الكومبيوتر والبرامج المعلوماتية دورا هاما، أو هي كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية".[3]

كما يعرفها البعض بأنها: " هي التي تقع على جهاز الكومبيوتر أو داخل نظامه فقط.[4]

يرى الأستاذ Massa أن المقصود بالجريمة الإلكترونية " الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".[5]

ويرى الأستاذtredmann أن الجريمة المعلوماتية تشمل أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات".[1]

---

[1]– خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص74.

[2]– نهلا عبد القادر المومني، المرجع السابق، ص48.

[3]– غربي جميلة ، أليات مكافحة الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون، تخصص قانون جنائي وعلوم جنائية، جامعة أكحلي محند أولحاج ، البويرة، 2021/2020، ص06.

[4]– خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص74.

[5]–عابد الفتاح بيومي حجاز، جرائم الكومبيوتر والأنترنت في التشريعات العربية، دار النهضة العربية، القاهرة، ط2009، ص44.

كذلك عرفها الأستاذ Rosenblatt على أنها :" نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الأنظمة أو التي تحول عن طريقه."[2]

كما نلاحظ فإن هذا التعريف يضيف من مفهوم الجريمة المعلوماتية إذ يخرج من نطاقها العديد من الأفعال غير المشروعة التي يستخدم الحاسب أداة لارتكابها."[3]

ثانيا: الاتجاه الموسع لتعريف الجريمة الإلكترونية.

بالنسبة لأنصار هذا الاتجاه فقد حاولوا التوسع في مفهوم الجريمة الإلكترونية على عكس الاتجاه الأول، فعرفها البعض على أنها:" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا، بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[4].

أو هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".[5]

أو هي:" نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات".[6]

وكذلك يعرف الأساتذة vivant و lestanc الجريمة المعلوماتية بأنها:" مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب".[7]

وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي أنه تتحقق المخالفة (الجريمة) في كل حالة يتم فيها " تغيير معطيات أو بيانات أو برامج الحاسوب أو محولها أو كتابتها أو

---

[1]–حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجيستر في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة، 2011–2012، ص14.

[2]–د. عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان، 2021، ص14.

[3]–نهلا عبد القادر المومني، المرجع السابق، ص48.

[4]–سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 2007، ص42.

[5]–سامي علي حامد العياد، المرجع السابق، ص43.

[6]–د.سي حمدي عبد المومن ود.قيرة سعاد، الجريمة الإلكترونية واليات التصدي لها في القانون الجزائري، مجلة البيان للدراسات القانونية، المجلد 07، العدد01، ص59–70، جوان 2022، ص61.

[7]–نهلا عبد القادر المومني، المرجع السابق، ص49

أي تدخل أخر في مجال انجاز البيانات أو معالجتها، وتبعا لذلك تسببت في ضرر اقتصادي، أو فقد حيازة ملكية شخص أخر، أو بقصد الحصول على كيس اقتصادي غير مشروع له أو لشخص أخر"[1]

وبتبني الخبير الأمريكي parker مفهوما واسعا للجريمة المعلوماتية حيث يشير إلى أنها:" كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل".[2]

ويمكن في الخلاصة تبني التعريف الذي أقره المؤتمر العاشر للأمم المتحدة لمنع الجريمة حول جرائم الحاسب الآلي وشبكاته الذي عقد في فيينا في الفترة ما بين 10-17 أفريل 2000، إذ عرف الجريمة المعلوماتية بأنها: " جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب وتشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[3]

يتفق جانبا من الفقه مع هذا التعريف، إذ أنه حاول الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة المعلوماتية سواء التي قد تقع على بواسطة النظام المعلوماتي أو داخل هذا النظام على المعطيات والبرامج والمعلومات، كما شمل التعريف الجرائم التي من الممكن أن تقع في بيئة الكترونية . فهذا التعريف لم يركز على فاعل الجريمة ومقدرته التقنية، ولا على وسيلة ارتكاب الجريمة أو على الغاية والنتيجة التي تسعى لها الجريمة المعلوماتية، بل إنه حاول عدم حصر الجريمة المعلوماتية في نطاق ضيق يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة العقاب.[4]

---

[1]-حمزة بن عقون، المرجع السابق، ص15.

[2]- نهلا عبد القادر المومني، المرجع السابق، ص49.

[3]- زيبحة زيدان، المرجع السابق، 2011، ص43.

[4]- نهلا عبد القادر المومني، المرجع السابق، ص50.

وبالنسبة للمشرع الجزائري نجده للدلالة على الجريمة الإلكترونية اصطلح على تسميتها بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال[1].

وعرفها بموجب أحكام المادة 02 من القانون رقم 09-04[2] على أنها:" جرائم المساس بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظمة معلوماتية أو نظام للاتصالات الالكترونية".

من خلال هذا التعريف نستخلص أن المشرع الجزائري تبنى معيار دور النظام المعلوماتي لتحديد معالم الجريمة، فسمى الجرائم الواقعة على النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما بينها في قانون العقوبات في المادة 394 مكرر إلى 394 مكرر 7[3]، وترك المجال واسع لأي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

كما أن المشرع الجزائري لم يقم بتحديد درجة دور المنظومة المعلوماتية أو نظام الاتصالات الالكترونية في ارتكاب هذه الجرائم ، إذ حسب التعريف فإنه يكفي مجرد أن ترتكب الجريمة أو يسهل ارتكابها المنظومة المعلوماتية أو نظام الاتصالات الالكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم حتى تلك الجرائم التي يكون فيها للتقنية المعلوماتية دور ثانوي.[4]

ومن بين الجرائم الالكترونية التي حدثت في الجزائر، هي قيام الشاب الجزائري حمزة بن دلاج بانتهاك أنظمة الأمن على الانترنت لـ 217 مصرفا وسرقة أكثر من 200 مليون دولار،

---

[1]- بوشعرة أمينة وموساوي سهام، الاطار القانوني للجريمة الالكترونية، دراسة مقارنة، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الخاص والعلوم الجنائية، جامعة عبد الرحمان ميرة، بجاية، 2017-2018، ص12.

[2]- القانون رقم 09-04 المؤرخ في 05-08-2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها ج.ر. العدد47.

[3]- القانون رقم 05-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-156، الصادر في 08 جوان 1966، المتضمن قانون العقوبات، ج.ر، العدد 71.

[4]- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الاجرام، جامعة أبو بكر بلقايد تلمسان، 2010-2011، ص16.

وفي سنة 2013 تم القبض عليه من طرف الشرطة التايلاندية وتم تسليمه للولايات المتحدة الأمريكية.[1]

الفرع الثاني: أركان الجريمة الإلكترونية.

للجريمة الإلكترونية ثلاثة أركان تتمثل في الركن الشرعي والركن المادي وكذا الركن المعنوي، هذا ما سنعرضه في العناصر الآتية:

أولا: الركن الشرعي:

إن الجريمة هي نتيجة أفعال مادية صادرة عن إنسان هذه الأفعال تختلف حسب نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو للمجرم والعقوبة المقررة لارتكابه.[2]

فالنص القانوني إذا هو مصدر التجريم وهو المعيار الفاصل بين ما هو مباح وما هو منهى عنه تحت طائلة الجزاء، وتبعا لذلك فلا جريمة ولا عقوبة بدون نص شرعي، وهذا ما يعرف بمبدأ الشرعية .[3]

وقد خص المشرع الجزائري قسما خاصا للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ضمن قانون العقوبات وهو القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان" المساس بأنظمة المعالجة الآلية للمعطيات"[4]، ويشتمل على ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 07 تضمنت كل أنواع الاعتداءات على الأنظمة المعلوماتية، ولم يكتف المشرع الجزائري لذلك فرض حماية جنائية على الحياة

---

[1]– نسرين محفوف، تاريخ النشر 2022/01/19، https://www.ennaharoline.com تاريخ الدخول 20-02-2023، بتوقيت 19:38.

[2]– أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومه الجزائر، ط10، 2011، ص27.

[3]– أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومه الجزائر، ط18، 2019، ص65.

[4]– غربي جميلة، المرجع السابق، ص14.

الخاصة للأفراد من خلال القانون رقم 06-23[1] والذي مس المادة 303 وإقراره بالمادة 303 مكرر 3 وهذا تصديا للاستخدام السيئ لوسائل التكنولوجيا الحديثة.[2]

ثانيا: الركن المادي:

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقق نتيجتها، مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل[3].

وباستقراء النصوص القانونية المنظمة لهذه الجريمة في قانون العقوبات الجزائري وبعض القوانين المقارنة نلاحظ أن المشرع الجزائري لم يشترط ضرورة أن تترتب نتيجة معينة بل اكتفى بتوفر السلوك المادي لقيام الجريمة المعلوماتية بغض النظر عن الضرر الذي تسبب فيه هذا السلوك للضحية، والدليل على ذلك أن القانون يعاقب على مجرد الدخول للمنظمة المعلوماتية دون أن يشترط حصول ضرر عن هذا الدخول، بل جعل تحقق النتيجة في الدخول والبقاء عن طريق الغش في المنظومة المعلوماتية كطرف مشدد وليس شرط للعقوبة.[4]

والسلوك الإجرامي قد يكون:

- إيجابيا بمباشرة الفعل من الجاني، وهو أغلب صور الجرائم الالكترونية- كأن يقوم باختراق شبكة الاتصال ويحصل على بيانات سرية ويقوم بنشرها.

---

[1]- القانون رقم 06-23 المؤرخ في 24 ديسمبر 2006، يعدل ويتمم الأمر رقم 66-156 الصادر في 08 جوان 1966، المتضمن قانون العقوبات ، ج.ر. العدد84.

[2]- إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الالكترونية، مجلة أفاق للبحوث والدراسات المركز الجامعي، اليزي، الجزائر، العدد04، جوان 2019.

[3]-بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 11، سبتمبر 2018، ص354.

[4]- د.عميمر عبد القادر، المرجع السابق، ص89.

- وقد يكون السلوك الإجرامي سلبيا، وهو الامتناع عن فعل كان من الواجب إتيانه: مثل : امتناع موظف أمن عن حماية بيانات ومعلومات الشركة التي يعمل بها، وهو نادر الحدوث، وفي الغالب يرتكب من قبل موظفين مختصين.[1]

ويتخذ الركن المادي عدة صور حسب كل جريمة، ففي جريمة حيازة البيانات أو المعطيات يتحقق الركن المادي بمجرد قيام الجاني بحفظ البيانات وجعلها بحوزته، وفي حال إفشائها يتحقق الركن المادي لجريمة الإفشاء.[2]

وفي جريمة الغش المعلوماتي الركن المادي فيها هو تغيير الحقيقة في التسجيلات الالكترونية والمحررات الالكترونية.[3]

ثالثا: الركن المعنوي.

الركن المعنوي هو النصف الأخر للجريمة، ويمكن التعبير عنه بأنه الحالة النفسية للجاني وقت ارتكابجريمة، حيث لا تقوم الجريمة قانونا بدونه، فلابد من توفر الإرادة الآثمة لدى الجاني عند إقدامه على السلوك الإجرامي كما يجب أن تكون الأفعال إرادية وإلا انتفى الركن المعنوي للجريمة، وأن تكون هذه الأفعال المتجهة نحو مخالفة القواعد القانونية، ليترتب على مخالفتها الجزاء الجنائي المناسب.[4]

يتكون القصد الجنائي من عنصرين هما العلم والإرادة والذي يعد شرطا ضروريا لقيام المسؤولية الجزائية.

العلم: هو إدراك الفاعل للأمور.

الإرادة: هي اتجاه السلوك الإجرامي لتحقيق النتيجة.

---

[1]– د.حمود بن محسن الدعجاني، الجريمة الإلكترونية (دراسة فقهية تطبيقية)، مجلة الجامعة الإسلامية، ملحق العدد، 183، ج16، ص558.

[2]– زيبحة بن زيدان، المرجع السابق، ص73.

[3]– د.بوضياف اسمهان، المرجع السابق، ص354.

[4]– بوشعرة أمينة وموساوي سهام، المرجع السابق، ص39.

ويتخذ القصد الجنائي صورا متعددة فقد يكون القصد عاما أو خاصا ومباشرا أو غير مباشرا، فالقصد العام متوفر في جميع الجرائم العمدية وهو انصراف إرادة الجاني لتحقيق الفعل المجرم مع العلم بعناصر هذا الفعل المنهي عنه قانونا كالاعتداء على الحق في الحياة في جريمة القتل العمدي مثلا.

أما القصد الخاص فهو الغاية التي يسعى إليه الجاني لتحقيقها من خلال ارتكاب الجريمة وهذا النوع من القصد يتطلبه القانون في بعض أنواع الجرائم إلى جانب القصد العام.[1] مثلا في جريمة القتل لا يكتفي الجاني بالفعل فقط بل يتأكد من إزهاق روح المجني عليه.

أما فيما يتعلق بالجريمة المعلوماتية فإنها تعد من الجرائم العمدية أي يكفي لقيامها توفر القصد الجنائي العام المتمثل في علم الجنائي بعناصر الجريمة واتجاه إرادته إلى إلحاق الضرر بالنفس أو المال أو البيانات المخزنة في الحاسوب[2]، ولكن هذا لا يمنع من القول أن هناك بعض الجرائم الالكترونية تتطلب توفر القصد الجنائي الخاص مثلا جرائم تشويه السمعة عبر الإنترنت.

ويرى الباحث أن القصد العام والخاص في جرائم المعلوماتية هو أساسي لتحديد المسؤولية الجزائية ، والذي يحدد وجود قصد خاص في بعض الجرائم المعلوماتية هو طبيعة الجريمة ونية الإضرار أو النية الخاصة للجاني والتي يمكن استشفائها من مكونات كل جريمة على حدا وبشكل مستقل، وبالتالي فإن الجرائم المعلوماتية وكجرائم مستحدثة هي كغيرها من الجرائم التقليدية يشترط وجود الركن المعنوي لقيام الجريمة.[3]

[1]– د.عميمر عبد القادر، المرجع السابق، ص90-91.

[2]– د. عميمر عبد القادر، نفس المرجع، ص91.

[3]– د.بوضياف اسمهان، المرجع السابق، ص355.

المطلب الثاني:خصائص و أطراف الجريمة الإلكترونية.

تتميز الجريمة المعلوماتية بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية، وذلك نتيجة ارتباطها بتقنية المعلومات والحاسب الآلي مع ما يتمتع به من تقنية عالية، وقد أضفت هذه الحقيقة على هذا النوع من الجرائم عدد من السمات والحقائق، والتي انعكست بدورها على مرتكب الجريمة الذي أصبح يعرف بالمجرم المعلوماتي لتميزه أيضا عن المجرم التقليدي[1](الفرع الأول)، كما أن هذه الجريمة وكغيرها من الجرائم لها طرفان أحدهما الجاني وهو المجرم الإلكتروني والآخر المجني عليه(الفرع الثاني).

الفرع الأول: خصائص الجريمة الإلكترونية.

عمل الارتباط الحقيقي للجريمة الإلكترونية بالحاسوب الإلكتروني و شبكة الإنترنت إلى إضفاء قدر من الخصائص و السمات المميزة لهذه الجريمة الإلكترونية عن غيرها من الجرائم التقليدية بسبب علاقتها الوظيفية بالحاسوب الإلكتروني والإرتباطها بالتقنية العالية فقد انعكست هذه التقنية على المجرم الإلكتروني[2]، وهذا ما سنحاول عرضه في العناصر التالية:

أولا: السمات الخاصة بالجريمة الإلكترونية.

تميزت الجريمة الإلكترونية عن الجريمة التقليدية بمجموعة من الخصائص، ومن أبرزها ما يلي:

1- الحاسب الآلي هو أداة ارتكاب الجريمة الإلكترونية.

تبرز خصوصية الجريمة المعلوماتية بصورة أكثر وضوحا في أسلوب ارتكابها وطريقتها، فإذا كانت الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي يكون في صورة ممارسة العنف و الإيذاء كما هو الحال في جريمة القتل أو الاختطاف أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة... فإن الجرائم المعلوماتية هي جرائم هادئة

[1]- سوير سفيان، المرجع السابق،ص17.

[2] نعمان عبد الكريم، الجرائم الإلكترونية وموقف المشرع الجزائري منها، رسالة لنيل شهادة الماجستر في القانون الجنائي، جامعة الجزائر1، يوسف بن خدة، 2017/2016، ص92.

بطبيعتها(soft crime) لا تحتاج إلى العنف، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة[1].

يمكن أن تقع بعض الجرائم بواسطة الحاسب مثل الجرائم التي تقع على الذمة المالية من سرقة ونصب وخيانة الأمانة والتزوير في عملات السحب على الجوائز وانتهاك حرمة الحياة الخاصة. بل وتستخدم في القتل وذلك عن طريق" برمجة جهاز تفجير"، يتم التحكم فيه آليا أو جهاز لإطلاق الأشعة القاتلة[2].

2- الجريمة الإلكترونية جريمة عابرة للحدود:

تتميز الجريمة الإلكترونية عن غيرها من الجرائم الأخرى بالقدرة على تنفيذها عن بعد، بمعنى التباعد الجغرافي بين الجاني و المجني عليه أو محل الجريمة.

كما أنها تعتبر شكلا جديدا من أشكال الجرائم العابرة للحدود الإقليمية بين دول العالم كافة، إذ يمكن من خلال النظام المعلوماتي ارتكاب العديد من الجرائم مقل: جرائم التعدي على قواعد البيانات، الاحتيال المعلوماتي و القرصنة... وغيرها من الجرائم .

فالجريمة المعلوماتية، هي نوع الجرائم التي يتم ارتكابها عن بعد on ligne عبر المسافات، حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كومبيوتر الفاعل وبين النتيجة أي المعطيات محل الاعتداء، وبالتالي لا تقف الجريمة المعلوماتية عند الحدود الإقليمية لدولة معينة بل تمتد إلى الحدود الإقليمية لدولة أخرى مما يزيد من صعوبة اكتشافها[3].

ولقد أثارت هذه الخاصية الدولية للجريمة عدة إشكالات قانونية تتعلق أساسا بتحديد الدولة صاحبة الاختصاص القضائي في محاكمة مرتكب هذه الجريمة، فهل هي الدولة التي وقع فيها

---

[1]- نهلا عبد القادر المومني، المرجع السابق، ص57-58.

[2]-عفيفي كامل عفيفي، فتوح الشادلي، جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة والقانون،الإسكندرية، 2000.، ص23.

[3]-خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص77-78.

النشاط الإجرامي أم التي أضيرت مصالحها نتيجة هذا التلاعب، بالإضافة إلى إشكالية مدى فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وغيرها من المشاكل التي يمكن أن تثيرها الجرائم العابرة للوطنية بشكل عام[1].

3- صعوبة اكتشاف و إثبات الجريمة الإلكترونية.

لا تحتاج جرائم المعلوماتية إلى أي عنف، أو سفك للدماء،أو آثار اقتحام لسرقة الأموال، وإنما هي أرقام وبيانات تغيير أو تمحى تماما من السجلات المخزونة في ذاكرة الحاسبات الآلية، ولأن هذه الجرائم في أغلب الأحيان لا تترك أي أثر خارجي مرئي لها، فإنها تكون صعبة في الإثبات[2].

كما أنها تتميز بصعوبة اكتشافها وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة ويعود السبب في ذلك إلى عدم ترك أي أثر خارجي بصور مرئية وبالإضافة إلى قدرة الجاني على تدمير دليل الإدانة في أقل من الثانية الواحدة، ومما يزيد من صعوبة إثبات هذه الجرائم أيضا ارتكابها عادة في الخفاء، وعدم وجود أي أثر كتابي لما يجري خلال تنفيذها من عمليات أو أفعال إجرامية[3].

وترجع صعوبة إثبات الجريمة الإلكترونية إلى عدة أسباب منها:

- عدم ترك هذه الجريمة آثار مادية بعد إرتكابها (فلا يوجد جثث لقتلى و لا آثار دماء).
- سرعة محو الليل وصعوبة الوصول إليه، فلا يسهل محو الدليل من شاشة الكمبيوتر في زمن قياسي باستعمال البرامج المخصصة لذلك، إذ يتم عادة في لمح البصر وبمجرد لمسة خاطفة على لوحة النفاتيح بجهاز الحاسوب:

---

[1]- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستر في العلوم القانونية ، تخصص علوم جنائية، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2013/2012، ص32.

[2]-محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والانترنت، المكتب العربي الحديث، الإسكندرية، 2007،ص97.

[3]- مولاي أبراهيم عبد الحكيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجلفة(الجزائر)، العدد 23 ، المجلد الثاني، جوان 2015،ص 213-214.

- نقص الخبرة التقنية و الفنية لدى الشرطة وجهات الادعاء و القضاء، حيث تتطلب جرائم الكمبيوتر و الانترنت إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات، وهذا من أجل التحقيق فيها وملاحقة مرتكبيها قضائيا.[1]

4- سهولة ارتكاب الجريمة الإلكترونية:

لا تحتاج الجريمة المعلوماتية إلى جهد عضلي في ارتكابها بل تعتد على القدرات الذهنية للجاني، وتحكمه الجيد في الحاسوب ووسائل الاتصال الحديثة، ولا يحتاج الجاني في ارتكابها إلى التنقل والاستعانة بمركبة لنقل المسروقات، كما أنه لا يحتاج في غالب الأحيان لمساعدة شخص آخر لارتكاب جريمته من أجل الترصد و الحماية بل يمكن للجاني أن يرتكب جريمته وهو يرتشف فنجان قهوة خلف مكتبه وفي قاعة مكيفة، ودون أن يشعر به أحد حتى ولو كان في مكان مزدحم بالأشخاص، كما أنه لا يوجد هناك احتمال لتعرض الجاني لخطر المواجهة و المقاومة من طرف المجني عليه أو من طرف قوات الأمن كما هو الشأن في بعض الجرائم التقليدية[2].

تقع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث عن قيام أو عدم قيام أركان الجريمة الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات، ذلك أنه في حالة تخلف هذا الشرط تنتفي الجريمة الإلكترونية.[3]

حيث يستلزم لقيام هذه الجريمة التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي بغرض معالجتها إلكترونيا، بما يمكن للمستخدم من إمكانية كتابتها من خلال العمليات المتبعة، و التي يتوافر فيها إمكانية تصحيحها أو تعديلها أو محوها أو تخزينها أو استرجاعها وطباعتها،

[1] – خالد ممدوح إبراهيم، الجرائم المعلوماتية، مرجع سابق، ص 77.

[2] – عميمر عبد القادر، المرجع السابق،ص28

[3] – شيخ سناء، شيخ محمد زكرياء، بحث حول مكافحة الجرائم الإلكترونية في القانون الجزائري، مجلة وميض الفكر للبحث، العدد5، سبتمبر 2020، ص3.

وهذه العمليات وثيقة الصلة بارتكاب الجرائم، ولابد من فهم الجاني لهل أثناء إرتكابها في حالات التزوير و التقليد.[1]

5- قلة الإبلاغ عن الجرائم الإلكترونية في الجرائم الإلكترونية غالبا ما يحجم المجني عليه عن طلب مساعدة السلطات المتخصصة في إثبات الجريمة و الكشف عنها، حتى في حالة الإبلاغ، فإن المجني عليه يتعاون مع جهات التحقيق خوفا مما يترتب عليه عادة بنكا أو مؤسسة مالية (شخص معنوي) يهمه المحافظة على سمعته وثقة عملائه، أكثر من اهتمامه بالكشف عن الجريمة و مرتكبيها، لذلك يفضل المجني عليه تقديم ترضية سريعة لعمليه وينهي الأمر داخليا.

كما أن المجني عليه قد يشارك بطريقة غير مباشرة في ارتكاب السلوك الإجرامي، ذلك في الحالات التي يكون فيها المجني عليه مثلا إمرأة، تم التحرش بها و ابتزازها عبر مواقع التواصل الاجتماعي (facebook)، فتضطر الضحية للرضوخ لطلبات الجاني خشية من تشويه سمعتها.[2]

ثانيا: السمات الخاصة بالمجرم الإلكتروني.

لم يكن لارتباط الجريمة الإلكترونية بالحاسب الآلي أثر على تميز هذه الأخيرة عن غيرها من الجرائم التقليدية فحسب، بل كان له أثر أيضا على تمييز المجرم الإلكتروني عن غيره من الجرمين التقليديين. ومن بين خصائص المجرم الإلكتروني نذكر:

1.مهارة المعرفة والذكاء:

الإجرام التقليدي يتم بالعنف وهو الوسيلة الوحيد لاقتراف جريمته بعكس الإجرام المعلوماتي فهو إجرام الأذكياء[3].

[1] – أحمد خليفة الملط، المرجع السابق، ص105.

[2] – بوشعرة أمينة وموساوي سهام، المرجع السابق، ص19.

[3]– سامي على حامد العياد، المرجع السابق،ص49.

يتمتع مجرمو المعلوماتية بقدر لا يستهان به من المهارة و المعرفة بتقنيات الحاسوب والانترنت، بل أن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا، فتنفيذ الجريمة المعلوماتية يتطلب قدرا من المهارة لدى الفاعل التي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات[1].

يتميز المجرم المعلوماتي غالبا بالذكاء، حيث أن الجريمة المعلوماتية تتطلب مقدرة عقلية وذهنية عميقة، خاصة في الجرائم المالية التي تؤدي إلى خسارة مادية كبيرة تلحق بالمجني عليه، فالمجرم المعلوماتي يستخدم مقدرته العقلية و لا يلجأ إلى استخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء[2].

فالمجرم المعلوماتي يكفي أن يقوم بالتلاعب في بيانات وبرامج الحاسب الآلي لكي يمحو هذه البيانات أو يعطل استخدام البرامج، وليس عليه سوى أن يلجأ إلى زرع الفيروسات في هذه البرامج أو باستخدام القنابل المنطقية أو الزمنية أو برامج الدورة لكي شل حركة النظام المعلوماتي ويجعله غير قادر على القيام بوظائفه الطبيعية[3].

و المجرم المعلوماتي يبقى شغفه السعي إلى معرفة طرق جديدة و مبتكرة لا يعرفها أحد سواه وذلك من أجل اختراق الحواجز الأمنية في البيئة الإلكترونية ومن ثم نيل مبتغاه[4].

وتبين إحصائيات العديدة من القضايا أن عددا من المجرمين لا يرتكبون سوى جرائم المعلوماتية، أي أنهم محترفون في هذا النوع من الإجرام دون أن تكون لهم صلة بأي نوع من الجرائم التقليدية.[5]

---

[1]– نهلا عبد القادر المومني، المرجع السابق،ص77

[2]– حمزة بن عقون، المرجع السابق،ص30.

[3]– محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004،ص62.

[4]– نهلا عبد القادر المومني، المرجع السابق،ص78.

[5] – حسين ربيعي، آليات البحث و التحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم في الحقوق، تخصص قانون العقوبات و العلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة (الجزائر)، 2015–2016، ص36.

2.المجرم الإلكتروني إنسان اجتماعي:

يختلف مرتكب جرائم الكمبيوتر عن المجرم التقليدي من حيث أن المجرم الإلكتروني من شأنه أن يحيا وسط المجتمع ويمارس عمله في المجال المعلوماتي أو في غيره من المجالات الأخرى،أي أنه إنسان اجتماعي وتطبيقا لذلك فالعديد من الجرائم المعلوماتية ترتكب بدافع الكبرياء(مستخدم طرد من عمله مثلا فيلجأ إلى ارتكاب الجريمة) أو بدافع النصب و الاحتيال أو بدافع اللهو أو لإظهار مدى ما يتمتع به الفاعل من قدره على التفوق في مواجهة أمن أنظمة المعلومات[1].

فهو لا يضع نفسه في حالة عداء سافر أمام المجتمع الذي يحيط به، بل إنه إنسان متوافق معه ذلك أنه أساسا مرتفع الذكاء مما يساعده على عملية التكيف مع المجتمع، فالذكاء في نظر الكثيرين ليس سوى القدرة على التكيف[2].

3.المجرم الإلكتروني يبرر ارتكاب جريمته:

يتولد مرتكب فعل الإجرام الإلكتروني إحساس و شعور بأن ما يقوم به لا يعتبر من عداد الجرائم، أو بمفهم آخر أنه لا يمكن لهذا العمل و الفعل أن يصنف بعدم الأخلاقية و خاصة في الحالات التي يقف فيها السلوك عند حد قهر نظام الحاسوب وتحطي الحماية المفروضة حوله، حيث يميز مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذي يعدونه غاية في للأخلاقية وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم[3].

ويبدو أن هؤلاء الأشخاص لا يدركون أن سلوكهم يستحق العقاب، فالاستخدام المتزايد للأنظمة المعلوماتية قد أوجد مناخا نفسيا موائما لتصور استبعاد فكرة الخير و الشر وقد ساهم في ذلك عدم وجود احتكاك مباشر بالأشخاص، ومما لا شك فيه أن هذا التباعد في العلاقة

---

[1]– سعدي سليمة، حجاز بلال، جرائم المعلومات و الشبكات في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، ط1، 2017،ص34.

[2]– عبد الفتاح بيومي حجاز، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الكتب القانونية، مصر، 2007،ص86.

[3]– حمزة بن عقون،المرجع السابق،ص32

الثنائية بين الفاعل و المجني عليه يسهل المرور إلى الفعل غير المشروع، ويساعد على أيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل[1].

ففي كثر من الأحيان بقوم العاملون بالمؤسسات المختلفة باستخدام أجهزة الحاسوب لأغراض شخصية توصف بأنها سلوك

شائع بين الجميع ولا ينظر إليه بوصفه فعلا إجراميا[2].

4. التنظيم والتخطيط :

ترتكب اغلب الجرائم من مجموعة مكونة من عدة أشخاص يحدد لكل شخص دور معين ويتم العمل بينهم وفقاً لتخطيط وتنظيم سابق على ارتكاب الجريمة ،فمثلا تحتاج جريمة مثل نسخ برامج الحاسب الآلي إلى شخص يقوم بنسخ تلك البرامج وقد يكونون مجموعة أشخاص وتحتاج أيضا إلى مجموعة تقوم بعملية البيع[3].

5. تمتع المجرم الالكتروني بالسلطة اتجاه النظام المعلوماتي:

يقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلومات والتي تمكنه من ارتكاب جريمته،وهذه السلطة إما تكون مباشرة كالشفرة الخاصة بالدخول إلى النظام المعلوماتي والتي تعطي للفاعل مزايا متعددة مثل فتح الملفات ومحو أو تعديل محتوياتها أو مجرد قراءتها أو كتابتها .

وقد تتمثل هذه السلطة في حق استعمال الحاسب الآلي نفسه أو الدخول إلى مكان تواجده كما هو الحال في الشبكات الداخلية لبعض الإدارات مثلا .

وقد تكون هذه السلطة غير مباشرة كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر[4].

---

[1]– نهلا عبد القادر المومني،المرجع السابق،ص78.

[2]– يرمش مراد،خصوصية الجريمة الالكترونية أطروحة لنيل شهادة الدكتوراه، علوم في القانون الخاص،فرع الملكية الفكرية،جامعة الجزائر –1–بن يوسف بن خدة، كلية الحقوق والعلوم السياسية، الجزائر، 2021/2020 ص 50.

[3] خالد ممدوح إبراهيم، الجرائم المعلوماتية ، المرجع السابق، ص 136.

[4] سوير سفيان، المرجع السابق، ص 24.

6. خوف المجرم الالكتروني من كشف جريمته:

يعرف عن مجرمو المعلوماتية خوفهم من انكشاف جرائمهم وانفضاح أمرهم، وبالرغم من أن هذه الخشية تصاحب المجرمين على اختلاف أنماطهم إلا أنها تميز مجرمي المعلوماتية بصفة خاصة لما يترتب عن كشف أمرهم من فقدان لمراكزهم في الكثير من الأحيان، ويساعد مجرمي المعلوماتية على الحفاظ على سرية أفعالهم طبيعة الأنظمة المعلوماتية نفسها، وذلك أن أكثر ما يعرض المجرم إلى اكتشاف أمره هو أن يستجد أو يطرأ أثناء تنفيذه لجريمته مجموعة من العوامل غير المتوقعة والتي لا يمكن التكهن والتنبؤ بها،في حين أن أهم الأسباب التي تساعد على نجاح الجريمة المعلوماتية هي أن الحواسيب إنما تؤدي عملها غالبا بطريقة آلية، بحيث لا تتغير المراحل المختلفة التي تمر بها[1].

الفرع الثاني: أطراف الجريمة الإلكترونية

إن الجريمة الإلكترونية كغيرها من الجرائم تحتاج إلى طرفين جاني ومجني عليه،غير أن أطراف هذه الأخيرة يختلفون نوعا ما عن أطراف باقي الجرائم، هذا ما سنوضحه في العناصر الاتية :

أولا: الجاني (المجرم المعلوماتي)

بما أن المجرم المعلوماتي يرتكب جرائمه وهو يمارس وظيفته في مجال الأجهزة الآلية فلابد أن يكون إنسانا اجتماعيا وسط المجتمع يقوم بواجباته ويمارس حقوقه دون وجود أي عائق من جهة، وإنسانا محترفا يتمتع بذكاء كبير من جهة أخرى[2]. ولهذا يوصف الإجرام المعلوماتي بإجرام الأذكياء[3].

[1]– حمزة بن عقون،المرجع السابق، ص 31

[2]– بوهرين فتيحة، الجريمة المعلوماتية في التشريع الجزائري، مجلة الحقوق والعلوم الإنسانية، جامعة قسنطينة 2 (الجزائر)،العدد 04، المجلد 14، نوفمبر 2021، ص 52.

[3]– عميمر عبد القادر،المرجع السابق، ص43.

وهناك عدة طوائف من المجرمين المعلوماتين: طائفة القراصنة طائفة صغار السن، طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية، طائفة مجرمو المعلوماتية أصحاب الآراء المتطرفة، طائفة مجرمو المعلوماتية في إطار الجريمة المنظمة، وطائفة الحكومات الأجنبية.

1- طائفة القراصنة :

قراصنة المعلومات هم في الغالب مبرمجون من أصحاب الخبرة، يهدفون إلى الدخول إلى أنظمة المعلوماتية غير المسموح لهم بدخولها وكسر الحواجز الأمنية المحيطة بهذه الأنظمة، ويمكن تصنيفها إلى صنفين هما[1] :

أ- القراصنة الهواة :(hackers)

الهاكرز هو الشخص الذي يستطيع أن يصمم ويحلل البرامج أو أنظمة التشغيل[2].

أو المتسلل هو شخص بارع في استخدام الحاسب الآلي وبرامجه ولديه فضول في استكشاف حسابات الآخرين وبطرق غير مشروعة .

فالهاكرز وكما يدل على ذلك اسمهم، متطفلون يتحدون إجراءات امن نظم الشبكات، لكن لا تتوفر لديهم في الغالب دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي واثبات الذات .وتتألف هذه الطائفة أساسا من مراهقين وشباب (طلبة وتلاميذ ثانويات) وشباب عاطل عن العمل.[3]

ب- القراصنة المحترفون:(crackers)

الكراكز أو المقتحم هو شخص يقوم بالتسلل إلى نظم الحواسيب للاطلاع على المعلومات المخزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها .[4]

---

[1]- حمزة بن عقون، المرجع السابق، ص 38

[2]- عبد الصبور عبد القوي علي مصري،الجريمة الالكترونية، دار العلوم للنشر والتوزيع، القاهرة، ط 1، 2008، ص 55.

[3]- نسرين عبد الحميد نبيه،الجريمة المعلوماتية والمجرم المعلوماتي،منشأة المعارف الإسكندرية 2008 ص 40، 41.

[4]-نسرين عبد الحميد نبيه،المرجع السابق، ص 41.

هذه الفئة تعكس اعتداءاتهم ميولات إجرامية خطيرة تنبئ عن رغبتها في أحداث التخريب ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات وهم أكثر خطورة من الصنف الأول فقد يحدثون أضرارا كبيرة[1].

وتوضح الدراسات التي أجراهاأحد المعاهد المتخصصة في محترفي الجرائم المعلوماتية من الجيل الحديث هم في الغالب من الشباب الذي تتراوح أعمارهم من 25 إلى 45 سنة، وتبين الإحصائيات في هذا المجال ما يلي :

- 25% من أفعال الغش المعلومات يرتكبها المحلل .
- 18% من هذه الأفعال يرتكبها المبرمج .
- 17٪ يرتكبها المستخدم الذي لديه أفكار خاصة بنظم المعلومات .
- 12% يرتكبها الشخص الأجنبي عن المكان الذي تتواجد فيه نظم المعلومات .
- 11% من هذه الأفعال ترتكب في التشغيل[2].

2-طائفة صغار السن:

يسميهم البعض بصغار نوابع المعلوماتية، ويطلق هذا اللفظ على المجموعات التي تميل للتحدي الفكري وهو غالبا ما يكونون في مرحلة المراهقة وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة البنكية والشركات والمؤسسات المالية[3].

تضم هذه الطائفة الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح دون أن تكون لديهم نية أحداث أي ضرر بالمجني عليهم،وذلك عن طريق استخدام حاسبات آلية محمولة خاصة بهم أو حاسبات آلية خاصة بمدارسهم ويكون هؤلاء الشباب مفتونين كثيرا بالتقنيات الرقمية[4].

---

[1]- نهلا عبد القادر المومي،المرجع السابق ص 84.

[2]-حمزة بن عقون،المرجع السابق، ص 41.

[3]- خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص 142 .

[4]- سعيداني نعيم،المرجع السابق، ص 53.

تثير هذه الطائفة جدلا واسعا فالبعض يرى أنه "لا يبدو من المناسب أن نصنف هؤلاء الشباب في طائفة من الطوائف الإجرامية"، في الوقت الذي يعتبرها البعض الأخر ممن يقدم خدمة لأمن المعلومات ووسائل الحماية ويصنفهم بالأخيار، وهناك من يصنف هذه الفئة ضمن مجرمي المعلوماتية كغيرهم من المجرمين، وفي الحقيقة يجب عدم التقليل بخطورة هؤلاء الشباب فقد تتعدى مرحلة الميل للمغامرة والتحدي[1].

1- طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية:

بحكم طبيعة عمل هؤلاء الموظفين ونظرا لان النظام المعلوماتي هو مجال عملهم الأساسي،ونظرا للمهارات والمعرفة التقنية التي يتمتعون بها فأنهم يقترفون بعض الجرائم المعلوماتية التي من الممكن أن تحقق أهدافهم الشخصية وأهمها الكسب المادي فالعلاقة الوظيفية التي تربط بين الموظفين والمجني عليهم تجعل عملية ارتكابه للجريمة المعلوماتية أسهل نظرا للثقة التي يتمتع بها .وهناك فئة من الموظفين الحاقدين على عملهم أو على مؤسساتهم الذين قد يقومون بأفعال إجرامية لا تهدف إلى الكسب المادي بل هدفها الانتقام والثأر من أصحاب عملهم وهذه الفئة يذهب البعض إلى تسميتها بفئة مجرمي المعلوماتية الحاقدين[2].

4- طائفة مجرمو المعلوماتية أصحاب الآراء المتطرفة:

هم فئة من المجرمون الذين يستخدمون الشبكات المعلوماتية ونشر أفكارهم الدينية والسياسية أو الاقتصادية المتطرفة ويتميزون بكونهم لا يهدفون لتحقيق مكتب شخصي أو الحصول على نفع مادي ما،بل يعملون على تغيير المجتمع ليتماشى ويتوافق مع ما يعتقدون

[1]- غربي جميلة، المرجع السابق، ص 30.

- [2]نهلا عبد القادر المومني، المرجع السابق ص 85.

صحته من الأفكار والمعتقدات وغالبا ما يتم ذلك عن طريق استخدمهم كافة المواقع الالكترونية التي تسعى لتحقيق أغراض دعائية لصالحهم[1].

5- مجرم والمعلوماتية في إطار الجريمة المنظمة.

في عالم الشبكات الالكترونية كما هو الحال في العالم الحقيقي يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة وقد يكون أفضل ما توصف به هذه الأعمال أنها جرائم غير منظمة آلا أن مجموعات الجريمة المنظمة بدأت بشكل متزايد باستغلال الفرص الجديدة التي يوفرها العالم الرقمي.

ومن التعريفات التي قيلت في الجريمة المنظمة أنها : "تعبير عن مجتمع إجرامي يعمل خارج إطار الشعب والحكومة ويضم بين طياته ألاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما كما يخضع أفرادها لأحكام قانونية سنوها لأنفسهم وتفرض أحكاما بالغة القسوة على من يخرج عن ناموس الجماعة ويلتزمون في أداء انشطتهم الإجرامية بخطط دقيقة مدروسة يلتزمون بها ويجنون من ورائها الأموال الطائلة".[2]

كما تقوم هذه المنظمات الإجرامية المنظمة بتبني أصحاب الكفاءات والخبرة والموهوبين في مجال تقنية معلومات وذلك بإغرائهم بالمال لينضموا إلى صفوفها، ويمارس مجرمو المعلوماتية في نطاق هذه المنظمات نشاطات تدر على المنظمة ارباحا هائلة، فيقومون بتزوير البرامج وتقليدها واختراق شبكات المعلومات الخاصة بالدول والمؤسسات المالية الكبرى[3].

6-طائفة الحكومات الأجنبية .

مهمتهم استخباراتية تقتصر على جمع المعلومات لمصلحة الجهات التي يعملون لحسابها سواء كانوا يعملون لمصلحة دولهم أو لمصلحة بعض الأشخاص أو الشركات التي

---

[1] – راضية بركايل، "التنظيم القانوني الجزائري للجريمة المعلوماتية في التشريع الجزائري" الملتقى الوطني حول الامن المعلوماتي مهدداته وسبل الحماية، جامعة مولود معمري، تيزي وزو، الجزائر، 03-04 نوفمبر 2015، ص 224.

[2]– نهلا عبد القادر المومني، المرجع السابق، ص 87.

[3]– حمزة بن عقون،المرجع السابق، ص 44، 45.

تتنافس فيما بينها ومن مقتضيات عملهم ألا يتركوا دليلا عن عملهم ويعرف الجاسوس "بأنه الشخص الذي يقوم بمجموعة من الأعمال المنجزة لصالح بلد أجنبي يهدف إلى إيقاع الضرر بسلامة بلد أخر وتكون غالبا معلومات سرية عن الجيوش أو أجهزة المخابرات وسواها وذلك بطرق ملتوية ومخالفة للقانون مما يعرضه لعقوبات قاسية"[1].

والملاحظ من هذه التعاريف أن التجسس يقتصر على الأسرار العسكرية فقط بينما مفهوم التجسس يتعدى ذلك إذا ما تعلق الأمر بمعلومات إلكترونية سرية[2].

ثانيا: المجني عليه

إن الضحية في الجريمة المعلوماتية بصفة عامة هو كل من إصابة ضرر مادي أو معنوي نتيجة استخدام غير المشروع للوسائل الالكترونية الرقمية الحديثة، والمجني علية هنا في الغالب الأعم هو شخص معنوي كالبنوك والشركات الكبرى والمؤسسات الحكومية والمنظمات والهيئات المالية الضخمة، وغيرها من الأشخاص الاعتبارية التي تعتمد في انجاز أعمالها على الحواسيب. كما يمكن أن يكون المجني عليه شخص عادي كالذين يحفظون أسرارهم وأعمالهم وشؤونهم داخل الحاسوب خاصة الأشخاص الذين يكون لهم منصب سياسي رفيع أو رجل أعمال مرموقة أو صاحب شهرة عالمية في قطاع من القطاعات الاقتصادية أو الاجتماعية أو العسكرية.[3] وعليه يمكن تقسيم المجني عليه في مجال الجريمة الالكترونية إلى ثلاثة فئات وهي:

1- المؤسسات المالية والجهات الحكومية:

تستهدف الجرائم الالكترونية الأشخاص المعنويين سواءا كانت العامة والمتمثلة في مؤسسات الدولة حيث يتم اختراقها لأخذ مشاريعها أو أسرارها أو إتلاف معلوماتها. أو الخاصة

[1]- عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة ابو بكر بلقايد، تلمسان ،الجزائر، 2018، ص 108 .

[2]- عزيزة رابجي، نفس المرجع، ص 108.

[3]- عزيز رابحي، مرجع السابق، ص 103 .

والمتمثلة في المؤسسات المالية كالبنوك والشركات المالية حيث ينجذب إليها مرتكبي هذه الجرائم نظرا لما بها من أموال. ومن أهم هذه المؤسسات المالية هي البورصة لان أي تعطيل في حركة البورصة يؤثر بدرجة كبيرة على حجم التعاملات المالية ليس فقط بين الأشخاص العاديين بل قد يصل الأمر إلى المعاملات المالية بين الدول[1].

2-المؤسسات العسكرية :

لم تقتصر حدود ثورة المعلومات على القطاع المدني بل كان لها الأكبر الأهمية في تطوير أنظمة الحرب الحديثة وأدت إلى ظهور ما يسمى بحرب المعلومات [2]وقد مست الجرائم المعلوماتية القطاعات الخاصة بالقوات المسلحة نظرا لطبيعة وأهمية المعلومات التي تحتويها وهو ما يبرزه الاهتمام المنصب على الجاسوسية العسكرية وما استتبعه من ظهور حرب من نوع جديد من الحرب المعلوماتية[3].

وتعتمد آليات هذه الحرب على الشبكات الحاسبات الآلية في نقل المعلومات عن طريق الشبكات ومن خلال الأقمار الصناعية حيث يؤدي ذلك بدوره إلى تعاظم دور القوات المسلحة ونظم المعلومات في أنظمة التسليح نظرا لحتمية وأهمية تخزين البيانات وسرعة معالجتها وعرضها بصورة مناسبة امام القادة لاتخاذ القرار المناسب على أساس أهمية تلك المعلومات.[4]

3- الأشخاص الطبيعيون:

لا يقتصر تصنيف ضحايا جرائم المعلوماتية على القطاعات المالية والهيئات الحكومية والمؤسسات العسكرية فقط، بل يتعدى كذلك إلى الأشخاص الطبيعيين. فكثيرا ما تعد شبكة الانترنت المجال الخصب لارتكاب تلك الجرائم ضدهم لاسيما ما يتعلق بالمساس بحق الخصوصية والبيانات الشخصية للأفراد، كما تعتبر جرائم الإتلاف المعلوماتية عن طريق الفيروسات من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر بريدهم الالكتروني

[1]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 150.

[2]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، نفس المرجع، ص 151 .

[3]- سعيداني نعيم، المرجع السابق، ص 65.

[4]- خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص 152..

والذي يعتبر من أهم البوابات التي يقفز منها القراصنة إلى أجهزة الحواسيب الخاصة بالأشخاص[1].

المبحث الثاني: دوافع ارتكاب الجريمة الالكترونية وأنواعها في التشريع الجزائري

بعد دراسة مفهوم الجريمة الالكترونية بما فيه من تعريف وخصائص وأطراف،اتضح لنا الفرق بين هذه الأخيرة والجريمة التقليدية خاصة من حيث فئات مرتكبي هذه الجرائم،لهذا من الطبيعي أن نجد هناك اختلاف أخر من حيث الأسباب والعوامل الباعثة لارتكاب هذا الفعل غير المشروع،وهذا ما سنتطرق إليه في المطلب الأول أما المطلب الثاني فسنحاول بيان أنواع الجريمة الالكترونية في التشريع الجزائري.

المطلب الأول: دوافع ارتكاب الجريمة الإلكترونية .

تتباين الدوافع إلى ارتكاب الجرائم المعلوماتية تبعا لطبيعة المجرم وماذا ثقافته وخبرته في مجال الحاسب الآلي لان المتهم يرتكب جريمته بناء على ما لديه من مهارة وخبرة فالمهتم في مجال البرمجة واستخدام شبكات الحاسب الآلي قد يكون هدفه مختلفا عن هدف المهتم الذي لا تتعدى خبرته مجرد تشغيل جهاز الحاسب الآلي[2].

وتنقسم الدوافع إلى ارتكاب هذه الجرائم إلى نوعين دوافع شخصية وأخرى موضوعية فالأولى تتمثل في الرغبة في كسب المال وفهم النظام المعلومات واثبات الذات(الفرع الأول)،والثانية تكون أما للانتقام أو بهدف التعاون والتواطؤ (الفرع الثاني).

الفرع الأول: الدوافع الشخصية

يمكن رد الدوافع الشخصية لدى المجرم الالكتروني إلى دوافع مادية وأخرى ذهنيه.

أولا: الدوافع المادية "تحقيق الربح وكسب المال"

[1]– سعيداني نعيم، المرجع السابق، ص 66.

[2]– خالد ممدوح ابراهيم، الجرائم الإلكترونية، المرجع السابق، ص 138.

يعد هذا الدافع والذي يمثل فيه الحقيقة غاية الفاعل، من بين أكثر الدوافع تحريكا للجناة لاقتراف جرائم الكمبيوتر، ذلك أن خصائص هذه الجرائم، وحجم الربح الكبير الممكن تحقيقه من بعضها خاصة غش الكمبيوتر أو الاحتيال المرتبط بالكمبيوتر يتيح تعزيز هذا الدفع[1].

فيعمد الجاني رغبة منه في تحقيق الثراء والكسب المادي إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية أن كان أحد موظفيها، أو اختراق نظم المعالجة الآلية لها من خلال اكتشافه فيه لفجواتها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه أو لحساب شركائه أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة، كما يمكن الحصول على المكاسب المادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب، وهذا ما تطرقت إليه مجلة (sécurité informatique)وهي مجلة متخصصة في الأمن المعلوماتي أن:

- 43% من حالات الغش المعلن عنها قد تمت من اجل اختلاس أموال.
- 23% من اجل سرقة معلومات.
- 19% أفعال إتلاف .

و 15% الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية[2] .

تجدر الإشارة إلى أنه في حال نجاح المجرم في ارتكاب جريمته المعلوماتية فان ذلك قد يضر عليه أرباحا تكون هائلة في زمن قياسي ويمكن أن نوضح ماذا الأرباح المادية التي يحققها المجرم نتيجة الاقتراف هذا النوع من الجرائم من خلال ما يرويه احد هؤلاء المجرمين المحترفين في سجن كاليفورنيا بقوله :

لقد سرقت أكثر من نصف مليون دولار بفضل أجهزة حاسوب جهاز الضرائب في الولايات المتحدة الأمريكية وبإمكاني أن اكرر ذلك في أي وقت...[3]

[1]– خالد ممدوح ابراهيم، الجرائم المعلوماتية، المرجع السابق، ص 138.

[2]– سعيدي سليمة، حجاز بلال، المرجع السابق، ص 38.

[3]– نهلا عبد القادر المومي، المرجع السابق، ص91 .

ثانيا: الدوافع الذهنية "التعلم وفهم النظام المعلوماتي واثبات الذات والمتعة"

قد تكون الدوافع لارتكاب الجريمة الالكترونية مجرد الشغف بالالكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الالكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه[1].

فالصورة الذهنية لمرتكبي جرائم الحاسوب والانترنت غالبا هي صورة البطل والذكي الذي يستحق الإعجاب لا صورة الجرم الذي يستوجب محاكمته، فمرتكبي هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة انه إزاء ظهور أية تقنية مستحدثة فان مرتكبي هذه الجرائم لديهم شغف الآلة ،فيحاولون إيجاد الوسيلة التي تحطمها أو التفوق عليها[2].

لذلك فان اغلب من يقومون بتلك الأفعال بدوافع إثبات التفوق العلمي هم الصبية والشباب أو المعروفون باسم صغار نوابع المعلوماتية لان يسعون دائما إلى اكتشاف ما هو جديد ومحاولة التعامل مع هذه البرامج واثبات تفوقهم العلمي عن طريق تخطي حاجز الحماية لهذه البرامج وتحطيمه ويتضح بالتالي أن المكتبة المادي ليس دائما دافعهم إلى ارتكاب تلك الجريمة[3].

الفرع الثاني: الدوافع الموضوعية

قد يتأثر المجرم الالكتروني ببعض المواقف التي تدفعه إلى اقتراف الإجرام الالكتروني وبالتالي لا يسعى إلى المتعة ولا التسلية ولا إثبات الذات ولا لكسب المال ويمكن إبراز أهم الدوافع عن الموضوعية أو الخارجية كالآتي :

[1]– سعيداني نعيم، المرجع السابق،ص 61.

[2]– نسرين عبد الحميد نبيه،المرجع السابق، ص 45.

[3] –خالد ممدوح ابراهيم،المرجع السابق، ،ص. 139.

أولا: دوافع الانتقام .

يعد دافع الانتقام من اخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب جريمته،وغالبا ما يصدر الانتقام من طرف أشخاص يملكون معلومات عن خصومهم والتي تكون في الغالب مؤسسات تعامل مرتكب الجريمة معها ووقع خصام بينهما سواء كان عاملا وتم فصله، أو عميلا للمؤسسة تم اخذ حقه وغيرها من الأمثلة المحتملة فيقوم هذا الأخير باستغلال المعلومات التي تحصل عليها بمناسبة تعامله مع هذه المؤسسة ويقوم باستعمال كلمة المرور الخاصة بشبكة المعلومات والولوج إليها والقيام بجريمته عن طريق حذف أو تغيير معلومات أو عن طريق زرع برامج خبيثة بها من اجل تعطيلها كما يمكن القيام بعملية تشهير ضد مؤسسات أو أشخاص من اجل الانتقام من تصرفاتهم.[1]

فدافع الانتقام غالبا ما يكون لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية أو الطرد من الوظيفة فيتولد لدى المجرم الالكتروني الرغبة في الانتقام من رب العمل[2].

ثانيا: دافع التعاون والتواطؤ .

وهو أكثر تكرارا في جرائم المعلوماتية وغالبا ما يكون متضامنا فيها متخصص في الحسابات الآلية يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه؛ كما أن من خصائص من يمارسون التلصص على الحسابات تبادل المعلومات بصفة منظمة حول أنشطتهم. [3]

وإذا كانت هذه ابرز الدوافع لارتكاب أنشطة الاعتداء على نظم المعالجة الالية ومع ذلك فهي ليست ثابتة ومعتمدة لدى الفقهاء والباحثين لان السلوك الاجرامي ودوافع ارتكاب الجريمة

[1] –عميمر عبد القادر ، المرجع السابق ص 51 .

[2] –مسعود شهيرة، الجريمة الالكترونية في التشريع الجزائري،مذكره لنيل شهادة الماستر في القانون، تخصص قانون جنائي،كليه الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، 2020 / 2021 ص 17.

[3] –محمد عبد الله ابو بكر سلامة،المرجع السابق، ص 95.

قد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة إلى تدميرها أو على الأقل حيازتها للقيام بعملية الابتزاز والحصول على الأموال لذلك فان الدوافع في ارتكاب الجرائم المعلوماتية قد لا تتوقف عند هذا الحد، إذا نجد في كل جريمة جديدة دوافع جديدة بل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما اذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق مأربه الخاصة[1] .

ثالثا: دوافع سياسية و تجارية

هي عموما محرك أنشطة الإرهاب الإلكتروني فكثيرة هي المنظمات الإرهاب الإلكتروني فكثيرة هي المنظمات في عصرنا الحالي و التي تتبنى بعض الآراء و الأفكار السياسية أو الدينية أو الإيديولوجية، ومن أجل الدفاع عن هذه الآراء تقوم بأفعال إجرامية ضد معارضيها.[2]

فعلى سبيل المثال هناك العديد من عمليات الاختراق تعود لأسباب عقائدية، حيث تقوم بعض المجموعات التي تتبنى فكرة الإصلاح، بعملية الرقابة الأخلاقية أو اجتماعية أو دينية، فتتجسس على المواقع التي تقدم خدمات أو معلومات تتعارض مع قناعاتها، وتعمل على كشف أسرارها أو حتى تدميرها، فهناك بعض المواقع أخذ على عاتقه مهمة التجسس على مواقع حكومية وكشف الأسرار الدبلوماسية و العسكرية. أما عن الدوافع الحصول على المعلومات التجارية في مختلف الأشكال فهي عموما دوافع تنافسية.[3]

المطلب الثاني:أنواع الجريمة الالكترونية في التشريع الجزائري

نظرا لاختلاف الفقهاء حول تسمية الجريمة الالكترونية،تعددت التقسيمات هذه الجرائم وذلك حسب الأساس والمعيار الذي يستند إليه التقسيم المعني فالبعض يصنفها حسب الأسلوب

[1]– بوكر رشيد،جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، ط1 2012، ص 96.

[2] – نسرين عبد الحميد نبيه، المرجع السابق، ص 45.

[3] – عزيزة رابحي، المرجع السابق، ص102.

المتبع في الجريمة والبعض الأخر يستند إلى دوافع ارتكابها، وآخرون يؤسسون تقسيماتهم على تعدد محل الاعتداء وتعدد الحق المعتدي عليه[1].

أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الالكترونية إلى جرائم مرتكبة بواسطة النظام المعلومات نص عليها المشرع ولم يحددها؛ وبالتالي تشمل كل الجرائم المرتكبة بواسطة وسائل تكنولوجيا الإعلام والاتصال، أما النوع الثاني من الجرائم فيتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات،[2] هذا ما سوف ننجزه في الفرعين الآتيين:

الفرع الأول: الجريمة الالكترونية المرتكبة باستخدام النظام المعلوماتي .

في هذا التصنيف لا يكون النظام المعلوماتي هو محل الجريمة، بل باستخدام النظام المعلوماتي ويكون الهدف من ورائها الربح بطريقة غير مشروع، الاعتداء على أموال الغير، الاعتداء على الأشخاص وسلامتهم أو المساس بحياتهم الخاصة وسمعتهم أو شرفهم، والاعتداء على امن الدولة وأسرارها.[3] وهذا ما سنوضحه في العناصر الموالية:

أولا: الجرائم الواقعة على الأشخاص.

تقع هذه الجرائم على الأشخاص وتنقسم بدورها إلى طائفتين تتمثل الأولى في الجرائم الواقعة على حقوق الملكية الفكرية والأدبية والثانية تكمن في الجرائم الواقعة على حرمة الحياة الخاصة.

1- الجرائم المعلوماتية الواقعة على حقوق الملكية الفكرية والأدبية:

يمكن أن يكون النظام المعلوماتي وسيلة فعالة للاعتداء على حقوق الملكية الفكرية والأدبية ومثال ذلك استخدام النظام المعلوماتي في السطو على بنوك المعلومات التي

---

[1]- رصاع فتيحة، الحمايه الجنائيه للمعلومات على شبكه الانترنت، مذكره لنيل شهاده الماجستير في القانون العام، جامعه ابي بكر بلقايد، تلمسان، 2011 -2012، 69.

[2]-نايري عائشة ،الجريمة الالكترونية في التشريع الجزائري،مذكره لنيل شهادة الماستر في القانون الاداري جامعه احمد دارية، ادرار، 2016- 2017 ص، 24.

[3]- غربي جميلة، المرجع السابق، ص 18 .

تتضمنها برامج نظام معلوماتي آخر، أو حالة تخزين واستخدام هذه المعلومات أو التفريط فيها دون إذن صاحبها ذلك أن استخدام معلومة معينة دون إذن صاحبها، يتضمن اعتداء على حق من الحقوق المعنية إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع إذا تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع وقد نص المشرع الجزائري على حقوق الملكية الفكرية وبراءات الاختراع من خلال عدة نصوص قانونية منها.[1]

الأمر رقم 03-05 [2]المتعلق بحقوق المؤلف والحقوق المجاورة والأمر رقم 03 -07[3] المتعلق ببراءة الاختراع.

2- الجرائم الالكترونية الواقعة على الحياة الخاصة.

المقصود بجرائم الاعتداء على الأشخاص هي تلك الجرائم التي تهدد بالخطر حقوق ذات طابع شخصي أي اللصيقة بشخص المجني عليه ومنها جرائم القذف والسب والذم،وجرائم حث قاصرين على أنشطة جنسية تتم عبر الوسائط الالكترونية، والتهديد والتحرش والمضايقة عبر الوسائل التقنية وأنشطة اختلاس النظر والاطلاع على البيانات الشخصية، وجرائم التنصت والتقاط الرسائل الالكترونية[4].

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي كفلها القانون وفي مقدمته الدستور الجزائري من خلال المادتين:

المادة 39: "تضمن الدولة عدم انتهاك حرمة الإنسان" .

والمادة 47: " لكل شخص الحق في حماية حياته الخاصة وشرفه.

لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت.

---

[1]- سوير سفيان. المرجع السابق، ص 34.

[2]- الأمر رقم 03- 05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف وحقوق المجاورة الجريدة الرسمية العدد 44.

[3]- الأمر رقم 03- 07 المؤرخ في 19 جويلية 2003 يتعلق ببراعة الاختراع ،ج ر، العدد 44.

[4]- م الينا محمد الاسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية(دراسة مقارنة)، دار حامد للنشر والتوزيع ،عمان ط 1، 2015، ص 35 -43.

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي .

يعاقب القانون على كل انتهاك لهذه الحقوق"[1].

ثانيا: الجرائم الواقعة على الأموال.

لم تعد تقتصر الجرائم المعلوماتية على إلحاق الأذى بالأشخاص، بل تعدى ذلك إلى الاعتداء على الأموال أو الذمة المالية للغير.

وجرائم الأموال بشكل عام هي الجرائم التي تنال بالاعتداء أو تهدد بالخطر الحقوق ذات القيمة المالية، ويدخل في نطاقها كل حق ذي قيمة اقتصادية ويدخل في إطار التعامل، وبالتالي يكون احد عناصر الذمة المالية للشخص[2].

من بين الجرائم الالكترونية الواقعة على الأموال نجد السرقة الواقعة على البنوك التي تتم عن طريق اختلاس البيانات والمعلومات الشخصية للمجني عليهم، وعملية السرقة الالكترونية كالاستيلاء على ماكينات الصرف الآلي. غسيل الأموال والتي تمارس عبر الانترنت الاستعمال غير الشرعي للبطاقات الانتمائية، تجارة المخدرات عبر الانترنت عن طريق الترويج لها والتحريض على إستخدامها[3].

ثالثا: الجرائم الواقعة على الأسرار وامن الدولة.

تقع هذه الجرائم باستعمال النظام المعلوماتي لإفشاء الأسرار سواء كانت أسرار عامة تخص مصالح الدولة ونظام الدفاع عنها أو أسرارا خاصة تتعلق بالأفراد أو المصالح الاقتصادية للمؤسسات المختلفة أو ما يطلق عليها الأسرار المهنية، ويتخذ هذا النوع من

---

[1]– المادة 39 و 47 من التعديل الدستوري لسنة 2020، المصادق عليه في إستفتاء أول نوفمبر سنة 2020، الصادر في 30 ديسمبر 2020 ج ر العدد 82.

[2]– م لينا محمد الاسدي، المرجع السابق، ص 48

[3]– غربي جميلة، المرجع السابق، ص 20–21.

الجرائم صورتين الأولى تتعلق بالجرائم الواقعة على أسرار الدولة[1]، حيث أتاح الانترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالاطلاع على الأسرار العسكرية والاقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات[2]والثانية تتعلق بجرائم الواقعة على الأسرار المهنية.

وتقع هذه الجريمة لسرقة معلومات قصد التشهير بالشخص أو جماعة معينة أو بيعها لتحقيق مصالح مختلفة كالحصول على عائد مادي لمن يهمه الأمر أو يستخدمها للضغط على أصحابها من اجل القيام بعمل أو الامتناع عن القيام بعمل[3].

قد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 .

96 مكرر من قانون العقوبات بالإضافة للمادة394 مكرر3 التي تنص على "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون إخلال بتطبيق عقوبات أشد"[4].

الفرع الثاني: الجرائم الإلكترونية الواقعة على النظام المعلوماتي.

من أجل سد هذا الفراغ القانوني الذي عرفه هذا المجال جاء قانون 04-15 المؤرخ في 10 نوفمبر 2004 المتضمن قانون العقوبات المعدل والمتمم الذي نص على تجريم كل أنواع الاعتداءات التي تستهدف انظمه المعالجة الآلية للمعطيات وهذا في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394

[1]- نايري عائشة، المرجع السابق، ص 20.

[2]- نايري عائشة، المرجع السابق، ص 26.

[3]- سوبر سفيان، نفس المرجع، صفحه 38.

[4]- الأمر رقم 04-15 القانون السابق الذكر.

مكرر إلى 394 مكرر 7 [1].وتأخذ صور الاعتداء على نظام المعلوماتي في التشريع الجزائري صورتان وهما:

- الدخول والبقاء في منظومة معلوماتية .
- المساس بمنظومة معلوماتية.

بالإضافة إلى بعض صور الغش المعلوماتي.

أولا: الدخول أو البقاء في منظومة معلوماتية:

نصت المادة 394 مكرر من قانون العقوبات على معاقبه كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك وتضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير في النظام المعلوماتي.

فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام[2].

1)فعل الدخول :

يقصد بالدخول من الناحية اللغوية الولوج أو النفاذ وبتحقيق الدخول إلى أي مكان عند تعدي الحدود المرسومة له والدلائل المحددة لمعالمه ويتبين من هذا التعريف أن مصطلح الدخول يعبر عن واقعه مادية....

ويقصد بالدخول عن طريق الغش لمنظومة المعالجة الآلية للمعطيات الولوج غير المصرح به عن طريق الغش والوصول إلى المعلومات والبيانات المخزنة في هذه المنظومة، كما يعد دخولا غير مشروع أي صوره تنطوي على اختراق منظومة المعالجة الآلية للمعطيات والبقاء فيها بصوره غير مشروعة. وهي من أكثر الجرائم انتشارا في هذا المجال[3].

[1]– حمزه بن عقون، المرجع السابق، ص 182.

[2]– حمزه بن عقون، المرجع السابق، ص 183.

[3]– عميمر عبد القادر، المرجع السابق، ص63-64.

يلاحظ بان المشرع الجزائري جرم الدخول بطريقة غير شرعيه إلى المنظومة المعلوماتية واعتبر هذا التصرف في حد ذاته جريمة إذ يستخلص لأول وهلة أن مجرد اختراق جهاز الكمبيوتر سواء كان ذلك بقصد الوصول إلى البيانات أو لمجرد تسليه يعد انتهاكا للنظام المعلوماتي بطريقه غير مشروعة ويمكن حسب نص المادة أن الجريمة تتحقق بالصور التالية:

- بمجرد الوصول إلى نظام معلوماتي لكن بطريق الغش أي أن الجريمة عمدية هنا تقوم بتوافر القصد الجنائي العام.
- أن يكون الجاني عالما بدخوله إلى منظومة معلومات لا تخصه وواضح من نص المادة 394 مكرر قانون العقوبات أن جريمة الدخول غير المشروع تصبح قائمة حتى لو لم يترتب عن ذلك أي أضرار بالمعلومات[1].

كما أنها تعتبر من الجرائم الوقتية حيث أنها تتم بمجرد تحقق دخول الفعل غير المصرح به[2].

2) فعل البقاء :

تعتبر جريمة البقاء في كل أو جزء من منظومة المعالجة الآلية للمعطيات جريمة تالية لجريمة الدخول للمنظومة المعلوماتية، لكنها تختلف عنها من حيث القصد الجنائي الذي يأخذ صورتين:

الصورة الأولى: هي دخول شخص إلى المنظومة المعلوماتية عن طريق الخطأ وبدون قصد، لكن بعد الدخول تتغير نيته ويقرر البقاء في لهذه المنظومة.

الصورة الثانية: تكون عندما يقرر الشخص منذ البداية الدخول إلى المنظومة المعلوماتية بطريقه غير مشروعه ويبقى فيها[3].

---

[1]– زيبحة زيدان، المرجع السابق، ص 49.

[2]– نهلا عبد القادر الماموني، المرجع السابق، ص 162.

[3]– عميمر عبد القادر، المرجع السابق،ص69 .

ويكون البقاء جريمة في الحالة التي يطبع فيها الشخص نسخة من المعلومات والتي كان بإمكانه الاطلاع عليها فقط ويتحقق كذلك بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية [1].

كما أنه يمكن الإشارة أن جريمة البقاء داخل النظام المعلوماتي تعتبر من الجرائم المستمرة نظرا لاستمرار الاعتداء على المصلحة التي يحميها القانون طالما استمر البقاء غير المصرح به داخل النظام[2].

ثانيا: جريمة المساس بمنظومة معلوماتية.

تنص المادة 394 مكرر 1بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات بطريق الغش.

وتقوم هذه الصورة من الاعتداء في حاله الإدخال بطريق الغش معطيات في نظام المعالجة الآلية وفي حاله إزالة أو تعديل المعلومات التي يتضمنها النظام المعلوماتي، وهو ما يعد مساسا بمصلحة السلامة والتكامل الذي يهدف المشرع إلى حمايتها[3].

كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوفر الركن المادي، وأفعال الإدخال أو الإزالة أو التعديل تنطوي على التلاعب بالمعطيات التي يضمنها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة بطريقه غير مشروعة أو معطيات وهمية غير صحيحة، أو محو تعليمات البرامج أو البيانات، أو تعديل معطيات موجودة من قبل[4].

[1] حمزه بن عقون، المرجع السابق، ص 184

[2]– فتيحة مهري ،جريمة الدخول والبقاء إلى أنظمة المعالجة الآلية للمعطيات، مذكره لنيل شهادة الماستر، تخصص قانون جنائي للأعمال، كليه الحقوق والعلوم السياسية،جامعه العربي بن مهيدي، ام البواقي ،الجزائر 2015/ 2016 ص 21.

[3]– عبد القادر المرجع السابق،ص 71.

[4]– حمزه بن عقون المرجع السابق،ص 185.

ثالثا :صور أخرى من الغش المعلوماتي

أو التعامل الغير قانوني في المعطيات، وقد نصت على هذه الجريمة المادة 394 مكرر2 من قانون العقوبات الجزائري وجرمت الأفعال الآتية:

- تصميم أو بحث، أو تجميع، أو توفير، أو نشر، أو الإتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- حيازة أو إفشاء أو نشر، أو استعمال أي غرض كان المعطيات المتحصل عليها من الجرائم المنصوص عليها في هذا القسم[1].

[1]– المادة 394 مكرر 2 من قانون رقم 04 –15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم، من الأمر رقم 66 165 الصادر في 8 جوان 1966 المتضمن قانون العقوبات الجزائري، ج ر،العدد 71

الفصل الثاني: الإطار القانوني للجريمة الإلكترونية

المبحث الأول: مواجهة الجريمة الالكترونية في القوانين الجزائرية

المبحث الثاني: آليات التحقيق في الجريمة الإلكترونية

نظرا لانتشار الجريمة الالكترونية في الآونة الأخيرة وازدياد خطورتها على المجتمع والأنظمة المعلوماتية سعى المشرع الجزائري إلى استصدار قوانين معدلة ومتممة لقانون العقوبات واستصدار قوانين خاصة كان أهمها على الإطلاق القانون 09-04 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة' للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام والاتصال ومكافحتها.[1] ومن خلال هذا الفصل سنحاول دراسة تعديلات قانون العقوبات والقوانين الخاصة المستحدثة في إطار مواجهة الجريمة الالكترونية في التشريع الجزائري (المبحث الأول) وكذا إجراءات التحقيق وجمع الأدلة الخاصة بالجريمة الالكترونية (المبحث الثاني).

[1]- سعيد بوزنون, مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد 30، العدد 3، ديسمبر 2019 (ص 47 57)، ص49.

المبحث الأول: مواجهة الجريمة الالكترونية في القوانين الجزائرية

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الالكتروني وما يصاحبها من أضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة ومحاولة منة لتدارك الفراغ التشريعي القائم في هذا المجال من جهة أخرى. عمد منذ الألفية الثانية إلى تعديل قانون العقوبات لجعله يتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال بالإضافة إلى إصدار قوانين خاصة للتصدي للجريمة الالكترونية وهذا ما سنوجزه في المطلبين الآتيين:

المطلب الأول: مكافحة الجريمة الالكترونية بموجب قانون العقوبات

لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون[1] رقم 04-15 المؤرخ في 10 نوفمبر 2004[2] المعدل والمتمم للأمر رقم 66-155 المتضمن قانون العقوبات وجاء تعديل آخر بموجب القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 [3]ومن خلال لهذا المطلب سنحاول بيان النصوص القانونية المستحدثة اثر هذه التعديلات، وسوف نقسمها إلى ثلاثة فروع في الفرع الأول سندرس العقوبات الأصلية،وفي الفرع الثاني العقوبات المقررة للشخص المعنوي، والفرع الثالث للعقوبات التكميلية.

الفرع الأول: العقوبات الأصلية

يمكن تعريف العقوبة على أنها جزءا يقرره المشرع ويوقعه القانون على من ثبتت مسؤوليته في ارتكاب جريمة، وتتمثل العقوبة في إيلام الجاني بالإنقاص من بعض حقوقه الشخصية

---

[1]- بوضياف إسمهان، المرجع السابق ص 362-360.

[2]- القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66 155 المتضمن قانون العقوبات ج ر العدد 71.

[3]- القانون رقم 06-23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66 155 المتضمن قانون العقوبات ج ر العدد 84.

وأهمها الحق في الحياة والحق في الحرية[1] وهي السجن أو الحبس أو الغرامة[2].وسنحاول فيما يأتي بيان العقوبات المقررة لمختلف السلوكات الإجرامية المتعلقة بالجريمة الالكترونية المنصوص عليها في قانون العقوبات.

1- **جريمتا الدخول والبقاء غير المصرح بهما:** حيث نصت المادة 394 مكرر من قانون العقوبات على ما يلي:"يعاقب بالحبس من (03)أشهر إلى سنة (01) وبغرامة من 50,000 دج إلى 100,000 دجكل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك".

بمعنى أنه في حالة الدخول غير المشروع من طرف المجرم الالكتروني للنظام كله أو جزءا منة أو متى كان مسموح له بالدخول إلى جزء معين من النظام وتجاوزه، ومتى كان هذا الدخول أو البقاء داخل النظام مخالفا لإدارة صاحبه.[3]تطبق علية هذه العقوبة.

أما إذا ترتب على الدخول أو البقاء في النظام حذف أو تغيير لمعطيات المنظومة، أو تخريب للنظام اشتغال المنظومة فان العقوبة تشدد وتضاعف وهذا حسب الفقرة الثانية من نص المادة 394 مكرر من ق. ع:"تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب في نظام اشتغال المنظومة،تكون العقوبة الحبس من ستة(6) أشهر إلى سنتين (2) والغرامة من 50,000 دج إلى 150,000 دج".

2.جريمة المساس العمدي بالمعطيات:وتتمثل في إدخال معطيات في نظام المعالجة الآلية أو إزالتها أو تعديلها، وكانت العقوبة المقررة لهذه الأفعال الحبس من ستة (6)أشهر إلى

---

[1]- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط 13، 2011 ص 289.

[2]- هدى أبوبكر، اعرف ما هي العقوبات الأصلية والتبعية في القانون، القاهرة 12 ديسمبر 2019، عن الموقع الالكتروني https//ww.youm7.com تاريخ الدخول 23-03-2023، بتوقيت 02: 14.

[3]- نايري عائشة، المرجع السابق، ص 37 .

ثلاثة(3) سنوات والغرامة من 500,000 د ج إلى 2.000.000 دج وهذا ما نصت علية المادة 394 مكرر 1 من ق.ع.

3-جريمة التعامل الغير قانوني بالمعطيات:

وهي الجريمة المتمثلة في نشر المعطيات المخزنة أو معالجة أو مرسلة بواسطة منظومة معلوماتية وحيازتها والاتجار فيها.[1]وجريمة تجميع أو توفير بيانات مخزنة أو معالجة آليا، وجريمة نشر المعطيات أو إفشائها... كل هذه الأفعال نصت على عقوبتها المادة 394 مكرر 2 من نفس القانون السابق الذكر. وكانت العقوبة المقررة الحبس من شهرين(02) إلى ثلاثة(03)سنوات وبغرامة من 1.000.000 د ج إلى 5.000.000 دج.

4-جرائم المساس بالحياة الخاصة:

ذهب المشرع الجزائري إلى تجريم الأفعال الماسة بالحياة الخاصة بأي طريقة من طرق التقنيات الحديثة بموجب التعديل الذي جاء به[2] القانون رقم 06-23 المؤرخ في 20 سبتمبر 2006.[3]

حيث نص في المادة 303 من ق ع على العقوبات المقررة لمنتهك البريد الالكتروني: [4]"كل من يفض أو يتلف رسائل أو مراسلات موجهة إلى الغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس من شهر (01) إلى سنة (10) وبغرامة من 25,000 دج إلى 100,000 دج أو بإحدى هذه العقوبتين فقط".

وفي جريمة انتهاك المحادثات الشخصية الالكترونية سواء بالتقاط الصور أو تسجيل أو نقل المكالمات نصت المادة 303 مكرر "يعاقب بالحبس من ستة (60)أشهر إلى ثلاثة

---

[1]- زيبحة زيدان، المرجع السابق، ص 56.

[2]- زيبحة زيدان،نفس المرجع، ص 80.

[3]- القانون رقم 06 23 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر 66 156 المؤرخ في 8 يونيو 1966 والمتضمن قانون العقوبات ج ر 84.

[4]- رابحي عزيزة، المرجع السابق، ص 243.

(03)سنوات وبغرامة من 50,000 دج إلى 300,000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص."

أما في الجرائم الالكترونية المرتكبة ضد مؤسسات الدفاع الوطني والهيئات والمؤسسات الخاضعة للقانون العام فقد اعتبرها المشرع بمثابة ظرف تشديد[1] من خلال نص المادة 394 مكرر 3:" تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد".

والملاحظ أن النص المشرع اعتبر صفة المجني علية ظرفا مشددا فمتى كانت الضحية المستهدفة إحدى الهيئات المنصوص عليها في المادة تكون العقوبة المقررة هي ضعف العقوبة المنصوص عليها لكل جريمة طبقا للمواد السالفة الذكر.[2]

الفرع الثاني: العقوبات المقررة للشخص المعنوي.

تبنى قانون العقوبات الجزائري مبدأ المسؤولية الجزائية للأشخاص المعنويين بموجب القانون 04-15 في نص المادة 51 مكرر ليعزز ذلك بالقانون رقم 06-23 بنص المادة 18 مكرر وفي مضمون هذا النص استثناء المشرع الأشخاص المعنويين العامة من الخضوع للمسؤولية الجزائية وعلى رأسها الدولة،[3] ومن خلال نص المادة 18 مكرر فإن: "العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات و الجنح هي:

1- الغرامة التي تساوي من مرة (01) إلى خمس (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

2- واحدة أو أكثر من العقوبات التكميلية الآتية:

- حل الشخص المعنوي،
- غلق المؤسسة أو فرع من فروعها لمدة ذا تتجاوز خمس (05) سنوات.

---

[1]- زيبحة زيدان، المرجع السابق، ص 99.

[2]- نسيمه جدي، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستر في القانون كلية الحقوق، جامعة وهران الجزائر، 2014 ، ص 128.

[3]رابحي عزيز، المرجع السابق، ص 248.

- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (05) سنوات.
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر نهائيا أو لمدة لا تتجاوز خمس (05) سنوات.
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.
- نشر أو تعليق حكم الإدانة.
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (05) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته".

كما تجدر الإشارة إلى أن هذه العقوبات ليست خاصة بجرائم الاعتداء على نظم المعالجة الآلية فحسب، بل تقع على كل الجرائم التي يرتكبها الشخص المعنوي، بينما ما يتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في المواد من 394 مكرر إلى 394 مكرر 7، فإن الغرامة المطبقة على هذا الأخير هي خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وهذا تطبيقا لنص المادة 394 مكرر 4 من ق ع ج [1] ويشترط لتقرير مسؤولية الشخص المعنوي ثلاثة شروط:

- يجب أن يكون الشخص المعنوي عاما أو خاصا باستثناء الدولة.
- يجب أن يرتكب الجريمة لصالح الشخص المعنوي.
- يجب أن يرتكب الجريمة من طرف عضو أو ممثل الشخص المعنوي دون أن تؤثر على مسؤولية الشخص الطبيعي[2]

[1]– رابحي عزيزة، المرجع السابق، ص 248.

[2]– نسيمة جدي، المرجع السابق، ص 129.

الفرع الثالث: العقوبات التكميلية.

نصت المادة 394 مكرر 6 من ق ع على العقوبات التكميلية إلى جانب العقوبات الأصلية والممثلة في:

1- المصادرة: وهي عقوبة تكميلية تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب جريمة من الجرائم الماسة بالأ**نظمة** المعلوماتية مع مراعاة حقوق الغير حسن النية.[1]

2-إغلاق الموقع:والأمر يتعلق بالمواقع (les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية[2].

3- إغلاق المحل أو مكان الاستغلال: يكون في الحالة التي يكون صاحب المحل مشاركا في الجريمة وذلك إذا تمت الجريمة وهو عالم بها ولم يتصدى لها بالإخبار عنها، أو بمنع مرتكبيها من ارتياد محلة لارتكاب مثل هذه الجرائم.[3]

أما بالنسبة لمدة الغلق لم تحددها المادة 394 مكرر 6 من ق ع وعليها يمكن أن تكون مؤبدة أو مؤقتة كما نصت على ذلك المادة 26 من ق ع 7: " يجوز أن يؤمر بغلق المؤسسة نهائيا أو مؤقتا في الحالات المنصوص عليها في القانون".[4]

الفرع الرابع: عقوبة الاشتراك والشروع في الجريمة

عقوبة الاتفاق الجنائي نصت علية المادة 11 من الاتفاقية الدولية للإجرام والمعلوماتي وقد تبنى عن المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي[5] لنص المادة 394 مكرر 5 بقولها: " كل من شارك في مجموعة أو في اتفاق تالف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التصريح مجسدا بفعل أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها".

---

[1]- سعيدي سليمة، حجاز بلال، المرجع السابق، ص 153.

[2]- آمال قارة الحماية الجزائية للمعلوماتية في التشريع الجزائري، هومة، الجزائر ط 2، 2007، ص 128.

[3]- نايري عائشة، المرجع السابق، ص 39.

[4]- نسيمة جدي، المرجع السابق، ص 127.

[5]- سعيدي سليمة، حجاز بلال، المرجع السابق، ص 155.

إن الحكمة التي ارتآها المشرع من تجريم الاشتراك في مجموعة أو في اتفاق بغرض الإعداد 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 إطار إتفاق جنائي، بمعنى أن الأعمال التحضيرية المرتكبة من طرف شخص منفرد غير مشمولة بالنص.[1]

أما عقوبة الشروع في الجريمة فقد نصت عليها المادة 394 مكرر7 من قعبقولها "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

يقصد بالشروع في الجريمة المرحلة التي تنصرف فيها إدارة الجاني إلى تنفيذ الجريمة فعلا فيبدأ في تنفيذ الركن المادي ولكنها لا تتم لأسباب لأدخل لإرادته فيها. [2]

يبدو من خلال النص أن رغبة المشرع في توسيع نطاق العقوبة لتشمل اكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في أحد الجرائم الماسة بالأنظمة المعلوماتية معاقب عليها بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة بنص المادة 394 مكرر 5 من ق ع أيضا مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي أيضا.[3]

المطلب الثاني: مكافحة الجريمة الالكترونية بموجب القوانين الخاصة

لقد سعى المشرع الجزائري إلى سن قوانين خاصة لمواجهة الجريمة الالكترونية، وفي هذا المطلب سنحاول عرض بعض التشريعات منها:

[1]– رابحي عزيزة، المرجع السابق، ص 249.

[2]– أحسن بوسقيعة، المرجع السابق،ط13 ، ص 127.

[3]– رابحي عزيزة، المرجع السابق، ص 250.

الفرع الأول:القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

القانون رقم 09-04 المؤرخ في 5 أوت 2009[1] المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، يحتوي هذا القانون على 6 فصول تناولت التعريف بالجريمة، مراقبة الاتصالات الالكترونية،القواعد الإجرائية،الهيئة الوطنية للوقاية من الجرائم المعلوماتية والاختصاص القضائي وهذا في 19 مادة[2].

وقد أورد المشرع في المادة2 من القانون رقم 09-04 أنه يقصد بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في ق ع وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.[3]

وطبقا لنص المادة 03 من نفس القانون فقد وضع المشرع الجزائري بين أيدي الجهات المختصة بمكافحة الجريمة المتصلة بتكنولوجيا المعلوماتية وسيلة قانونية جديدة من خلال وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية و تجميع وتسجيل محتواها في حينها وهو ما أطلق علية مصطلح مراقبة الاتصالات الالكترونية في عنونة الفصل الثاني من هذا القانون[4].

كما نصت المادة 04 من نفس القانون 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.

---

[1]- القانون رقم 09- 04 الصادر بتاريخ 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بيتكنولوجيا الإعلام والاتصال ومكافحتها ،ج ر ، العدد 47.

[2]- بوهرين فتيحة، المرجع السابق، ص 56 .

[3]- غربي جميلة، المرجع السابق، ص 52.

[4]- ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، تلمسان، الجزائر السداسي الأول 2018، ص 76.

- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية،عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.[1]

كما قد ألزم المشرع الجزائري مقدمي الخدمات من خلال نص المادتين 10 و 11 من القانون رقم 09-04 بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبحفظ المعطيات المتعلقة بحركة السير ووضعها تحت تصرف السلطات المذكورة.[2]

ونص هذا القانون على إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها طبقا للمادة 13، وتتولى هذه الهيئة تنشيط وتنسيق عمليات الوقاية من الجرائم، وكذلك مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات، وتبادل المعلومات مع الدول.[3]

الفرع الثاني:القانون المتعلق بالتوقيع والتصديق الالكترونيين

أصدر المشرع الجزائري بتاريخ 01 فبراير 2015 القانون رقم 15-04 المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين.[4]

ولقد عرف في المادة الثانية منة مجموعة المصطلحات المتعلقة بالتوقيع والتصديق الالكترونيين نذكر منها:

---

[1]- نص المادة 04 من القانون 09-04.

[2]- غربي جميلة، المرجع السابق، ص 52.

[3]- سي حمدي عبد المومن، قيرة سعاد، المرجع السابق، ص 65.

[4]- القانون رقم 15 -04 المؤرخ في 01 فبراير 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، جر، العدد 06.

– التوقيع الالكتروني يقصد به: "بيانات في شكل الكتروني، مرفقة أو مرتبطة منطقيا ببيانات الكترونية أخرى، تستعمل كوسيلة توثيق".

– شهادة التصديق الالكتروني: عرفت بأنها "وثيقة في شكل الكتروني تثبت الصلة بين بيانات التحقق من التوقيع الالكتروني والموقع"[1].

إذا يرتبط التوقيع والتصديق الالكترونيين بمجموعة من البيانات والمعلومات ذات الطابع الشخصي التي يشكل الاعتداء عليها جريمة يعاقب مرتكبيها بأحكام جزائية وردت في هذا القانون تتمثل في:[2]

1–إفشاء البيانات الشخصية أو إساءة استعمالها: وهذا طبقا لنص المادة 68 من القانون رقم 15–04 : "يعاقب بالحبس من ثلاثة (03)أشهر إلى ثلاثة (03) سنوات وبغرامة من مليون دينار 1.000.000 دينار جزائري إلى خمسة ملايين دج5.000.000 دج أو بإحدى هاتين العقوبتين فقط كل من يقوم بحيازة أو إفشاء أو استعمال بيانات إنشاء توقيع الكتروني موصوف خاصة بالغير".

2– الإخلال بسرية البيانات المتعلقة بشهادة التصديق الالكتروني الممنوحة طبقا لنص المادة 42 من نفسي القانون فإنه: "يجب على مؤدي خدمات التصديق الالكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادات التصديق الالكتروني الممنوحة". وعلية إذا اخلوا بهذا الالتزام فتطبق عليهم العقوبة المحددة في المادة 70من هذا القانون" يعاقب بالحبس من (03) أشهر إلى سنتين (02)وبغرامة من مائتي ألف دينار (200.000دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الالكتروني أخلى بأحكام المادة 42 من هذا القانون".

3– جمع البيانات الشخصية للمعني دون موافقته.

[1]– أنظر المادة 02 من القانون رقم 15–04.

[2]– شيخ سناء، شيخ محمد زكرياء، بحث حول مكافحة الجرائم الالكترونية في القانون الجزائري ،مجلة وميض الفكر للبحوث، العدد 5 سبتمبر 2020، ص7.

نص ساعة القانون رقم 15-04 في المادة 43 منة على أنه لا يمكن لمؤدي خدمات التصديق الالكتروني أن يجمع البيانات الشخصية للمعني إلا بموافقته الصريحة، ومتى أخل بهذا الواجب يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات، وبغرامة من 200,000 دج إلى مليون دينار أو بإحدى هاتين العقوبتين فقط.[1]

الفرع الثالث: القانون المتعلق بالبريد والاتصالات الالكترونية

أصدر المشرع الجزائري القانون رقم 18-04 [2] الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات التكنولوجيا والذي ألغى بموجبة رقم 03/2000، والذي أكد فيه على وجوب عدم مساس استعمال شبكات وخدمات الاتصال الإلكترونية بحفظ الحياة الخاصة للأفراد، وفي حالة مخالفة ذلك يتعرض المخالف للأحكام الجزائية التي تضمنها هذا القانون[3] والمتمثل في:

1- انتهاك سرية المراسلات الإلكترونية: نصت المادة 164 من هذا القانون على:"يعاقب بالحبس من سنة (01) إلى خمس(05) سنوات وبغرامة من 500,000 دج إلى 1.000.000 دج كل شخص ينتهك سرية المراسلات المرسلة عن طريق البريد أو الاتصالات الإلكترونية أو يفشي مضمونها أو ينشره أو يستعمله دون ترخيص من المرسل أو المرسل إليه أو بخبر وجودها."

2-تحويل المراسلات الصادرة عن طريق البريد: حسب نص المادة 165 من نفس القانون يعاقب بالحبس من سنة إلى ثلاث سنوات وبغرامة من مليون دينار إلى خمس ملايين دينار جزائري أو بإحدى هاتين العقوبتين كل متعامل للاتصالات الإلكترونية يحول بأي طريقة كانت، المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق الاتصالات الإلكترونية.[4]

---

[1]- شيخ سناء، شيخ محمد زكرياء، المرجع السابق، ص7.

[2]- القانون رقم 18-04 المؤرخ في 10 ماي 2018 يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، ج ر ، العدد 27.

[3]- سي حمدي عبد المومن قيرة سعاد،المرجع السابق، 66.

[4]- شيخ سناء، شيخ محمد زكرياء، المرجع السابق، ص8.

الفرع الرابع : قانون التأمينات.

قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا الجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن لة اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة للبطاقة الإلكترونية حسب المادة 93 مكرر 2.[1]

بحيث نصت هذه المادة على ما يلي:" دون الإخلال بالعقوبات المنصوص عليها في التشريع المعمول به، يعاقب بالحبس من (02) إلى(05) سنوات وبغرامة من 100,000 دج إلى 200,000 دج كل من يسلم أو يستلم بهدف الاستعمال غير المشروع البطاقة الالكترونية للمؤمن له اجتماعيا أو المفتاح الالكتروني لهيكل العلاج أو المفتاح الالكتروني لمهني الصحة[2].

الفرع الخامس: القواعد المتعلقة بحقوق المؤلف والحقوق المجاورة

اعتبر المشرع الجزائري برنامج الحاسوب الآلي ضمن المصنفات الأدبية والفنية بموجب المادة 04 من الأمر رقم 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف والحقوق المجاورة[3]، والتي نصت على:" تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يأتي:

---

[1]- فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر الجريمة الالكترونية، طرابلس بتاريخ 24-25 مارس 2017، ص 132.

[2]- المادة 93 مكرر 02 من القانون رقم 08-01 المؤرخ في 23 يناير 2008 يتمم القانون رقم 83-11 المؤرخ في 02 يونيو 1983 والمتعلق بالتأمينات الاجتماعية، ج ر، العدد 04.

[3]- الأمر رقم 03-05 المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف والحقوق المجاورة ، ج ر، العدد 44.

أ- المصنفات الأدبية المكتوبة:مثل المحاولات الأدبية، والبحوث العلمية والتقنية، والروايات، والقصص، والقصائد الشعرية،وبرامج الحاسوب، والمصنفات الشفوية...".

وهو محمي بالأمر03-05 ذاته فيها فالحقوق المادية أو المالية هي الإطار الذي يمكن صاحب البرنامج من استغلاله بشتى الطرق دون غيره، أو لمن يخوله هو نفسه هذا الحق وله في ذلك وفقا لأحكام المادة 27 من الأمر المشار له إبلاغه للجمهور بأية منظومة معالجة معلوماتية ويترتب عن ذلك حقوق مادية للمؤلف صاحب البرنامج بالاستغلال التجاري له ولورثته بمختلف الطرق وهذا ما يستخلص من نص المادة 03 من نفس الأمر[1].

كما أن المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية،حيث عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي، والتي تمكن من القيام بنشاط علمي أو أي نشاط من نوع أخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم باندفاعات الكترونية بالحاسوب.[2]

من بين الجرائم الإلكترونية التي جاء بها هذا القانون نذكر:

1- ارتكاب جنحة التقليد عن طريق: الكشف غير المشروع للمصنف أو المساس بسلامة مصنف أو أداء لفنان مؤد أو عازف، استنساخ مصنف أو أداء بأي أسلوب من الأساليب في شكل نسخ مقلدة،استيراد أو تصدير نسخ مقلدة، أو مصنف أداء، بيع أو تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف أو أداء. هذا ما نصت علية المادة 151 من هذا القانون.

2- ارتكاب جنحة التقليد عن طريق: انتهاك الحقوق المحمية بموجب هذا الأمر فيبلغ المصنف أو الأداء عن طريق أي منظومة معالجة، وهذا ما أوردته المادة 152 من الأمر رقم 03-05.

[1]- زيبحة زيدان، المرجع السابق، ص 88.

[2]- بدري فيصل، مكافحة جريمة معلوماتية في القانون الدولي والداخلي، أطروحة لينين شهادة الدكتورة، علوم في القانون تخصص قانون عام، كليه الحقوق، جامعه الجزائر 1، 2017 2018، ص 140.

3- الاشتراك بالعمل أو الوسائل الحائز عليها للمساس بحقوق المؤلف أو أي مالك للحقوق المجاورة طبقا لنص المادة 154 من نفس الأمر أما بالنسبة للعقوبات فقد نصت المادة 153 على عقوبة مرتكب جنحة التقليد المنصوص عليها في المادتين 151 و 152 من القانون السابق الذكر في نصها:"يعاقب مرتكب جنحة تقليد مصنف أو أداء كما هو منصوص علية في المادتين 151 و 152 أعلاه، بالحبس من ستة(06)أشهر إلى ثلاثة(03) سنوات وبغرامة من خمسمائة ألف دينار(500,000 دج) إلى مليون دينار (1.000.000دج) سواء كان النشر قد حصل في الجزائر أو في الخارج".

أما في المادة 154 فقد نص على أن الشريك في ارتكاب جنحة التقليد سواء بأعماله أم بالوسائل الحائز عليها للمساس بحقوق المؤلف يعاقب بنفس العقوبة المقررة في المادة 153 من نفس القانون.

ونفس العقوبة لكل من يرفض عمدا دفع المكافأة المستحقة للمؤلف أو لأي مالك حقوق مجاورة أخرى (نص المادة 155).

وأكثر من هذا كله، فإن المشرع خول للقاضي الجزائي أن يضاعف ويشدد العقوبة الأصلية في حالة توافر ظرف العود، وأن يأمر بغلق المؤسسة التي يستغلها المقلد أو شريكه لمدة لا تتجاوز ستة أشهر، أو الأمر بالغلق النهائي إذا اقتضى الأمر.[1] وهذا كله وفقا للقانون.

الفرع السادس: القانون المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

اصدر المشرع الجزائري حديثنا القانون رقم 18-07[2]المؤرخ في 10 يونيو 2018 الذي يهدف إلى حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي في إطار إحترام الكرامة الإنسانية والحياة الخاصة والحريات العامة.[1]

[1]- انظر المادة 156 من الأمر 03-05، السابق الذكر.

[2]- القانون رقم 18-07 المؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ج ر، العدد 34.

ويقصد بالمعطيات ذات الطابع الشخصي وفقا للمادة 03 من هذا القانون: " كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه...بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية.

كما أن نفس المادة[2] تطرقت إلى معالجة المعطيات وقصدت بها:"كل عملية أو مجموعة عمليات منجزة بطرق أو بوسائل آلية أو بدونها على معطيات ذات طابع شخصي مثل الجمع أو التسجيل أو التنظيم أو الحفظ أو الملائمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصال عن طريق الإرسال أو النشر أو أي شكل أخر من أشكال الإتاحة أو التقريب أو الربط البيني وكذا الإغلاق أو التشفير أو المسح أو الإتلاف، كما تجدر الإشارة إلى أن أي مخالفة لأحكام هذا القانون تعرض المخالف للأحكام الجزائية المتمثلة في:

1-خرق الحياة الخاصة عند معالجة المعطيات: أوجب المشرع الجزائري أن تتم معالجة المعطيات ذات الطابع الشخصي مهما كان مصدرها أو شكلها في إطار حماية الحياة الخاصة للأفراد.[3] وكل خرق لهذا الواجب يعاقب المخالف بالحبس من سنتين (2) إلى خمسة (5) سنوات وبغرامة من200,000 دج إلى 500,000 دج، طبقا لنص المادة 54 من القانون رقم 18-07.

2- معالجة المعطيات الشخصية رغم اعتراض الشخص المعني: حسب نص المادة 07 من هذا القانون فإنه لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة الشخص المعني، فإذا تمت معالجة هذه المعطيات رغم اعتراضه فتطبق على المخالف العقوبة المنصوص عليها في المادة 55 من نفس القانون بنصها: " يعاقب بالحبس

---

[1]- المادة 02 من القانون رقم 18-07

[2]- أنظر المادة، رقم 03 من القانون رقم 18-07.

[3]- سي حمدي عبد المومن، قيرة سعاد، المرجع السابق، ص 67.

من سنة(01) إلى ثلاث سنوات وبغرامة من 100,000 دج إلى 300,000 دج كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 07 من هذا القانون".

3- طبقا لنص المادة 12 من القانون رقم 18-07 فإنه يجب إخضاع كل عملية معالجة معطيات شخصية لتصريح مسبق من السلطة المختصة أو في حالة القيام بالمعالجة دون الحصول على هذا التصريح فإنه يعاقب المسؤول بالحبس من(02) سنتين إلى خمس(05) سنوات وبغرامة من 200,000 دج إلى 500,000 دج وفقا لنص المادة 56 من نفس القانون.

1-جمع المعطيات الشخصية بطريقة غير شرعية: تنص المادة 59 من القانون رقم 18-07 على أنه: "يعاقب بالحبس من سنة(01) إلى ثلاثة (03) سنوات وبغرامة من 100,000 دج إلى 300,000 دج كل من قام بجمع معطيات ذات طابع شخصي بطريقة تدليسية أو غير نزيهة أو غير مشروعة". فهذا الفعل فيه انتهاك للحياة الخاصة للأفراد يتمثل في جمع معلومات صحيحة عنهم لكن بطريقة غير قانونية وغير مشروعة.

ويستمد هذا الجمع صفته غير المشروعة المستخدمة للحصول على هذه البيانات أو المعلومات إما من حيث الأساليب كمراقبة الرسائل المتبادلة أو اعتراضها عن طريق البريد الالكتروني أو توصيل أسلاك بطريقة خفية إلى الحاسوب الذي تختزن بداخلة البيانات، أو من حيث طبيعة مضمونها كأن تتعلق بالمعتقدات الدينية والسياسية و الانتماءات الحزبية والأصل العرقي للأفراد،لابد أن تكون بعيدة عن عمليات التجميع في الحواسيب، لأن مضمون هذه البيانات يدخل في نطاق الحياة الخاصة للأفراد.[1]

المبحث الثاني: آليات التحقيق في الجريمة الالكترونية

إن طبيعة الجرائم الالكترونية بعناصرها ووسائل ارتكابها قد تدفع المشرع الجزائي إلى أن يعيد النظر في كثير من المسائل الإجرائية، خاصة فيما يتعلق بمسالة الإثبات باعتبارها أهم موضوعات هذا القانون.

[1]- نهلا عبد القادر المومني، المرجع السابق، ص 174 175.

ذلك أن الدليل الذي يقوم على إثبات هذا النوع من الجرائم لابد أن يكون من ذات طبيعتها التقنية، وهو الأمر الذي لا تكون فيه القواعد الإجرائية التقليدية لاستخلاص الدليل قادرة على القيام بة مما يستوجب تدخل المشرع لتكريس قواعد إجرائية يمكن للجهات المكلفة بالبحث والتحري عن الجريمة الإلكترونية الاعتماد عليها في الوصول إلى الدليل المناسب لإثبات هذه الجريمة.[1]

وعلية هذا ما سيكون محل دراستنا في هذا المبحث حيث سنتطرق إلى إجراءات التحقيق في الجريمة الإلكترونية في المطلب الأول أما المطلب الثاني فسنخصصه لإجراءات جمع الأدلة.

المطلب الأول: التحقيق في الجريمة الالكترونية

تعتبر مرحلة جمع المعلومات والمعطيات من أهم مراحل الدعوى الجزائية التي تسبق المحاكمة فمن خلالها يتم التعرف على من ارتكب الفعل وهذا ما يعرف بالتحقيق.[2]

فتحقيق هو مجموعة الإجراءات التي تتخذ بعد وقوع الجريمة، قصد التنقيب والكشف عن الأدلة في شان الجريمة التي ارتكبت ثم مدى كفايتها لإحالة المتهم للمحكمة. [3]

كما أن لهذا الأخير أهمية في إثبات وقوع الجرائم وإقامة الدليل على مرتكبيها بأدلة الإثبات على اختلاف أنواعها ومن يقوم بالتحقيق هم الضبطية القضائية وقضاة التحقيق وفق إجراءات البحث والتحري[4] المحددة في الباب الأول من قانون الإجراءات الجزائية تحت عنوان" في البحث والتحري عن الجرائم."

وعلية سنعالج في هذا المطلب الأجهزة المكلفة بالبحث والتحري (الفرع الأول)، وخصائص التحقيق والمحقق (الفرع الثاني)

---

[1]– سعيداني نعيم، المرجع السابق، ص 101.

[2]– براء منذر عبد اللطيف، شرح قانون المحاكمات الجزائية دار حامة للنشر والتوزيع، عمان، ط1، 2009 ،ص 71.

[3]– د. فلاح عبد القادر، د. ايت عبد المالك نادية،التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريح الجزائري، مجلة الأستاذة الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2, 2019 ،ص 1694.

[4]– يوسف جفال، التحقيق في الجريمة الالكترونية، مذكرة شهادة الماستر أكاديمي في الحقوق، تخصص قانون جنائي، جامعه محمد بوضياف، المسيلة، 2016. 2017 ، ص 18.

الفرع الأول: الأجهزة المكلفة بالبحث والتحري

نظرا للخصوصية التي تتميز بها الجريمة الإلكترونية كان الأمر لازما لتوفير كوادر وأجهزة مختصة تعني بعملية البحث وتحري على الجريمة الإلكترونية[1] وكان ذلك إما على مستوى جهاز الضبطية القضائية أو على مستوى مركز الوقاية من جرائم الإعلام الآلي وان الجرائم الإلكترونية.

أولا: الضبطية القضائية

أناط المشرع جزائري بالضبطية القضائية مهمة البحث والتحري عن الجرائم المقرر ' في ق ع وهذا طبقا لما ورد في المادة 12 من ق إ ج. فالضبطية القضائية تعتبر صاحبة الاختصاص الأصيل في كل الجرائم بما فيها الجرائم الإلكترونية وقد منحها القانون أساليب تحري جديدة نبينها فيما يلي:[2]

1- على مستوى جهاز الشرطة

أنشأت المديرية العامة للأمن الوطني مخبر مركزي بمركز الشرطة بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي على فروع تقنية من بينها خلية الإعلام الآلي وفرق متخصصة مهمتها التحقيق والكشف عن جرائم الانترنت[3] بالإضافة لإنشائها ثلاثة مخابر أخرى على مستوى بشار، ورقلة وتمنراست قيد الانجاز لأجل تعميم هذا النشاط على كافة ربوع الوطن [4].

كما يضم المخبر الجهوي للشرطة العلمية على مستوى قسنطينة ووهران مخبرا خاصا يتولى مهمة التحقيق في الجريمة الإلكترونية تحت اسم "دائرة الأدلة الرقمية والآثار التكنولوجية" والتي تضم ثلاثة أقسام فرعية هي:

---

[1]- سعيداني نعيم، المرجع السابق، ص 106-107.

[2]- فلاح عبد القادر، أيت عبد المالك نادية، المرجع السابق، ص 1695.

[3]- سعيداني نعيم، المرجع السابق، ص107.

[4]- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة الدكتورة في الحقوق جامعه باتنة، 2016/2015 ص 177.

- قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات
- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات، وذلك باستعانة بوسائل مادية للكشف عن جرائم الإلكترونية.[1]

2- على مستوى جهاز الدرك الوطني.

يعمل جهاز الدرك الوطني على مكافحة الجريمة الإلكترونية بواسطة المعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام ولإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية[2]وأيضا بواسطة مديرية الأمن العمومي والاستغلال والمصلحة المركزية لتحريات الجنائية، وهي هيئة ذات اختصاص وطني من مهامها مكافحة الجريمة الإلكترونية[3].

ثانيا:مركز الوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية

انشأ هذا المركز بموجب المرسوم الرئاسي رقم 15-261[4]ومقرة ببئر مراد رايس وهو تابع لمديرية الأمن للدرك الوطني. وقد نصه المادة الأولى منه على تحديد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وتمارس هذه الهيئة العديد من المهام في مجال التصدي للجريمة الإلكترونية المنصوص عليها في المادة 04 من هذا المرسوم وقد ورد النص عليها في المادة 14 من القانون رقم 09-04 السابق الذكر وهي:

- ضمان المراقبة المستمرة والدائمة على شبكة الانترنت.

---

[1]- ربيعي حسين، المرجع نفسه، ص 179.

[2]- سعيداني نعيم، مرجع السابق، ص 107.

[3]- ربيعي حسين، المرجع السابق، ص 183.

[4]- المرسوم رئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحاتها، ج ر، العدد 53 الصادرة في 18 أكتوبر 2015 .

- القيام بمراقبة الاتصالات الإلكترونية بما يسمح القانون لفائدة وحدات الدرك الوطني والجهات القضائية. [1]
- المشاركة في عمليات البحث والتحري عن الجرائم الإلكترونية.
- إدارة وتنسيق العمليات الوقائية من الجرائم الإلكترونية.

الفرع الثاني: خصائص التحقيق والمحقق في الجريمة الإلكترونية

يختلف التحقيق في الجريمة الإلكترونية عن التحقيق في الجنائي التقليدي ببعض الميزات الخاصة، وكذا المحقق الجنائي وهدا نظرا لطبيعة التقنية التي تتمتع بها هذه الجرائم.

أولا: خصائص التحقيق في الجريمة الإلكترونية

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى فهو له قواعد ثابتة راسخة وبدونها ما كان ليتمتع التحقيق بتلك الصفة. وهذه القواعد إما قانونية و إما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزائها شيء سوى الخضوع والامتثال أما الثانية فتتميز بي المرونة التي يضفي عليها المحقق من خبرته وفطنته ومهاراته الكثير. [2]

وبالتالي فإن الفكرة البشري المتعلق بالمجرم المعلوماتي يجب أن يقابله فكر بشري من قبل المحقق وعلية فان أسلوب التحقيق وفكر المحقق الجنائي يجب أن يتغير ويتطور أيضا وذلك نتيجة طبيعية لمواجهة فكر أسلوب المجرم المعلوماتي.[3]

1- أسلوب التحقيق الابتدائي في الجريمة الإلكترونية:

التحقيق عموما هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة ومعرفة مرتكبيها تمهيدا لتقديمهم إلى المحاكمة وقد تكون هذه الإجراءات عملية كالتفتيش أو

---

[1]-ربيعي حسين، المرجع السابق ،ص 185.

[2]- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية مصر، ط 1، 2009، ص 16.

[3]- خالد ممدوح ابراهيم، نفس المرجع، ص 17.

فنية كمظاهرات البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام المعلوماتي.

والهدف من التحقيق الابتدائي هو التأكد أولا من وقوع جريمة يعاقب عليها القانون، ومن تمت معرفة نوع هذه الجريمة ومن هو الجاني ومن هو المجني عليه، وكاد معرفة وقوعها وما هي الوثائق التي استعملت في ارتكابها ويكون ذلك في الجريمة الإلكترونية وفقا لمنهج تحقيق يختلف عن غيرة بالنسبة للجرائم الأخرى.[1]

أ- تشكيل فريق التحقيق:

إن التحقيق الابتدائي في الجرائم المعلوماتية يكون غالبا اكبر من أن يتولاه شخص واحد بمفرده حتى ولو كانت المضبوطات هي مجرد حاسب شخص واحد، ولذلك فأنه يفضل أن يتعاون عدة محققين في انجاز مهمة التحقيق والعثور على الأدلة.[2]

ويجب أن تشكيل فريق التحقيق من فنيين أو أخصائيين ذوي خبرة في مجال الحاسوب والانترنت، ويتميزون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الالكتروني بشكل خاص لهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والانترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة. [3]

وان كان أسلوب عمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلا أنه يأخذ عملية خاصة في الجرائم الإلكترونية لما تتطلبه من مهارات فنية وخبرات متنوعة قد لا تتوافر لدى المحققين، وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا، ومن الناحية العملية غالبا ما يتكون فريق التحقيق في الجرائم المعلوماتية من:

- المحقق الرئيسي ويكون ممن لهم خبرة في التحقيق الجنائي.

---

[1]- سعيداني نعيم، المرجع السابق، ص 110.

[2]- عبد الله حسين محمد، إجراءات جمع الأدلة في الجريمة المعلوماتية مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 26-28 ابريل 2003، ص 612.

[3]- عبد الله حسين محمد المرجع السابق ص 613.

- خبراء الحاسوب وشبكات الانترنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم.
- خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب.
- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.
- خبراء التصوير و البصمات والرسم التخطيطي.[1]

وفي هذا الإطار نجد أن المشرع الجزائري قد أشار إلى إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المختصين في مجال الحاسوب والنظم المعلوماتية، ومن الذين لهم دراية بعمل المنظومة المعلوماتية أو من لهم دراية بالتدابير المتخذة لحماية المعطيات المعلوماتية وذلك بغرض مساعدة جهات التحقيق في انجاز مهمتها وتزويدها بكل المعلومات الضرورية لذلك.[2]

2- العناصر الأساسية للتحقيق الابتدائي في الجريمة الإلكترونية

نقصد بها تلك الإجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها، وهناك إجراءات واحتياطات يتعين على الضبطية القضائية مراعاتها قبل البدء في عمليات التحقيق الابتدائي وإجراءات أخرى يجب على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي.[3]

أ- الإجراءات التي يجب مراعاتها قبل البدء في التحقيق.

- تحديد نوع نظام المعالجة الآلية للمعطيات فهل هو كمبيوتر معزول ام متصل بشبكة معلومات.

---

[1]- عبد الله حسين محمد المرجع السابق ص 613.

[2]- انظر الفقرة الأخيرة من المادة 05 من القانون رقم 09 04 السابق الذكر.

[3]- عبد الفاتح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الأنترنت، دار الكتب القانونية ، ط 1 ، ص 84.

- وضع مخطط تفصيلي للمنشاة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.
- إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الاتصال بها أو منها لمعرفة الطريقة التي تمت بها عملية الاختراق من عدمه.
- مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة المعلوماتية.
- مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.
- يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الاستدلالات لشل فعالية الجاني في أن يقوم بطريقة ما بمحو أثار جريمته.
- فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها ، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون استخدامها لطمس البيانات.
- التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنهمن الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتف مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتقليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.
- تصوير الأجهزة المستخدمة من الأمام والخلف لإثبات بأنها كانت تعمل[1].

ب- الإجراءات التي يجب مراعاتها أثناء التحقيق:

- عمل نسخة احتياطية من الأقراص الصلبة قبل استخدامها والتأكد فنيا من دقة النسخ عن طريق الأمر (diskcomp).
- نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.

[1]- سعيداني نعيم, المرجع السابق ص 112-113.

- العمل على فحص العلاقة بين برامج التطبيق والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.
- حفظ المعدات والأجهزة التي تضبط بطريقة فنية وسليمة.
- العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلوماتي.
- أن يكون الهدف من نسخ محتوى الاسطوانة والأقراص تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات الممسوحة، وكذا معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب. [1]

ثانيا: خصائص المحقق في الجريمة الإلكترونية.

المحقق الجنائي في الجريمة الإلكترونية هو المكلف بالبحث عن الحقيقة في الجريمة الإلكترونية، والكشف عن مرتكبيها وتجميع أدلة الإدانة أو البراءة ضدهم لإحالتهم للقضاء، فالمحقق هو المكلف بتنفيذ إجراءات القانون المطبق، كل حسب اختصاصه. [2]

واذا كانت مهارات التعامل مع مسرح الجريمة والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع احد عدم توافرها لدى المحقق، إلا أنه يلزمه عند مباشرته التحقيق في الجريمة الإلكترونية معرفة العديد من الجوانب الفنية ليقوم بعملة على أحسن وجه ونذكر منها: [3]

- معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والانترنت والتي تتعلق بالجريمة المرتكبة ذلك أن افتقار ضابط الشرطة القضائية للتأهيل الكافي في الميدان التقني قد يفضي إلى إتلاف وتدمير الدليل على اعتبار أن جهله بأساليب ارتكاب الجريمة الإلكترونية يجعله يقع في

---

[1]– عدلي دحمان، سعد الدين تامر البشير، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي والعلوم الجنائية جامعة زيان عاشور الجلفة 2020 2021 ص 21.

[2]– مصطفى محمد موسى التحقيق الجنائي في الجرائم الإلكترونية مطابع الشرطة، القاهرة، ط 1، 2008، ص 253.

[3]– سعيداني نعيم المرجع السابق ص 116.

كثير من الأحيان في أخطاء من شأنها أن تؤدي إلى محو الأدلة الرقمية أو تدميرها مثل إتلاف محتويات الأقراص الممغنطة أو أوعية المعلومات التي تخزن بها البيانات.[1]

- إتباع الإجراءات الصحيحة والمشروعة من اجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة، وتخزينها في الأقراص المعدة لذلك ومنع حذفها.[2]

- معرفة الإشكال المختلفة للملفات وتطبيقات الحاسوب الرئيسية، فالملفات تعتبر الوعاء الحقيقي لأدلة الإدانة في الكثير من القضايا المتعلقة بشبكة الانترنت وبما تحتويه من معلومات. [3]

- أن يكون المحقق على معرفة بالأساليب المستخدمة في ارتكاب الجرائم المعلوماتية وتقنيات الأمن المعلوماتي لأنها من الأمور التي تساعده في معرفة الجناة ومواقع ارتكاب الجريمة ومن أي طرفية الكترونية صدر السلوك الإجرامي.[4]

المطلب الثاني:إجراءات الحصول على الأدلة.

إن تطور التقني الذي لحق نظام المعالجة الآلية فضلا على الطبيعة الخاصة للدليل الرقمي سيؤدي حتما إلى تغيير كثير من المفاهيم السائدة حول إجراءات وطرق الحصول عليها، وهو الأمر الذي يحتاج بالضرورة إلى إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية فضلا على استحداث قواعد إجرائية تتلاءم مع طبيعة البيئة التقنية فتطور الإثبات ووسائله أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم،[5] وهو الأمر الذي سنسلط علية الضوء في هذا المطلب من خلال دراسة إجراءات جمع الأدلة التقليدية والمألوفة في الفرع الأول ثم في الفرع الثاني سنحاول عرض الإجراءات المستحدثة في استخلاص الدليل في الجرائم الإلكترونية.

---

[1]- جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي والتكنولوجي الحديثة دار النهضة العربية القاهرة، 2022 ص 115.

[2]- يوسف جفال،المرجع السابق ،ص 24.

[3]- خالد علي نزل الشعار التحقيق الجنائي في الجرائم الإلكترونية رسالة الدكتورة في الحقوق جامعة المنصورة، ص 43.

[4]- سعيداني نعيم، المرجع السابق، ص 117.

[5]- يوسف جفال، المرجع السابق ص 30.

الفرع الأول: الإجراءات التقليدية لجمع الأدلة

اعتمدت الجزائر في البداية على النصوص الجزائية القائمة بمختلف فروعها الموضوعية والإجرائية وذلك من اجل معاقبة الجاني[1] والتي تتمثل في: المعاينة، التفتيش، الضبط، الشهادة، الخبرة.

أولا: المعاينة

يقصد بها المشاهدة والرؤية بالعين لمكان أو شخص أو شيء له علاقة بالجريمة لإثبات حالته والآثار المادية التي خلفها ارتكاب الجريمة الإلكترونية، وضبط كل ما يلزم ويفيد من الأشياء لكشف الحقيقة عن الجريمة الإلكترونية ومرتكبيها بهدف المحافظة على الأدلة التقنية من التلف أو المحو أو التعديل. [2]

ولقد أشار المشرع الجزائري إلى إجراء المعاينة في المادة 79 من قانون الإجراءات الجزائية بقولها:"يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة...."[3] قد تكون المعاينة إجراء تحقيق أو استدلال يستهدف إظهار الحقيقة في واقعة يبلغ أمرها إلى السلطات المختصة بحيث لا تتوقف طبيعتها على صفة من يجريها بل على ما يقتضيه إجراؤها من مساس بحقوق الأشخاص، فإذا تم إجراء المعاينة في مكان عام كانت إجراء استدلال،أما إذا اقتضت دخول حرمة مسكن خاص كانت إجراء تحقيق.[4]

والمعاينة جوازيه للمحقق شانها شان سائر إجراءات التحقيق فهي متروكة إلى تقديره سواء طلبها الخصوم أو لم يطلبوها وتتمتع المعاينة في مجال كشف غموض الجريمة المعلوماتية بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية. [5]

---

[1]– د. فلاح عبد القادر، د. ايت عبد المالك ناديه،المرجع السابق ص 1697.

[2]– فهد عبد الله عبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الاسكندرية 2016، ص 241.

[3]– المادة 79 من القانون رقم 18–06 المؤرخ في 10 جوان 2018 يتضمن تعديل قانون الإجراءات الجزائية ج ر العدد 34.

[4]–أمير فرج يوسف الجرائم المعلوماتية على شبكة الانترنت دار المطبوعات الجامعية الإسكندرية 2008 ص 219–220.

[5]– خالد ممدوح ابراهيم فن التحقيق الجنائي في الجرائم الإلكترونية المرجع السابق ص151.

وهذا ما قضت به أحكام المواد 42، 79، 80 من ق .إ .ج .ج على أن المعاينة تجري أما من طرف قاضي التحقيق وذلك بعد إخطار وكيل الجمهورية الذي له الحق في مرافقته، وكما يمكن تمديد اختصاص قاضي التحقيق إذا اقتضت ضرورة الحالة إلى دوائر اختصاص المحاكم المجاورة،ويمكن أن يتم إجراء المعاينة من طرف ضباط الشرطة القضائية الذين عليهم إخطار وكيل الجمهورية فور وصول خبر الجريمة إلى علمهم وانتقالهم بدون تمهل إلى أماكن الواقعة الإجرامية.[1]

لتحقيق المعاينة لابد من إتباع الإجراءات التالية:

- تصوير أجهزة الكمبيوتر المضبوطة بمحل ارتكاب الجريمة والأجهزة الطرفية المتصلة بها، مع التركيز بصفة خاصة على الأجزاء الخلفية للكمبيوتر وملحقاته ومراعاة تسجيل وقت وتاريخ ومكان التقاط كل صورة.
- ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عملية المقارنة والتحليل عند عرض الأمر فيما بعد على القضاء.
- إثبات ما قد يعثر علية بسلة المهملات من أوراق ملقاة أو ممزقة و الشرائط و الأقراص الممغنطة لفحصها ورفع البصمات. [2]

ثانيا: التفتيش.

يعتبر هذا الإجراء من أهم الإجراءات لأنه يمس حق الإنسان في احترام شخصيته كإنسان.[3] التفتيش في قانون الإجراءات هو البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة منها وعن مرتكبيها وقد يقتضي التفتيش إجراء البحث في محل له حرمة خاصة وقد

[1]– مرابطن حياة، الجريمة الإلكترونية في التشريعة الجزائري، مذكرة لنيل شهادة الماستر في الحقوق تخصص قانون جنائي جامعة عبد الحميد بن باديس مستغانم، 2018/ 2019، ص 37.

[2]– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق ص 164.

[3]– مصطفى محمد موسى، المرجع السابق ص 190.

أحاط القانون هذا التفتيش بضمانات عديدة ومحل التفتيش أما أن يكون مسكنا أو شخصا، وهو بنوعيه قد يكون متعلقا بالمتهم أو بغيره[1].

ويشمل التفتيش المكونات المادية للحاسب الآلي التي قد تكون في مسكن المتهم أو مكان عمله. [2] ومن خلال المواد من 44 إلى 47 من ق. إ .ج . ج. بين المشرع الجزائري إجراءات التفتيش مثل الحصول على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق لإجراء التفتيش، وأن يكون التفتيش نهارا من الساعة الخامسة صباحا إلى الثامنة مساء.

كما قد نصت المادة 5 الفقرة الأولى من القانون رقم 09-04[3]:" يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية".

إن سلبية التكنولوجيا الرقمية قد عقدت من التحدي أمام أعمال التفتيش، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش، كما قد يكون الموقع الفعلي للبيانات ضمن اختصاص قضائي أخر أو حتى في بلد أخر مما يصعب عملية التفتيش.[4] ونستطيع أن نميز هذه الصور بين احتمالين على النحو الآتي:

الاحتمال الأول:اتصال حاسب متهم بحاسب أخر أو منظومة معلوماتية موجودة في مكان أخر داخل الدولة:

يتحقق هذا الاحتمال حينما يقوم المتهم بتحويل عبر الانترنت معلومات أو بيانات متعلقة بجريمة إلكترونية من حاسبه إلى حاسب أخر أو منظومة معلوماتية في مكان أخر مملوكة

[1]- امير فرج يوسف، المرجع السابق، ص 223.

[2]- د. فلاح عبد القادر د. ايت عبد المالك نادية المرجع السابق ص 1697.

[3]- انظر عن مادة 5 من القانون رقم 09-04 السابق الذكر.

[4]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 202.

لشخص أخر خلاف المتهم.[1] ولقد نص المشرع في المادة 05 الفقرة الثانية من القانون رقم 09-04 على أنه إذا كانت هناك أسباب تدعو للاعتقاد بان المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى فيجوز تمديد التفتيش بسرعة إلى هذه المنظومة بعد إعلام السلطة القضائية المختصة مسبقا بذلك[2].

الاحتمال الثاني:اتصال حاسب متهم بحاسب أخر أو منظومة معلوماتية موجودة في مكان أخر خارج الدولة.

يتحقق هذا الاحتمال حينما يقوم المجرم الإلكتروني بتخزين بيانات أو معلومات تفيد إثبات الجريمة في حاسب أو منظومة معلوماتية متواجدة خارج الإقليم الجغرافي للدولة، عن طريق شبكة الانترنت بهدف عرقلة سلطات البحث والتحري من الوصول إلى الدليل.[3]

لذا فإنه من المشاكل الحقيقية التي تواجه جهات التحقيق في جمع الأدلة حالة امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن بالتفتيش ودخوله في المجال الجغرافي لدولة أخرى، وهو ما يسمى بالتفتيش العابر للحدود، وقد يعتذر القيام به بسبب تمسك كل دولة بسيادتها وحدودها الإقليمية.[4]

وفي هذا الصدد نص المشرع الجزائري في المادة 05 الفقرة الثالثة من القانون رقم 09-04 على انه:"...إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة وفقا لمبدأ المعاملة بالمثل...."

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 204.

[2]- انظر المادة 05 من القانون رقم 09 04 السابق الذكر.

[3]- مرابطن حياة، المرجع السابق، ص 40.

[4]- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 205.

ثالثا: الضبط

الضبط هو العثور على أدلة في الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها، والضبط هو الغاية من التفتيش والنتيجة المباشرة المستهدفة، ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تنطبق بشأن التفتيش، ويؤدي بطلان التفتيش إلى بطلان الضبط.[1]

ويقصد بضبط الأدلة إجراءات جمعها، وهو الخلاصة النهائية لآلية التفتيش الذي يقصد به وضع اليد على الجريمة المتعلقة به كالأقراص الصلبة والأشرطة الممغنطة، الطباعة، البرامج اللينة، البطاقات الممغنطة وبطاقات الائتمان...[2]

والضبط بحسب الأصل،لا يرد إلا على أشياء مادية فلا صعوبة، وبالتالي بضبط أدلة الجريمة الواقعة على المكونات المادية للكمبيوتر، كرفع البصمات. مثلا عنها وكذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخة غير المشروع أو إتلافه بوسائل تقليدية كالكسر أو الحرق.

ولكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس، وفي ضبط بيانات الكمبيوتر data لعدم وجود أي دليل مرئي في هذه الحالات ولسهولة تدمير الدليل في ثواني معدودة ولعدم معرفة كلمات السر أو شفرات المرور أو ترميز البيانات[3].

وقد تبنى المشرع الجزائري في القانون رقم 09-04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المؤرخ في 05-08-2009 إجراءات مستحدثة خاصة بالضبط البيانات المعلوماتية تحت عنوان" حجز المعطيات المعلوماتية". وخص لها المواد 06، 07، 08[4].

---

[1]- مصطفى محمد موسى،المرجع السابق، ص 208.

[2]- براهيمي جمال،التحقيق الجنائي في الجرائم الإلكترونية اطروحة دكتوراه، كلية الحقوق والعلوم السياسية ،جامعة مولود معمري ،تيزي وزو، 2018 ص 46 47.

[3]- خالد ممدوح ابراهيم فن التحقيق الجنائي في الجرائم الإلكترونية المرجع السابق ص 274.

[4]- انظر المادة 06. 07. 08 من القانون رقم 09-04 السابق الذكر.

رابعا: الشهادة

الشهادة في الأصل هي اختبار الشخص بما يكون قد رآه أو سمعة بنفسه أو أدركه على وجه العموم بحواسه، ومن ثم فإن الشاهدة هي دليل مباشر في الدعوى.

وتعتبر من بين الأساليب والإجراءات التقليدية للتحقيق في الجريمة واستخلاص الأدلة عموما، ولم يتطرق المشرع الجزائري لتعريف الشهادة بل عمد إلى تنظيمها وتحديد مجالها وشروط قبولها وحجيتها في الإثبات، فهي من إجراءات التحقيق وهي الأقوال التي يدلي بها غير الخصوم أمام سلطة قضاء التحقيق بشان جريمة وقعت، سواء تعلقت تلك الأقوال بثبوت الجريمة وظهور ارتكابها وإسنادها إلى المتهم أو براءته منها.[1]

والشاهد في الجرائم الإلكترونية هو ذلك الشخص صاحب الخبرة والتخصص في تقنيات الحاسوب، والذي تكون لدية معلومات ومكاسب عن شبكات الحاسوب والاتصال والخدمات الخاصة بذلك،إذا كانت مصلحة التحقيق تقتضي البحث عن الأدلة داخلها، والشاهد الالكتروني عدة أصناف يجوز لقاضي التحقيق استدعاء من شاء منهم لسماعه.[2]

1- القائم على تشغيل الحاسوب الآلي والمعدات المتصلة به: وهو شخص لدية خبرة كبيرة في مجال تشغيل الجهاز واستخدام.

2- المبرمجون: وهم الأشخاص المختصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين هما كاتبوا برامج التطبيقات وكاتبوا برامج النظم.

3- المحللون: هم الأشخاص الذين يحللون الخطوات ويقومون بجمع بيانات النظام المعلوماتي ثم تحليلها، أي تقسيمه إلى وحدات مفصلة واستنتاج العلاقات الوظيفية بين هذه الوحدات.

[1]- مباركية رابح، اجراءات التحري والتحقيق في الجريمة الالكترونية،مذكرة ماستر في الحقوق، تخصص قانون الإعلام الآلي والانترنت، كلية الحقوق والعلوم السياسية ،جامعة محمد البشير الابراهيمي، برج بوعريريج، 2022/2021، ص 71.

[2]- مباركية رابح، المرجع السابق، ص 72.

4- مهندسو الصيانة والاتصالات: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الكمبيوتر بمكوناته وشبكاته.

5- مديريو النظام: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[1].

خامسا: الخبرة

تعتبر الخبرة من بين أهم الإجراءات التي ينبغي الاهتمام بها في إطار التحقيق في الجريمة الإلكترونية، وذلك راجع إلى صعوبة التعامل مع هذا النوع من الجرائم وعدم الدراية بمجالاتها التقنية و المعرفية و الفنية.[2]

الخبرة القضائية هي إجراء التحقيق يعهد به القاضي إلى شخص مختص ينعت بالخبير، تتعلق بواقعة أو وقائع مادية يستلزم بحثها أو تقديرها إبداء رأي يتعلق بها علما أو فنا لا يتوافر في الشخص العادي ليقدم له بيانا أو رأيا فنيا لا يستطيع أن المحقق الوصول إليه وحده.[3]

ومن المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة الإلكترونية ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات وكذلك إعداد البرمجيات وتشغيل الحاسب الآلي وعلومه، وأن نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة هؤلاء الخبراء، وكذا يجب على المحقق الجنائي أن يحدد للخبير الإلكتروني دورة في المسالة الانتداب فيها على وجه الدقة.[4]

والخبير في الجريمة الإلكترونية هو الفني المتخصص وصاحب الخبرة في التقنية الإلكترونية وشبكاتها، والذي يكون قد رأى أو سمع أو أدراك بحواسه معلومات هامة لازمة

---

[1]- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 264.

[2] - رابح وهيبة، الجريمة المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية كلية الحقوق و العلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم ، العدد4، ديسمبر 2014، ص328.

[3]- خالد ممدوح ابراهيم، نفس مرجع، ص 283.

[4]- بخي فاطمة الزهراء، اجراءات التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، 2013/ 2014، ص 89.

للدخول في نظام المعالجة الآلية الرقمية للبيانات، إذا كانت مصلحة التحقيق تقتضي البحث عن الدليل الرقمي داخلة ويمثل الخبراء الإلكترونيون فيما يلي[1]:

-المبرمجون، المحللون، مهندس الصيانة والاتصالات، مشغل الحاسب الآلي وشبكاته، مدير النظام المعلوماتي، وقد سبق التعرف عليهم في العنصر السابق.

الفرح الثاني: الإجراءات الحديثة لجمع الأدلة

كان لتطور أساليب ارتكاب الجريمة الإلكترونية وأخذها منحنى تصاعديا بين الجرائم المرتكبة في الجزائر، وهو ما فرض على المشرع الاعتماد على قواعد إجرائية خاصة في سبيل مكافحة الجريمة الإلكترونية، وهذا ما جاء به القانون رقم 06-22 [2] المؤرخ في 20 ديسمبر 2006 المتضمن قانون الإجراءات الجزائية، وتتمثل هذه الإجراءات في التسريب واعتراض المراسلات [3] وكذلك من خلال القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها تم استحداث إجراءين هما المراقبة الإلكترونية وحفظ المعطيات.

أولا: التسرب

التسرب مشتق من الفعل تسرب تسربا أي دخل و انتقل خفية وهي الولوج و الدخول بطريقة أو بأخرى إلى مكان أو جماعة. [4]

نظم المشرع الجزائري أحكام التسرب في الفصل الخامس من قانون الإجراءات الجزائية من المادة 65 مكرر 11 إلى 65 مكرر 18، حيث بين كيفية القيام بعملية التسرب وكذا شروط القيام بهذا الإجراء، وكذلك الأحكام الجزائية لمن تسبب في الكشف عن هوية الضابط أو العون

---

[1]- مصطفى محمودي موسى، المرجع السابق، ص 172.

[2]- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66 155 المؤرخ في 8 جوان 1966 والمتضمن قانون الإجراءات الجزائية، ج ر، العدد 84.

[3]- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير في العلوم القانونية كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر باتنة، 2012/2011، ص 106.

[4] - رابحي عزيزة، المرجع السابق، ص296.

المتسرب، ويتم الاستماع إلى الضابط المتسرب بوصفه شاهدا عن الجرائم المرتكبة بعد انتهاء المهلة المحددة في رخصة التسرب [1].

ولقد عرف المشرع الجزائري التسرب في المادة 65 مكرر 12 من القانون رقم 06-22 السابق الذكر بقولها:" يقصد بالتسرب قيام ضابط أو عون 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 أو عون 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 تحريضا على ارتكاب الجرائم.[2]

ويستعمل الضابط أو العون هوية مستعارة إذا ما ارتبط البحث والتحري بواحدة من هذه الجرائم:

- جرائم المخدرات.
- الجريمة المنظمة العابرة للحدود الوطنية.
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- جرائم تبييض الأموال.
- الجرائم الموصوفة بأفعال إرهابية أو تخريبية.
- الجرائم المتعلقة بالتشريع الخاص والصرف وجرائم الفساد. [3]

من بين شروط صحة التسرب:

- صدور إذن من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، وهذا ما أوردته المادة 65 مكرر 11 من قانون الإجراءات الجزائية: "...يجوز لوكيل الجمهورية أو

[1]- يوسف جفال،المرجع السابق، ص 36.

[2]- انظر المادة 65 مكرر 12 من قانون الإجراءات الجزائية.

[3]- يوسف جفال،المرجع السابق، ص 37.

لقاضي التحقيق بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبينة في المواد أدناه".

- أن يكون الإذن مكتوبا و مسببا.
- يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الأجراء وهوية ضابط الشرطة.
- يحدد في الإذن مدة عملية التسرب الذي لا يمكن أن تتجاوز أربعة أشهر[1].

ثانيا: اعتراض المراسلات الالكترونية.

لقد نظم المشرع جزائري أحكام اعتراض المراسلات في الفصل الرابع من قانون الإجراءات الجزائية في المواد من 65 مكرر 05 إلى 65 مكرر 10 تحت عنوان " في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور".

وقد اعتبر المشرع مراقبة المراسلات بأنها:"اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض[2]."

فبموجب المادة 65 مكرر 5 من قانون الإجراءات الجزائية يجوز لقاضي التحقيق أن يأمر ضابط الشرطة القضائية بترخيص كتابي، وتحت إشرافه مباشرة للقيام باعتراض المراسلات التيتم عن طريق وسائل اتصال السلكية واللاسلكية، ووضع الترتيبات التقنية دون موافقة الشخص المعني من أجل القيام بالتقاط وتثبيت وبث وتسجيل الكلام في سرية من طرف أي شخص وفي أي مكان عام أو خاص والتقاط الصور ولكل شخص.[3]

وهذا ما جاء به القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في المادة 02 من الفقرة "و" في تعريفة للاتصالات

[1]- انظر المادة 65 مكرر 15 من قانون الإجراءات الجزائية.

[2]- بن نعوم خالد أمين، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر في الحقوق كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم، 2018/ 2019، ص 96.

[3]- قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائري، مذكرة ماجيستر في الحقوق كلية الحقوق والعلوم السياسية جامعة قاصدي مرباح ورقلة، 2013/ 2014، ص 27.

الالكترونية :"بأنها تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية."[1]

وتجدر الإشارة في هذا الصدد إلى أن المراسلات التي يمكن اعتراضها يجب أن تتسم بالخصوصية ولكي تكون كذلك يلزم أن يتوفر فيها عنصران أساسيان هما:

- عنصر موضوعي يتعلق بموضوع ومضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي وسري.
- عنصر شخصي والمراد به إرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالاطلاع على مضمون الرسالة.

وعند توفر هذان العنصران في الرسالة فإنها تتصف بالمراسلة الخاصة التي لها خصوصيتها وسريتها المحمية قانونا ولا أهمية لشكل الرسالة أو طريق نقلها وتوصيلها إلى المرسل إليه.

لا يمكن لضابط الشرطة القضائي اللجوء إلى اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي[2].

ثالثا: المراقبة الالكترونية

تعد الرقابة على الاتصالات الإلكترونية أو كما يطلق عليها بمصطلح " المراقبة الإلكترونية للاتصالات" من أهم مصادر التحري التي يستعان بها في التقصي على مختلف الجرائم بما في ذلك الجرائم المتصلة بالتكنولوجيا الحديثة، خاصة في ظل لجوء الجناة إلى وسائل التقنية

[1]– أنظر المادة 02 من القانون رقم 09-04 السابقة الذكر.

[2]– يوسف جفال،المرجع السابق ص 39.

الحديثة للاتصال في تنفيذ مخططاتهم الإجرامية والتواصل فيما بينهم، كما تعد مراقبة الاتصالات الإلكترونية مصدرا لأدلة الرقمية.[1]

من خلال استقراء نصوص القانون رقم 09-04 السابق الذكر، نجد أن المشاريع الجزائري لم يعرف صراحة المراقبة الإلكترونية وتركها للفقه الذي عرفها بأنها عبارة عن عمل امني أساسي له نظام معلومات إلكتروني يقوم فيه المراقب بالمراقبة بواسطة الأجهزة الإلكترونية وعبر شبكة الانترنت لتحديد غرض محدد وإفراغ النتيجة في ملف الكتروني[2].

إلا إننا يمكن أن نعرفها على أساس أنها إجراء تحقيق يباشر الجلسة وتنتهك فيه سرية الإحداث الخاصة تأمر السلطة القضائية في الشكل المحدد قانونيا بهدف الحصول على دليل غير مادي للجريمة المعلوماتية ويتضمن من ناحية استراق السمع إلى الأحاديث من ناحية أخرى حفظة بواسطة أجهزة متخصصة لذلك.[3]

ونجد بان المشرع ومن خلال القانون رقم 09-04 في المادة 03 منة حدد كيفية مراقبة الاتصالات الإلكترونية على النحو التالي:" مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"[4].

وبالتالي فإن مراقبة الاتصالات حددها القانون على السبيل الاستثناء وفي الحالات المحددة حصريا في المادة 04 من القانون رقم 09-04السالفة الذكر[5]

---

[1]- عيدة بلعابد،خصوصية التحقيق في الجريمة المعلوماتية، مجلة الباحث الاكاديمي في العلوم القانونية والسياسية جامعة مولاي الطاهر، سكيكدة ،العدد 06، 2011، ص 145.

[2]- د. فلاح عبد القادر، د. ايت عبد المالك نادية،المرجع السابق ص 1699.

[3]- بوشعرة امينه، موساوي سهام، المرجع السابق، ص 81.

[4]- انظر المادة 03 من القانون رقم 09-04 السابق الذكر.

[5]- بوشعرة أمينة، موساوي سهام، المرجع السابق، ص 82.

رابعا: حفظ المعطيات

يمكن اعتبار الحفظ على المعطيات الإلكترونية بأنه قيام مزودي خدمات الاتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة وحفظها وحيازتها في أرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل قصد تمكين جهات الاستدلال من الاستفادة منها واستعمالها لأغراض التحقيق. فعملية الحفظ إذا هي من مهام مقدمي الخدمات.[1]

وقد حصر المشرع الجزائري المعطيات الإلكترونية الواجب حفظها من طرف مزودي الخدمة وهي المعطيات المتعلقة بحركة السير (معطيات المرور) وقد عرفتها المادة 02 من القانون رقم 09-04 في الفقرة "ه" بأنها:" أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة".[2]

ومن ضمن معطيات المرور التي يتعين على مقدمي الخدمات التحفظ عليها بطلب من السلطات القضائية المختصة لأغراض التحقيق[3]تلك التي حددها المشرع في المادة 11 من القانون رقم 09-04 على النحو التالي:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال(كرقم التسلسلي لجهاز الاتصال ونوعه).
- الخصائص التقنية وكذا تاريخ ووقت ومدة الاتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

---

[1]- براهيمي جمال، المرجع السابق، ص 101.

[2]- انظر المادة 02 من القانون رقم 09-04 السالف الذكر.

[3]- براهيمي جمال، المرجع السابق، ص 103.

– المعطيات التي تسمح بالتعرف على المرسل والمرسل إليهم كأرقام الهواتف مثلا وكذا عناوين المواقع المطلع عليها.[1]

[1]– انظر المادة 11 من القانون رقم 09 04 السالف الذكر.

الخاتمة

وبناء على ما سبق نلاحظ بأنها بالرغم مما رتبته الانترنت من مزايا في شتى المجالات الحياة، إلا أنها كما هو شأن كل اكتشاف واختراع جديد أدت إلى ظهور مشاكل قانونية دعت الدول إلى البحث عما إذا كانت القوانين القائمة كافية لمواجهة بعض الاستعمالات السيئة وغير المشروعة للانترنت أم انه يتعين مواجهتها بنصوص تجريمية جديدة كما نجد أن الجريمة الإلكترونية لا تستخدم الوسائل التقنية الحديثة كوسيلة اتصال بين المجرمين؛إنما تعدت ذلك وأصبحت تستخدم كأداة للجريمة ووسيلة لتنفيدها بشكل مباشر.

وفي هذا الشأن، فقد حرص المشرع الجزائري على مواكبة النهضة التكنولوجية والمعلوماتية التي يعيشها العصر الحالي؛ حيث أحدث بعض التعديلات في بعض النصوص القانونية العقابية كقانون رقم 04-15 والقانون 06-23 المتضمن قانون العقوبات، وكدا القانون 06 -22 والقانون رقم 18- 06 المتضمن قانون الإجراءات الجزائية، كما تم سن قوانين خاصة في القانون رقم 09- 04 المتضمن القواعد الخاصة الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها.

من خلال هذه الدراسة والبحث توصلنا إلى النتائج التالية:

- بالنظر لحداثة هذه الظاهرة الإجرامية(الجريمة الالكترونية) فإنه لا يوجد إجماع فقهي موحد حول تعريفها نظرا للاختلاف القائم حول تحديد نطاق هذه الجريمة، وفي هذا الصدد نجد بأن المشرع الجزائري وفي القانون رقم 09- 04 قد حدد نطاق الجريمة الإلكترونية بأنها الجريمة التي تمس بالنظام المعلوماتي أو بأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.
- إن هذه الجريمة أخذت في النمو والتزايد بشكل مذهل وخطير للغاية وبأنماطها الجديدة للمجرم الإلكتروني واحترافه في ارتكابها مما يجعلها تتسم بالغموض وصعوبة إثباتها والتحقيق فيها مما يطرح ذلك مسؤولية وتحديات أمام المختصين بمتابعتها.

- إن المجرم المعلوماتي يختلف عن المجرم التقليدي فهو مجرم ذكي ذو علم وكفاءة علمية وتقنية تمكنه من الإفلات من العقاب.
- لا تكفي الإجراءات التقليدية لمواجهة الجرائم الإلكترونية.
- ظهور دوافع جديدة وراء ارتكاب الجرائم الإلكترونية كتحقيق الكسب المادي وإثبات التفوق العلمي والتسلية.
- قيام المشرع الجزائري بتجريم بعض الأفعال و السلوكيات المتعلقة بالجريمة الإلكترونية من خلال تعديل قانون العقوبات، وكذا استدراكه للفراغ القانوني في المجال الإجرائي فقام بسن قانون جديد متعلق بهذه الظاهرة حيث تضمن قواعد و أحكام جزائية ووقائية وهو القانون رقم09-04.
- إغفالا لمشرع الجزائري لبعض الجرائم الإلكترونية كجريمة التزوير المعلوماتي التي أخضعها للنصوص التقليدية الخاصة بتزوير المحرر، كما أنه لم يوسع من مفهوم المحرر ليشمل المستند المعلوماتي.

من خلال هذه النتائج التي أظهرتها دراستنا يمكننا تقديم بعض التوصيات والاقتراحات :

- ضرورةإعطاء تعريف موحد واسع وشامل الجريمة الإلكترونية.
- إعادة النظر في بعض القوانين والنصوص الجزائية الجزائرية التي لها علاقة بالجرائم الإلكترونية والتوسيع من نطاقها نظرا لتفاقم وتطور هذه الظاهرة الإجرامية.
- تأهيل أفراد الضبطية القضائية والنيابة العامة على كيفية التعامل ومواجهة هذا النوع من الجرائم.
- على الجزائر الدخول وإبرام اتفاقيات عربية ودولية في مجال مكافحة الجرائم الإلكترونية من أجل الاستفادة من تجارب باقي الدول وكدا تبادل المعلومات.

- تنظيم حملات توعية للمجتمع وخاصة مستعملي الوسائط المعلوماتية وفئة الشباب وتعريفهم بهذه الظاهرة الإجرامية وخطورتها، وإخبارهم بأن هذه الجرائم ما هي إلاأفعال غير مشروعة وغير قانونية وتعرض مرتكبيها إلى العقوبات جزائية.
- ضرورة إبلاغ ضحايا الجرائم المعلوماتية الجهات المختصة من أجل متابعة مرتكبي هذه الجرائم.
- ضرورة إنشاء فروع أو مقاييس جديدة في كليات الحقوق لدراسة هذا الموضوع بتعمق مثل ما يسمى بالحماية القانونية المعلوماتية أو مقياس بعنوان الجرائم الالكترونية.
- تخصيص شرطة خاصة لمكافحة الجرائم الإلكترونية وذلك من الشرطة المدربين على كيفيه التعامل مع أجهزة الحاسوب والانترنت.

قائمة المصادر والمراجع

أولاً: النصوص التشريعية التنظيمية:

❖ **النصوص التشريعية:**

1. التعديل الدستوري لسنة 2020، المصادق عليه في استفتاء أول نوفمبر سنة 2020، الصادر بتاريخ 30 ديسمبر 2020، الجريدة الرسمية، العدد 82.
2. رقم 04-15 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66-155 الصادر في 08 جوان 1966، المتضمن قانون العقوبات الجزائري، الجريدة الرسمية، العدد71.
3. القانون رقم 06-23 المؤرخ في 20ديسمبر2006، يعدل ويتمم الأمر رقم 66-155 الصادر في 08 جوان، المتضمن قانون العقوبات الجزائري، الجريدة الرسمية، العدد 84.
4. القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 66-156 الصادر في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية، العدد84.
5. لقانون رقم 08-01 المؤرخ في 23يناير2008، يتمم القانون رقم 83-11 المؤرخ في 02 يونيو 1983 والمتعلق بالتأمينات الاجتماعية، الجريدة الرسمية، العدد 04.
6. القانون رقم 09-04 المؤرخ في 05 أغسطس 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيات الإعلام و الاتصال ومكافحتها، الجريدة الرسمية، العدد 47.
7. القانون رقم 15-04 المؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع و التصديق الإلكترونيين، الجريدة الرسمية، العدد 06.
8. القانون رقم 18-04 المؤرخ في 10 ماي 2018، يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية، الجريدة الرسمية، العدد 27.
9. القانون رقم 18-06 المؤرخ في 10 جوان 2018،يعدل ويتمم الأمر رقم 66-155 المؤرخ في 08 جوان 1966 و المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد 34.
10. القانون رقم 18-07 المؤرخ في 10 يونيو 2018 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، العدد 34.

الأوامر:

11. الأمر رقم 03-05 المؤرخ في 19 جويلية 2003 المتعلق بحقوق المؤلف و الحقوق المجاورة، الجريدة الرسمية ، العدد 44.

12. الأمر رقم 03-07 المؤرخ في 19 جويلية 2003 يتعلق ببراءة الإختراع، الجريدة الرسمية، العدد 44.

❖ **النصوص التنظيمية:**

المراسيم:

13. المرسوم رئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحاتها، الجريدة الرسمية، العدد 53 الصادرة في 18 أكتوبر 2015 .

14. المرسوم الرئاسي رقم 14 -252 المؤرخ في 08 سبتمبر 2014،الجريدة الرسمية، العدد 57.

ثانيًا: الكتب:

❖ **الكتب العامة:**

15. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للطباعة والنشر والتوزيع، الجزائر، ط 10، 2010 .

16. أحسن بوسقيعة ، الوجيز في القانون الجزائي العام، دار هومة للطباعة و النشرو التوزيع، الجزائر، ط13 ن 2013

17. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة للطباعة و النشر و التوزيع، الجزائر، ط18، 2019.

❖ **الكتب المتخصصة:**

18. احمد خليفة الملط، الجريمة المعلوماتية، دار الفكر الجامعي، الاسكندرية، الطبعة 2، 2006.

19. آمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري ،دار هومة، الجزائر ،الطبعة الثانية، 2007 .

20. أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت ،دار المطبوعات الجامعية الإسكندرية، 2008 .

21. براء منذر عبد اللطيف، شرح قانون المحاكمات الجزائية، دار حامة للنشر والتوزيع، عمان، الطبعة الأولى، 2009 .

22. بوكر رشيدة ،جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية ،الطبعة الأولى، 2012 .

23. جميل عبد الباقي الصغير ، أدلة الإثبات الجنائي والتكنولوجيا الحديثة دار النهضة العربية، القاهرة، الطبعة الأولى،2012.

24. خالد ممدوح إبراهيم ،الجرائم المعلوماتية، دار الفكر الجامعي، الاسكندرية، الطبعة الأولى، 2009.

25. خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي ،الإسكندرية (مصر)، الطبعة الأولى، 2009.

26. زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدوري ،دار الهدى للطباعة والنشر، الجزائر،2011.

27. سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، الإسكندرية، 2007،

28. سعدي سليمة، حجاز بلال، جرائم المعلومات و الشبكات في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2017.

29. عبد الصبور عبد القوي علي مصري،الجريمة الالكترونية، دار العلوم للنشر والتوزيع ،القاهرة،الطبعة الأولى ، 2008.

30. عبد الفتاح بيومي حجاز، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الأنترنت، دار الكتب القانونية ، الطبعة الأولى.

31. عبد الفتاح بيومي حجاز، جرائم الكومبيوتر والأنترنت في التشريعات العربية، دار النهضة العربية، القاهرة، 2009.

32. عبد الفتاح بيوني حجاز، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الكتب القانونية، مصر، 2007.

33. عفيفي كامل عفيفي، فتوح الشادلي، جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة و القانون، الإسكندرية، 2000.

34. عميمر عبد القادر، التحديات القانونية لإثبات الجريمة المعلوماتية، النشر الجامعي الجديد، تلمسان، الجزائر ، 2021.

35. فهد عبد الله عبد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة ،الإسكندرية، 2016 .

36. محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، 2004.

37. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، القاهرة، الطبعة الأولى، 2008.

38. ناني لحسن، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، تلمسان، الجزائر، السداسي الأول 2018 .

39. نسرين عبد الحميد نبيه،الجريمة المعلوماتية والمجرم المعلوماتي، منشأة، الاسكندرية، 2008 .

40. نهلا عبد القدر المومني، الجرائم المعلوماتية، دار الثقافة، عمان، الطبعة 02، 2010.

41. الينا محمد الاسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية دراسة مقارنة ،دار حامد للنشر والتوزيع، عمان،الطبعة الأولى، 2015.

ثالثًا: أطروحات الدكتوراه و الماجيستر و المذكرات:

42. ي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، الجزائر ، 2013/ 2014.

43. بدري فيصل، مكافحة الجريمة معلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة الدكتوراه علوم في القانون، تخصص قانون عام، كلية الحقوق والعلوم السياسية، جامعه الجزائر 1،الجزائر ، 2017 -2018

44. براهيمي جمال،التحقيق الجنائي في الجرائم الإلكترونية،أطروحةلنيل شهادة دكتوراه في العلوم، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر ، 2018 .

45. برمش مراد،خصوصية الجريمة الالكترونية أطروحة لنيل شهادة الدكتوراه، علوم في القانون الخاص،فرع الملكية الفكرية،جامعة الجزائر -1-بن يوسف بن خدة، كلية الحقوق، الجزائر، 2021/2020 ص 50.

46. بن نعوم خالد أمين، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس مستغانم،الجزائر، 2018/ 2019.

47. بوشعرة أمينة، وموساوي سهام ،الإطار القانوني للجريمة الإلكترونية دراسة مقارنة، مذكرة لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية،كلية الحقوق و العلوم السياسية، جامعة عبد الرحمان ميرة، بجاية،الجزائر، 2017-2018.

48. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجيستر في العلوم القانونية، تخصص علم الإجرام والعقاب، كلية الحقوق و العلوم السياسية ،جامعة باتنة، الجزائر،2011-2012.

49. خالد علي نزال الشعار، التحقيق الجنائي في الجرائم الإلكترونية، رسالة دكتوراه في الحقوق، جامعة المنصورة ، الجزائر.
50. ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه في الحقوق ، كلية الحقوق و العلوم السياسية ،جامعه باتنة، الجزائر، 2016/2015 .
51. رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الانترنت، مذكرة لنيل شهادة الماجستير في القانون العام،كلية الحقوق و العلوم السياسية، جامعةأبو بكر بلقايد، تلمسان،الجزائر، 2011 -2012.
52. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجيستر في العلوم القانونية ، تخصص علوم جنائية، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2013/2012.
53. سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الاجرام، كلية الحقوق و العلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، الجزائر، 2011-2010.
54. عدلي دحمان و سعد الدين تامر البشير، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر في الحقوق، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق و العلوم السياسية، جامعة زيان عاشور، الجلفة، الجزائر،2020-2021.
55. عزيزة رابحي،الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعةأبو بكر بلقايد، تلمسان ،الجزائر 2018 .
56. قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائري، مذكرة ماجيستر في الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر ، 2013/ 2014.

57. غربي جميلة، أليات مكافحة الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق و العلوم السياسية ،جامعة أكحلي محند أولحاج، البويرة،الجزائر ، 2021/2020.

58. فتيحة مهري ،جريمة الدخول والبقاء إلى أنظمة المعالجة الآلية للمعطيات، مذكره لنيل شهادة الماستر، تخصص قانون جنائي للأعمال، كلية الحقوق والعلوم السياسية،جامعة العربي بن مهيدي، ام البواقي ، الجزائر، 2015/ 2016 .

59. مباركية رابح، إجراءات التحري والتحقيق في الجريمة الالكترونية،مذكرة ماستر في الحقوق، تخصص قانون الإعلام الآلي والانترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الابراهيمي، برج بوعريريج، الجزائر،2022/2021.

60. مرابطن حياة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي و علوم جنائية ،كلية الحقوق و العلوم السياسية ، جامعة عبد الحميد بن باديس، مستغانم،الجزائر، 2018/ 2019.

61. مسعود شهيرة، الجريمة الالكترونية في التشريع الجزائري،مذكره لنيل شهادة الماستر في القانون، تخصص قانون جنائي وعلوم جنائية،كلية الحقوق والعلوم السياسية، جامعه عبد الحميد بن باديس، مستغانم، الجزائر ،2020 / 2021 .

62. معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة العقيد الحاج لخضر، باتنة، الجزائر ،2012/2011.

63. نايري عائشة ،الجريمة الالكترونية في التشريع الجزائري،مذكره لنيل شهادة الماستر في القانون الاداري ، كلية الحقوق و العلوم السياسية ، جامعة أحمد دراية ، أدرار ، الجزائر ، 2016-2017

64. نسيمه جدي، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة ماجستر في القانون، كليه الحقوق والعلوم السياسية، جامعه وهران، الجزائر،2014 .

65. نعمان عبد الكريم، الجرائم الإلكترونية وموقف المشرع الجزائري منها، رسالة لنيل شهادة الماجستر في القانون الجنائي،كلية الحقوق و العلوم السياسية، جامعة الجزائر1، يوسف بن خدة، 2017/2016.

66. يوسف جفال، التحقيق في الجريمة الالكترونية، مذكرة لنيل شهادة الماستر أكاديمي في الحقوق، تخصص قانون جنائي، كلية الحقوق و العلوم السياسية، جامعة محمد بوضياف، المسيلة،الجزائر، 2016. 2017 .

67. قنديل نور الهدى، جرائم إفشاء الأسرار في مجال المعلوماتية، مذكره لنيل شهاده الماستر في الحقوق، تخصص قانون عام ، كلية الحقوق والعلوم السياسية ، جامعه الجيلالي ليابس، سيدي بلعباس ، الجزائر، 2018 2019 .

رابعًا: المداخلات:

68. راضية بركابل "التنظيم القانوني الجزائري للجريمة المعلوماتية في التشريع الجزائري"، الملتقى الوطني حول الأمن المعلوماتي مهدداته وسبل الحماية، جامعة مولود معمري، تيزي وزو، الجزائر، 03-04 نوفمبر 2015.

69. عبد الله حسين محمد، إجراءات جمع الأدلة في الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي ، 26-28 ابريل 2003.

70. فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر الجريمة الالكترونية، طرابلس، بتاريخ 24-25 مارس 2017.

71. مفتاح أبوبكر المطرودي، الجريمة الإلكترونية والتغلب على تحدياتها ورقة مقدمة إلى المؤتمرات الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 23-2021/09/25.

خامسًا: المجلات:

72. إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الالكترونية، مجلة أفاق للبحوث والدراسات، المركز الجامعي، إيليزي 5الجزائر– العدد04، جوان 2019

73. بوضياف اسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، العدد 11، سبتمبر 2018.

74. حمود بن محسن الدعجاني، الجريمة الإلكترونية دراسة فقهية تطبيقية، مجلة الجامعة الإسلامية، ملحق العدد، 183، ج16.

75. سامي حمدي عبد المومن ود.قيرة سعاد، الجريمة الإلكترونية واليات التصدي لها في القانون الجزائري، مجلة البيان للدراسات القانونية، المجلد 07، العدد01، ص59– 70، جوان 2022.

76. سعيد بوزنون, مكافحةالجريمة الالكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد 30، العدد 3، ديسمبر 2019 .

77. شيخ سناء، شيخ محمد زكرياء، بحث حول مكافحة الجرائم الالكترونية في القانون الجزائري، مجلو وميض الفكر للبحوث، العدد5، سبتمبر 2020.

78. عيدة بلعابد، خصوصية التحقيق في الجريمة المعلوماتية ، مجلة الباحث الأكاديمي في العلوم القانونية والسياسية ، جامعة مولاي الطاهر، سعيدة ، الجزائر ،العدد 06 ،2011.

79. فلاح عبد القادر، د. ايت عبد المالك نادية،التحقيق الجنائي للجرائم الالكترونية وإثباتها في التشريح الجزائري، مجلة الأستاذة الباحث للدراسات القانونية والسياسية، المجلد 4، العدد 2, 2019 .

80. مولاي أبراهيم عبد الحكيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، جامعة زيان عاشور، الجلفة(الجزائر)، العدد 23 ، المجلد الثاني، جوان 2015.

81. بوهرين فتيحة، الجريمه الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم الانسانية، جامعة قسنطينة 02،الجزائر، العدد 04، المجلد 14، نوفمبر 2021 .

سادسًا: مواقع الأنترنت:

82.نسرين محفوف، تاريخ النشر 2022/01/19، https://www.ennaharoline.com تاريخ الدخول 20-02-2013، بتوقيت 19:38.

83.هدى أبوبكر، اعرف ما هي العقوبات الأصلية والتبعية في القانون، القاهرة 12 ديسمبر 2019، عن الموقع الالكتروني https//ww.youm7.com تاريخ الدخول 23-03-2023، بتوقيت 02 :14.

سابعًا: الإتفاقيات:

84.اتفاقيةبودابستالاتفاقية الاوروبية المتعلقه بالجرائم المعلوماتيه رقم 185 المصادقة عليها في 2001/11/23.

85.الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ،القاهرة،2010.

فهرس
المحتوى

فهرس المحتوى

الملخص:

إزاء التطور التكنولوجي الذي شهده العالم في الآونة الأخيرة، ظهرت بعض الجرائم المستحدثة، والتي يستخدم فيها الحاسب الآلي والأنترنت كأداة لارتكاب الأفعال غير المشروعة.

فالجرائم المعلوماتية تعتبر من اعقد الجرائم وأخطرها في الوقت الحالي، نظرًا للمميزات التي تتمتع بها هي كجريمة مستحدثة والمجرم الإلكتروني كونه يتسم بقدر عالي من الكفاءة العلمية والتقنية، مما يزيد من صعوبة ملاحقتها وإثباتها واكتشافها.

ومواكبةً لهذا التطور استحدث المشرع الجزائري قوانين لمكافحة هذه الأفعال والحد منها.

الكلمات المفتاحية: الجريمة الإلكترونية، التشريع الجزائري، المجرم الإلكتروني، المعلوماتية، تكنولوجيا الإعلام والاتصال.

ABSTRACT:

In view of the technological development that the world has witnessed recently, some new crimes have emerged, in which the computer and the Internet are used as a tool to commit illegal acts.

Information crimes are considered one of the most complex and dangerous crimes at the present time, due to the advantages that it enjoys as a new crime, and the cybercriminal being characterized by a high degree of scientific and technical competence, which increases the difficulty of prosecuting, proving and discovering it.

Keeping pace with this development, the Algerian legislator has introduced laws to combat these acts and take them seriously.

Keywords: cybercrime, Algerian legislation, cybercriminal, informatics, information and communication technology.

key words: Cybercrime, Algerian legislation, Cybercriminal, informatics, information and communication technology