الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف المسيلة

كلية: الحقوق والعلوم السياسية ميدان: الحقوق والعلوم السياسية

قسم: الحقوق فرع: الحقوق

رقم:..... تخصص: قانون جنائي

مذكرة مقدمة لنيل شهادة الماستر أكاديمي

إعداد الطالبتين:

سحنون إيمان ضيف الله إشراق

تحت عنوان:

الجريمة الالكترونية في التشريع الجزائري

لجنة المناقشة:

أ.د والي عبد اللطيف	جامعة المسيلة	رئيسا
أ.د دحية عبد اللطيف	جامعة المسيلة	مشرفا ومقررا
د مقروف محمد	جامعة المسيلة	مناقشا

السنة الجامعية: 2022/2021

بسم الله الرحمان الرحيم

﴿فَتَبَسَّمَ ضَاحِكًا مِنْ قَوْلِهَا وَقَالَ رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَىٰ وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ﴾

سورة النمل الآية 19

إهداء

إلى من أوصاني ربي خيرا بهما إلى من كانا

عونا دائما لي إلى من لا يمكن للكلمات

أن توفي حقهما الوالدين الكريمين.

إلى مصدر دعمي الذي يساعدني بالتشجيع والدعاء.

إلى كل عائلتي الصغيرة والكبيرة إلى إخوتي وأخواتي.

إلى عمتي منصورة إلى أصدقائي وزملائي اللذين احترمهم

اهدي ثمرة جهدي.

إيمان

إهــداء

أهدي ثمرة جهدي إلى الوالدين الكريمين

أطال الله في عمرهما

إلى سندي في الحياة زوجي الكريم

إلى ينابيع حياتي إخوتي وأخواتي إلى عائلة زوجي

إلى كل قريب وبعيد.

إشراق

شكر و عرفان

الشكر أولا وأخيرا لله عز وجل الذي انعم علينا بنعمة العقل والعلم.

ثم يشرفني أن أتقدم بأسمى آيات الشكر والعرفان:

إلى الأستاذ والدكتور المشرف دحية عبد اللطيف على

توجيهاته وإرشاداته القيمة.

إلى كل أساتذة قسم الحقوق كلية الحقوق والعلوم السياسية

بجامعة المسيلة وعلى رأسهم عميد الكلية الأستاذ حمزة خضري.

إلى كل من ساعدني في إتمام هذا العمل ولو بنصيحة أو بكلمة

طيبة.

قائمة المختصرات

ق إ ج	قانون الإجراءات الجزائية
ج ر	الجريدة الرسمية
ص	صفحة
ط	طبعة
ق ع ج	قانون العقوبات الجزائري

مقدمـــــة

مقدمة :

إن الجريمة ظاهرة قديمة عرفتها البشرية، حيث ارتبط لفظ الجريمة منذ ظهور الإنسان وذلك مصداقا لقوله تعالى في كتابه الكريم:﴿ ظَهَرَ الْفَسَادُ فِي الْبَرِّ وَالْبَحْرِ بِمَا كَسَبَتْ أَيْدِي النَّاسِ لِيُذِيقَهُمْ بَعْضَ الَّذِي عَمِلُوا لَعَلَّهُمْ يَرْجِعُونَ ﴾[1] ذلك أن الفساد ظاهرة سابقة لجميع الجرائم، وأنها من أشد ظواهر السلوك الإنساني من حيث خطورتها وتهديدها لأمن وسلامة الفرد والمجتمع.

والعالم في الفترة الأخيرة شهد تطورا في عالم المعلوماتية والتي فرضت نفسها في شتي الميادين، حيث أصبح تقدم الدول يقاس بالرأس المال المعلوماتي، لكن رغم الإيجابيات التي وفرها النظام المعلوماتي في العديد من المعلومات إلا أنه لا يخلو من بعض المخاطر، حيث أصبح يثير عدة مشكلات من الناحية القانونية وذلك من خلال استخدامها السيئ الذي ينتج عنه ارتكاب مجموعة من جرائم والتي تسمى بالجرائم الإلكترونية.

ومن هنا نشأت الجريمة الإلكترونية والتي يستخدم فيها الكمبيوتر بطريقة غير شرعية مثل التجسس على المعلومات الشخصية أو سرقتها وذلك عن طريق اختراق شبكة اتصالات معلوماتية أو سرقة الأموال عن طريق اختراق نظام الكمبيوتر الخاص بمؤسسة أو شركة أو مصرف معين، أو يكون الاختراق لسبب أو هدف شخصي أو سياسي أو ديني أو عسكري أو غير ذلك، والجريمة الإلكترونية من بين الجرائم الظاهرة والمنتشرة حديثا في معظم دول العالم بشكل كبير والتي لم تقتصر فقط على دول العالم الثالث كما كان مألوفا من قبل ذلك بسبب التطور التكنولوجي الحاصل في العالم الافتراضي الجديد.

[1] الآية 41 سورة الروم

أهمية الموضوع:

تبرز أهمية الموضوع في النقاط التالية:

- للموضوع أهمية من الناحية النظرية والعملية لكونه يمس كثيرا من مصالح المجتمع وكذا يعالج قضية المساس بالحياة الخاصة للأفراد .
- كما تكمن أهمية الدراسة في محاولة إيجاد الحلول للمشكلات التي تنتج عن الجريمة الإلكترونية نظرا لعدم وجود تشريع خاص لهذه الجريمة.
- وكذا تظهر أهمية هذه الدراسة من خلال استفادة الباحثين والقضاة من نتائجها وتوصياتها.

أهداف الدراسة:

تهدف هذه الدراسة إلى:

- التعريف بماهية الجريمة الإلكترونية ومحاولة التعمق في كيفية محاربتها من خلال التشريعات منها التشريع الجزائري.
- إبراز الواقع الحالي للجريمة الإلكترونية ومعرفة حجمها، أسبابها آثارها، أساليبها في العالم على وجه عام وفي الجزائر على وجه خاص.
- المساهمة في إيجاد الحلول والمشكلات العلمية والقانونية في الجرائم الإلكترونية.

- وضع ما توصلت إليه من نتائج واقتراحات بين يدي المشرع الجزائري على أمل أن نجد أذنا صاغية منه في ضرورة التدخل ووضع تشريع خاص متكامل يهدف إلى مواجهة الجرائم الإلكترونية.

أسباب اختيار الموضوع:

يرجع اختيار موضوع "**الجريمة الإلكترونية في التشريع الجزائري**" إلى العديد من الأسباب منها ما هو ذاتي وما هو موضوعي.

أسباب ذاتية:

- توعية المجتمع والأفراد بالأخطار الناجمة عن هذه الجريمة.
- رغبتي في إنجاز هذا الموضوع والذي يتعلق بواقع دراستي.

أسباب موضوعية:

- وجوب المعرفة والإطلاع على أحكام وتشريعات الجريمة.
- كثرة الجريمة الإلكترونية على الصعيد الوطني والدولي وتأثيرها على المجتمع مما يستوجب علينا دراسة جوانبها العقابية والتجريمية والتدابير المتخذة لقمع هذه الجريمة.

صعوبات الدراسة:

الباحث في "**موضوع الجريمة الإلكترونية في التشريع الجزائري**" من الممكن أن يواجه عدة صعوبات منها:

- كونه موضوع جديد تقل فيه المراجع خاصة باللغة العربية والإحصائيات الدقيقة، كما لا توجد دراسات كافية في هذا الموضوع على وجه التحديد.
- كذلك من بين أكبر الصعوبات التي واجهتنا في إعداد بحثنا هو الأزمة الوبائية بسبب فيروس كورونا الذي مرت به الجزائر والعالم ما أدى إلى غلق المكاتب الخارجية.

الدراسات السابقة :

- الدسوقي محمد دراسة بعنوان "**الحماية الجنائية لسرية المعلومات**" دار الكتب القانونية 2003 مصر: وقد تطرق في دراسته إلى ضخامة التدفق والمخزون المعلوماتي الإلكتروني وتنوعه، وقام في دراسته بتقديم اقتراح للدول العربية للانضمام لاتفاقية بودابست المتعلقة بالجرائم الإلكترونية سنة 2001 وذلك بغية توسيع نطاق التعاون العربي والدولي لمكافحة الجريمة الإلكترونية.

- أجرى رعد فجر فتيح (2017) دراسة بعنوان "**إثبات الجريمة الإلكترونية بالدليل العلمي**" في ضوء طبيعة وخصوصية الجريمة الإلكترونية وكيفية مواجهتها وإثباتها، تمحورت هذه الدراسة حول ما إذا كان بالإمكان الاكتفاء بقواعد الإثبات العادية لإثبات الجريمة الإلكترونية وتطبيق النصوص التي تتعلق بجرائم الأموال في صورتها التقليدية مثل السرقة، والنصب، وخيانة الأمانة، والإتلاف، أم أن الأمر يتطلب وضع نصوص وقواعد إثبات خاصة بها تنسجم مع طبيعتها وخصوصيتها.[2]

[1] سليمة ذياب، بلال بوترعة **الجريمة الإلكترونية الأسس والمفاهيم**، مجلة تطوير العلوم الاجتماعية العدد 1 مجلد 13، جامعة الوادي الجزائر سنة 2020 ص 11.

إشكالية الدراسة:

انطلاقا من الأفكار التمهيدية للموضوع يمكننا حصر الإشكالية العامة للدراسة في:

ما هو مفهوم الجريمة الإلكترونية وفيما تتجلى سبل مكافحتها ؟

وتتفرع عن هذه الإشكالية الرئيسية مجموعة من التساؤلات الفرعية نوردها فيما يلي:

- ما المقصود بالجريمة الإلكترونية؟
- ما هو موقف المشرع الجزائري من هذه الجريمة؟
- ما هي الآليات التي اتبعها المشرع الجزائري لمكافحة الإجرام الإلكتروني؟
- ما هي الأجهزة والهيئات المسخرة من طرف الدولة لمتابعة هذه الجرائم؟

منهج الدراسة:

ينتهج هذا البحث المنهج الوصفي التحليلي ذلك من خلال شرح مفاهيم وتسميات الجريمة الإلكترونية وكذا تحديد ماهيتها وطبيعتها وأسبابها وآثارها بأسلوب وصفي مع المنهج التحليلي الذي من خلاله حللنا المواد التشريعية والروابط والتعرف على حقيقتها وحجمها وأفضل الوسائل والآليات لمواجهتها مع إيجاد الحلول وتقديم الاقتراحات.

وللإجابة على هذه الإشكالية تم تقديم البحث إلى فصلين مقسمة على النحو التالي:

خطة الدراسة:

الفصل الأول:

والذي اندرج تحت عنوان "**مفهوم الجريمة الإلكترونية**" وبدورنا قسمناه إلى:

المبحث الأول: تعريف الجريمة الإلكترونية.

المبحث الثاني: أركان الجريمة الإلكترونية ودوافع ارتكابها.

الفصل الثاني:

والذي يتحدث عن "**مواجهة الجريمة الإلكترونية**" حيث قسمناه إلى:

المبحث الأول: المواجهة التشريعية للجريمة الالكترونية.

المبحث الثاني: المواجهة الإجرائية للجريمة الالكترونية.

الفصل الأول

مفهوم الجريمة الإلكترونية

تمهيد:

ترتب عن الاستخدام الزائد لنظم المعلومات إلى ظهور ما يسمي بالجريمة المعلوماتية أو الغش المعلوماتي، والبعض الآخر أطلق عليه اسم جرائم الحاسب الآلي وكذا الجريمة الإلكترونية، حيث تعد هذه الجريمة صنف جديد من الجرائم والمجرمين والتي اختلفت كثيرا عن الجريمة التقليدية في صورها وطبيعتها وكذا مضمونها ووسائلها التي أصبحت كلها ذات نطاق إلكتروني يصعب التعامل معه، وسنحاول التطرق في هذا الفصل إلى تعريف الجريمة الإلكترونية في المبحث الأول، والى تبيان أركان الجريمة الإلكترونية ودوافع ارتكابها من خلال المبحث الثاني.

المبحث الأول: تعريف الجريمة الإلكترونية.

من خلال هذا المبحث سنتناول مجموعة من التعريفات للجريمة المعلوماتية والتي تختلف باختلاف الآراء سواء التعريفات اللغوية والإصلاحية منها أو الفقهية والقانونية، وذلك من خلال هذين المطلبين:

المطلب الأول: التعريف اللغوي والاصطلاحي.

تعد الجرائم الإلكترونية من الجرائم التي ظهرت حديثا والتي يعتمد فاعلها على وسائل تقنية كافية باستخدام النظم المعلوماتية، حيث أنها جريمة "نتجت عن تزاوج ثورة التكنولوجيا المعلوماتية والعولمة".[1]

الفرع الأول: التعريف اللغوي للجريمة الإلكترونية.

تتكون الجريمة الإلكترونية أو الافتراضية (cyber crimes) من مقطعين هما الجريمة (crime) والإلكترونية (cyber)، ويستخدم مصطلح الإلكترونية لوصف فكرة جزء من الحاسب أو عصر المعلومات، أما الجريمة فهي السلوكات والأفعال الخارجة عن القانون.[2]

---

[1] رصاع صفيحة **الحماية الجنائية للمعلومات على شبكة الإنترنت**، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بالقائد تلمسان 2011–2012 ص 36. نقلا عن محمود صالح العادلي **الجريمة المعلوماتية(ماهيتها وصورها)** ورقة المقدمة ص 2 .

[2] ذياب البداينة **الجرائم الإلكترونية المفهوم والأسباب**، الملتقي العلمي "**الجرائم المستحدثة في ضل المتغيرات والتحولات الاقتصادية والدولية**" خلال الفترة 2/09/2014 _4 الأردن ص3.

فالجريمة الالكترونية هي تلك الجريمة التي يقصد بها المعالجة الآلية للحاسوب، والتي تكون فيها الشبكات الحاسوبية الوسيلة أو الهدف للقيام بها، كما هي نشاط إجرامي يستخدم فيه الحاسوب بياناته الرقمية لصورة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الغير مشروع به للمصلحة العامة ومصلحة الأفراد الخاصة وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.

بمعني أنها تقع على الأفراد أو المؤسسات الذين يستخدمون جهاز الحاسب الآلي أو الهواتف الذكية، لذا تعتبر فعل لا أخلاقي وغير مصرح به يرفضه المجتمع والقانون ويعاقب عليه ويدينه المشرع وبالنظر لتوسع أدوات الاتصال الحديثة بالإضافة إلى مجموعة البرامج والتقنيات المعدة سهلت عملية الجريمة الإلكترونية.[1]

الفرع الثاني: التعريف الاصطلاحي للجريمة الإلكترونية.

تعرف الجريمة على أنها تلك السلوكات والأفعال التي يقوم بها الأفراد والتي هي خارجة عن القانون،أما الإلكترونية فهو مصطلح لوصف فكرة من الحاسوب أو عصر المعلومات.

والجريمة الإلكترونية جريمة تشمل جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية والتي تعد نشأتها من التقدم والتطور الذي طرأ على التكنولوجيا.

[1] سليمة ذياب، بلال بوترعة، مرجع سابق ص 11.

لا يوجد إجماع ولا تعريف موحد للدلالة على الجريمة المعلوماتية سواء من حيث تعريفها أو ما تتضمن، وذلك لاختلاف وجهات النظر وحداثة الجرم حتى في خصوصية مرتكبها. حيث يقول دير هلست و وتيف "هناك غياب لتعريف عام وإطار نظري منسق في هذا الحقل من المعلومة ... وفي اغلب الأحيان نستخدم مصطلحات افتراضية والحاسوب والإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف".[1]

وكذا عرفت الجريمة الإلكترونية على أنها "تلك الأعمال ضد السرية والنزاهة حيث يقول المجرم المعلوماتي بهذا الجرم لغرض شخصي أو تحقيق مكسب مالي أو إحداث أضرار،"[2] هذا لأنها جريمة يستخدم فاعلها الحاسوب والمعدات النفسية وبدخول غير مصرح به لنظام الجهاز سواء الهاتف أو الحاسوب، ويكون دافعه الأساسي لارتكاب هذا الجرم إما لتحقيق مكاسب مالية أو الانتقام أو إلحاق الضرر بالضحية أو دوافع سياسية أو اقتصادية ...الخ

والجريمة الإلكترونية جريمة متجددة بصفة دائمة ومستمرة لهذا أطلق عليها جرائم التكنولوجيا الحديثة والتي تستهدف المعلومات الشخصية في نظام حاسب أو هاتف الضحية، تعمد لإيذاء سمعته أو إيذائه ماديا أو عقليا مباشرة أو غير مباشرة وذلك باستخدام الانترنت مثل رسائل الهاتف أو البريد الإلكتروني، مواقع التواصل الاجتماعي، التهديد بالصور أو فيديوهات أو تسجيلات صوتية ...الخ.

---

[1] ذياب البداينة، مرجع سابق ص03.

[2] مرجع نفسه نفس ص.

ولهذا عرفت الجريمة الإلكترونية بصفة عامة على أنها كل فعل مشروع صادر عن إرادة آثمة يقرر له القانون عقوبة أو تدبيرا احترازيا، وتعتمد الجرائم الناشئة عن الاستخدام غير مشروع لشبكة الانترنت على المعلومة بشكل رئيسي هذا الذي أدى إلى إطلاق مصطلح الجريمة المعلوماتية على هذا النوع من الجرائم.[1]

المطلب الثاني: التعريف الفقهي والتعريف القانوني.

من خلال هذا المطلب سنتطرق إلى التعريفات الفقهية والتي اختلفت باختلاف الآراء والاتجاهات وإلى التعريفات القانونية والتي تتمثل في تعريفات المؤتمرات والتشريعات العربية والغربية.

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية.

لم يتفق الفقهاء الجنائيين لوضع تسمية موحدة للجريمة الالكترونية، إذ سماها البعض منهم بجريمة المعلومات والبعض الأخر أطلق عليها اسم "جرائم إساءة استخدام التكنولوجيا،[2] الجرائم الناعمة، إجرام ذوي الياقات السوداء..."[3]

---

[1] محمد عبيد الكعبي **الجرائم الناشئة عن الاستخدام غير مشروع لشبكة الإنترنت**، دار النهضة العربية القاهرة ص 32. نقلا عن صغير يوسف **الجريمة المرتكبة عبر الإنترنت**، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو ص 7.

[2] مجمع البحوث والدراسات **الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها**، بحث مقدم في مسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية سلطنة عمان سنة 2016 ص 20.

[3] مليكة عطوي **الجريمة المعلوماتية** حوليات جامعة الجزائر مجلة علمية 2012 العدد 21 ص 8.

وبما أن إيجاد تعريف للجريمة الالكترونية كان محلا لاجتهاد الفقهاء فقد ذهبت في ذلك مذاهب مختلفة ووضعوا تعريفات شتى وبالتالي فلا نجد تعريفا محددا للجريمة الالكترونية،[1] حيث اختلف الباحثين في ما بينهم على تعريف الجريمة الإلكترونية، فبعض الفقهاء اتجهوا إلى الجانب التقني من الجريمة والبعض الأخر تبنى جانبها القانوني.

فالذين يتناولونه من الجانب التقني يذهبون إلى القول بأن "الجريمة المعلوماتية ما هي إلا نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود".[2]

أما أنصار الاتجاه القانوني فيذهبون إلى أن تعريف الجرائم الإلكترونية يتطلب تعريف المفردات الضرورية المتعلقة بارتكاب جرائم الحاسب الآلي وهي الحاسب الآلي، برامج الحاسب الآلي، البيانات، الممتلكات، الدخول، الخدمات الحيوية.[3]

حيث أن الجريمة الإلكترونية مرتبطة بتقنية الحاسوب وأن لمرتكبها معرفة واسعة في المجال التقني، كما عرفها الفقهاء بأنها جريمة غير مشروعة وغير أخلاقية ناتجة بطريقة مباشرة أو غير مباشرة عن الدخول أو التجسس بشكل سري و دون التصريح به إلى الأجهزة التكنولوجية والتقنيات المعلوماتية أو البيانات أو الصور... والتي يقوم المجرم المعلوماتي بنقلها أو إرسالها لتحقيق أسبابه ودوافعه الخاصة التي تجعله يقوم بهذا الفعل.

---

[1] مجمع البحوث والدراسات، مرجع سابق ص 20.

[2] محمد الأمين البشري **التحقيق في جرائم الحاسب الآلي**، بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت،كلية الحقوق والشريعة جامعة الإمارات 21 ماي 2005 ص 6. نقلا عن مجمع البحوث والدراسات مرجع سابق ص 20.

[3] عبد الفتاح بيومي حجازي **مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي**، دار الفكر الجامعي الإسكندرية سنة 2006 ص 20، نقلا على مجمع البحوث والدراسات مرجع سابق ص 20.

حيث عرف الأستاذ **Donn porker** الجريمة الإلكترونية بأنها: "كل فعل إجرامي متعمد أيا كانت صلته المعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل".[1]

ويعرفها الفقيه **Rosenblatt** على أنها "نشاط غير مشروع موجه لنسخ أو تغيير أو الوصول إلى المعلومات المخزنة داخل الحاسب والتي تحول عن طريقه".[2]

وهناك اتجاه آخر من الفقه يركز على الجانب الموضوعي في تعريفه للجريمة الالكترونية حيث يرى أنه لا يكفي لإطلاق هذا الوصف عليها بمجرد استخدام الحاسب الآلي فيها ولكن يشترط أن يقع الفعل داخل نظام الحاسب الآلي لاحتسابها جريمة إلكترونية.[3]

وفي فريق آخر من الفقه يركز على الجانب المعرفي – لا على الوسيلة أو الموضوع – للجريمة الإلكترونية وذلك لكونها مرتبطة بالجوانب المعرفية الفنية أو المعرفة باستخدام الحاسب الآلي، ولذلك عرف أنصار هذا الاتجاه الجريمة الإلكترونية بأنها" أية جريمة يكون متطلبا لافتراضها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب الآلي،" وعرفها الدكتور هشام فريد رستم بأنها" أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه".[4]

---

[1] نهلا عبد القادر المومني، **الجرائم المعلوماتية ماجستير في القانون الجنائي المعلوماتي**، دار الثقافة للنشر والتوزيع ط 2 سنة 2004 ص 49.

[2] غازي عبد الرحمان الرشيد **الحماية القانونية من جرائم المعلوماتية**، أطروحة لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق سنة 2004 ص 92. نقلا على صغير يوسف، مرجع سابق ص 12.

[3] عبد الفتاح بيومي حجازي، مرجع سابق ص 25. نقلا على مجمع البحوث والدراسات، مرجع سابق ص 21.

[4] عبد الفتاح بيومي حجازي، مرجع سابق ص 25. نقلا على مجمع البحوث والدراسات، مرجع سابق رجع نفسه ص 22.

ولقد خلص "فان دير هولست ونفيه van der hulst and Neve" إلى أن حقل علم الجريمة يفتقر إلى التعريف المشترك والإطار ألمفاهيمي المتسق، ويستخدم ترسانة حية من المصطلحات وتكون أحيانا على شكل تركيبة مع البدايات مثل الإنترنت، والكمبيوتر، والبريد أو المعلومات الرقمية، حيث انتشرت هذه المصطلحات وطبقت بشكل عشوائي وهذا يعكس التداخل في المحتوى أو يعكس فجوات مهمة.[1]

ولقد عرفها "ليوكفيلدت فنسترا و ستول، stol & Leukfeldt veenstra" كمصطلح عام لجميع أشكال الجريمة التي تلعب فيها تكنولوجيا المعلومات والاتصالات دورا أساسي، وهنا تقع الكثير من الجرائم ضمن هذا التعريف.

لقد قدم ليوكفيلدت وآخرون قائمة بـ 28 جريمة بدءا من قرصنة الأنظمة الرقمية، وتثبيت برامج التجسس للاحتيال باستخدام الخدمات المصرفية عبر الإنترنت والمطاردة الافتراضية.[2]

وفي اتجاه آخر دمج العديد من التعريفات نظرا لتعدد وتشعب وجهات النظر وقد عرفها على أنها الجريمة التي يستخدم فيها الحاسب الآلي كوسيلة أو أداة لارتكابها أو إغواء ذلك أو جريمة يكون الحاسب نفسه ضحيتها.[3]

---

[1] van der hulst and Neve .2008 p 18 forum scientifique " **Nouveaux crimes à la lumière des changements et transformation régionaux et internationaux**" . Référence précédente p 4.

[2] Leukfeldt veenstra & stol, 2013 forum scientifique **"Nouveaux crimes à la lumière des changements et transformation régionaux et internationaux**" . Référence précédente p 4.

[3] غازي عبد الرحمان الرشيد، مرجع سابق ص 108_109. نقلا عن صغير يوسف، مرجع سابق ص 13.

كما عرفها محمد علي العربان بأنها:"فعل إيجابي أو سلبي عمدي يهدف إلى الاعتداء على التقنية المعلوماتية أي كان غرض الجاني.[1]

الفرع الثاني: التعريف القانوني للجريمة الإلكترونية.

ستتناول في هذا الفرع بعض من الاتفاقيات الدولية التي عرفت الجريمة الالكترونية وكذلك تعريفات التشريعات العربية والغربية لهذه الجريمة دون أن ننسى نظرة المشرع الجزائري لها.

أولا: الاتفاقيات الدولية.

- عرفتها الاتفاقية الأوروبية للجرائم السيبيرانية "اتفاقية بودابست"[2] بأنها:كافة النشاطات غير القانونية أو الغير مشروعة المرتبطة بأجهزة الكمبيوتر باستخدام الشبكة العنكبوتية، وصنفت هذه الاتفاقية الجرائم المرتكبة إلى عدة فئات منها الجرائم التي ترتكب ضد سلامة المعلومات وخصوصيتها والجرائم ذات الصلة بالكمبيوتر والجرائم المتعلقة بمحتوى الكمبيوتر والجرائم المتعلقة بالعلامات التجارية والملكية الفكرية.[3]

---

[1]انشاش منية **مداخلة حول الركن المفترض في الجريمة الإلكترونية**، جامعة بسكرة سنة2016_2015 ص 2_3.

[2]انعقدت اتفاقية بودابست في دولة المجر 2001-11-23 وتعتبر الأساس الأول للتعاون الدولي في مجال المكافحة الدولية للجريمة المنظمة عبر الانترنت وقعت عليها 30 دولة أوروبية بالإضافة إلى 4 دول أعضاء في المجلس الأوروبي (كندا ،و. م .أ ، اليابان ، جنوب إفريقيا).

[3]حاتم أحمد محمد بطيخ **تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات (دراسة تحليلية مقارنة)**، مجلة الدراسات القانونية والاقتصادية، جامعة عين الشمس كلية الحقوق مصر، مقال 5 مجلد 7 عدد 1 أغسطس 2021 ص 15.

- عرف المؤتمر العاشر للأمم المتحدة الجريمة المعلوماتية ومعاقبة فاعلها على أنها أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية.[1]

- عرفها بعض المتخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية (OECD)[2] بأنها:كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشر عن تدخل التقنية المعلوماتية[3].

ثانيا: التشريعات العربية.

[1]عقد المؤتمر في فيينا في الفترة ما بين 10 إلى 17 افريل 2000.

[2]organisation économique de commerce et développement.

[3]موقع منظمة التعاون الاقتصادي والتنمية www.ocd.org تمت الرؤية 21:20 في 05_03_2022.

- عرف المشرع السعودي الجريمة الإلكترونية بأنها: "أي فعل يرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".[1] حيث أصدر عام 2007 أولى قوانينها في مجال المكافحة التشريعية لجرائم تقنية المعلومات تحت عنوان نظام المكافحة للجرائم المعلوماتية وأقره مجلس الوزراء بالقرار رقم 79 بتاريخ 2007/03/7 وتم التصديق عليه بالمرسوم الملكي رقم 17 بتاريخ 2007/03/8 وصدر بالقرار رقم 11567/ب بتاريخ 9-03-2007 وكان الهدف منه الحد من نشوء هذه الجرائم المعلوماتية[2].

- عرفت المادة الأولى من القانون المصري رقم 15 سنة 2003 وسائل الاتصال بأنها: "أية وسيلة الإرسال أو استقبال الرموز أو الإشارات أو الرسائل أو الكتابات أو الصور وذلك أيا كان طبيعتها وسواء كان الاتصال سلكيا أو لاسلكيا[3]،"كما أن دولة مصر لم تصدر أي قانون خاص بالجرائم الالكترونية بل لجأ المشرع إلى تنظيم هذه الجريمة في بعض التشريعات الخاصة منها قانون الأحوال المدنية رقم 143 لسنة 1994 وقانون حماية المؤلف والذي عدل وتمم بموجب القانون رقم 29 لسنة 1994 وقانون التوقيع الإلكتروني رقم 15 لسنة 2004 والذي نظم أحكام التوقيع الإلكتروني والحماية الجنائية المقرر له،[4] وقانون الطفل المعدل سنة 2008.

---

[1] المادة الأولى من نظام المكافحة لجرائم المعلوماتية السعودي.

[2] حاتم أحمد محمد بطيخ مرجع سابق ص 2.

[3] المادة الأولى من القانون المصري رقم 15 لسنة 2003.

[4] ماهية الجريمة الإلكترونية University.lifestyle.Net تمت الرؤية 12:01 في 05_03_2022.

ثالثا: التشريعات الغربية.

- جاء في الفصل الأول من القانون الفرنسي العدد 451 لسنة 2013 والمؤرخ في 19 جوان 2013 بعض التعريفات لمصطلحات أقرتهم الجمعية الوطنية والذي أصدره رئيس الجمهورية ومن بين هذه المصطلحات (الجرائم الإلكترونية) والتي عرفت على أنها: "جميع الجرائم التي ترتكب عن طريق شبكه اتصالات أو نظام معلومات" كما عرفت الاتصالات الالكترونية في نفس القانون على أنها: "أي بث، إرسال أو استقبال الإشارات أو الإشارات أو الكتابات أو الصور أو الأصوات أو مقاطع الفيديو الكهرومغناطيسية أو البصرية أو أي شيء آخر".[1]

- لا يبدو أن لدى حكومة **و. م** . أ تعريفا رسميا للجرائم الالكترونية يميزها عن الجرائم المرتكبة في العالم الحقيقي، وبالمثل لا يوجد تعريف الجريمة الإلكترونية وغالبا ما يستخدم المصطلح بالتبادل مع الأعمال الخبيثة الأخرى المرتبطة بالانترنت والتكنولوجيا فغالبا ما تعرف وكالات إنفاذ القانون الفدرالية الجرائم الإلكترونية بناءا على احتجاجاتها والجرائم المكلفة بالتحقيق فيها، ومثلما لا يوجد تعريف شامل للجرائم الالكترونية لا توجد وكالة تم تعيينها كوكالة تحقيق رائدة للمكافحة.[2]

رابعا: المشرع الجزائري.

[1] الجريدة الرسمية للقانون الوطني الفرنسي.

[2]Kristin finklea &Catherine **A Theohary congressional research service informing the lesgislatine debatesince 1914** Cybercrime: conceptual issues for congress and V.S.Law Enforcement January 15.2015 page 2.

اهتم المشرع الجزائري كباقي الدول بالجريمة الإلكترونية وذلك بإصدار مجموعة قوانين وتشريعات خاصة بمكافحتها، ذلك لمدى خطورة وحداثة هذه الجريمة وذلك بموجب القانون 04\15 المؤرخ في 10 نوفمبر 2014،[1] المعدل بموجب القانون رقم 06/2 الصادر في 2006/12/20 ووضع قانون الخاص المتمثل في قانون 09|04 والمتضمن القواعد الخاصة بالوقاية من الجرائم الإعلام ومكافحتها.

حيث أطلق المشرع الجزائري على الجريمة الإلكترونية مصطلح الجرائم المتعلقة بجرائم الإعلام والاتصال وعرفها بموجب المادة 2 الفقرة (أ) من القانون 04/09 بأنها[2]:"جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نضام الاتصالات الالكتروني".كما عرف المنظومة المعلوماتية على أنها: "أي نظام منفصل أو مجموعة من الأنظمة المنفصلة مع بعضها البعض أو مترابطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.[3]"

[1]القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 156/66 المؤرخ في 1966 المتضمن قانون العقوبات (ج ر عدد 71الصادرة بتاريخ 10_11_2004).

[2]القانون رقم 04/09 الصادر في 14 شعبان الموافق ل 5 غشت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها ج ر العدد 47 الصادر بتاريخ(16/08/2009 ص 5).

[3]راجع المادة 2 الفقرة (ب) من القانون رقم 04/09.

ولـم يغفـل المشـرع الجزائـري عـن تعريـف المعطيـات المعلوماتيـة فـي صـلب القـانون 04/09 حيث نصت المادة الأولى منه على انه "أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية تؤدي وظيفتها" .[1]

ومن خلال مجموعة التعريفات التي ذكرناها سابقا تبين أن المشرع الجزائري يتبنى مبدأ تعريف المؤتمر العاشر للأمم المتحدة.[2]

بحيث أن ارتكاب الجريمة الالكترونية يحقق وقوعها أو يسهل ارتكابها عن طريق نظام الاتصالات والمنظومات المعلوماتية، فمن خلال هذا يستنتج لنا أن المشروع الجزائري يميل إلى معيار دور النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات كما جاء في قانون العقوبات للمادة 394 مكرر إلى 394 مكرر 07.[3]

ووفـق للمشـروع الجزائـري فـي تعريفـه لنظـام المعالجـة الآليـة للمعطيـات مقارنـة مـع التشريعات الأخرى اشترط ضرورة الترابط بين مكونات أو أجهزة النظام أو بين الأنظمة فيما بينها وركز على وظيفة المعالجة الآلية للمعطيات موسعا بذلك المجال ليشمل كلا من المعالجة الآلية للمعطيات، أما فيما ينص الشرط الثاني لمجلس الشيوخ الفرنسي والتعلق

---

[1] بردال سمير **الجريمة المعلوماتية في التشريع الجزائري**، المجلد 1 العدد 2 ص 183.

[2] راجع ص تعريفات الاتفاقات الدولية.

[3] قانون رقم 04/15الصادر في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66/156 الصادر في 08 جوان 1966 المتضمن قانون العقوبات ج ر عدد 71 .

بضرورة توافر النظام على حماية فنية فيبدو أن النظام المشروع قد حسم موقفه إلى جانب الفقه الذي لا يشترط هذا الشرط لحماية نظام المعالجة الآلية للمعطيات الجنائية[1].

كما نص القانون الجزائري للعقوبات على ثلاث أنواع من الجرائم المعلوماتية هي :

1- جريمة الدخول أو البقاء غير مشروع في أنظمة المعالجة الآلية للمعطيات :

هذه الجريمة من أهم الجرائم وأخطرها إذ تشكل في كثير من الأحيان مفترضا لحدوث الجرائم الأخرى ذلك أن الجاني يحتاج الدخول إلى الأنظمة المعلوماتية حتى يرتكب مختلف الجرائم الأخرى،[2] حيث نصت المادة 394 مكرر على أن كل تواجد عمدي غير مشروع داخل أنظمة المعالجة الآلية للمعطيات هو جريمة بحد ذاتها سواء أدى إلى نتيجة معينة أم لم يؤدي إلى ذلك.

حيث عرف الدخول الغير مصرح به بأنه الولوج إلى المعلومات والمعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام،[3] أما البقاء فيعرف بأنه التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام.[4]

---

[1] أنشاش منية مرجع سابق ص 4.

[2] محمد خليفة **خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها**، كلية الحقوق والآداب والعلوم الاجتماعية جامعة 8 ماي 1945 قالمة الجزائر ص 378 .

[3] Bainbridge (David) hacking **the unavthorisedaccess of computer system the legal implication m.l.rev**. March 1989 .vol 52 p 237 citation sur Mohammed Khalifa **confidentialité du crime électronique et les efforts du législateur algérien pour y faire face**. Référence précédente p 379.

[4] علي عبد القادر القهوجي **الحماية الجنائية للبيانات المعالجة إلكترونيا**،بحث مقدم لمؤتمر القانون والكمبيوتر والانترنيت كلية الشريعة والقانون جامعة الإمارات سنة 2000 ص 52 نقلا عن محمد خليفة،مرجع سابق ص 379.

2 -جريمة التلاعب بالمعطيات:

والتي تتمثل في إدخال أو تعديل أو إزالة المعطيات ما يؤدي إلى جريمة تغير حالة المعطيات، والذي نصت عليه المادة 394 مكرر 01 من ق ع ج.

بحيث أن كل من يضيف معطيات جديدة غير مصرح بإدخالها أو يعدل في حالة المعطيات الموجودة أو إزالتها هي جريمة يعاقب عليها المشرع الجزائري.

3 -جريمة التعامل في معطيات غير مشروعة:

لاشك أن المشرع عندما يدرك أهمية مصلحة ما، يسعى لإحاطتها بالحماية من كل الجوانب، ويوجد كل باب يمكن أن يلجأ من يريد الاعتداء عليها في مصدره، أو في حال حصل هذا العدوان يسعى المشرع على الحد من آثاره، ورغبة من المشرع في حماية أكبر للمعطيات ورغبة منه في حماية أكبر لها في جرائم الدخول أو البقاء غير المصرح بهما وجرائم التلاعب، قام بتجريم التعامل في المعطيات الصالحة لارتكاب تلك الجرائم، وهذان هما صورتان جريمة التعامل في معطيات غير مشروعة[1].

هذا ما تجرمه المادة 394 مكرر 02 من قانون العقوبات الجزائري والتي وضعت مجموعة من العقوبات وفرضت غرامات مالية على كل من يقوم به.[2]

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الانجاز في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

---

[1] محمد خليفة **الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري المقارن**، دار الجامعة الجديدة مصر سنة 2007 ص 159 نقلا عن محمد خليفة **خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها**، مرجع سابق ص 383-384.

[2] راجع المادة 394 مكرر 02 من ق ع ج.

- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم.

المبحث الثاني: أركان الجريمة الإلكترونية ودوافع ارتكابها.

تتخذ الجريمة المرتكبة عبر الانترنت من القضاء الافتراضي مسرحا لها، مما يجعلها تتميز بخصوصيات تنفرد بها إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي فهي تشترك بوجود الفعل غير المشروع، ومجرم يقوم بهذا الفعل، ومن خلال هذا التشابه سوف نتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة[1] في المطلب الأول، والى أسباب ودوافع ارتكابها من خلال المطلب الثاني.

المطلب الأول: أركان الجريمة الإلكترونية

تنهض الجريمة الإلكترونية على ثلاثة أركان أساسية: هما الركن الشرعي والركن المادي والركن المعنوي.

فلا بد للجريمة المعلوماتية إذن من (ركن مادي) يمثل كيانها الملموس ويعبر عن إرادة الفاعل بصورة يمكن إثباتها ولابد أيضا من (ركن معنوي) يعبر عن إرادة المجرم المعلوماتي،[2] كما يجب على المشرع وضع قوانين تسن على تجريم وعقاب المجرم المعلوماتي (الركن الشرعي).

[1] صغير يوسف **الجريمة المرتكبة عبر الإنترنت** مرجع سابق ص 59.

[2] مطماطي راوية **الجريمة الإلكترونية في التشريع الجزائري**، رسالة دكتوراه تخصص قانون أعمال، كلية حقوق جامعة عبد الحميد بن باديس مستغانم الجزائر دون ص.

وفي تعريف هذا الأخير نقول انه شخص يتمتع بالمهارة والمعرفة والوسيلة والسلطة، وكذلك الباحث من أجل تنفيذ نشاطه الإجرامي، فالجاني في جرائم التقنية شخص طبيعي يتوافر لديه كشرط أساسي معرفة كافية بآلية عمل وتشغيل الحاسب الآلي، وبناء على هذا التعريف فان الجريمة الإلكترونية (cyber criminals) تقوم على ثلاثة أركان أساسية وهم الركن الشرعي، الركن المادي، والركن المعنوي.[1]

سنحاول في هذا المطلب إلى تبيان أركان الجريمة الالكترونية والتي لا تختلف أركانها عن أركان الجريمة التقليدية رغم خصوصيتها وحداثتها.

الفرع الأول: الركن الشرعي للجريمة الإلكترونية.[2]

انطلاقا من مبدأ الشرعية ووفقا لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على: "لا جريمة ولا عقوبة أو تدابير أمن بغير قانون".

جرم القانون رقم 04-15 بعض صور الجريمة المعلوماتية ونص على العقوبات المقررة لمرتكبها في القسم السابع مكرر تحت عنوان:"المساس بأنظمة المعالجة الآلية للمعطيات" من الفصل الثالث المعنون: " الجنايات والجنح ضد الأموال من الباب الثاني

[1] مطماطي راوية،مرجع سابق، دون ص.

[2] حمزة خضري، حمزة عشاش، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، مجلة الدراسات القانونية والسياسية، مجلد 6،عدد 02جوان 2020، ص173.

المتعلق بالجنايات والجنح ضد الأفراد" وذلك في المواد من 394 مكرر إلى 394 مكرر 08 من قانون العقوبات المعدل والمتمم.

في حين جاء القانون 09-04 السابق الذكر متضمنا القواعد الخاصة الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كجانب وقائي يحد من وقوع الجرائم المعلوماتية من خلال وضع ترتيبات تقنية لمراقبة الاتصالات التكنولوجية وتسجيل وتجميع محتواها في حينها والقيام بإجراءات التفتيش داخل المنظومة المعلوماتية.

الفرع الثاني: الركن المادي للجريمة الإلكترونية.

كنا قد ذكرنا سابقا أن الجريمة الإلكترونية قائمة على 3 أركان من بينهم الركن المادي الذي سنتناوله الآن، حيث أنه في الركن المادي لابد من فعل أو امتناع يمكن إثباته، إذ لا عبرة بما في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، الركن المادي هنا يختلف من حال لآخر حسب التصنيف الذي يقع على فعل، وعليه لا يمكن حصر الجريمة المعلوماتية واقعة القذف أو التهديد أو التحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طريق جهاز الكمبيوتر، وهذا لا يسبب إشكالا إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقتها وهذا ما يدعو للتدخل التشريعي.[1]

وعليه فإن الركن المادي الإلكترونية يتكون من السلوك الإجرامي والنتيجة والعلاقة السببية.

[1] بوضياف أسمهان، **الجريمة الالكترونية والإجراءات التشريعية لمواجهتها**، مجلة الأستاذ الباحث للدراسات القانونية، العدد 11 سبتمبر 2018 ص 353_354.

أولا: السلوك الإجرامي.

يعتبر السلوك الإجرامي عنصر أساسي في الركن المادي، ويكون هذا السلوك بفعل إيجابي وذلك بقيام الجاني للفعل الإرادي بغية إحداث نتيجة معينة، كما يمكن أن يقوم بفعل سلبي بأخذه صفة الامتناع عن إثبات أمر يوجبه الشرع .

ثانيا: النتيجة الإجرامية.

يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث في العالم الخارجي كأثر للسلوك الإجرامي فالسلوك قد أحدث تغييرا حسيا ملموسا في الواقع الخارجي، ومفهوم النتيجة كعنصر في الركن المادي للجريمة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج بغض النظر عما يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى.[1]

ثالثا: الرابطة السببية.

تتمثل الرابطة السببية في الصلة التي تربط بين الفعل والنتيجة وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة، وأهمية رابطة السببية ترجع إلى أن إسناد النتيجة إلى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحقق رابطة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت، أما إذا كانت الجريمة غير عمدية، فإن نفي رابطة السببية يؤدي إلى انتفاء مسؤولية كلية عنها، ذلك أنه لا شروع في الجرائم غير العمدية.[2]

علما أنه يمكن تحقيق الركن المادي دون تحقيق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها مثل إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلى أنه لا مناص من معاقبة الفاعل، بحيث يتخذ الركن المادي في هذه الجريمة عدة صور

[1] صغير يوسف مرجع سابق، ص 66 .

[2] صغير يوسف،مرجع سابق،نفس ص.

حسب كل فعل إيجابي مرتكب مثل جريمة الغش المعلوماتي بحيث أن الركن المادي فيها هو تغيير الحقيقة في التسجيلات أو المحررات الإلكترونية.[1]

وكذا جريمة التجسس الإلكتروني بحيث أن الركن المادي فيها هو الحصول مباشرة على الدعامة الإلكترونية الحاوية للسر أو المعلومات كالحصول على "CD" مخزنة فيه الأسرار والوثائق.[2]

الفرع الثالث: الركن المعنوي للجريمة الإلكترونية.

الركن المعنوي وهو العلم بعناصر الجريمة وإرادة ارتكابها وبالتالي يتكون الركن المعنوي للجريمة الإلكترونية من عنصرين هما العلم والإرادة.

أولا: العلم.

الذي يعرف بأنه إدراك الفاعل للأمور، حيث لا يتحقق القصد الجنائي إلا إذا كان الجاني يعلم بالعناصر الأساسية لقيام الجريمة سواء تعلق ذلك بسلوكه الإجرامي أم بموضوع الاعتداء فإذا كان الجاني جاهلا بشيء من ذلك فلا يتحقق القصد الجنائي.[3]

ثانيا: الإرادة.

والتي هي اتجاه السلوك الإجرامي لتحقيق النتيجة، والإرادة هي نشاط نفسي يهدف إلى تحقيق غرض معين فإذا كان غرض الجاني تحقيق نتيجة إجرامية، كانت الإرادة المتجهة إلى الفعل المنطوي على إحداث النتيجة هي "القصد الجنائي" والغرض هو الهدف القريب الذي تتجه إليه الإرادة، أما الباعث فهو عبارة عن الدافع إلى إشباع حاجة معينة، وهذا الدافع له طبيعة نفسية بخلاف الغاية التي لها طبيعة موضوعية.[4]

---

[1] بوضياف أسمهان، مرجع سابق، ص 354.

[2] مطماطي راوية، مرجع سابق، دون ص.

[3] صغير يوسف مرجع سابق ص 69.

[4] مرجع نفسه نفس ص.

وطبقا للمبادئ العامة المعروفة في قانون العقوبات قد يكون القصد الجنائي عاما وخاصا، وعليه فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء، ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص مثل جرائم تشويه السمعة عبر الانترنت، وفي كل الأحوال يرجع الأمر إلى السلطة التقديرية للقاضي.[1]

وكذلك تعد الجرائم المعلوماتية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام لتحديد المسؤولية الجنائية، ولا يمكن تصور وجود قصد خاص بالجريمة، دون أن يسبقه القصد العام، أما عن وجود القصد الخاص في الجرائم المعلوماتية فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة، والنية الخاصة لدى الجاني من وراء القيام بالفعل غير مشروع. وأنا كباحثة أرى أن القصد العام والخاص في الجرائم المعلوماتية هو أساس لتحديد المسؤولية الجزائية، والذي يحدد وجود قصد خاص في بعض الجرائم المعلوماتية هو طبيعة الجريمة ونية الأضرار أو النية الخاصة للجاني، والتي يمكن استشفاؤها من مكونات كل جريمة على حدة وبشكل مستقل.

أما عن الإثبات في توافر الركن المعنوي في الجرائم المعلوماتية فهو يقع على عاتق النيابة العامة والمحكمة مختصة بالنظر في مثل هذا النوع من القضايا.[2]

المطلب الثاني: أسباب ودوافع ارتكاب الجريمة المعلوماتية.

[1] مطماطي راوية، مرجع سابق، دون ص.

[2] بوضياف أسمهان، مرجع سابق ص 355.

يسعى المجرم من خلال قيامه بالجريمة المعلوماتية إلى تحقيق مجموعة من المكاسب والأهداف والتي تنقسم إلى دوافع شخصية ودوافع أخرى سنناقشها في هذا المطلب.

الفرع الأول: الدوافع الشخصية.

من بين أسباب ارتكاب المجرم للجريمة الالكترونية تحقيق دوافع شخصية والتي تتجلى في العناصر التالية:

أولا: السعي لتحقيق الكسب المالي.

يعد هذا الدافع أكثر الدوافع تحريكا للجناة، لاقتراف جرائم الكمبيوتر خاصة المحترفون، ذلك أن خصائص هذه الجرائم، وحجم الربح الكبير والممكن تحقيقه من بعضها، خاصة غش الكمبيوتر أو الاحتيال المرتبط به يبرز هذا الدافع،[1] وغالبا ما تكون ضحية هؤلاء المجرمين مؤسسات مالية أو اقتصادية، حيث أشارت مجلة (sécurité informatique) المتخصصة في الأمن المعلوماتي أن 43% من حالات المعلن عنها قد تمت من اجل اختلاس الأموال، و23% من اجل سرقة المعلومات، و19% أفعال إتلاف، و15% سرقة وقت الآلة أي الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية.[2]

ثانيا: الرغبة في اختراق نظام الكمبيوتر والتفوق على تعقيد وسائل تقنية.

أكثر من شهوة الحصول على الربح خاصة طائفة الفضوليين، يميل مرتكبو هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة انه إزاء ظهور أي تقنية مستجدة فإن مرتكبي هذه الجرائم (لديهم شغف الآلة) يحاول إيجاد الوسيلة لاختراقها، وهو ما تهدف إليه طائفة الفضوليين ومخترقو امن المعلومات.[3]

---

[1] علي حسن الطواليه، **الجرائم الالكترونية**، جامعة العلوم التطبيقية سنة 2008 ص 69، نقلا عن محمود احمد طه، **المواجهة التشريعية لجرائم الكمبيوتر والانترنت**، ط 1 دار الفكر والقانون للنشر والتوزيع مصر سنة 2013 ص 16.

[2] نهلا عبد القادر مومني، مرجع سابق ص 93.

[3] جميل عبد الباقي الصغير، **الانترنت والقانون الجنائي**، دار النهضة العربية سنة 2002 ص 160. نقلا عن احمد محمود طه ، مرجع سابق نفس ص.

ثالثا: الرغبة في الانتقام.

إن من اخطر الدوافع التي تجعل المجرم المعلوماتي يقون بهذا الفعل هو رغبته في الانتقام إما من شخص أو عدة أشخاص بغية إلحاق الضرر به إما ماديا أو معنويا، كرغبته في الانتقام من رب العمل مثلا، أو انه يملك معلومات كبيرة وحساسة عن شخص أخر أو مؤسسة أو شركة يعمل بها فيستعمل تلك المعلومات ضدهم. حيث لوحظ إن العاملين في القطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى، يتعرضون للضغوطات نفسية كبيرة ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفرة في حالات معينة، هذه الأمور مثلت قوة محركة لبعض العاملين لارتكاب جرائم الكمبيوتر باعثها الانتقام من المنشأة أو رب العمل والرغبة في قهر النظام والتفوق على تعقيد وسائل التقنية وهو ما يهدف إليه خاصة الحاقدين من طائفة المجرم المعلوماتي[1].

الفرع الثاني: دوافع أخرى.

من بين الأسباب التي تدفع المجرم المعلوماتي لارتكاب الجريمة الالكترونية أسباب عديدة منها السياسية، الاقتصادية، كدافع المنافسة بين شركتين اقتصاديين حيث يدفع الجرم للاستيلاء على المعلومات الالكترونية للمنافس أو استعمالها ضده.

أو دوافع دينية وعقائدية، حيث توجد مجموعات الحادية تنشط على مواقع الكترونية عبر شبكة الانترنت تعمل على محاربة الأديان والقيم الخلقية والاجتماعية والروابط الأسرية، وفي رأيهم ومعتقداتهم يهدفون إلى تحسين العالم، ويعد أيضا التسابق الفضائي والعسكري بين الدول دافعا مهما لهذه الجريمة، فقد قام القراصنة بالإغارة على شبكات معلوماتية تابعة لوكالة الفضاء ناسا ومواقع أسلحة ذرية تابعة لحكومة الولايات المتحدة الأمريكية.[2]

[1] محمد سامي الشوأ، **الجرائم المستحدثة والبحث العلمي، جرائم الحاسب الآلي**، أكاديمية نايف العربية للعلوم الأمنية سنة 2001 ص 9. نقلا عن احمد محمود طه ، مرجع نفسه ص 16.

[2] نهلا عبد القادر مومني، مرجع سابق، ص 93.

الفصل الثاني

مواجهة الجريمة الإلكترونية

تمهيد:

تعكف الحكومة الجزائرية على إعداد مشروع قانون مكافحة الجرائم الإلكترونية الذي ينص على جملة إجراءات تحدد آليات الرقابة على الإنترنت ومحاربة الجنح المرتبطة بالشبكة الافتراضية، بعدما أصبحت الجرائم الإلكترونية ذات مستويات قياسية بناءا على ما تقدمه حصيلة المصالح الأمنية في الجزائر سنويا، وقام بوضع مجموعة قوانين أخرى خاصة لضمان الحماية الجنائية للمعاملات الالكترونية، كما شرع في مواجهة الجريمة من خلال مجموعة وسائل القديمة والحديثة، فهل المواد القانونية التي أدرجها المشرع كافية لمحاربة الجرائم المعلوماتية؟ وما مدى انطباق القواعد الإجرائية لضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس؟.

على ضوء ذلك سأقسم هدا الفصل إلى:

المبحث الأول: المواجهة التشريعية للجريمة الالكترونية.

المطلب الأول: مكافحة الجريمة الإلكترونية بموجب القوانين العامة.

المطلب الثاني: مكافحة الجريمة الالكترونية بموجب القوانين والهياكل الخاصة.

المبحث الأول: المواجهة الإجرائية للجريمة الالكترونية.

المطلب الأول: الإجراءات القديمة لمواجهة الجرائم الالكترونية.

المطلب الثاني: الإجراءات المستحدثة لمواجهة الجريمة المعلوماتية.

المبحث الأول : المواجهة التشريعية للجريمة الإلكترونية.

تعددت أضرار ومخاطر الجرائم الإلكترونية وباتت تهدد أمن المجتمعات والمؤسسات على حد سواء، نظرا للتطور الملحوظ الذي طرأ على الأنظمة المعلوماتية حيث أصبح الحفاظ على أمن المجتمع والأفراد تحديا كبيرا لرجال التشريع والقضاء في مواجهة هذا الإجرام، ولقد سارع المشرع الجزائري كباقي التشريعات الأخرى لمكافحة الجريمة الالكترونية وذلك بسن جملة من النصوص والقواعد القانونية.

المطلب الأول: مكافحة الجريمة الإلكترونية بموجب القوانين العامة.

أصدر المشرع الجزائري قوانين خاصة وعامة وأجهزة للتصدي للجرائم الإلكترونية، فهناك جهود معتبرة قام بها المشرع الجزائري في محاربة قراصنة الانترنت وإحالتهم قانونا على المحاكم، متأثرا بجل الدول العربية التي وضعت قوانين مكافحة الجريمة الإلكترونية، ومن أهم الأمور التي أولاها المشرع أهمية قصوى من أجل الحفاظ على أمن الدولة والنظام العام.

الفرع الأول : مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري والقانون المدني.

سنتناول في هذا الفرع القوانين التي سنها المشرع الجزائري لمكافحة لجريمة المعلوماتية وذلك بموجب الدستور والقانون المدني.

أولا: مكافحة الجريمة الإلكترونية بموجب الدستوري الجزائري.

سارع المشرع الجزائري إلى مواكبة التطور الذي شهدته التشريعات العالمية، وإلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من

أشكال جديدة للإجرام، مسايرة للتطور الذي مس النظام المعلوماتي وذلك بموجب القوانين والدستور.

تطرق الدستور الجزائري المعدل سنة 2020 إلى حرمة الحياة الخاصة للمواطن في الباب الثاني المعنون "بالحقوق الأساسية والحريات العامة والواجبات" في الفصل الأول "الحقوق الأساسية والحريات العامة"، حيث نصت المادة 46 منه على انه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون على انتهاك هذا الحكم، حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه[1].

ثانيا: مكافحة الجريمة الإلكترونية بموجب القانون المدني.

ترتيبا على الأهمية الدستورية لحرمة الحياة الخاصة فقد سارع المشرع ونص على أن كل من وقع عليه اعتداء غير مشروع في حق من حقوقه الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما قد يكون لحقه من ضرر في المادة 124 من التقنين المدني الجزائري (كل عمل أي كان يرتكبه المرء يسبب ضررا للغير يلزم من كان سببا في حدوثه بالتعويض) وقد جاء هذا عاما وشاملا لأي اعتداء يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة، قد أورد هذا النص مبدأ مهما هو حق من وقع الاعتداء على حياته الخاصة في التعويض عما لحقه من ضرر، فالمسؤولية المدنية ترتب الحق في الحكم على التعويض وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الاعتداءات الالكترونية التي تمس بالحياة الخاصة على شبكة الانترنت، وهو

[1] المادة 46 الدستور الجزائري المعدل سنة 2020.

عنصر متحول صعب التحديد في الجرائم التي تمس الخصوصية على المواقع الالكترونية لما تشكله من صعوبات في الإثبات، وفي تحديد هوية المعتدي، وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الالكتروني الشخصي على أساس الخطأ الواجب الإثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الالكتروني قد وصل إلى درجة الخطأ الذي يشكل اعتداء قابل للإثبات وإن وقع على الشبكة.[1]

الفرع الثاني: مكافحة الجرائم الالكترونية بموجب قانون العقوبات الجزائري وقانون الإجراءات الجزائية.

استمر المشرع الجزائري في إصداره للقوانين والمواد الخاصة بتجريم الجريمة الالكترونية، ومن بين هذه التشريعات قانون ع ج و قانون إ ج.

أولا: مكافحة الجريمة الالكترونية بموجب قانون العقوبات الجزائري.

سارع المشرّع الجزائري إلى تجريم الأفعال التي تمس بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 15\04 المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم 15\22 [2] المتضمن قانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 7 ونصت هذه المواد على ما يلي:

المنظومة للمعالجة الآلية أو يحاول ذلك، وتضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة، وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال

[1] بوضياف أسمهان، مرجع سابق، ص 362.

[2] قانون رقم 04-15، مرجع سابق.

المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج".

نصت المادة 394 مكرر 1 على انه "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات كل وبغرامة من 500.000 دج إلى 2.000.000 دج كل من أدخل بطريقة الغش المعطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[1].

نصت المادة 394 مكرر 2 على انه "يعاقب بالحبس من شهرين إلى ثلاث سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج كل من يقوم عمدا و عن طريق الغش بما يأتي:

_تصميم أو بحث أو تجميع أو توفير أو نشر أو الانجاز في المعطيات المخزنة 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 لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

نصت المادة 394 مكرر 3 على انه: "تضاعف العقوبة المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام ،دون الإخلاء بتطبيق عقوبات اشد".

نصت المادة 394 مكرر 4 على انه: "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عنها في هذا القسم بغرامة تعادل 5 مرات بالحد الأقصى للغرامة المقررة للشخص الطبيعي".

[1] المادة 394 مكرر 1، القانون رقم 04\15، مرجع سابق.

نصت المادة 394 مكرر 5 على انه: "كل من شارك في مجموعة أو في اتفاق تالف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

نصت المادة 394 مكرر 6 على: "مع الاحتفاظ بحقوق الغير حسن النية، يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل راو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها".

نصت المادة 394 مكرر 7 على انه: "يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها".

ثانيا: مكافحة الجريمة الالكترونية بموجب قانون الإجراءات الجزائية.

بالنسبة لمتابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية كالتفتيش والمعاينة واستجواب المتهم والشهادة والخبرة.

نجد أن المشرع نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الالكترونية في المادة 37 ق إ ج، ونص على التفتيش في المادة 45 الفقرة 7.

كما نص على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 05 إلى 65 مكرر 10.

ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6.

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لا بدّ من مصاحبة هذه القواعد بقواعد أخرى إجرائية تحفظية ووقائية، والتي من شأنها أن تتفادى وقوع جرائم الكترونية أو على الأقل الكشف عنها في وقت مبكر وهو ما استدركه المشرع بتضمين قانون رقم 06\22

المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الالكترونية تتمثل في مراقبة الاتصالات الالكترونية وتسجيلها ويقصد باعتراض المراسلات أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال و العرض، التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها.[1]

المطلب الثاني: مكافحة الجريمة الالكترونية بموجب القوانين والهياكل الخاصة.

سارع المشرع الجزائري كغيره لإصدار مجموعة قوانين وهياكل خاصة لمجابهة الجريمة الالكترونية والتي كان لها الفضل الكبير في مساعدة القوانين العامة لأداء هذه المهمة الصعبة.

الفرع الأول: مكافحة الجريمة الالكترونية بموجب القوانين الخاصة.

من بين القوانين الخاصة التي اعتمدها المشرع الجزائري لصد الجريمة المعلوماتية القانون الخاص بحماية حقوق المؤلف والحقوق المجاورة وقانون البريد و الاتصالات اللاسلكية، وأيضا القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها هذا ما سنتناوله في هذا الفصل.

أولا: القانون الخاص بحماية حقوق المؤلف والحقوق المجاورة.

الحالات يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو اسم تجاري أو مصنف بهدف تحديد هويته على الشبكة لكي يعرض ما يرد من سلعة أو خدمة عند إبرام

[1] براهيمي جمال، **مكافحة الجريمة الالكترونية في التشريع الجزائري**، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود العمري، تيزي وزو العدد 2 الصادرة في 15\11\2016 ص 138-139-140.

العقد مع إحدى الشركات التي تقدم الخدمات على الشبكة وبمجرد تسجيل اسم الموقع يحظى بالحماية القانونية المقررة لحق الملكية الفكرية الذي يتضمنه، فعند تسجيل الموقع كمصنف أدبي أو فني (لا يجوز أن يعتدي على أي جانب من جوانب الحياة الخاصة للأفراد) كاستعمال الاسم كامل لشخص معين معروف دون الحصول على موافقة من صاحبها، إنّ حماية مواقع الإنترنت التي تستغل مصنفا أدبيا أو فنيا على شبكة الانترنت بقانون حق المؤلف والحقوق المجاورة ينتج عنه حماية الحق الأدبي والمالي للموقع المسجل كمصنف[1].

ثانيا: قانون البريد والاتصالات اللاسلكية.

عمد المشرع الجزائري عند إصداره لقانون البريد والاتصالات اللاسلكية إلى وضع مجموعة من المواد تضمن انتهاك حرمة المراسلات أو إتلاف الرسائل المرسلة إلى البريد أو التجسس عليها.

حيث نصت المادة 127 من القانون رقم 2000-03 المؤرخ في 5 أوت 2000 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية على أن : "كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم باختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها يعاقب بالحبس من ثلاث أشهر إلى خمس سنوات وبغرامة من 30.000 دج إلى 500.000 دج، ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق أو يختلس أو يتلف برقية أو يذيع محتواها، كما يعاقب بالحرمان من كافة الوظائف والخدمات العمومية من خمس إلى عشر سنوات".[2]

[1] بوضياف أسمهان، مرجع سابق ص365.

[2] المادة 127 من القانون رقم 03-2000 المؤرخ في 5 اوت 2000 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

ثالثا: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[1]

لقد جاء في القانون 09\04 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية وأهمها:

– مراقبة الاتصالات الالكترونية: لقد نصت المادة 04 من القانون 09\04 على أربع حالات يجوز فيها لسلطات الأمن لقيام بمراقبة المراسلات والاتصالات الالكترونية وهي:

– للوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب وجرائم ضد أمن الدولة.

– عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام

– لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

– في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

رابعا : قانون التأمينات.

جاء في المادة 93 مكرر 2 على انه: "يعاقب كل من يسلم أو يستلم البطاقة الالكترونية يغرض استعمالها بطريقة غير مشروعة بحيث يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة من 100.000 دج إلى 200.000 دج".[2]

كما نصت المادة 93 مكرر 3 على انه: "من يقوم عن طريق الغش بتعديل أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة

---

[1] فضيلة عاقلي، **الجريمة الالكترونية و إجراءات مواجهتها من خلال التشريع الجزائري**، المؤتمر الدولي الرابع عشر (الجرائم الالكترونية) طرابلس، 24–25 مارس 2017 ص 131.

[1]– المادة 93 مكرر 02، القانون رقم 01\08 المؤرخ في 23 جانفي 2008 المتمم للقانون 83\01 المتعلق بالتأمينات.

نفس العقوبة على كل من يقوم بتعديل أو نسخ بطريقة غير مشروعة البرمجيات التي تسمح بالوصول أو باستعمال المعطيات المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو مهن الصحة.[1]

الفرع الثاني: مكافحة الجريمة الالكترونية بموجب الهياكل الخاصة.

سنتحدث في هذا الفرع عن مكافحة الجريمة الالكترونية بموجب الهياكل الخاصة والتي تتمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، والهيئات القضائية الجزائية المتخصصة ،والمعهد الوطني للأدلة الجنائية على الإجرام.

أولا:الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

نصت المادة 13 من القانون 09\04 سالف الذكر والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال انه: "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته".

مهام الهيئة:

تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام التالية[2]:

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

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشان الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع معلومات وانجاز الخبرات القضائية.

[1] المادة 93 مكرر 03، نفس المرجع.

[2] المادة 13 من القانون 09\04، مرجع سابق.

_ تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

ثانيا: المعهد الوطني للأدلة الجنائية على الإجرام.

يتكون من إحدى عشر دائرة متخصصة في مجالات مختلفة، جميعها تتضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات.

ثالثا: الهيئات القضائية الجزائية المتخصصة.

إن السلطة القضائية ستتعامل تأكيدا في قضايا الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ولا سيما بعد اللجوء الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطن، بينما يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي.[1]

المبحث الثاني: المواجهة الإجرائية للجرائم الالكترونية.

ما يميز الجريمة المعلوماتية هو أنها ترتكب في مجال مفرغ يختلف كلياً عن المسرح التقليدي الذي ترتكب فيه الجريمة حيث تتم إجراءات الاستدلال عليها وضبطها وإثباتها بالوسائل التقليدية المتمثلة في إجراءات الاستدلال والتحقيق. هذه الإجراءات وضعت لضبط وإثبات جرائم ترتكب في عالم مادي ملموس، يلعب فيه السلوك المادي الدور الأبرز والاهم،[2]

[1] أحمد مسعود مريم، مرجع سابق، ص50 .

[2] احمد محمد براك، **المواجهة التشريعية للجريمة المعلوماتية بين الواقع والمأمول**، مجلة جامعة الأزهر– غزة، عدد خاص بمؤتمر كلية الحقوق الخامس المحَّكم، المجلد 19 ص 72.

وكذا إجراءات التحقيق المستحدثة المتعلقة في التسرب المعلوماتي ومراقبة الاتصالات الالكترونية وحفظ المعطيات المتعلقة بحركات السير.

ومن خلال هذا المبحث سنبرز أهم النقاط التالية من خلال المطلبين:

المطلب الأول: إجراءات التحري والتحقيق القديمة لمواجهة الجريمة الالكترونية.

المطلب الثاني: إجراءات التحري والتحقيق الحديثة لمواجهة الجريمة الالكترونية.

المطلب الأول: الإجراءات القديمة لمواجهة الجريمة الالكترونية.

كنا قد ذكرنا سابقا من خلال الإجراءات التشريعية بموجب ق إ ج عن مجموعة الإجراءات التقليدية لمواجهة الجريمة الالكترونية والمتمثلة في التفتيش، المعاينة والضبط... الخ ومن خلال هذا المطلب سنفصل هذه الإجراءات.

الفرع الأول: الخبرة والمعاينة في الجرائم المعلوماتية

المعاينة هي إجراء ينتقل بمقتضاه المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه (عن طريق العين المجردة) مكانا أو شخصا له علاقة بالجريمة لإثبات حالته والتحفظ على كل ما قد يفيد من آثار في كشف الحقيقة.[1]

والمعاينة تكون شخصية أو عينية، المعاينة الشخصية إذا تعلقت بشخص المجني عليه، أو مكانية إذا تعلقت بالمكان الذي تمت فيه الجريمة. أما المعاينة العينية فهي التي تتعلق بالأشياء أو الأدوات المستخدمة في ارتكاب الجريمة، وقد يقتضي الأمر الاستعانة بخبير للتعرف على طبيعة المادة أو نوعها إذا كان ذلك يحتاج لرأي المتخصص، وفي هذه الحالة يتم إرسال هذه الأشياء إلى الخبير لنكون أمام إجراء آخر من إجراءات التحقيق وهو

[1] براهيمي جمال التحقيق الجنائي في الجرائم المعلوماتية رسالة لنيل شهادة دكتوراه في القانون كلية الحقوق بجامعة مولود معمري تيزي وزو سنة 2018 ص56.

الخبرة، فالخبرة هي أحد أهم وسائل جمع الأدلة، يلجأ إليها المحقق عند وجود واقعة مادية أو شيء مادي يحتاج التعرف إلى الخبير المتخصص، فهو يأخذ حكم الشاهد من حيث الحجية أو القوة في الإثبات. يثور التساؤل هنا عن مدى إمكانية معاينة الجريمة المعلوماتية من حيث الوجود المادي وكيفية معاينته.

فالمحقق في هذه الحالة يتعامل مع بيئة الكترونية والبيانات المخزنة داخل نظام معلوماتية شديد الحساسية ولا يتعامل مع الأوراق وهو ما يؤكد القواعد الإجرائية التقليدية التي سنت لتواجه سلوكاً مادياً يرتكب بواسطة آلات وأدوات قابلة للربط. أما السلوك الإجرامي في الجريمة المعلوماتية فهو عبارة عن بيانات مخزنة في نظام معلوماتي يتطلب إثباته انتقال شخص متخصص حيث يتم التفتيش عن البيانات عن طريق نقل محتويات الأسطوانة الصلبة الخاصة بالجهاز، مثل القيام بالبحث في بنوك المعلومات وفحص كل الوثائق المحفوظة ومراسلات مرتكب الجريمة مثل الرسائل الإلكترونية وفك شفرات الرسائل المشفرة. وهو ما يحدث عندما ترتكب الجريمة عبر شبكة الانترنت كما يقتضي ذلك أيضا أن يعمل المحقق على الوصول إلى الملفات التاريخية التي تبين لحظات مختلف الاتصالات. من أين صدرت؟ ومن الذي يحتمل إجراؤها، بالإضافة إلى ضرورة إلمام المحقق بالحالات التي يكون عليه فيها التحفظ على الجهاز أو الاكتفاء بأخذ نسخة من الأسطوانة الصلبة للحاسب، والأوقات التي يستخدم فيها برامج استعادة المعلومات التي تم إلغاؤه.[1]

[1] احمد محمد براك، مرجع سابق ص73.

الفرع الثاني: التفتيش المعلوماتي.

عرف المجلس الأوروبي إجراء التفتيش في الجرائم المعلوماتية بأنه "الإجراء الذي يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني"وهو الإجراء الذي يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات والأدلة المطلوبة وبإمعان النظر في المشكلات الإجرائية الخاصة بالتفتيش في الجرائم المعلوماتية نجدها في مشكلة امتداد الإذن بالتفتيش في شبكات الحاسب حيث يتم التفتيش عن الأدلة في مكان آخر في نظام معلوماتي آخر، ويمكن التغلب على ذلك كما في بعض الأنظمة القانونية كالقانون الهولندي في المادة 25 منه بالنص في إذن التفتيش على الإذن بتفتيش أي نظام معلوماتي آخر يوجد في أي مكان غير مكان البحث شريطة أن تفيد بشكل معقول في كشف الحقيقة وإذا ما وجدت هذه البيانات يجب تسليمها، وكذلك هناك إشكالية أخرى تتعلق بمشكلة التفتيش في الجرائم المعلوماتية العابرة للحدود وذلك عندما يتم إجراء التفتيش على جهاز حاسب آلي خارج النطاق الجغرافي للدولة التي أصدرت الإذن بالتفتيش، وبالتالي تثور مشكلة شرعية هذا الإجراء ومساسه بسيادة الدولة الأخرى وهذه المشكلة يجب تجاوزها من خلال تعزيز التعاون الدولي في مكافحة الجرائم المعلوماتية من خلال إبرام اتفاقيات ثنائية وجماعية تنظم مباشرة هذا الإجراء، ومثال ذلك الاتفاقية العربية لمكافحة تقنية المعلومات واتفاقية بودابست المشار إليهما آنفاً.[1]

حرصت معظم التشريعات الإجرائية على عدم جواز إجراء التفتيش إلا بحضور المتهم أو من يمثله أو شاهدين من غير المعنيين بالتحقيق، وهو ما نص عليه المشرع الجزائري في المادة 01\45 من ق إ ج، إلى انه استثنى بموجب الفقرة الأخيرة من نفس المادة حضور الأشخاص المحددين في الفقرة الأولى– وهم المتهم أو ممثله وفي حالة

[1] احمد محمد براك مرجع سابق ص74.

امتناعه أو هروبه حضور شاهدين من غير الموظفين الخاضعين لسلطة ضابط الشرطة القضائي– في عدة جرائم من بينها جرائم المساس بنظم المعالجة الآلية للمعطيات نظرا لطبيعتها التقنية الخاصة التي تستدعي السرعة في استخلاص الدليل الرقمي قبل فقدانه.[1]

إن تفتيش النظم المعلوماتية يكون بناء على القواعد العامة الواردة في ق إ ج والتي تقتضي أن يأخذ ضباط الشرطة القضائية إذن مكتوب من اجل القيام بتفتيش المساكن،[2] حيث نصت المادة 05 من القانون 09\04 انه "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار ق إ ج..."

الفرع الثالث: ضبط الأدلة الرقمية.

إن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة المتحصل عليها أثناء التفتيش المنظومة المعلوماتية، والضبط يعني وضع اليد على أي شيء يتصل بالجريمة المعلوماتية للكشف عن مرتكبها.

نصت المادة 6 من القانون 04/09 المذكور سابقا على انه: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وانه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في ق إ ج".[3]

---

[1] والي بدرة **المواجهة الإجرائية لجرائم المعلوماتية**، مذكرة مقدمة لنيل شهادة الماستر الأكاديمي، تخصص قانون جنائي كلية الحقوق والعلوم السياسية جامعة محمد بوضياف المسيلة، سنة 2018–2019 الجزائر ص46.

[2] خالد ممدوح إبراهيم **فن التحقيق الجنائي في الجرائم المعلوماتية**، دار الفكر الجامعي الإسكندرية، ط1 سنة2009 ص 220، نقلا عن والي بدرة مرجع نفسه نفس ص.

[3] المادة 6 من القانون 04/09، مرجع سابق.

وضبط الأدلة في الجريمة المعلوماتية يكون على أشياء مادية كجهاز الحاسوب وملحقاته أو الأقراص الصلبة والطابعة وبطاقات الائتمان أو المعدات المستعملة في شبكة الانترنت أو أشياء معنوية كالبرامج والبيانات المعالجة آليا والمراسلات والاتصالات الالكترونية عبر البريد الالكتروني أو شبكات التواصل الاجتماعي.

كل هذه الأشياء المضبوطة والمحجوزة توضع في بيئة يصعب الوصول إليها أو التعامل بها أو تخريبها وذلك بموجب المادة 7 من القانون المذكر أعلاه حيث نصت على انه: "إذا استحال إجراء الحجز وفا لما هو منصوص عليه في المادة 6 أعلاه، لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة للوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".[1]

وللضبط المعلوماتي مجموعة إجراءات تتمثل فيما يلي:[2]

- الحصول على إذن من السلطات المختصة تجيز تفتيش المنظومة المعلوماتية وان يتضمن الإذن لتحديد النظام محل كل التفتيش بدقة وعنوان المتهم واسمه والجهاز الذي يقوم بالدخول لنظام الحاسوب وضبط ما يحتويه من معطيات وبيانات.
- قدرة المحقق المعلوماتي على التعامل مع الدليل بطريقة فنية والمحافظة عليها دون إتلافها أو محوها وكذا إتباع القواعد الفنية لتحرير الدليل الرقمي المضبوط.
- أخذ نسخة احتياطية عن الجهاز وعن وسائط تخزين المعلومات لضمان عدم المساس بالدليل الأصلي الذي يترك للخبراء لفحصه.

[1] المادة 7 من القانون 04/09، مرجع سابق.

[2] والي بدرة ،مرجع نفسه ص 47- 48.

●تخزين الدليل في أماكن غير معرضة لمجالات كهرومغناطيسية أو الكهرباء الساكنة أو الغبار ودرجة الحرارة تتراوح بين 4 و32 درجة مؤوية وقد تصل مدة تخزين الأقراص و الأشرطة لثلاث سنوات.

المطلب الثاني: إجراءات التحري والتحقيق الحديثة لمواجهة الجريمة الالكترونية.

ذهب المشرع الجزائري كغيره من المشرعين لاستحداث إجراءات التحري والتحقيق الخاصة بالجريمة الالكترونية، نظرا لسرعة وسهولة محو آثار الجريمة وصعوبة اكتشافها بغية تسهيل ضبطها والحد منها قبل تفاقم خطرها، حيث قسمنا هذه الإجراءات إلى:

الفرع الأول: التسرب المعلوماتي.

لجأ المشرع الجزائري إلى صد الجريمة المعلوماتية بالإجراءات الحديثة حيث اعتمد على عملية التسرب المعلوماتي والتي هي أولى الإجراءات لمواجهة الجريمة.

أولا: تعريف التسرب المعلوماتي.

نصت المادة 65 مكرر 12 من ق إ ج بأن التسرب المعلوماتي هو "قيام ضابط الشرطة أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيمائهم انه فاعل معهم أو شريك".[1]

حيث خصص المشرع الجزائري الفصل الخامس من القانون رقم 22\06 والمؤرخ سنة 2006 المتضمن ق إ ج تحت عنوان "في التسرب" المواد 65 مكرر 11 إلى المادة 65

[1] المادة 65 من القانون رقم 01\06، المؤرخ في 20 فيفري 2006 المتعلق بالوقاية من الفساد ومكافحته ج ر العدد 14، الصادرة بتاريخ 08 مارس 2006.

مكرر 18، والذي تناول من خلالها مفهوم التسرب وشروط إجراءاته والحماية الجنائية للقائم بهذه العملية.

ثانيا: شروط صحة التسرب المعلوماتي.

للتسرب المعلوماتي مجموعة الشروط تتمثل في:

1_ الشروط الشكلية

أ_ صدر بإذن قضائي: جاء في المادة 6 مر ر 11 ق إ ج أن وكيل الجمهورية أو قاضي التحقيق من يصدر الإذن القضائي للتسرب المعلوماتي وانه لا يمكن الشروع بالعملية إلا بعد الحصول على الإذن.

ب_أن يكون مكتوبا: جاء في المادة 65 مكرر 15 من ق إ ج أن يكون الإذن المسلم مكتوبا تحت طائلة البطلان، مع ضرورة ذكر نوع الجريمة ومحل عملية التسرب واسم ضابط الشرطة القضائية الذي تمت عملية التسرب على مسؤوليته.

واشترطت نفس المادة تحديد مدة عملية التسرب والتي لا تتجاوز أربعة أشهر مع إمكانية تجديدها حسب متطلبات التحقيق.

2_ الشروط الموضوعية:

أ_السبب: ويعني الأسباب والدوافع التي منحت الإذن بالتسرب هذا ما جاء في المادة 65 مكرر 15 من ق إ ج.[1]

ب_نوع الجريمة: يجب أن تكون التسرب في الجرائم الستة[2] المنصوص عليها في المادة 65 مكرر 5 .

[1] راجع المادة 65 مكرر 15 من ق إ ج.

[2] الجرائم الستة هي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بنظم المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب الجرائم المتعلقة بالتشريع الخاص بالصرف.

ج_ السرية التامة للعملية: نصت المادة 65 مكرر 16 من ق إ ج بوجوب السرية التامة والمطلقة لعملية التسرب وقد حصر المشرع مجال العلم بها للجهات المختصة المانحة للإذن بالتسرب (وكيل الجمهورية، قاضي التحقيق).

الفرع الثاني: مراقبة الاتصالات الالكترونية.

من بين الإجراءات الحديثة التي لجأ إليها المشرع الجزائري مراقبة الاتصالات الالكترونية نظرا لعجز الإجراءات القديمة في مجابهة الجريمة المعلوماتي.

أولا: تعريف مراقبة الاتصالات الالكترونية.

نص المشرع الجزائري في ق إ ج على مراقبة الاتصالات الإلكترونية والتي تعد احد أساليب التحري الخاصة والمستحدثة التي تمس بحرمة الحياة الخاصة للأشخاص المكفولة دستوريا.[1]

حيث جاء في المادة 3 من القانون 09\04 انه 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 ق إ ج وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

ثانيا: حالات اللجوء للمراقبة الالكترونية.

يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 أعلاه في الحالات التالية:[2]

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو جرائم الماسة بأمن الدولة.

[1] انظر المادة 34 من دستور سنة 1996.

[2] انظر المادة 04 من القانون 09\04.

- 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.

ثالثا: ضوابط المراقبة الالكترونية.

جاء في المادة 04 من القانون المذكور سابقا على حالات اللجوء للمراقبة الالكترونية والتي تسري عليها مجموعة ضوابط هي:

- صدور الإذن من السلطة القضائية المختصة.
- تكون مدة الإذن 6 أشهر قابلة للتجديد.[1]
- يباشر عملية المراقبة ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13.

رابعا: إجراءات المراقبة الالكترونية.

تتمثل إجراءات المراقبة في:

1_ اعتراض المراسلات: جاء في المادة 65 من ق إ ج أن المراسلات هي تلك التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

2_ تسجيل الأصوات: تتمثل في تسجيل كل الاتصالات السلكية واللاسلكية والكلام بصفة سرية دون موافقة المعني من طرف شخص أو عدة أشخاص.[2]

[1] انظر المادة 13 من القانون 09\04.

[2] راجع المادة 65 مكرر 5 و 65 مكرر 10 ق إ ج المعدل سنة 2006.

3_ التقاط الصور: كفل المشرع الجزائري التقاط الصور لشخص أو عدة أشخاص إلا في بعض الضوابط التي تطرقنا إليها سابقا نظرا لسرية هذا الإجراء ومساسه بالحياة الخاصة

الفرع الثالث: حفظ المعطيات المتعلقة بحركات السير.

يعتبر حفظ المعطيات المتعلقة بحركات السير من أهم مصادر التحري الحديثة التي لجأ إليها المشرع، والتي غالبا ما يستعان بها في البحث والتحقيق سواء في الجرائم التقليدية والمستحدثة كجرائم الانترنت.

عرف المشرع الجزائري المعطيات المتعلقة بحركات السير في المادة 02 الفقرة (هـ) من القانون 09\04 سالف الذكر على أنها "أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة الاتصالات توضح مصدر اتصال والوجهة المرسلة إليها والطريق الذي يسلكه ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة".[1]

حيث اقر المشرع الجزائري كباقي التشريعات إلزامي مقدمي الخدمات حفظ المعطيات المتعلقة بحركات السير بغية الوصول لآثار الجرائم مهما كانت وعرفه بموجب المادة 02 الفقرة د من القانون 09/ 04 على انه "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام اتصالات وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو مستعملها"[2].

جاء في المادة 11 من القانون 09\04 انه "مع مراعاة نوعية وطبيعة الخدمات يلزم مقدمو الخدمات بحفظ":[3]

---

[1] انظر المادة 02 الفقرة هـ من القانون 09\04 المذكور سابقا.

[2] انظر المادة 02 الفقرة د من قانون 09\04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته.

[3] راجع المادة 11 من القانون 09\04.

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.
- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

خاتمـــــــة

نستخلص مما سبق أن الجريمة الإلكترونية من أخطر الجرائم الحديثة والتي يصعب اكتشافها وإثباتها ذلك نظرا إلى التطور السريع التي شهدته المعلوماتية، والجريمة الإلكترونية قضية حساسة في كل المجتمعات العربية والغربية حيث أنها جرائم نائمة شديدة الإغراء للمجرمين عابرة للحدود، هذا مع جعل المشرع الجزائري يتصدى لمحاربة هذه الجريمة بسن القوانين ووضع الآليات المحصورة في قانون العقوبات الجزائري (القانون 09/04 _ القانون 15/04) والذي صنف الجريمة الإلكترونية إلى ثلاثة أنواع:

- جريمة الدخول أو البقاء الغير المشروع في أنظمة المعالجة الآلية للمعطيات.
- جريمة التلاعب بالمعطيات.
- جريمة التعامل في المعطيات غير المشروعة.

وبهذا يعتبر المشرع الجزائري قد خطى خطوة كبيرة في المجال المعلوماتي وتشريعاته لا تقل شأنا عن التشريعات الأوروبية، إلا أنه يجب الاستفادة من الدول الرائدة في محاربة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال عموما والجريمة الإلكترونية خصوصا حيث توصلنا إلى النتائج التالية:

- رغم الجهود الدولية المبذولة لمكافحة الجريمة المعلوماتية إلا أنها تبقى محدودة وعديمة الفعالية في كثير من الأحيان الأمر الذي يتطلب مزيدا من الجهود والعمل وعقد المؤتمرات وإبرام اتفاقيات دولية من أجل الوصول إلى أفضل السبل والآليات الممكنة لمكافحة الجريمة المعلوماتية.
- خطى المشرع الجزائري خطوات إيجابية في مجال سن تشريعات حديثة سهلت للقاضي آليات البث في قضايا الجريمة المعلوماتية بما يتضمن عدم المساس بمبدأ الشرعية الجنائية.
- قصور القوانين التقليدية أمام هذه الجرائم المستحدثة.

- إن لمبدأ الشرعية الجنائية في المجال المعلوماتي خصوصية من حيث الركن المادي والمعنوي للجريمة.

- يثير الركن الشرعي في جرائم المعلوماتية إشكالية استخدام مصطلحات مختلفة ذات دلالة متباينة وإن كانت بعض التشريعات قد اعتمدت إلى تحديدها فإن غالبية المشرعين يوكلون تلك المهمة للفقه والقضاء وقد اتجه المشرع الجزائري إلى الاتجاه الثاني.
- أن الجريمة المعلوماتية لها جوانب سلبية خطيرة تهدد امن وسلامة الفرد والمجتمع وتتسم بالغموض حيث يصعب إثباتها والتحقيق فيها مما يضع مسؤولية كبيرة على ضباط الشرطة والقضاء.
- قام المشرع الجزائري بمكافحة الجريمة الإلكترونية على غرار باقي الدول بموجب تعديل قانون العقوبات رقم 15/04 حيث اعتبر الدخول غير مشروع للنظام المعلوماتي والبقاء فيه والمساس بالمنظومة المعلوماتية وبعض الأفعال الأخرى أفعال إجرامية وسطر لها عقوبات، واستدرك النقص في المجال الإجرامي بإصدار قانون رقم 04/09 إذ تضمن قواعد إجرامية وأخرى وقائية وهذه الخطوة إيجابية إلا أنها غير كافية لمواجهة خطر الجريمة الإلكترونية مقارنة بالتطور الإجرامي المعلوماتي.

الاقتراحات:

- ضرورة مراجعة التشريعات الوطنية أو تعديلها من خلال تشديد الوصف الجنائي والعقوبات المقررة للأنماط الإجرامية للجريمة الإلكترونية بغية تحقيق الردع والقضاء عليها .
- التعاون الدولي من الناحية الإجرائية لكشف وتشخيص الجرائم وتسليم المجرمين .
- التعاون الدولي لتطوير الخبرة والتقنية لحماية البرامج والمعطيات الآلية وكل شبكات الإنترنت.
- الاستعانة بمختصين وخبراء قادرين على تشخيص الجريمة والعمل على تكوين فرق من الضبطية القضائية والقضاة مع توفير كافة الوسائل المادية والتقنية اللازمة لها لأداء عملها ومهامها على أحسن صورة .

- إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية وتسهيل تطبيقها في القطاعين العام والخاص .
- ضرورة إبرام اتفاقيات عربية ودولية في مجال مكافحة جرائم تقنية المعلومات وذلك لتحديد إطار الاختصاص القضائي الدولي والتعاون في كشف وإثبات الجريمة الإلكترونية .
- تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحته والحد من آثاره.

قائمة المصادر والمراجع

أولا: المصادر والمراجع باللغة العربية.

1_القرآن

2_القوانين والأوامر:

- القانون رقم 04/15 الصادر في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66/156 الصادر في 08 جوان 1966 المتضمن قانون العقوبات ج ر عدد 71 .
- القانون رقم 06\01، المؤرخ في 20 فيفري 2006 المتعلق بالوقاية من الفساد ومكافحته ج ر العدد 14، الصادرة بتاريخ 08 مارس 2006.
- القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 156/66 المؤرخ في 1966 المتضمن قانون العقوبات (ج ر الصادرة بتاريخ 10_11_2004).
- القانون رقم 04/09 الصادر في 14 شعبان الموافق ل 5 غشت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها ج ر العدد 47 الصادر بتاريخ 16/08/2009.
- المادة 65 من القانون رقم 06\01، المؤرخ في 20 فيفري 2006 المتعلق بالوقاية من الفساد ومكافحته ج ر العدد 14، الصادرة بتاريخ 08 مارس 2006.
- المادة 93 مكرر 02، القانون رقم 01\08 المؤرخ في 23 جانفي 2008 المتمم للقانون 83\01 المتعلق بالتأمينات.
- المادة 127 من القانون رقم 03-2000 المؤرخ في 5 اوت 2000 والذي يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.
- الدستور الجزائري المادة 35 سنة 1996.
- المادة 46 الدستور الجزائري المعدل سنة 2020.
- مولود ديدان، ق إ ج، الأمر رقم 11-02 دار بلقيس الجزائر

3_المراجع:

- جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، دار النهضة العربية سنة 2002
- خالد ممدوح إبراهيم فن التحقيق الجنائي في الجرائم المعلوماتية، دار الفكر الجامعي الإسكندرية ط 1 سنة 2009.
- عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي الإسكندرية سنة 2006.
- علي حسن الطواليه، الجرائم الالكترونية، جامعة العلوم التطبيقية سنة 2008.
- محمد خليفة الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري المقارن، دار الجامعة الجديدة مصر سنة 2007.
- محمد خليفة خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها، كلية الحقوق والآداب والعلوم الاجتماعية جامعة 8 ماي 1945 قالمة الجزائر.
- محمود احمد طه، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، ط 1 دار الفكر والقانون للنشر والتوزيع مصر سنة 2013.
- نهلا عبد القادر المومني الجرائم المعلوماتية ماجستير في القانون الجنائي المعلوماتي، دار الثقافة للنشر والتوزيع ط 1 سنة 2008.
- نهلا عبد القادر المومني الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع ط 2 سنة 2004.

4_الرسائل الجامعية:

- أحمد مسعود مريم، آليات مكافحة الجرائم تكنولوجيا الاتصال والإعلام في ضوء القانون رقم 09\04، مذكرة لنيل الشهادة الماجستير، تخصص قانون جنائي، جامعة قاصدي مرباح كلية الحقوق ورقلة 2012– 2013

- انشاش منية مداخلة حول الركن المفترض في الجريمة الإلكترونية، جامعة بسكرة سنة 2015_2016

- رصاع صفيحة الحماية الجنائية للمعلومات على شبكة الإنترنت، مذكرة لنيل شهادة الماجستير في القانون العام جامعة أبي بكر بالقائد تلمسان 2011-2012.

- صغير يوسف الجريمة المرتكبة عبر الإنترنت، مذكرة لنيل شهادة الماجستير في القانون تخصص القانون الدولي للأعمال، جامعة مولود معمري تيزي وزو.

- غازي عبد الرحمان الرشيد الحماية القانونية من جرائم المعلومات**ية**، أطروحة لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان كلية الحقوق سنة 2004.

- محمد عبيد الكعبي الجرائم الناشئة عن الاستخدام غير مشروع لشبكة الإنترنت، دار النهضة العربية القاهرة.

- محمود صالح العادلي الجريمة المعلوماتية (ماهيتها وصورها) ورقة المقدمة.

- مطماطي راوية الجريمة الإلكترونية في التشريع الجزائري، رسالة دكتوراه تخصص قانون أعمال، كلية حقوق جامعة عبد الحميد بن باديس مستغانم الجزائر.

- والي بدرة المواجهة الإجرائية لجرائم المعلوماتية، مذكرة مقدمة لنيل شهادة الماستر الأكاديمي، تخصص قانون جنائي كلية الحقوق والعلوم السياسية جامعة محمد بوضياف المسيلة، سنة 2018-2019.

5_ المجلات المقالات القانونية:

- براهيمي جمال، مكافحة الجريمة الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود العمري، تيزي وزو العدد 2 الصادرة في 2016\11\15.

- بردال سمير الجريمة المعلوماتية في التشريع الجزائري، ASJP: Algerian Scientific Journal plat Form المجلد 1 العدد 2.

- بوضياف أسمهان، الجريمة الالكترونية والإجراءات التشريعية لمواجهتها،مجلة الأستاذ الباحث للدراسات القانونية، العدد 11 سبتمبر 2018.
- حاتم أحمد محمد بطيخ تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات (دراسة تحليلية مقارنة)، مجلة الدراسات القانونية والاقتصادية، جامعة عين الشمس كلية الحقوق مصر، مقال 5 مجلد 7 عدد 1 أغسطس 2021.
- حمزة خضري، حمزة عشاش، خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري، مجلة الدراسات القانونية والسياسية، مجلد 6، عدد 02جوان 2020.

مليكة عطوي الجريمة المعلوماتية حوليات جامعة الجزائر مجلة علمية 2012 العدد 21.

6_ الملتقيات والمؤتمرات العلمية:

- ذياب البداينة الجرائم الإلكترونية المفهوم والأسباب، الملتقى العلمي" الجرائم المستحدثة في ضل المتغيرات والتحولات الاقتصادية والدولية" خلال الفترة 2/09/2014 _4 الأردن.
- علي عبد القادر القهوجي الحماية الجنائية للبيانات المعالجة إلكترونيا،بحث مقدم لمؤتمر القانون والكمبيوتر والانترنيت كلية الشريعة والقانون جامعة الإمارات سنة 2000.
- فضيلة عاقلي، الجريمة الالكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر(الجرائم الالكترونية) طرابلس، 24-25 مارس 2017.
- محمد الأمين البشري التحقيق في جرائم الحاسب الآلي، بحث مقدم إلى مؤتمرات القانون والكمبيوتر والانترنت، كلية الحقوق والشريعة جامعة الإمارات 21 ماي 2005.

- مجمع البحوث والدراسات الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها، بحث مقدم في مسابقة جائزة الأمير نايف بن عبد العزيز للبحوث الأمنية سلطنة عمان سنة 2016.

7_ المواقع الالكترونية:

- موقع منظمة التعاون الاقتصادي والتنمية www.ocd.org
- ماهية الجريمة الإلكترونية University .lifestyle.Net

- Symantec corporation what is cyber crime http:||US.morton.com | cyber crime-definition.

ثانيا: المراجع الأجنبية.

1_ القوانين الأجنبية:

- المادة الأولى من نظام المكافحة لجرائم المعلوماتية السعودي.
- المادة الأولى من القانون المصري رقم 15 لسنة 2003.

- Le Journal officiel nationale de droit français. -

2_ مؤلفات باللغة الأجنبية:

- Bainbridge (David) hacking the unavthorisedaccess of computer system the legal implication m.l.rev. March 1989 volume 52.

- Catherine A Theohary congressional resrarch &Kristin finklea service informing the lesgislatine debatesince 1914 Cybercrime: conceptual issues for congress and V.S.Law Enforcement January 15.2015

- Nouveaux " van der hulst and Neve .2008 p 18 forum scientifique crimes à la lumière des changements et transformation régionaux et internationaux

"forum scientifique stol, 2013& Leukfeldt veenstra

- Nouveaux crimes à la lumière des changements et transformation internationaux"régionaux et .

الفهـــرس

الفهرس :

مقدمة...ص أ

الفصل الأول: مفهوم الجريمة الالكترونية......................ص 9

المبحث الأول: تعريف الجريمة الإلكترونية.......................ص 10

المطلب الأول: التعريف اللغوي والاصطلاحي.........................ص 10

الفرع الأول: التعريف اللغوي للجريمة الإلكترونية.......................ص 10

الفرع الثاني: التعريف الاصطلاحي للجريمة الإلكترونية...................ص11

المطلب الثاني: التعريف الفقهي والتعريف القانوني......................ص 13

الفرع الأول: التعريف الفقهي للجريمة الإلكترونية.......................ص 13

الفرع الثاني: التعريف القانوني للجريمة الإلكترونية....................... 17

المبحث الثاني: أركان الجريمة الالكترونية ودوافع ارتكابها....................ص25

المطلب الأول: أركان الجريمة الالكترونية.......................................25

الفرع الأول: الركن الشرعي للجريمة الإلكترونية.........................ص 26

الفرع الثاني: الركن المادي للجريمة الإلكترونية..........................ص 27

الفرع الثالث: الركن المعنوي للجريمة الإلكترونية..........................29

المطلب الثاني: أسباب ودوافع ارتكاب الجريمة المعلوماتية....................ص 31

الفرع الأول: الدوافع الشخصية.......................................ص 31

الفرع الثاني: دوافع أخرى.. ص 32

الفصل الثاني: مواجهة الجريمة الالكترونية.....ص 35

المبحث الأول: المواجهة التشريعية للجريمة الالكترونية.....ص 36

المطلب الأول: مكافحة الجريمة الإلكترونية بموجب القوانين العامة.....ص 36

الفرع الأول : مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري والقانون المدني.... 36

الفرع الثاني: مكافحة الجرائم الالكترونية بموجب قانون العقوبات الجزائري وقانون الإجراءات الجزائية..... ص 38

المطلب الثاني: مكافحة الجريمة الالكترونية بموجب القوانين والهياكل الخاصة.... ص 41

الفرع الأول: مكافحة الجريمة الالكترونية بموجب القوانين الخاصة..... ص 41

الفرع الثاني: مكافحة الجريمة الالكترونية بموجب الهياكل الخاصة..... ص 45

المبحث الثاني: المواجهة الإجرائية للجريمة الالكترونية..... ص 45

المطلب الأول: الإجراءات القديمة لمواجهة الجرائم الالكترونية..... ص 46

الفرع الأول: الخبرة والمعاينة في الجرائم المعلوماتية..... ص 46

الفرع الثاني: التفتيش المعلوماتي..... ص 47

الفرع الثالث: ضبط الأدلة الرقمية..... ص 49

المطلب الثاني: الإجراءات المستحدثة لمواجهة الجريمة المعلوماتية.....ص 50

الفرع الأول: التسرب المعلوماتي..... ص 50

الفرع الثاني: مراقبة الاتصالات الالكترونية..... ص 52

الفرع الثالث: حفظ المعطيات المتعلقة بحركات السير............................. ص 54
خاتمة... ص 57
قائمـة المصـادر والمراجـع... ص 61

ملخص:

الجريمة الالكترونية ظاهرة عالمية أدى بها إلى المساس بجوانب مختلفة منها الاجتماعية السياسية الاقتصادية وحتى الشخصية، فأصبحت بمثابة خطر على الصعيد الوطني والدولي لذا عمدت الدراسة في معرفة الجريمة على المستوى الوطني والدولي من خلال تعريفها والتعرف على أركانها وأحكامها والعقوبات المقررة لها، حيث أن المشرع الجزائري اضطر كباقي الدول إلى وضع مجموعة من القوانين لمكافحة ومجابهة هذه الجريمة التي تختلف تماما عن الجرائم التقليدية، وسارع إلى استحداث المواد القديمة للحد من وقوعها وانتشارها وذلك بسبب التزايد اللامتناهي للاعتداءات على الأنظمة المعلوماتية في العالم والجزائر على وجه الخصوص.

Summary:

Cybercrime is a global phenomenon that has affected various aspects, including social, political, economic and even personal, it has become a danger at the national and international levels, so the study proceeded to know the crime at the national and international level by defining it and identifying its elements, provisions and penalties prescribed for it, as the Algerian legislator was forced, like other countries, to put in place a set of law to combat and confront this crime, which is completely different from the traditional crime, he hastened to develop old materials to limit their occurrence and spread, due to the endless increase in attacks on information systems in the world and Algerian in particular.

تم بحمـــد
الله