وزارة التعليم العالي والبحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

قسم: القانون الخاص

المرجع:

مذكرة نهاية الدراسة لنيل شهادة الماستر

الجريمة الالكترونية وطرق مكافحتها

الشعبة: الحقوق.

التخصص: قانون قضائي.

من إعداد الطالب

عبود عبد الرحمان جمال الدين

تحت إشراف الأستاذ

مزيود بصيفي

أعضاء لجنة المناقشة

الأستاذ(ة)..... بن عزوز سارة .....رئيسا

الأستاذ(ة)..... مزيود بصيفي .....مشرفا مقررا

الأستاذ(ة)..... بوسحبة جيلالي .....مناقشا

السنة الجامعية: 2022-2023

نوقشت يوم: 2023/07/04

قَالُواْ سُبۡحَٰنَكَ لَا عِلۡمَ لَنَآ إِلَّا مَا عَلَّمۡتَنَآۖ إِنَّكَ أَنتَ ٱلۡعَلِيمُ ٱلۡحَكِيمُ ٣٢

سورة البقرة: الآية 32 .

... ۚ وَمَا تَوۡفِيقِيٓ إِلَّا بِٱللَّهِۚ عَلَيۡهِ تَوَكَّلۡتُ وَإِلَيۡهِ أُنِيبُ ٨٨

سورة هود: الآية 88 .

الإهـــــــداء

الحمد لله الذي وفقني لإتمام هذا العمل فله الشكر والثناء

أهدي ثمرة جهدي المتواضع إلى من وقفوا بجانبي في كل الصعاب

إلى من ربياني وشملاني بعظيم عطفهما.

وكانا عونا دائما وحضنا واقيا بدعوتهما للخطوات التي سرت على دربها

إلى والدي أطال الله في عمرهما

إلى زملائي وزميلاتي وكل الأهل والأقارب

إلى كل من ساعدني في اتمام هذا العمل من قريب أو من بعيد

الشكـــــر والعرفان

الحمد لله الذي أعاننا على القصد ورزقنا من العلم ما لم نكن نعلم وأمدنا بالعزيمة والإرادة على إنجاز هذا العمل وامتثالا لقول المصطفى عليه الصلاة والسلام من لا يشكر الناس لا يشكر الله

ولا يسعنا في هذا المقام إلا أن تتقدم بخالص الشكر والتقدير إلى الأستاذ المشرف "مزيود بصيفي" على ارشاداته وتوجيهاته القيمة، وكذا على اشرافه، جزاه الله عنا خير جزاء أملا أن تجد كلامنا هذا الامتنان والعرفان.

كما لا يفوتني أن أتقدم بالعرفان والشكر لجميع أعضاء لجنة المناقشة على قبولهم لتحكيم هذه المذكرة، وعما كلفتهم من وقت في دراستها وقبولها للمناقشة.

ودون أن أنسى أساتذة كلية الحقوق.

أطال الله في أعمارهم جميعا وأمدهم بالصحة والعافية، وجزاهم عنا أعظم الجزاء.

قائمـــــــة المختصـــــرات

- ج، ر، ج، ج: الجريدة الرسمية للجمهورية الجزائرية
- دذدن دون ذكر دار النشر
- دذط دون ذكر الطبعة
- ط الطبعة
- ص الصفحة
- ص ص من الصفحة إلى الصفحة

مقدمة

إن الجريمة ظاهرة قديمة، عرفتها المجتمعات البشرية منذ القدم، وظهرت في المجتمعات السلطة الحاكمة انطلاقا من رب الأسرة إلى شيخ القبيلة، حيث وضعت بعض القيود على تصرفات الأفراد لاستتباب الأمن لدى الفرد والمجتمع، واعتبرت أن كل فعل يمس أمن الجماعة أو حياة الفرد أو ماله أو سلامته الجسدية فعلا مجرما يستوجب العقاب المناسب.

لكن بعد ظهور وتطور فكرة الدولة تولت هذه الأخيرة بنفسها سلطة تجريم الأفعال، حيث أصدرت القوانين والتشريعات، منها ما هو موضوعي يجرم الأفعال ويحدد العقوبات لها، ومنها ما هو إجرائي حيث يحدد الإجراءات الواجب إتباعها.

غير أنه وبالتقدم العلمي والتكنولوجي الهائل الذي تشهده البشرية في عصر الحديث والذي يلقي بضلاله ونتائجه على كافة جرائمي الحياة، والعلاقات بين الأفراد والدول فقد أصبحت تكنولوجيا المعلومات اليوم سمة من سمات العصر الراهن فالتقدم العلمي والتكنولوجي فتح أفاقا ضخمة أمام تقدم البشرية وتحقيق مستوى أفضل من الحياة، إلا أنه يحمل في نفس الوقت بين طياته مخاطر ضخمة تهدد قيم وحقوق وأمن الأفراد والجماعة فقد أدى الاستعمال الغير المشروع إلى ظهور نوع جديد من الجرائم سميت بالجرائم الإلكترونية أو الجرائم المعلوماتية أو جرائم الأنترنت وهذه المصطلحات كلها تعبر عن مجموعة من الجرائم المرتبطة بالأنظمة الإلكترونية والشبكة المعلوماتية وخصوصا على شبكة الأنترنت.

إن الأضرار الوخيمة للجرائم الإلكترونية المستحدثة في يومنا هذا، سواء على الأفراد ككل، أو على مؤسسات الدولة، أدّت بالمشرع الجزائري إلى التفكير في ضرورة التصدي لها وقمعها أو على الأقل العمل على الحدّ منها. وهو ما لا يتحقق في نظرنا إلا بالتنظيم القانوني الفعال لهذا الصنف من الجرائم.

وسعيا وراء تحقيق هذا الهدف فإنّ مشرعنا قد اتجه إلى استحداث نصوص قانونية وطنية كثيرة بهدف التماشي مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال.

تبعا لذلك، عمد المشرع الجزائري إلى تعديل وإعادة النظر في العديد من التشريعات الوطنية وعلى رأسها قانون العقوبات كقانون عام، وأكثر من ذلك، فإنّه استحدث قوانين أخرى خاصة لم تكن معروفة من قبل، وكل ذلك من أجل ضمان الحماية الجنائية للمعاملات الإلكترونية.

تتجلى أهمية هذه الدراسة في كون هذا النوع المستجد من الإجرام مرتبط بالتقنية الحديثة المتمثلة في الحاسب الآلي وشبكة الانترنيت والتي هي في تطور دائم، حيث تمتد خطورتها إلى المساس بسلامة الأفراد من جهة والمساس بكيان وأمن الدولة من جهة أخرى، مما يستدعي الضرورة الملحة لإيجاد سبل كفيلة وفعالة لمكافحة الجريمة الإلكترونية وذلك بتوعية المواطنين بمدى خطورة هذه الجريمة لمسايرة التطور الحاصل لتكنولوجيا الإعلام والاتصال والحد من ظاهرة الإجرام الإلكتروني من خلال الجهود الدولية والوطنية الفعالة في إطار الكشف عنها من طرف المحققين، وإثبات حدوثها لإدانة المتهم بارتكابها.

أما العوامل التي حفزتنا على اختيار هذا الموضوع، فيمكن إرجاعها إلى كون الجريمة الإلكترونية تعتبر من الجرائم الحديثة والأكثر تعقيدا من حيث الإثبات والإتيان بالدليل لإدانة المتهم، وكذلك معرفة الطرق القانونية التي وضعها المشرع الجزائري من أجل محاربة ومكافحة هذا النوع من الجرائم، وكذلك الرغبة في الوقوف على حقيقة التعامل مع هذه الظاهرة من الناحية الإجرائية، وكذا الوصول إلى نتائج تخدم المجتمع بالإضافة إلى إظهار أنواع هذه الجرائم وعقوبتها في القانون.

كما أن الهدف من دراسة هذا الموضوع يتمثل في إثراء المكتبة وسد النقص في المراجع المتخصصة في هذا المجال، ومحاولة دراسة الظاهرة وتحليلها وبيان كيفية مكافحتها، غير أنه قد واجهتنا بعض الصعوبات في إنجاز البحث كون أن الموضوع له علاقة بالجانب التقني والفني، وهذا ما يستدعي التخصص للإلمام أكثر بالموضوع، كما أن حداثة موضوع الجريمة الإلكترونية الذي لا يزال في أول مراحله أدت إلى عدم كفاية النصوص القانونية المعالجة له، وكذا اختلاف

أراء الفقهاء حول الكثير من المسائل والمفاهيم المرتبطة بالجريمة الإلكترونية وعدم استقرارهم على اتجاه واحد الأمر الذي زادها تعقيدا.

والإشكال الذي يطرح في هذا الصدد هو :

- **ما مدى نجاعة الطرق المنتهجة في مكافحة الجريمة الالكترونية؟**

ويندرج تحت هذا التساؤل الأسئلة الفرعية الآتية:

ما مفهوم الجريمة الإلكترونية؟ وما أركانها وصورها؟ وماهي طبيعتها القانونية؟ وفيما تتمثل إجراءات متابعتها في التشريع الجزائري؟ وما هي الآليات المختصة في مكافحتها؟

وللإجابة على الإشكالية الرئيسية والأسئلة الفرعية المطروحة اعتمدنا في معالجة موضوع دراستنا على المنهج الوصفي وهذا من أجل تعريف الجريمة الإلكترونية والوقوف على خصائصها، بالإضافة إلى مناهج تكميلية أخرى متمثلة في المنهج التحليلي والمنهج المقارن لدراسة حيثيات موضوعنا بكل جوانبه.

متبعة في ذلك خطة منهجية ثنائية الفصول، حيث خصص الفصل الأول إلى الإطار المفاهيمي للجريمة الإلكترونية حيث تم التعرض إلى ماهية الجريمة الالكترونية في المبحث الأول أما المبحث الثاني صور الجريمة الالكترونية ودوافع ارتكابها؛ أما الفصل الثاني فقد تطرق إلى آليات مكافحة الجريمة الالكترونية من خلال إظهار طرق مكافحة الجريمة الالكترونية في المبحث الأول وفي الأخير تم عرض الحماية الإجرائية للجريمة الالكترونية في المبحث الثاني.

الفصل الأول:

الإطار المفاهيمي للجريمة الإلكترونية

عرفت البشرية في نهاية القرن الماضي اتساعا وتزايدا مطردا لنطاق استخدام تقنية المعلوماتية في المجتمع، ونظرا للتطور السريع لهذه التقنية فقد مكنت من استعمالات متعددة وفي جميع المجالات، مما أدى إلى ظهور نوع جديد من الجرائم أطلق عليها مصطلح "الجرائم الإلكترونية". وقد أثارت هذه الجرائم تساؤلات كثيرة باعتبارها ظاهرة جديدة ونظرا لجسامة أخطارها وفداحة خسائرها وسرعة انتشارها أصبح التعامل مع صور هذه الجرائم موضع اهتمام بالغ من الفنيين والمهتمين بأمن الصرح المعلوماتي وذلك لتحديد مفهومها وخصائصها[1]. كما أن هذه الجريمة الإلكترونية جلبت معها طائفة جديدة من المجرمين[2].

وفي خضم هذه الدراسات التي تحاول تحديد الجرائم الإلكترونية ووضعها في قالب قانوني وعلى هذا الأساس قمنا بتقسيم الفصل إلى مبحثين:

المبحث الأول: ماهية الجريمة الالكترونية

المبحث الثاني: صور الجريمة الالكترونية ودوافع ارتكابها

[1]– سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير، تخصص العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2011/2010، ص 08.

[2]– نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 01، دار الثقافة للنشر والتوزيع، عمان، 2008، ص46.

المبحث الأول: ماهية الجريمة الالكترونية

تعتبر الجريمة المعلوماتية من الظواهر الحديثة وذلك لارتباطها بتقنية حديثة هي تكنولوجيا المعلومات والاتصالات والكمبيوتر، وقد أحاطت بتعريف الجريمة المعلوماتية الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لهما، ولكن الفقه لم يتفق على تعريف محدد، بل إن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب إلكتروني.

فالجرائم المعلوماتية هي صنف جديد من الجرائم، ذلك أنه مع ثورة المعلومات والاتصالات ظهر نوع جديد من المجرمين، انتقل بالجريمة من صورها التقليدية إلى أخرى إلكترونية قد يصعب التعامل معها ففي بداية ظهور هذه الجرائم كانت هناك إشكالية تواجه المختصين في كيفية مكافحتها لأنها تتعلق بالبيانات والمعلومات، أي الكيان المنطقي للحاسب الآلي.

فنتيجة التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات حتى الآن، حال ذلك دون وضع تعريف فقهي جامع وشامل لمفهوم الجريمة المعلوماتية أو الإلكترونية، وما ورد من تعريفات في الفقه إنما اقتصر على الناحية محل بحث الفقيه[1]، ومما لا شك فيه أن وضع تعريف للجريمة المعلوماتية يثير العديد من المشكلات العملية لعل أهمها، صعوبة مواجهتها، وتعذر إيجاد الحلول المناسبة لمكافحتها.

حيث تم تحديد الجريمة الالكترونية في المطلب الأول ونتناول فيه عدة تعريفات منها تعريفات فقهية وتعريف منظمة التعاون الاقتصادي والتنمية وصولا للتعريف التشريعي الجزائري

وكمطلب ثاني تم التطرق إلى الخصائص التي تتميز بها الجريمة الالكترونية عن باقي الجرائم وكذا عرض أركان الجريمة الالكترونية.

[1]– خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2009، ص 73.

المطلب الأول: مفهوم الجريمة الإلكترونية

إن مفهوم الجريمة الالكترونية من المفاهيم الحديثة والتي لا يوجد لها تعريف دولي شامل وموحد، حيث تعتبر الجريمة الالكترونية من الظواهر الحديثة وذلك لارتباطها بتكنولوجيا المعلومات والاتصالات. وقد أحاط بتعريف الجريمة الكثير من الغموض حيث تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع ولكن الفقه لم يتفق على تعريف محدد بل أن البعض ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هي إلا جريمة تقليدية ترتكب بأسلوب الكتروني[1].

حيث تم التطرق في هذا المطلب إلى التعاريف المختلفة للجريمة الإلكترونية وتبيان طبيعتها القانونية من خلال ما يلي:

الفرع الأول: تعريف الجريمة الالكترونية

لا يوجد اجماع على تعريف ثابت وشرعي للجريمة الإلكترونية لما يثيره المصطلح من تعقيدات مفاهيمية[2]، لذا نحاول ان نتعرض لبعض التعاريف من حيث الجانب اللغوي ثم من الجانب الفقهي، وأخيرا ما جاء به التشريع الجزائري.

أولا: التعريف اللغوي والفقهي للجريمة الإلكترونية

1- التعريف اللغوي للجريمة الإلكترونية: وقبل أن نشرع بالتعريف الفقهي لكلمة جريمة الكترونية سنبدأ بالتعريف اللغوي أولا لأن مدلولات اللغة غالبا ما تؤثر في المصطلحات والمعاني التي يصطلح عليها الناس تتكون الجريمة الإلكترونية من كلمتين:

---

[1]- حفيظ نقادي معالم الجريمة المعلوماتية في القانون الجزائري مجلة الحقوق و العلوم الانسانية ، العدد 20 جامعة زيان عاشور بالجلفة، 2014، ص 170.

[2]- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية – شبكة الانترنت وشبكة الهواتف التقليدية والآليات والمطبوعات–، دار الثقافة للنشر والتوزيع، 2019، ص37.

أ- **جريمة:** اصلها من جرم بمعنى كسب وقطع والجرم بمعنى الحر، وقيل أنها كلمة فارسية معربة والجرم مصدر الجارم الذي يجرم نفسه وقومه شرا، كما تعني التعدي والذئب فالجريمة والجارم بمعنى الكاسب، واجرم فلان أي اكتسب الإثم كما تعني ما يأخذه الوالي من المذنب ورجل جريم وامرأة جريمة أي ذات جرم أي ذات جسم: وجرم الصوت جهارته والجريمة تعني الجناية والذنب[1].

والجريمة اصطلاحا: وهي مجموع السلوكيات والأفعال الخارجة عن نطاق القانون.

ب- **الكترونية:** يوصف جزء من الحاسوب وعمله.

وعرفتها الأستاذة بوزيدي مختارية[2]: " مجموع المخالفات التي ترتكب ضد الأفراد والمجموعات من طرف أفراد أو مجموعات أخرى بدافع الجريمة وبقصد ايذاء سمعة الضحية او القيام بأذى مادي او عقلي للضحية بطريقة مباشرة أو غير مباشرة باستخدام شبكات الاتصالات مثل الأنترنت".

كما عرفتها الدكتورة غنية باطلي[3]: " ان استعمال مصطلح الجريمة الإلكترونية من شأنه ان يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية والغش المعلوماتي او جرائم الاعتداء على معطيات الحاسب الآلي وجرائم الانترنت وبالتالي كان فيه من التوسع ما ينطوي تحت جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة علما انه لم يركز الفقهاء على التعريف اللغوي للجريمة الإلكترونية لتقارب المفاهيم التقنية في هذا المجال والمشتقة من الغش الإلكتروني والإجرام المعلوماتي حيث يرتكب الجرم بواسطة الحاسوب الآلي.

---

[1]– سامية عزيز، مازيا عيساوي، الجريمة من منظور سوسيولوجي الأسباب الآثار، مجلة دراسات في سيكولوجية الانحراف، السنة 2021، المجلد 6، العدد 1، ص 128.

[2]– بوزيدي مختارية ماهية الجريمة الإلكترونية مورقة بحثية مقدمة ضمن ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع، يوم 29 مارس 2017 ،الجزائر، ص 234.

[3]– غنية باطلي الجريمة الالكترونية دراسة مقارنة – الدار الجزائرية للنشر والتوزيع، الجزائر، طبعة 2015 ، ص 23.

2- التعريف الفقهي للجريمة الالكترونية

اختلف الفقهاء ورجال القانون على تعريف الجريمة الإلكترونية، حيث ان كل اتجاه اسس تعريفه بناء على الزاوية التي يرى فيها الجريمة (وسيلة ارتكابها – وهناك من يوسع في رؤيته للجريمة وهناك من يركز على جزء من الجريمة) وسنتطرق الى بعض التعاريف الفقهية وفقا لما يلي:

أ/التعريف الفقهي الضيق للجريمة الإلكترونية

كل اتجاه فقهي اعتمد وجهة نظر ضيقة في تعريفه للجريمة الإلكترونية، فمنهم من اعتمد على أداة الجريمة ومنهم من اعتمد على توافر المعرفة بتقنيات جهاز الحاسب الآلي، ومنهم من اعتمد على تعريفه بناء على موضوع الجريمة.

- **على اساس معيار أداة الجريمة**

تم تعريف الجريمة الإلكترونية وفقا لهذا المعيار على اساس اداة الجريمة فالجريمة تكون جريمة الكترونية طالما ان الحاسوب أو احدى الوسائل التقنية من وسائل ارتكابها (الهواتف الذكية....).

عرفها الأستاذ MASS بأنها:" الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق ربح".

أما الفقيه الألماني TIEDMANN فعرفها كما يلي: "كل اشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بواسطة جهاز الحاسوب".

كما عرفها الفقيهMAWRE :" الجريمة الإلكترونية هي الفعل غير المشروع الذي يتورط الحاسب الآلي في ارتكابه[1].

- **على اساس معيار توفر المعرفة بتقنية المعلومات**

اصحاب هذا الاتجاه لا يعتمدون على الحاسوب الآلي ولكن على الشخص الذي يستخدمه فبدون امتلاكه المعرفة بالتقنية لا يمكنه ان يستعمل الحاسوب ولا ان يرتكب جريمة اصلا، فالأستاذ

[1]– غنية باطلي، المرجع السابق، ص 15.

DAVID THOMSONعرفها بأنها " أي جريمة يكون متطلب لاقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب"، هنا المعيار الشخصي المتعلق بالجاني هو المعيار المعتمد، إذا تتم متابعة وملاحقة مقترف الفعل غير المشروع في حالة واحدة وهي علمه بتكنولوجيا الحاسبات الآلية.

- **على اساس معيار موضوع الجريمة**

يرى آخرون أن تعريف الجريمة الالكترونية انما يرجع الى موضوعها وغير متعلق بالوسيلة المستعملة او الفاعل، حيث يرى هؤلاء ان الجريمة الالكترونية هي التي يكون موضوعها المال المعلوماتي المعنوي دون النظر فيما إذا كان الحاسب هو الأداة المستعملة في ارتكابها[1].

ب/التعريف الموسع للجريمة الإلكترونية

من المتعارف عليه ان الوسيلة التي ترتكب بها الجريمة التقليدية لا تدخل في تعريفها ولا حتى تمكن الجاني من التقنية، فقد لا يكون الجاني متمكنا ويرتكب الجريمة ولا موضوع الجريمة، وتفاديا للانتقادات التي وجهت للمفهوم الضيق ظهر المفهوم الواسع كما يلي:

عرفها PARKER بما يلي: " كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه ".

" كل استخدام في صورة فعل او امتناع من شأنه الاعتداء على أي مصلحة مشروعة، سواء كانت مادية أو يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ومعاقب عليه قانونا أيا كان غرض الجاني"[2].

اما الفقيهان: MIEL وCREDO فعرفاها بأنها: "تشمل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج كل المصرح به لحاسوب المجنى عليه أو بياناته".

[1]– غنية باطلي، المرجع السابق، ص 17.

[2]– دمان ذبيح عماد بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في الجزائر، مجلة الحقوق والعلوم السياسية، العدد 13 جانفي 2020، ص 140.

المنظمة الأوروبية للتعاون والتنمية الاقتصادية عرفتها على أنها:" كل عمل او امتناع يأتيه الإنسان اضرارا بمكونات الحاسب الآلي المادية والمعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد تحت مظلة قانون العقوبات لحمايتها[1]".

عمل الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا هاما، او هي فعل اجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية"[2].

وعرفها مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقدة في فيينا 2000 ب:" يقصد بالجريمة الإلكترونية أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي او شبكة حاسوبية، او داخل نظام حاسوبي، والجريمة تلك التي تشمل من الناحية المدني جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[3].

واشمل تعريف للجريمة الإلكترونية الذي جاء به الدكتور عبد الفتاح بيومي حجازي جريمة تقنية تنشأ في الخفاء، يقترفها مجرمون اذكياء يمتلكون أدوات المعرفة التقنية، وتوجه للنيل من الحق في المعلومات، وتطال اعتداءاتها معطيات الحاسب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات ".

ج/ التعريف الفقهي المختلط أو الجامع

ان اعطاء تعريف موسع للجريمة الإلكترونية ادخل في نطاقها كل التصرفات غير المشروعة التي لها علاقة بالحاسب، سواء، وسيلة او موضوع او مناسبة ارتكاب هذا ما ادى الى ظهور

[1]– غنية باطلي، المرجع السابق، ص 19.

[2]– نياب سليمة بوترعة بلالا الجريمة الالكترونية الأسس والمفاهيم مجلة تطوير العلوم، المجلد 13 العدد 01 الجزائر. جامعة زيان عاشور الجلفة 2020، ص 10

[3]– عبد الفتاح بيومي حجازي مكافحة جرائم الكمبيوتر والأنترنت في القانون العربي نموذجي الأسكندرية، ، دار الفكر العربي، القاهرة، ص 33

اتجاه ثالث وهو الاتجاه الجامع ويعتمد هذا الاتجاه في تعريف الجريمة الإلكترونية على معيار المصلحة المحمية.

وقد اعتمده M. ALTERMAN وH .BALOCH "كل سلوك غير مشروع او يتعارض مع قواعد السلوك او غير مرخص والذي يخص المعالجة الآلية للمعطيات او لنقل المعطيات".

وهو تعريف منظمة التعاون والتنمية الاقتصادية للغش المعلوماتي والذي أوردته بلجيكا في تقريرها بان الجرائم المعلوماتية: " هي كل فعل او امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية[1].

ثانيا: تعريف الجريمة الالكترونية في التشريع الجزائري

وضع المشرع الجزائري مفهوما للجريمة المتصلة بتكنولوجيات الإعلام والاتصال ضمن **القانون 09-04** المؤرخ في 14 شعبان عام 1430 الموافق لـ عام 1430 الموافق لـ : غشت سنة 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذا القانون المنشئ للقطب الجزائي الوطني المختص الأمر رقم 21-11 المؤرخ في: 16 محرم عام 1443 الموافق ل 25 غشت سنة 2021 يتمم الأمر رقم 1966 المؤرخ في 18 صفر عام 1386 الموافق ل 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية جريدة رسمية رقم 65.

بداية فإن ملاحظة هامة ملفتة للانتباه تتعلق بالتسمية التي اعتمدها المشرع الجزائري بخصوص هذا النوع من الجرائم، حيث وعلى خلاف ما درج عليه الفقه من تسميات وكذا ما اعتمدته بعض التشريعات المقارنة من قبيل: "الجرائم السيبرانية "، و "الجرائم الإلكترونية" والجرائم المعلوماتية وجرائم الأنترنات وغيرها، فإن المشرع الجزائري قد اعتمد تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في محاولة منه لمد نطاق التجريم الى أقصى الحدود الممكنة ومن أجل لفت

[1]- خالد داودي، الجريمة المعلوماتية، دار الاعصار العلمي للنشر والتوزيع، الجزائر، ط1، 2008، ص 25.

الانتباه الى السلوك الإجرامي يتجاوز المساس أو التلاعب بالمعطيات الآلية الى استعمال الوسائل التكنولوجية لارتكاب حتى الجريمة بصورها التقليدية.

هذا وتحقيقا لمبدأ الشرعية وضمانا لمد مجال تطبيق الأحكام الجزائية الخاصة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال الى كل السلوكيات المشتبه في اعتبارها جرائم من هذا النوع، تدخل المشرع الجزائري بوضع تعريف تشريعي للجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال القانون 09-04 كما تضمن أيضا القانون 21-11 إضافة هامة بهذا الخصوص.

حيث عرفها المشرع ضمن القانون 09-04 في الفقرة أ من المادة 2 على أنها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية او نظام للاتصالات الإلكترونية".

ومن خلال هذا النص يبدو ان المشرع الجزائري قد أحسن بوضع هذا التعريف الذي جمع فيه بخصوص هذا النوع من الجرائم بين تلك السلوكيات الماسة بأنظمة المعالجة الآلية للمعطيات، والتي وردت ضمن قانون العقوبات كجرائم معلوماتية وبين جملة الأفعال التي ترتكب بواسطة او ضد أنظمة المعلومات.

حيث تتمثل الأولى في جملة الأفعال الماسة بنظام المعالجة الالية للمعطيات، بينما تتمثل الثانية في تلك الجرائم التقليدية التي ترتكب أو يسهل ارتكابها باستخدام منظومة معلوماتية والتي تختلف بين تلك التي نص عليها المشرع ضمن قانون العقوبات وتلك التي تناولتها نصوص خاصة.

وبالرجوع الى قانون 21-11 نجد ان المشرع قد حافظ على التعريف ذاته الخاص بجرائم الإعلام والاتصال ضمن المادة 211 مكرر 23 غير أنه جاء بالجديد من ناحيتين هما:

- تحديد أصناف الجرائم التي تمثل اختصاصا نوعيا حصريا للقطب الجزائي الوطن وكذا استعماله لمصطلح "الجرائم المرتبطة بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ويقصد

بها كل الجرائم ذات الارتباط بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال في محاولة لمد التجريم الى كل ما يتم أو يرتبط بالنظم المعلوماتية.

- اعتماد مفهوم الجريمة المتصل بتكنولوجيات اعلام والاتصال الأكثر تعقيدا والتي عرفها بأنها:" .....الجريمة التي بالنظر الى تعدد الفاعلين او الشركاء او المتضررين او يسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة او جسامة اثارها او الأضرار المترتبة عليها أو لطابعها المنظم او العابر للحدود الوطنية او لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة أو خبرة متخصصة أو اللجوء الى تعاون قضائي دولي[1].

الفرع الثاني: الطبيعة القانونية للجريمة الالكترونية

تتفرد الجريمة الإلكترونية بطبيعة خاصة بها، والتي استمدتها من الوسيلة التي ترتكب بها والمتمثلة في الشبكة العالمية للإنترنت[2].

حيث يتمحور الحديث عن الطبيعة القانونية للجريمة الإلكترونية حول الوضع القانوني للبرامج والمعلومات، وقد انقسم الفقه في هذا الشأن إلى اتجاهين:

أولا: الطبيعة الخاصة للمعلومات

يرى هذا الاتجاه وفقا للقواعد العامة فإن الأشياء المادية وحدها هي التي تقبل الحيازة والاستحواذ، وأن الشيء موضوع السرقة يجب أن يكون ماديا أي له كيان مادي ملموس حتى يتمكن انتقاله وحيازته عن طريق الاختلاس المكون للركن المادي في جريمة السرقة، ولما كانت المعلومة ذات طبيعة معنوية ولا يمكن اعتبارها من قبيل القيم القابلة للحيازة والاستحواذ، إلا في ضوء حقوق

[1]– بن عمير امينة، بوحلايس الهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ورقة بحثية مقدمة ضمن فعاليات الملتقى الدولي القانون الجنائي للأعمال نمو توجه جديد للتجريم، المنعقد يوم 21 أكتوبر 2021، عبر التحاضر المرئي عن بعد zoom، المجلد 7 العدد1، لسنة 2022، ص 71.

[2]– يوسف صغير، الجريمة المرتكبة عبر الإنترنت مذكرة ماجسي في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013/2014، ص 06.

الملكية الفكرية، لذلك تستبعد الأفكار والمعلومات من مجال السرقة، ما لم تكن مسجلة على أسطوانة أو شريط[1].

ثانيا: المعلومات مجموعة مستحدثة من القيم

يرى هذا الاتجاه أن المعلومات ماهي إلا مجموعة من القيم القابلة للاستحواذ مستقلة عن دعامتها المادية، ذلك أن المعلومات لها قيمة اقتصادية قابلة لأن تحاز حيازة غير مشروعة، وأنها ترتبط كما يقول الأستاذان (Vivant &Catala) عن طريق علاقة التبني التي تقوم بينهما كالعلاقة القانونية التي تتمثل في علاقة المالك بالشيء الذي يملكه، بمعنى أن المعلومات مال قابل للتملك أو الاستغلال على أساس قيمته الاقتصادية وليس على أساس كيانه المادي، ولذلك فهو يستحق الحماية القانونية ومعاملته معاملة المال[2].

وهناك من يقول أنه يجب أن نفرق بأن هناك مالا معلوماتيا ماديا فقط ولا يمكن أن يخرج عن هذه الطبيعة وهي آلات وأدوات الحاسب الآلي مثل وحدة العرض البصري، ووحدة الإدخال، وأن هناك من المال المعلوماتي المادي ما يحتوي على مضمون معنوي هو الذي يعطيه القيمة الحقيقية وهي المال المادي للشريط الممغنط أو الأسطوانة الممغنطة أو الذاكرة أو الأسلاك التي تنتقل منها الإشارات عن بعد كما هو الحال في "جرائم التجسس عن بعد"[3].

كما ترتكب هذه الجرائم في مجال الكلمات أو معالجة النصوص وتعود صعوبة التكييف القانوني لهذه الجرائم إلى طبيعتها الخاصة، بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر

[1]– عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة مذكرة ماجستير في القانون العام، جامعة الشرق الأوسط الأردن، 2014، ص 14.

[2]– عبد الله دغش العجمي المرجع السابق، ص 15.

[3]– المرجع : نفسه، ص 15.

الإجرامية المستحدثة، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الإثبات ومتابعة مرتكبيها[1].

المطلب الثاني: خصائص وأركان الجريمة الالكترونية

ان الجريمة الالكترونية تختلف عن الجرائم التقليدية ليس فقط من حيث التعريف والوسائل والتقنيات المستعملة وطرق المحاربة، بل انه يمكن تمييز هذا النوع من الجرائم عن غيرها من خلال تحديد خصائص هذه الأخيرة وذكر أركانها وهذا ما سنقوم بتحديده في هذا المطلب من خلال الفرعين التاليين:

الفرع الأول: خصائص الجريمة الالكترونية

أضفى ارتباط الجريمة الإلكترونية بجهاز الحاسوب وشبكة الأنترنت مجموعة من الخصائص تنفرد بها عن غيرها من الجرائم التقليدي وهذا ما كسبها لونا وطابعا قانونيا خاص.

أولا: جريمة تكنولوجيا المعلومات الحديثة متعددة الحدود أو جريمة عابرة للحدود الدولية

يكمن القول إن أهم الخصائص التي تميز جريمة تكنولوجي المعلومات الحديثة هي تخطيها الحدود الجغرافية، ومن ثم اكتسابها طبيعة دولية أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعددة الحدود. فالمجتمع التقنية الحديثة لا يعترف بالحدود الجغرافية، فهو مجتمع متفتح عبرة شبكات تخترق الزمان والمكان

دون أن يخضع لحرس الحدود، فهي تربط بين دول لا تتحدها حدود الطبيعة أو حدود السياسة وتسمح لمستخدميها بالتنقل المعنوي والافتراضي بين الدول والقارات بدون تعقيدات أو صعوبات أو عوائق، فهي عالم ضخم متنوع متجدد خالي من الحدود والعوائق حيث أن أماكن متعددة في دول مختلفة قد تتأثر بجريمة تكنولوجيا المعلومات الحديثة الواحدة في آن واحد، فالسهولة في

[1]– فضيلة عاقلي، "الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري ، كتاب أعمال مؤتمر الجرائم الإلكترونية، المنعقد في طرابلس يومي 24 مارس 2017 ص ص : 115–136، ص 121

حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكاب جريمة عن طريق نظام معلومات إلكتروني موجود في دولة معينة، بينما يتحقق الفعل الإجرامي في دولة أخرى.

هذه الطبيعة التي تتميز بها جريمة تكنولوجيا المعلومات الحديثة كونها جريمة عابرة للحدود خلقت العديد. من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، كذلك حول تحديد القانون الواجب تطبيقه بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وبالتالي فإن الوصول للحقيقة بشأنها يستوجب الاستعانة بخبرة فنية عالية المستوى[1].

ثانيا: صعوبة اكتشاف وإثبات الجرائم الإلكترونية

إقامة الدليل وإسناده إلى المجرم هو الأصل في الجريمة ومع التطورات العلمية الحاصلة يمكن نقل بسرعة البيانات المأخوذة من شبكات الالكترونية ومن التجهيزات الحاسوبية من مكان إلى آخر أو العبث بها وإلغاءه نظرا لطبيعة هذه البيانات التي تسمى بالدليل الرقمي[2].

فالجريمة الالكترونية لا تترك أثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية[3].

واثبات الجريمة الالكترونية صعب مرجعه لعدة أسباب منها وسيلة التنفيذ التي تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية

[1]– علي جعفر، جرائم تكنلوجية المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة، مكتبة زين الحقوقية والأدبية، الطبعة الأولى، 2013، ص ص 98–99.

[2]– صورية بوربابة، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد 01، جامعة طاهري محمد، بشار، 2019، ص93.

[3]– نائلة عادل محمد فريد قورة – جرائم الحاسب الالي الاقتصادية دراسة نظرية وتطبيقية منشورات الحاتي الحقوقية، 2005، ص 55

يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات[1].

وتتجلى صعوبة إثباتها لأن الجاني لا يترك خلفه أي أثر مادي ملموس يمكن فحصه مما يصعب إجراءات اكتشافها فكثير من الأحيان لا يتم اكتشافها إلا صدفة فهي جرائم مخفية لا تتقيد بمكان ولا زمان[2].

ثالثا: قلة الإبلاغ عن الجريمة الإلكترونية

من صعوبات الكشف عن الجريمة الإلكترونية قلة التبليغ عنها، وهذا ما دل على قلة القضايا الإلكترونية، حيث أن اكتشافها لا يكون الا بعد مدة من ارتكابها ويكون صدفة خاصة أن الضحايا مؤسسات عامة أو خاصة أو متعددة الجنسيات لا يلجؤون الى التبليغ حتى لا تتأثر سمعتهم، وحتى لا تهتز ثقة زبائنهم فيهم خاصة إذا كنت بنوكا او مؤسسات مالية، أو خوفا من التداعيات النفسية والاجتماعية إذا كان الضحايا أشخاصا طبيعيين لاسيما في حالة الابتزاز والتهديد بنشر معلومات او صور خاصة[3]

رابعا: صعبة الاكتشاف لخصوصية الوسيلة

لأنها هادئة وناعمة فيصعب اكتشاف حدوثها لأنها تقنية بحتة وهي معقدة ليست في متناول الجميع من حيث الاستعمال والتشغيل، فمعظم الجرائم الإلكترونية يكتشف صدفة بعد وقت طويل من اقترافها، فالجريمة تتم في اقل من بضع ثواني وبمجرد لمسة على لوح المفاتيح، وتحدث وتنتهي بلا صخب ولا ضجة من طرف مجرم بعيد عن مسرح الجريمة قد يتواجد في بلد اخر وفي قارة أخرى.

---

[1]– صورية بوربابة، المرجع السابق، ص 93.

[2]– سعيدة بعرة، الجريمة الإلكترونية في التشريع الجزائري مذكرة لنيل شهادة الماستر جامعة محمد خيضر بسكرة 2015–2016، ص 36.

[3]– خالد ممدوح إبراهيم، المرجع السابق، ص86.

- أنها مخفية لا يلاحظ ارتكابها الا بمعاينة اثارها بعد مدة من ارتكابها والتخمين بوقوعها فالسرقة الإلكترونية تتم عن طريق نقل البيانات من حاسوب الى آخر: مثلا لا تلاحظ الا بعد مدة عكس السطو المسلح الذي يكون باشتباك مع رجال الأمن وهناك عنف وتحطيم. وحتى في حالة اكتشاف الجريمة قد يصعب اثباتها من قبل رجال الضبطية القضائية والمحققين لأسباب عديدة:

- عدم وجود الاعتراف القانوني من طرف المجرم كما في الجريمة التقليدية وعدم وجود الشهود للاستدلال بأقوالهم.

- سرعة تنفيذ الجريمة الإلكترونية التي تكون في ثواني رغم أن التخطيط لها والتحضير قد يكون في مدة زمنية معتبرة وبمجرد لمسة زر في اقل من ثواني.

- عدم وجود دليل مادي لأن الجريمة الإلكترونية لا تترك أثرا ماديا خارجيا ملموسا في مسرح الجريمة، يمكن فحصه فهو ليس مسروقات مادية كالمجوهرات او اوراق نقدية وليس جثة تعاين أو بصمات يتم التحقق من صاحبها ولكن ارقام محفوظة ومخزنة في سجلات يمكن محو اثارها بفضل أجهزة الاتصال بكل سهولة، كما يمكن التلاعب بها بالتغيير او الإزالة حتى عند ضبط الدليل من طرف رجال الضبطية القضائية ورجال التحقيق قد يصعب عليهم التعامل معه، فهو يحتاج الى مهارة وخبرة فنية من طرف افراد مؤهلين وخبراء في هذا المجال متمكنين من تقنيات الكمبيوتر والأنظمة المعلوماتية، وهناك دول لازالت لحد الآن تتعامل مع الجريمة الإلكترونية بنفس الاساليب واجراءات البحث والتحري والتحقيق التي تتبعها في الجرائم التقليدية، عدم تكوين وخبرة رجال الضبطية القضائية في متابعة الجرائم الإلكترونية وعدم امتلاكهم الوسائل التقنية المتطورة والمعرفة العلمية اللازمة، مما يصعب عليهم عملهم عند اكتشاف الجريمة في الحصول على الدليل الإلكتروني.

- رجال الضبطية القضائية والمحققون يجدون صعوبة في التعامل مع الدليل الإلكتروني فقد لا يستطيعون تقدير أهميته، كما يمكن أن يتجاهلوه أو قد يتسببون في اتلافه او تدميره بمجرد

لمس لوح المفاتيح او لا يقومون بمصادرة الدليل او اداة الجريمة مثل: جهاز الذاكرة او الكمبيوتر او لواحقه مثل جهاز الماسح الضوئي.

- غالبا ما يرفض القاضي الدليل الإلكتروني لعدم اقتناعه بأدلة الإثبات التي حصل عليها المحققون[1] ويدمر الدليل كذلك بمجرد استعماله .

وحسب رجال القانون لا يتم اكتشاف الجريمة غالبا الا لغباء الجاني وسوء تخطيطه.

رابعا: تتطلب خبرة وتحكما في تكنولوجيا المعلوماتية عند متابعتها

إن الجريمة الالكترونية لها طبيعة تقنية وبذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري، لذلك لابد أن يكون المحقق متخصص في الجريمة الالكترونية حتى لا يتسبب في إتلاف الدليل الالكتروني[2].

خامسا: اعتماد الجريمة الالكترونية على الخداع والتضليل

يتميز مرتكبو الجرائم الالكترونية بالذكاء والدراية بالأساليب المستخدمة في أنظمة المعالجة الآلية وطريقة تشغيلها وكيفية تخزين المعلومات إذ يعتبر الإجرام الالكتروني إجرام الأذكياء مقارنة مع الإجرام التقليدي كما أن الدافع لارتكابها في اغلب الحالات هو إثبات الذات في التغلب على الأنظمة[3].

الفرع الثاني: أركان الجريمة الالكترونية

لا تختلف الجريمة الإلكترونية رغم ارتكابها على الفضاء الافتراضي عن الجريمة العادية في اشتراط توفر أركان لقيامها. فلها ركن معنوي وركن مادي وركن تشريعي وكل نوع منها يختص

[1]– عبد الصديق الشيخ، الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة معالم للدراسات القانونية والسياسية، المجلد 4 العدد 1 لسنة 2020، ص 196.

[2]– سعيدة بعرة، المرجع السابق، ص 38.

[3]– صورية بورباية، المرجع السابق، ص ص 93-94.

بميزة عن جريمة أخرى حيث كل جريمة تكاد تنفرد وتختلف عن الأخرى كما أن هذه الأركان تتسم بالافتراض أي ترتكب في العالم الافتراضي ونوجزها فيما يلي:

أولا: الركن الشرعي

أي أن هناك نص قانوني يجرم هذا الفعل ويدينه ويكون بعد صدور هذا النص فلا يمكن ملاحقة الفاعل بعد الغاء النص، ولا يمكن التوسع في تفسيره بل يجب الالتزام به من طرف القاضي عملا بمبدأ عدم رجعية القوانين الا بنص صريح في حالة تطبيق الأصلح للمتهم، وهناك من دمج الجريمة الالكترونية في القوانين العادية بتكييف النصوص القديمة مع هذه الجرائم الحديثة وهناك من وضع نصوص جديدة خاصة بها.

ثانيا: الركن المادي

هو الأفعال والسلوكيات الصادرة عن الانسان العاقل، ومعرفة بداية النشاط والشروع فيه وتحقيق نتيجة، فالأعمال التحضيرية في الجريمة التقليدية لا يعاقب عليها القانون عكس الجريمة الإلكترونية حيث يختلف الأمر، فشراء برامج الاختراق ومعدات فك الشفرات وكلمات المرور، أو حيازة صور دعارة الأطفال هي جريمة بحد ذاتها دون الدخول في نشاط فارتكاب الجريمة يكون بإتيان تصرف (الايجابي) أو الامتناع عن فعل (السلبي) تسبب في إحداث نتيجة هي الحاق ضرر بحق دستوري او قانوني وفي الجريمة الالكترونية أيضا لابد من وجود فعل مادي و لابد من وجود البيئة الرقمية والانترنت و معرفة أنه شرع في ارتكاب الفعل و سيرتب نتيجة إذا لابد من توفر:

1- سلوك مادي

فلا عقاب على الأفكار والخيال والخواطر التي تجول بنفس الفرد، مالم يكن هناك سلوك مادي ايجابي بالقيام بالفعل أو الامتناع عنه، وهو الذي يحدد عدم المشروعية الفعل، وفي الجريمة المعلوماتية لابد من وجود البيئة الرقمية التي هي مسرح الجريمة وأداتها ولابد من وجود شبكة الأنترنت.

2- مباشرة النشاط التقني

السلوك المادي وحده لا يكفي لوجود الجريمة الالكترونية فلا بد من مباشرة نشاط تقني بالدخول غير المشروع الى نظام معالجة أو قواعد المعطيات، فبمجرد وجود دخول الى النظام يعد سلوكا اجراميا حتى ولو لم يتم المساس بالأنظمة والمعطيات، فالنشاط الذي قام به باستخدام جهاز الكمبيوتر والدخول الى شبكة الأنترنت شكل نشاطا أو جزءا منه[1] ورصد هذا الدخول يعد جريمة والنشاط الاجرامي يكون بالاطلاع على المراسلات السرية وعلى البريد الالكتروني، او الادلاء ببيانات كاذبة.

ثالثا: الركن المعنوي

هو الركن الثالث للجريمة ويتمثل في الحالة النفسية للجاني والمسلك الذهني وتوافر الإرادة الإجرامية حين ارتكابه الفعل وتوجيهها الى القيام بعمل غير مشروع كانتحال شخصية الغير كما يكون على علم بنتيجة افعاله.

ويتميز الركن المعنوي للجريمة الالكترونية بالتنوع والتغير حسب الجريمة الالكترونية المرتكبة كونها جريمة افتراضية.

1- القصد الجنائي

أي ان الجاني يوجه ارادته لإحداث أمر يعاقب عليه القانون علمه مع بذلك وليس عن طريق الخطأ أو حسن النية.

- فالدخول غير المشروع أولا الى النظام: ويجب أن يكون على علم بكافة عناصر الجريمة من أن الفعل الذي قام به يشكل جريمة واعتداء على نظام المعالجة الآلية وعلى المعلومات والبيانات الموجودة فيه، كما أن دخوله كان بسبب الاختراق الغير مسموح به وان هناك غش في الدخول، فهو على علم بأن الدخول غير مسموح لان نظام المعالجة محمي لكن اعتدى

[1]– نبيلة هبة هروال، الجوانب الاجرائية لجرائم الأنترنات _في مرحلة جمع الاستدلالات_، د ذ ط، دار الفكر الجامعي الاسكندرية، 2006، ص 47.

عليه، وأحيانا يكون مسموحا لشخص بالدخول الى النظام المعلوماتي ويتجاوزه فهو مقيد بحدود فلا يمكنه الدخول الى انظمة اخرى. لكن هنا الجريمة التي ارتكبها هي جريمة ولوج الى الأنظمة التي ليس مسموحا له بدخولها.

- حالة توافر القصد الجنائي أي يرتكب الفعل قصد إحداث الضرر.
- حالة تجاوز الضرر الذي حدث ما كان متوقعا.
- يفترض القصد إذا قام الفاعل أو امتنع عن الفعل فأدى ذلك النتيجة كانت ضرر جسيم كانت بسبب نشاط الجاني وبالتالي يتحمل النتيجة حتى ولو كان لم يقصدها او يتحملها[1] كما ان البقاء ايضا جريمة فحتى لو كان دخوله خطا وبدون قصد فإن استمراره في البقاء متعمدا غير مشروع، ويظهر ذلك من خلال تفحص النظام والعمليات التي قام بها اثناء تواجده فيه.
- الاعتداء على سير نظام المعالجة هنا يكون الاعتداء عمديا لان المجرم يقوم بأفعال اما تعرقل سير النظام ببث فيروسات أو تعطله تماما، أو باللهو بمحتوى المعطيات وتعد جريمة الكترونية الحالة التي يستعمل فيها الموظف الحاسوب لحسابه الشخصي وبحسن نية واثناء ذلك يلحق ضررا بنظام الحاسوب او عند ادخال قرص مرن خاص به فتنقل فيروسات.

[1]– نبيلة هبة هزوال، المرجع السابق، ص 49.

المبحث الثاني: صور الجريمة الالكترونية ودوافع ارتكابها

تعتبر الجريمة الالكترونية من الجرائم المستحدثة وهي تستهدف العديد من القطاعات، مما جعل تصنيفها من قبل الفقهاء يتميّز بالصعوبة على عكس الجرائم التقليدية التي يمكن تصنيفها بسهولة فائقة. لم يستقر الفقهاء على معيار واحد لتصنيف الجريمة الالكترونية وذلك لتشعب هذه الجرائم وسرعة تطورها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة أو دافع المجرم، أو على اساس محل الجريمة.

وعلى هذا الأساس يقسم هذا المبحث إلى مطلبين:

المطلب الأول: صور الجريمة الالكترونية

المطلب الثاني: دوافع ارتكاب الجريمة الإلكترونية

المطلب الأول: صور الجريمة الالكترونية

ان تصنيف الجريمة الإلكترونية أصعب من تصنيف الجريمة التقليدية وتستهدف الكثير من القطاعات من أشخاص معنويين وطبيعيين وحتى الدول امنيا واقتصاديا لذا لم يستقر الفقهاء ورجال القانون على معيار واحد لتصنيف الجريمة الالكترونية وذلك لتشعب هذه الجرائم وسرعة تطوّرها، فمنهم من يصنفها بالرجوع إلى وسيلة ارتكاب الجريمة أو دافع المجرم، أو على اساس محل الجريمة.

وعلى هذا الأساس نعتمد في تقسيم هذا المطلب على مختلف معايير التصنيف وهي الجرائم الواقعة على الأموال والجرائم الواقعة على الأشخاص (الفرع الأول) ثم الجرائم الواقعة على أمن الدول (الفرع الثاني).

الفرع الأول: جرائم واقعة على الأموال وجرائم واقعة على الأشخاص

أصبحت معظم المعاملات التجارية تتم من خلال شبكة الانترنيت مثل البيع والشراء، مما انجر عنه وسائل الدفع والوفاء. وفي خضم هذا التداول المالي عبر الانترنيت، انتهز بعض المجرمين

الفرصة من أجل السطو عليها مرتكبين بذلك جرائم ضد الأموال (أولا). إن الهدف الأول والأسمى من وضع القوانين هو حماية سلامة الأشخاص من مختلف الانتهاكات التي قد يتعرضون لها سواء في أبدانهم أو في حياتهم الخاصة، أو في سمعتهم وشرفهم. تطور الأمر بعد ذلك مع ظهور شبكة الانترنيت التي أصبحت سلاحا فتاكًا في يد المجرمين يقترفون جرائم ضد الأشخاص (ثانيا).

أولا: جرائم واقعة على الأموال

تتمثل في مختلف الجرائم التالية:

1- جريمة السطو والسرقة

وتعرف جريمة السطو والسرقة بأنها اختلاس شيء منقول مملوك للغير بدون رضاه بنية امتلاكه، وتتم سرقة المال المعلوماتي عن طريق اختلاس البيانات والمعلومات والاستفادة منها باستخدام السارق للمعلومات الشخصية مثل (الاسم، العنوان، الأرقام السرية) الخاصة بالمجني عليه، والاستخدام غير الشرعي لشخصية المجني عليه ليبدأ بها عمليات السرقة المتخفية عبر الشبكة المعلوماتية، بحيث تؤدي بالغير إلى تقديم المال إلى الجاني عن طريق التحويل البنكي[1].

2- جريمة التحويل الإلكتروني غير المشروع للأموال

نظام التحويل الإلكتروني للأموال (Electronic funds Transfer –EFT) هو جزء بالغ الأهمية من البنية التحتية لأعمال البنوك الإلكترونية، التي تعمل عن طريق شبكة الإنترنت، ويتيح هذا النظام بطريقة إلكترونية آمنة نقل التحويلات المالية من حساب بنكي إلى حساب آخر، بالإضافة إلى نقل المعلومات المتعلقة بهذه التحويلات[2].

وغالبا ما يتم الولوج إلى شبكات الإنترنت من طرف المخترقين إلى بيانات حساب الآخرين من خلال الحصول على كلمة مرور (password) مدرجة في ملفات أنظمة الكمبيوتر الخاصة

[1]– محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، ط 01، دار الثقافة للنشر والتوزيع، عمان، 2004، ص138.

[2]– خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية 2008، ص 74.

بالمجني عليه، ويحصل المجرمون في نطاق الجريمة الإلكترونية على كلمات المرور الخاصة بالغير، إما بالتقاطها أثناء تواجدهم في النظام المعلوماتي، أو من خلال بث برامج تتعقب الأنظمة المعلوماتية التي يتجه إليها أكثر المستخدمين وسرقة كلمات المرور الخاصة بهم، وكذا الحصول على البيانات الخاصة بالجاني واستخدام المفيد منها في إجراء التحويلات المالية الإلكترونية من حساب المجني عليه وإدخالها في أرصدتهم وفي نظام المعلوماتي الخاص بهم[1].

وتتم عملية التحويل الإلكتروني غير المشروع للأموال عن طريق "الاحتيال"، وقد ذهب بعض فقهاء القانون إلى إطلاق عدة تسميات مختلفة منها (الغش المعلوماتي أو غش الحاسوب) ويعرف الاحتيال بأنه:

" سلوك احتيالي يرتبط بعملية التحسيب الإلكتروني بهدف كسب فائدة أو مصلحة مالية"[2].

3- جريمة السطو على أرقام بطاقات الائتمان

بما أن بطاقة الائتمان هي أحد أنواع بطاقات الدفع البلاستكية، كان لابد من توضيح المقصود ببطاقات الدفع البلاستكية، بحيث يطلق هذا الاصطلاح على تلك البطاقات التي تتم معالجتها إلكترونيا لاستخدامها في أغراض متعددة، من خلال المعلومات المخزنة عليها والدخول بها على الآلات المعدة لذلك بغية تحقيق أغراض معنية[3].

[1]– محمد أمين أحمد الشوابكة المرجع السابق، ص 178

[2]– خديجة دحمان صبايحية، جرائم السرقة والاحتيال عبر الانترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم الإسلامية، تخصص شريعة وقانون، قسم الشريعة، كلية العلوم الإسلامية، جامعة الجزائر، 2013/2012، ص 16.

[3]– كميت طالب البغدادي، الاستخدام غير المشروع لبطاقة الائتمان المسؤولية الجزائية والمدنية، ط01، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 52.

وقد ظهرت أولى هذا النوع من الاحتيال بالنقاط الأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود، إلى أن ظهرت الصرافة الآلية (ElectronicBanking) والنقود المالية(Digital Cash)[1].

أما جرائم الاعتداء والسطو على هذه البطاقات، فتتمثل في استخدامها من قبل غير أصحاب الحق بعد سرقتها أو سرقة الأرقام السرية الخاصة بها، وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات[2].

4- جريمة القمار عبر الأنترنت

ظهرت بظهور النوادي والكازينوهات الافتراضية التي انتشرت عبر المواقع الإلكترونية والخاصة بألعاب القمار لكن هذه المواقع غير مسموح[3] بها في أغلب البلدان وغير مصرح لها بممارسة نشاطها حيث اصبحت فيما بعد مسرحا لجريمة غسيل الأموال.

5- جريمة غسيل الأموال

هي جريمة تقليدية تطورت عن طريق التطور التكنولوجي حيث يتم ارتكابها عن طريق تطهير الأموال التي يكون مصدرها غير مشروع ويتم استثمارها بطريقة شرعية عن طريق البنوك ، عن طريق نقلها بعملية اقتصادية ومالية للأموال من مصدر غير مشروع الى دائرة الاقتصاد الشرعي، والمصدر غير الشرعي يكون مخدرات او اختلاس، ويتمثل ضرر وخطورة تبييض الأموال في انها تدخل الى الاقتصاد حيث انها اموال غير مستقرة يمكن تحويلها الى الخارج في أي وقت كما انها جريمة مركبة حيث تغطي على الجريمة الأولى، ولها اضرار امنية واجتماعية وقانونية وسياسية.

---

[1]– فاطمة الزهراء خبازي، جرائم الدفع الإلكتروني وسبل مكافحتها، أعمال الملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد في الجزائر يوم 29 مارس 2017، ص 36

[2]– خالد ممدوح إبراهيم أمن الجريمة الإلكترونية، المرجع السابق، ص ص76–77.

[3]– غانم مرضي الشمري، الجرائم المعلوماتية –ماهيتها، خصائصها، كيفية التصدي لها قانونا، دذدن ، دذط، ص58.

6- جرائم المخدرات عبر الإنترنت

هناك مواقع منتشرة عبر الإنترنت والتي لا تتعلق بالترويج للمخدرات وتشويق النشء لاستخدامها، بل تتعداه إلى تعليم كيفية صناعة المخدرات بكافة أصنافها وأنواعها وكذا زراعتها وبأبسط الوسائل المتاحة[1].

والأمر هنا لا يحتاج إلى رفاق، سوء، بل يمكن للمراهق الدخول إلى هذه المواقع ومن ثم يطبق ما يقرأه، وقد أكد الخبراء التربويين بالولايات المتحدة الأمريكية أنه ثمة علاقة يمكن ملاحظتها بين ثالوث المراهقة والمخدرات والإنترنت[2].

7- التزوير الإلكتروني

من بين الجرائم الإلكترونية جريمة التزوير وهو من بين أخطر ما يقوم به المجرم المعلوماتي نظرا لما يتمتع به الحاسب الآلي من خطورة، فيتم التزوير عن طريق الوسائل المتطورة كتزوير العملة عن طريق الماسح الضوئي وما يسببه ذلك من اضرار بالاقتصاد الوطني، او تقليد وتزييف الوثائق والمستندات الكترونيا او التوقيع (المحررات الرسمية)[3].

ثانيا: جرائم واقعة على الأشخاص

إن الهدف الأول والأسمى من وضع القوانين هو حماية سلامة الأشخاص من مختلف الانتهاكات التي قد يتعرضون لها سواء في أبدانهم أو في حياتهم الخاصة، أو في سمعتهم وشرفهم تطور الأمر بعد ذلك مع ظهور شبكة الانترنيت التي أصبحت سلاحا فتاكا في يد المجرمين وهذا ما سنوضحه فيما يلي:

1- جريمة التهديد والمضايقة والملاحقة

---

[1]– محمد محمد صالح الألفي، "أنماط جرائم الانترنت"، مقال متوفر على الموقع التالي:http://www.eastlaws.com : تاريخ الولوج 2023/05/29 على الساعة: 12:52.

[2]–يوسف صغير، المرجع السابق، ص 49.

[3]– عامر محمود الكسواني، التزويز المعلوماتي للعلامة التجارية، دار الثقافة للنشر والتوزيع، ط2، الاردن، 2014، ص151.

التهديد هو الوعيد بالشر، الذي يقصد به زرع الخوف في النفس بالضغط على إرادة الإنسان وتخويفه من أضرار ما سيلحقه أو سيلحق أشياء أو أشخاص له به صلة[1].

يعتبر تهديد الغير من خلال البريد الالكتروني واحد من أهم الاستخدامات غير المشروعة للأنترنيت حيث يقوم الفاعل بإرسال رسالة إلكترونية إلى المجني عليه تنطوي على عبارات تسبب خوفا له.

تتم جرائم الملاحقة على شبكة الانترنيت غالبا باستخدام البريد الالكتروني أو وسائل الحوارات الآلية المختلفة على الشبكة وتشمل الملاحقة وسائل تخويف ومضايقة تتفق مع مثيلاتها خارج الشبكة في الأهداف المجسدة في رغبة التحكم في الضحية، وتتميز عنها بسهولة إمكانية إخفاء هوية المجرم، علاوة على تعدّد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة.

2- انتحال الشخصية و التغرير و الاستدراج

يقصد بانتحال الشخصية استخدام المجرم شخصية شخص آخر للاستفادة من سمعته مثلا أو ماله أو صلاحيته ولذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية وسرية المعلومات الشخصية للمستفيدين على شبكة الانترنيت.

[1]– محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت، دار النهضة العربية، القاهرة د.ت.ن، ص 88.

تتخذ جريمة انتحال الشخصية عبر الانترنيت أحد الوجهين التاليين: انتحال شخصية الفرد وانتحال شخصية المواقع[1]. ولقد سماها بعض المختصين في أمن المعلومات جريمة الألفية الجديدة، وذلك نظرا لسرعة انتشار ارتكابها خاصة في الأوساط التجارية[2].

أما عن التغرير والاستدراج فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين صداقة على الانترنيت والتي قد تتطور إلى التقاء مادي بين الطرفين.

3- المساس بصور الأشخاص عن طريق الصناعة الإباحية

إن شبكة الانترنيت ليس لها فقط وجه، ايجابي وإنما لها وجه سلبي أيضا، منها وجود مواقع على شبكة الانترنيت تحرص على ممارسة الجنس للكبار والصغار على حدّ سواء، وتقوم هذه المواقع بنشر صور وأفلام جنسية فاضحة للبالغين والقصر.

إن التشهير عن طريق صناعة ونشر المقاطع الإباحية تعد جريمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم[3] الأطفال، حيث يضم استغلال المستخدمين في إنتاج هذه المواد ويمثل اعتداءا عليهم في كل مرة يتم فيها عرض هذه الصور ويتخذ الاستغلال الجنسي للأطفال على الانترنيت أشكالا متعددة انطلاقا من الصور وصولا إلى التسجيلات المرئية للجرائم الجنسية

[1]– انتحال شخصية الفرد إن التطور المتزايد لشبكة الانترنيت أعطى للمجرمين قدرة أكبر على جمع المعلومات عن شخصية الصحية والاستفادة منها في ارتكاب جرائمهم، فتنتشر في شبكة الانترنيت الكثير من الإعلانات المشبوهة فهناك مثلا إعلان عن جائزة فخمة يكسبها من يساهم بمبلغ رمزي لجهة خيرية، الذي يتطلب الإفصاح عن المعلومات الشخصية كالاسم والعنوان ورقم بطاقة الائتمان لخصم المبلغ الرمزي لصالح الجهة الخيرية، الأمر الذي يؤدي إلى الاستيلاء على رصيده البنكي أو حتى الإساءة إلى سمعة الضحية.

[2]– عمرو عيسى الفقي، الجرائم المعلوماتية. جرائم الحاسب الالي والانترنيت في مصر والدول العربية المكتب الجامعي الحديث، الاسكندرية، 2006، ص 102.

[3]– خالد محي الدين أحمد، "الجرائم المتعلقة بالرغبة الاشباعية باستخدام الكمبيوتر"، الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، أيام 2018 جوان 2007، ص 37.

العنيفة. وتستمر معاناة الضحايا حتى بعد انتهاء الاعتداء الفعلي الذي تعرض له بسبب إمكان تناقل الصور على الانترنيت إلى ما لا نهاية[1].

4- جرائم القذف والسب وتشويه السمعة

يستعمل الجاني حسب القواعد العامة لجرائم القذف والسب عبارات بدائية تمس شرف المجني عليه، مهما كانت الوسيلة المعتمدة وبالتطور التكنولوجي أصبحت الانترنيت إحدى هذه الوسائل فأصبحت ترسل هذه العبارات عبر البريد الصوتي أو ترسم أو تكتب على صفحات الويب[2].

تعتبر شبكة الانترنيت مسرحا غير محدود، فهي تتلقى كل ما يدرج عليها دون قيد أو رقابة، حيث يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن الضحية، التي قد تكون فردا أو مجتمعا أو مؤسسة تجارية أو سياسية[3] حيث بلغ عدد القضايا المسجلة في مجال الجرائم الماسة بالأشخاص سنة 2017 إلى 430، أين تمت معالجة 200 قضية، وبلغ عدد المتورطين فيها 365 لتصل نسبة القضايا المعالجة إلى 68%.

الفرع الثاني: الجرائم الواقعة على أمن الدولة

استغلت الكثير من الجماعات المتطرفة، الطبيعة الاتصالية للإنترنت من أجل بث معتقداتها وأفكارها، بل تعداه الأمر إلى ممارسات تهدد أمن الدولة المعتدى عليها، خاصة المتمثلة في الإرهاب والجريمة المنظمة، بل الأخطر من ذلك أتاحت الإنترنت للكثير من الدول ممارسة

[1]– علوي مصطفى "الضحية المنسية أمام لغة الكبار"، مجلة الشرطة المديرية العامة للأمن الوطني، العدد 87 جوان، 2008، ص30

[2]– عبد الرحمن بن عبد الله السند، الأحكام الفقهية للمعاملات الالكترونية، الحاسب الآلي و شبكة المعلومات (الانترنيت)، دار الوراقين للنشر والتوزيع، بيروت، 2004، ص318 محمد أمين أحمد الشوابكة، المرجع السابق، ص ص 31–32

[3]– محمد أمين أحمد الشوابكة، المرجع السابق، ص ص31–32.

التجسس على دول أخرى وذلك بالاطلاع على مختلف الأسرار العسكرية والاقتصادية لهذه الأخيرة، ويبقى المساس بالأمن الفكري من بين أخطر الجرائم الإلكترونية[1].

1- الإرهاب الإلكتروني

يعرف الإرهاب الإلكتروني بأنه العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو عرضه أو عقله أو ماله، بغير حق بشتى صنوف وصور الإفساد في الأرض[2].

ولم يكن للجماعات الإرهابية أن تلجأ إلى وسائل الاتصال المستحدثة لارتكاب الجرائم الإلكترونية لإحداث أضرار جسيمة في دولة، أو خلق جو من عدم الاستقرار والرعب والفوضى أو في سبيل الضغط على أي دولة لتلبية طلباتهم الغير مشروعة، بالإضافة إلى ذلك يمكن أيضا للجماعات الإرهابية أن تستعمل هذه التكنولوجيا لنشر أفكارهم المتطرفة والترويج لأنفسهم عبر الشبكة العالمية "الإنترنت كوسيلة اتصال فيما بين أعضائها، والتي تقلت غالبا من رقابة السلطات العمومية[3].

ومهما كانت فئة المجرم المعلوماتي لا يمكن له أن يكون مرتكبا للإرهاب الإلكتروني إلا إذا نتج عن تصرفه إحداث عدم الاستقرار والخوف في دولة معينة، وبالتالي يعد من الجرائم الإلكترونية الإرهابية مثلا إذا اخترق هاكرز النظام المعلوماتي الخاص بإدارة وتنظيم توزيع الكهرباء في ولاية ما وتسبب في إتلافه وانقطاع الكهرباء، فهذا التصرف حسب رجال القانون يعد عملية إرهابية[4].

2- الجريمة المنظمة

---

[1]– محمد محمد صالح الألفي " أنماط جرائم الانترنت، مقال متوفر على الموقع التالي: تم الاطلاع عليه بتاريخ 07/02/2018 على الساعة: 11:25 http://www.eastlaws.com

[2]– يوسف صغير، المرجع السابق، ص 49.

[3]– نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة 2012/2013، ص ص157–158.

[4]– المرجع نفسه، ص 159.

عرفها المؤتمر الخامس لمنع الجريمة ومعاملة المجرمين الذي انعقد في جنيف عام 1975 بأنها:

" الجريمة التي تتضمن نشاطا إجراميا معقدا وعلى نطاق واسع، تنفذه مجموعة من الأشخاص على درجة من التنظيم، ويهدف إلى تحقيق ثراء للمشتركين فيها على حساب المجتمع وأفراده، وهي غالبا ما تتم عن طريق الإهمال التام للقانون وتتضمن جرائم ضد الأشخاص ونكون مرتبطة في معظم الأحيان بالفساد السياسي"[1].

ولقد انتقد التعريف السابق لأنه لم يشر إلى المنظمة الإجرامية بشكل مباشر، بل ركز على السلوك الإجرامي دون بيان العناصر الأساسية لقيام المنظمة الإجرامية، ومنها الدوام والاستمرار والتخطيط لارتكاب الجريمة أو استخدام وسائل العنف أو التهديد بارتكابها[2].

وتعتبر الجريمة المنظمة خطر يهدد الأمن والسلم للدول وتشمل النشاطات الإجرامية المنظمة عدة مجالات من أهمها: (الاتجار بالأسلحة المحظورة وتهريب الآثار وخطف السيارات... الخ)[3].

وتعد الجريمة المنظمة من أخطر النظم الإجرامية الحديثة، لما لها من آثار وخيمة تنعكس سلبا على استقرار المجتمعات البشرية واستمرارها فهي مرتبطة بالحياة الاقتصادية والاجتماعية والثقافية والسياسية للأشخاص والمجتمع على حد سواء[4]، فقد استطاعت الجماعات المنظمة تدويل أنشطتها الإجرامية عبر العالم، مستغلة ما حققته العولمة من انفتاح على العالم الخارجي، فأصبحت هذه الجماعات ترتكب أنشطتها الإجرامية عبر الدول والقارات، حيث تعتبر هذه المنظمات قوى فساد

[1]– جهاد محمد البريزات، الجريمة المنظمة: دراسة تحليلية، ط01، دار الثقافة للنشر والتوزيع، عمان، 2008، ص 33

[2]– المرجع نفسه، ص 33.

[3]– مايا خاطر، الجريمة المنظمة العابرة للحدود الوطنية وسبل مكافحتها، مجلة جامعة للعلوم الاقتصادية والقانونية، جامعة دمشق، العدد 03، المجلد 27، 2011، ص 509.

[4]– محمد الحبيب عباسي، الجريمة المنظمة العابرة للحدود، أطروحة لنيل شهادة دكتوراه علوم، تخصص القانون العام، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2017/2016، ص15.

وشر استطاعت أن تصل إلى مرحلة متطورة ومتقدمة، بفضل القدرة الفائقة التي تمتلكها للتكيف ومواكبة التطور الحاصل في المجتمع وتسخيره في أنشطتها الإجرامية[1].

وتهدف هذه الجماعات المنظمة إلى جني المال وبسط النفوذ هذا ما جعل هذه الظاهرة من أكبر التحديات التي تواجه الدول ككل، ولهذا وجب تنسيق الجهود والحث على التعاون الدولي للحد من انتشارها[2]

3- جرائم التجسس الإلكتروني

ينتج عن الاستخدام المتزايد للحاسبات الآلية في العديد من المجالات، تجميع المعلومات بدرجة كبيرة في موضع واحد، ويؤدي هذا التخزين في الحاسبات المركزية إلى سهولة التجسس عليها، وعلى المعلومات المخزنة فيها بمختلف درجة سريتها[3].

ويقصد بالتجسس في هذا الموضع الاطلاع على المعلومات الخاصة بالغير مؤمنة في جهاز آخر، وليس مسموحا لغير المخولين بالاطلاع عليها.

وتستهدف عملية التجسس في عصر المعلومات ثلاث أهداف رئيسية هي: التجسس العسكري والتجسس السياسي والتجسس الاقتصادي، كما تمارس العديد من الدول التجسس باستخدام التقنية المعلوماتية، وهذه الأنشطة تمارس من قبل دولة على دول أخرى، أو من قبل الدولة على مواطنيها، أو من قبل شركة على شركات منافسة لها.

4- الجرائم الماسة بالأمن الفكري

[1]– محمد الحبيب عباسي، المرجع نفسه، ص ص03-04.

[2]– محمد فوزي صالح، الجريمة المنظمة وأثرها على حقوق الإنسان، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي لحقوق الانسان كلية الحقوق جامعة يحي فارس المدية، 2009/2008، ص 09.

[3]– يوسف صغير، المرجع السابق، ص 57.

ويبقى الأمن الفكري من بين أخطر الجرائم الإلكتروني، حيث تعطي الإنترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية ويسهل خلق الفوضى.

بناءا على خصائص الشبكة العالمية للأنترنيت التي منحت المستخدم الكثير من الخيرات من خلال عدم خضوعها لأي رقابة و عبورها بالحدود الجغرافية بين الدول و نموها السريع المتواصل و إمكانية مشاركة الجميع من مختلف دول العالم، مع ما تمنحه من القدرة على التخفي و عدم المواجهة الافتراضية التي تعد من أهم خصائص هذه الشبكة، بالإضافة إلى الكم الهائل من المعلومات التي يمكن الحصول عليها من عدة مصادر لا يمكن التحكم فيها ومتابعتها أو الإشراف عليها ، كل ذلك جعل هذه الشبكة من أهم مقومات المجتمع المعلوماتي[1] التي تؤدي إلى الانحراف الفكري من خلال تعرض الشخص إلى الكثير من المؤثرات الفكرية التي تستخدم الشبكة العالمية للأنترنيت و تهدّد الأمن بأبعاده كافة. فكما اندهشنا بالتلفزيون وتخوفنا من آثاره على حياتنا لأول مرة وتغيرنا رغم النقد والتردد، فليس هناك ما يدعونا لاعتقاد غير ذلك بسبب ثورة المعلومات اليوم وخاصة الانترنيت.

المطلب الثاني: دوافع ارتكاب الجريمة الالكترونية

من خلال ما سبق يتضح لنا، أن الجريمة التقليدية والمحرم التقليدي يختلفان تماما عن الجريمة الإلكترونية والمحرم الإلكتروني، لذا من الطبيعي أن تجد نفس الاختلاف في الأسباب والعوامل التي تدفع إلى ارتكاب الفعل غير المشروع، فالدافع (الباعث)، الغرض، الغاية، مفاهيم مسألة لكل منها دلالته في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي تثير جدلا فقهيا وقضائيا واسعا، ذلك أن القاعدة القضائية تقرر أن الباعث ليس عنصرا من عناصر القصد الجرمي، وأن الباعث لا أثر له في وجود القصد الجنائي، وإذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإنها من حيث الدلالة تتمايز، فالدافع هو العامل المحرك للإرادة والذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء

[1]– سمير إبراهيم حسن "الثورة المعلوماتية عواقبها و آفاقها"، مجلة جامعة دمشق، العدد الأول، 2002، ص213

والانتقام، وهو إذن قوة نفسية تدفع الإرادة إلى ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى. أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي، ويتمثل بتحقيق النتيجة التي اصرف إليها القصد الجنائي أو الاعتداء على الحق الذي يحميه قانون العقوبات وأما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام، أو سلب مال المجني عليه في جريمة القتل. وبالنسبة للجريمة الإلكترونية، فثمة دوافع عديدة تحرك الجناة لارتكاب أفعال الإعداء المختلفة المنطوية تحت هذا المفهوم[1]، وأهم هذه الدوافع سيتم بيانها من خلال الفرعين الآتيين.

الفرع الأول: الدوافع الشخصية لارتكاب الجريمة الإلكترونية

تصنف هذه الدوافع إلى دوافع مادية وأخرى ذهنية، وذلك بمدى تأثير العنصر المادي التحقيق الربح في ارتكاب الجريمة الإلكترونية، أو تأثير العنصر الذهبي المعتدي على المحرم الإلكتروني ودفعه لارتكاب جريمته هذا ما سيتم بيانه من خلال ما يلي:

أولا: الدوافع المادية

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الإلكتروني إلى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الاحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الألية لها من خلال اكتشافه 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 مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل

[1]– حمزة بن عقون السلوك الإجرامي للمحرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية تخصص علم الإجرام و علم العقاب جامعة الحاج لخضر، باتنة، 2011–2012، ص ص46–47.

عليها بطريق الاختلاس من جهاز الحاسوب، وقد أشارت في هذا الإطار مجلة securite" informatique"وهي مجلة متخصصة في الأمن المعلوماتي، أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، 23% من أجل سرقة معلومات، و19% أفعال إتلاف، و15% الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية، وفي حقيقة الأمر أن في حال نجاح المحرم الإلكتروني في ارتكاب جريمته فإن ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الإلكترونية، حيث تبين أن 85% من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة للأنظمة المعلوماتية، وأن 64% لحقت بهم خسائر مادية جراء هذه الاعتداءات[1].

ثانيا: الدوافع الذهنية لارتكاب الجريمة الإلكترونية

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات.

وقد تكون هذه الدوافع مجرد شعف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه، وعلى صعيد آخر قد يكون إقدام الحرم الإلكتروني على ارتكاب حياته بدافع الرقبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يميل

[1]– سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر باتنة 2012–2013، ص 60–61، نقلا عن تملا عبد القادر المومني، الجرائم المعلوماتية، ط02، 2010، ص 90، ونقلا عن ضاح محمود الحمود ونشأت مفضي المجالي، جرائم الأنترنت، دار المنار للنشر والتوزيع، 2005، ص 31

المحرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو التخريبية، وإنما ينطلق من دافع التحدي و إثبات المقدرة[1].

الفرع الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية

قد يتأثر المحرم الإلكتروني ببعض المواقف قد تكون دافعة له على اقتراف الإحرام الإلكتروني ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن إبراز أهم الدوافع من خلال ما يلي:

أولا: دافع الانتقام وإلحاق الضرر برب العمل

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته[2]، كما يعتبر هذا الدافع من أخطر المواقع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المجرم الإلكتروني الرغبة في الانتقام من رب العمل، ومثال ذلك أن الانتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

ثانيا: دافع التعاون والتواطؤ

هذا النوع يتكرر كثيرا في الجرائم الإلكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو خارج

[1]– سعيداني نعيم رسالة الماجستير السابقة الذكر، من 61–62

[2]– يوسف صغير، مرجع سابق، ص 42

المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم[1].

وإذا كانت هذه أبرز الدوافع لارتكاب الجريمة الإلكترونية، مع ذلك فهي ليست ثابتة ومعتمدة الدى الفقهاء والباحثين لأن السلوك الإجرامي والدوافع لارتكاب الجريمة الإلكترونية قد للغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة، إلى تدميرها أو على الأقل حيازتها للقيام بعملية الابتزاز والحصول على الأموال، لذلك فإن هذه الدوافع قد لا تتوقف عند هذا الحد، إذ نجد في كل جريمة جديدة دوافع جديدة، بل كثيرا ما نجد الجريمة الواحدة لها دوافع متعددة خاصة ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة[2].

[1]– سعيداني نعيم، المرجع السابق، ص 62.

[2]– المرجع نفسه، ص62.

خاتمة الفصل الأول

من خلال ما تعرضنا له في دراستنا لماهية الجريمة الالكترونية، تبين لنا جليا بأنها من الجرائم التي تتسم بالخطورة المطلقة وفي نفس الوقت جرائم ناعمة، لكن تحقق النتيجة الإجرامية على أكمل وجه، فهي تلك الجريمة الرامية إلى عدم ترك أثر أو دليل قد يدين فاعلها فتميزها بهذا الطابع الفريد والأقل عنها جعل الإقبال عليها متزايد خاصة ما نراه في السنين الأخيرة، فالربح كثير والجهد أقل وبثوان معدودة تتحقق الجريمة، فالبعد بينها وبين الجرائم العادية يكمن هنا، فتعد الأكثر فتكا ومنعدمة الوجود فتتحقق بلمسة زر واحدة، وأكثر من هذا عدم التقاء الجاني والمجني عليه وهذا ما يزيد من صعوبتها ومن صعوبة مكافحتها، وكذلك نصوص التجريم التي وضعها المشرع الجزائري لم تكن كافية فركز على الجريمة بحد ذاتها وأهمل نسبيا المجرم الذي يقوم بها (المجرم الالكتروني)، لهذا دعت الضرورة لمكافحة هذه الظاهرة المستحدثة وهذا ما تم التطرق له في الفصل الثاني.

الفصل الثاني:

آليات مكافحة الجريمة الالكترونية

صاحب ظهور شبكة الانترنيت بروز تحديات جديدة للمنظومة القانونية الموضوعية و الاجرائية على المستوى الدولي والمحلي خاصة بعد أن أصبحت هذه الوسيلة يعتمد عليها الجناة في ارتكاب طائفة من الجرائم المستحدثة التي تختلف عن الجرائم التقليدية في الطريقة و المناهج ، و ألقت بضلالها على العالم بأسره، فكانت الأضرار و الخسائر التي انجزت عنها فادحة على المستويين الدولي و المحلي، الأمر الذي أدى بمختلف الدول إلى الإسراع من أجل المحاولة للتصدي لهذه الظاهرة فتضافرت الجهود من أجل ايجاد طرق مكافحة الجريمة الالكترونية بنجاعة و فعالية أكثر (المبحث الأول).

وبالرغم كل ما حققته وسائل التكنولوجيا الإلكترونية الحديثة من إيجابيات إلا أن وجهها السلبي طغى عليها بشكل خطير أدى إلى ارتكاب الجريمة الإلكترونية التي باتت مكافحتها شبه مستحيلة، وهذا راجع إلى عدة خصوصيات منها طبيعة مسرح الجريمة الذي تقع فيه وذكاء المجرم الإلكتروني بالإضافة إلى ارتكابها من أي رقعة جغرافية حول العالم، مما استوجب وضع قواعد الحماية الإجرائية لمتابعة مرتكبي هذا النوع من الجرائم الخطيرة (المبحث الثاني).

المبحث الأول: طرق مكافحة الجريمة الالكترونية

تتجسد أول طرق مكافحة الجريمة الالكترونية في الجهود التشريعية سواء على المستوى الدولي والعربي لتنظيم منظومة قانونية للوقاية من هذه الجريمة المستحدثة وهذا ما تم عرضه في (المطلب الأول).

أما (المطلب الثاني) فقد تم التطرق إلى المكافحة المؤسساتية للجريمة الإلكترونية التي تتمثل هذه المؤسسات في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والضبطية القضائية.

المطلب الأول: الجهود التشريعية لمكافحة الجريمة الالكترونية

دأبت المجتمعات والدول عبر الزمن في سن تشريعات وقوانين من أجل مواجهة كل الجريمة الالكترونية، فبالرغم من قلتها إلا أنها تعتبر محاولات هامة وملموسة في هذا المجال وتتمثل هذه الجهود على المستوى الدولي في الجهود التي تبذلها مختلف الهيئات والمنظمات العالمية بالإضافة إلى المنظمات الإقليمية (الفرع الأول).

تعتبر الجهود الدولية داعمة للجهود التي تبذلها مختلف الدول في تشريعاتها الداخلية فتعتبر بمثابة قوانين استرشادية تأخذ بها الدول لمواجهة الجرائم المستحدثة بما فيها الجريمة الالكترونية، فهناك العديد من الدول التي اتخذت سبيل تطوير قوانين العقوبات، وهناك دول ارتأت أفرادها بقوانين خاصة، وفي هذا الإطار سوف نستعرض تجربة المشرع الجزائري التي انتهجها للحد من هذه الجريمة (الفرع الثاني).

الفرع الأول: على المستوى الدولي

تعددت الجهود الدولية والإقليمية في سبيل مكافحة الجريمة الالكترونية، نظرا للتهديدات الكبيرة التي أتت بها الجريمة على هذين المستويين، وفي هذا المجال سنبين الجهود الدولية في مواجهة الجريمة الالكترونية (أولا) وكذا الجهود الاقليمية في هذا السياق (ثانيا).

أولا: الجهود الدولية لمكافحة الجريمة الالكترونية

تتمثل الجهود الدولية في إطار مكافحة الجريمة الالكترونية في:

1- جهود منظمة الأمم المتحدة

بذلت منظمة الأمم المتحدة جهودا كبيرة في سبيل العمل على مكافحة جرائم الانترنيت نظرا لما ينتج منها من أضرار بالغة وخسائر فادحة بالإنسانية جمعاء.

توصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة الالكترونية ومعاملة المجرمين[1] إلى اصدار قرار خاص بالجرائم المتعلقة بالحاسوب وأشار في مضمونه إلى أن الإجراء الدولي لمواجهة الجريمة الالكترونية يتطلب من الدول الأعضاء اتخاذ عدة اجراءات أهمها:

- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان تطبيق القوانين الجنائية الراهنة (التخفيف قبول الأدلة) على نحو ملائم وادخال التعديلات إذا دعت الضرورة.
- مصادرة العائد والأصول من الأنشطة غير المشروعة.
- اتخاذ تدابير أمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.
- رفع الوعي لدى الجماهير والقضاة والأجهزة العاملة على مكافحة هذه الجريمة بأهمية مكافحة هذه الجريمة ومحاكمة مرتكبيها.
- التعاون مع المنظمات المهتمة بهذا الموضوع، ووضع وتدريس الآداب المتبعة في استخدام الحاسوب ضمت المناهج المدرسية.
- حماية مصالح الدولة وحقوق ضحايا الجريمة الالكترونية.

[1]– نجاري بن حاج علي فايزة، الآليات القانونية لمكافحة الإرهاب الالكتروني، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، ص70.

عقدت منظمة الأمم المتحدة اتفاقية خاصة بمكافحة اساءة استعمال التكنولوجيا لأغراض اجرامية سنة 2000 أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة اساءة استعمال تكنولوجيا المعلومات لأغراض اجرامية.

- كما عقدت كذلك المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية وذلك بالبرازيل أيام 12-19 أفريل 2010، بحيث ناقشت فيه الدول الأعضاء مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة الالكترونية. إضافة إلى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات وذلك تحت اشراف الأمم المتحدة عام 1944، الذي نتج عنه عدة توصيات وقرارات ذات صلة بالجريمة الالكترونية[1].

2- منظمة التعاون الاقتصادي و التنمية[2]

تهدف هذه المنظمة إلى تحقيق أعلى مستويات النمو الاقتصادي وتناغم التطور الاقتصادي مع التنمية الاجتماعية بدأت هذه المنظمة تهتم بالجريمة الالكترونية منذ عام 1978، ذلك بوضعها لمجموعة أدلّة وقواعد ارشادية تتصل بتقنية المعلومات. يعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة سنة 1980 مع التوصية للأعضاء بالالتزام بها.

في عام 1983 أصدرت هذه المنظمة تقريرا بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء، حيث تضمن التقرير الحد الأدنى لأفعال سوء استخدام الحاسوب التي يجب على الدول أن تجرمها وتفرض لها عقوبات في قوانينها، ومن أمثلة هذه الأفعال الاستخدام أو

[1]- نجاري بن حاج علي فايزة، المرجع السابق، ص71.

[2]- المنظمة التعاون الاقتصادي والتنمية (OECD)، تضم مجموعة من الدول استراليا النمسا بلجيكا، كندا، جمهورية التشيك الدنمارك، فنلندا، فرنسا، اسبانيا، ايسلندا، اليونان المانيا، ايرلندا السويد سويسرا، لكسمبورغ، المكسيك، هولندا، نيوزيلندا، النرويج، بولندا، البرتغال، تركيا، بريطانيا، الولايات المتحدة الأمريكية، تعمل هذه الدول متحدة في ايطار المنظمة على تنمية الاقتصاد العالمي والتنمية الاجتماعية.

الدخول إلى نظام ومصادر الحاسوب على نحو غير مصرح به، ويشمل ذلك الحاسب والمعلومات المخزنة في قواعد الحاسب. كما أوصت اللجنة المصدرة للتقرير إلى وجوب أن تمتد الحماية إلى صورة أخرى الإساءة استخدام الحاسوب، منها الاتجار في الأسرار والاختراق غير المأذون فيه للحاسب أو لأنظمته.

وفي عام 1992 وضعت المنظمة توصيات إرشادية خاصة بأمن أنظمة المعلومات حيث تمخضت جهود المنظمة من أجل معالجة الجريمة الالكترونية بالتوصية بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء الأفعال التالية[1]:

- التلاعب في البيانات المعالجة آليا بما في ذلك محوها.
- التجسس المعلوماتي ويندرج تحته الحصول أو الاقتناء أو الاستعمال غير المشروع للمعطيات.
- التخريب المعلوماتي ويندرج تحته الاستخدام غير المشروع أو سرقة وقت الحاسب.
- قرصنة البرامج.
- الدخول غير المشروع على البيانات أو نقلها.
- اعتراض استخدام المعطيات أو نقلها.

تعقد المنظمة سنويا عدد من الملتقيات وورش العمل المعقمة للقطاعات ذات العلاقة بهذا المجال تركز فيها على معايير الأمن ومستوياته، إضافة إلى معايير تنفيذ وتطبيق القانون وذلك بهدف مواكبة التطورات في مجال جرائم الانترنيت.

3- المنظمة العالمية للملكية الفكرية

تم توقيع المنظمة العالمية للملكية الفكرية في استوكهولم في السويد سنة 1967[2]، وأصبحت إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتبارا من 17 ديسمبر 1974.

[1]– www.oecd-ong ، تاريخ الاطلاع 2023/06/02، على الساعة 20:36.

[2]– محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر، الأردن، 2005، ص159.

اهتمت هذه المنظمة في دعم الملكية الفكرية في جميع أنحاء العالم بهدف تشجيع النشاط الابتكاري كما اهتمت هذه المنظمة في المجال المعلوماتي بتوفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، فبعد أن يستقر الرأي لديها بعدم امكانية توفير الحماية لهما في تشريعات براءات الاختراع تم الاتفاق على توفيرها بواسطة الاتفاقيات العالمية وخاصة التريس و برن اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، وخاصة تشريعات حق المؤلف، وكذلك وضع عقوبات على كل أعمال تزوير في العلامات التجارية والقرصنة المتعمدة والمرتكبة في إطار تجاري وتعتبر الانترنيت من الأماكن الخصبة لهذا النوع من التصرفات و التي وفرت بموجبها الحماية القانونية للبرامج و قواعد البيانات المعلوماتية.

حيث تنص المادة الرابعة من معاهدة المنظمات العالمية للملكية الفكرية والمعتمدة سنة 1996على أنه " تتمتع برامج الحاسوب بالحماية باعتبارها مصنفات أدبية في معنى المادة الثانية من اتفاقية برن وتطبيق تلك الحماية على برامج الحاسوب أيا كانت طريقة التعبير عنها أو شكلها، وتنص المادة الخامسة على أنه: تتمتع مجموعات البيانات أو المواد بالحماية بصفتها هذه أيا كان شكلها إذا كانت تعتبر ابتكارات بسبب اختيار محتوياتها أو ترتيبها"[1].

ثانية: دور الهيئات والمنظمات الاقليمية في مكافحة الجريمة الالكترونية

تتمثل الجهود الاقليمية في مكافحة الجريمة الالكترونية في:

1- الاتحاد الأوروبي

توجت الجهود التي يبذلها الاتحاد الأوربي والمجلس الأوربي بصدور اتفاقية بودابست لمكافحة الجريمة الالكترونية وتعرف بالاتفاقية الأوربية لمكافحة الجريمة الالكترونية. وتتخلص أهم أهدافها في السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوربية والدول المنظمة للاتفاقية من غير الدول الاوربية. والتأكيد على أهمية التعاون الاقليمي والدولي في ميدان مكافحة الجريمة

[1]– محمود أحمد عبابنة، المرجع السابق، ص162.

الالكترونية، وتحقيق التوازن بين حقوق الإنسان والاجراءات المتخذة لمواجهة هذه الجريمة[1]. وضعت اتفاقية بودابست من قبل مجلس أوربا بالتعاون مع كندا، واليابان وجنوب افريقيا والولايات المتحدة الأمريكية، وعرضت للتوقيع في بودابست في عام 2001 ودخلت حيز التنفيذ سنة 2004.

لا تعتبر اتفاقية بودابست المجهود الأول الذي بذله المجلس الأوربي في هذا المجال، بل بذل جهود عديدة من قبل لاسيما الاتفاقية المتعلقة بحماية الأشخاص في مواجهة المعالجة الالكترونية للبيانات ذات الصبغة الشخصية وذلك في 28 جانفي 1981، لكن تبقى اتفاقية بودابست الحيّز الأمثل لمواجهة الجريمة الالكترونية.

2- مجموعة الدول الثمانية[2]

تمثل هذه المجموعة إطارا ناضجا لإجراء الدراسات البحثية والتطبيقية في مختلف المواضيع التي تهم المنظمة، تقوم على فكرة تبادل زعماء هذه الدول الرأي في المسائل ذات الاهتمام المشترك. تناولت مجموعة الثمانية في المؤتمر الذي عقدته في باريس عام 2000 موضوع الجريمة الالكترونية وحثت إلى منع ملاذات الرقمية غير الخاضعة للقانون. وكانت مجموعة الثمانية قد ربطت منذ ذلك الوقت محاولاتها الرامية إلى ايجاد حلول دولية باتفاقية مجلس أوربا بشأن الجريمة الالكترونية. في عام 2001 ناقشت مجموعة الثمانية الأدوات الاجرامية لمكافحة الجريمة الالكترونية في ورشة عمل عقدت بطوكيو، ركزت على ما إذا كان ينبغي تنفيذ الالتزامات باحتجاز البيانات أو ما إذا كان حفظ البيانات يعد حلا بديلا.

3- على المستوى العربي

[1] -KURBALIJA Jouan, GELBSTEIN Eduardo, Gouvernance de l'internet, actems et fractures, public par diplo fondation et global knowledge partnership, Suisse 2005, p98

[2] – مجموعة الثمانية G8 نشأتها ومؤتمراتها السنوية، أجندتها عملها على الموقع www.g8utoriontо.com

نجد من الجهود العربية في سبيل مواجهة الجريمة الالكترونية القرار الصادر عن مجلس وزراء العدل العرب الخاص بإصدار القانون الجزائي الموحد كقانون عربي نموذجي، أين نجد الباب السابع الخاص بالجرائم ضد الأشخاص، قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن المعالجة المعلوماتية وذلك في المواد 461-464 التي أشارت على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيفية الاطلاع عليها والعقوبة المطبقة في حال ارتكاب هذه الجرائم.

كذلك فإن الجمعية المصرية للقانون الجنائي لها اتجاه موحد في هذا المجال، وتمثل ذلك في مؤتمرها السادس المنعقد في القاهرة من 25-28 أكتوبر 1993، حول جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات التي أكد فيها المؤتمرون على عالمية الجرائم الالكترونية ووجوب تكاتف الجهود لمكافحتها، لأنها تمثل وجها سلبيا، ووجوب تعديل نصوص قانون العقوبات التقليدية، وإضافة نصوص جديدة، لأن النصوص الحالية لا يحيط معظمها بالأنشطة المراد تجريمها.

وفي بيروت انعقد مؤتمر في قانون الملكية الفكرية فيما بين الفترة 25-28 مارس 1997. تمثلت توصيات المؤتمر بضرورة انشاء محاكم متخصصة للبحث في الالتزامات المغلقة بالحماية الالكترونية وتشجيع التعاون بين الدول العربية[1].

الفرع الثاني: في التشريع الجزائري

واكب المشرع الجزائري مختلف التطورات التشريعية التي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الالكترونية بما فيها الانترنيت، خاصة التي تهدف إلى الحد من الاستخدام غير المشروع لها، وذلك مراعاة منه لما يشهده العالم من تطورات كبيرة في مجال الاعلام والاتصال خاصة الانترنيت وكذلك إيمانا منه بأن الجزائر ليست بمعزل عن التطورات الاجرامية

[1]- عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 59

التي تحدث في العالم، خاصة في ظل التنامي المتصارع لاستعمال الانترنيت في الجزائر، فكانت محاولاته في الحد من هذه الظاهرة المستحدثة على النحو التالي:

أولا: مكافحة الجريمة الالكترونية في قوانين الملكية الفكرية

نظرا للاعتداءات التي تتعرض لها مختلف المفتحات الفكرية عبر الانترنيت تطرقنا في بحثنا هذا إلى مدى امكانية الحماية من خلال نصوص قانون الملكية الفكرية، وسنتوصل في ذلك من خلال نقطتين أساسيتين:

- الحماية في إطار قانون الملكية الصناعية.
- الحماية في إطار قانون الملكية الأدبية والفنية.

1- مكافحة الجريمة الالكترونية في إطار الملكية الصناعية

أ- في الأمر 03-06 المتعلق بالعلامات التجارية

تطرق المشرع الجزائري إلى تنظيم أحكام العلامات التجارية من خلال عدة قوانين آخرها الأمر رقم 03-06 المؤرخ في 2003/07/19[1]، والمتعلق بالعلامات وتعرف العلامات التجارية على أنها كل ما يتخذ من تسميات أو رموز أو أشكال توضع على البضائع التي يبيعها التاجر أو يضعها المنتج أو يقدم بإصلاحها أو تجهيزها، أو ختمها لتمييزها عن بقية المبيعات أو المصنوعات أو الخدمات ومن شروط العلامة التجارية: أن تكون مميزة، أن تكون جديدة، أن تكون غير مخالفة للنظام العام.

ب- في الأمر رقم 03-07 المتعلق ببراءات الاختراع

[1]- تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة مقدمة للحصول على درجة دكتوراه الفلسفة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009، ص 17.

عرفت المادة 02 من الأمر 03-07 الاختراع بأنه فكرة لمخترع تسمح عمليا بإيجاد حل لمشكل محدد في مجال للتقنية، وبشأن الشروط التي يجب توافرها في الاختراع فتتمثل فيما يلي[1]: (شرط الابتكار، شرط الجدة، القابلية للتطبيق الصناعي، المشروعية)

تجدر الاشارة الى ان المشرع الجزائري قد استبعد البرامج المعلوماتية صراحة من مجال الحماية بواسطة براءات الاختراع وذلك طبقا للمادة 07 من الأمر 03-07[2] المتضمن براءة الاختراع التي نصت على أنه:

"لا تعد من قبيل الاختراعات في مفهوم هذا الأمر برامج الحاسوب"[3]

2- مكافحة الجريمة الالكترونية من خلال القوانين الأدبية والفنية

نظرا للتطور الذي واكب مجال الاتصال والذي رافقه تطور في وسائل نقل الإنتاج الفكري، على اختلاف صوره من علوم وفنون وآداب، مما أوجد مصنفات جديدة جديرة بحماية حق المؤلف، وقد كان من أهم هذه المصنفات التي حضها بالاهتمام من قبل المختصين في مجال الملكية الفكرية نجد: المصنفات الخاصة ببرامج الحاسبات الالكترونية وقواعد البيانات التي كانت طبيعتها التقنية تختلف عن المصنفات التقليدية الأمر الذي تطلب متابعتها باستمرار ووضع قواعد قانونية محددة وثابتة لحمايتها.

- اتجه المشرع الجزائري إلى الاعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي، وذلك من خلال تعديله للأمر 73-14 بموجب الأمر 97-10[4].

---

[1]- الأمر رقم 03-06 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات التجارية، ج ر عدد 44، صادر في 23 جويلية 2003.

[2]- الأمر رقم 03-07 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع ج ر عدد 44 صادر في 23 جويلية 2003.

[3]- الأمر رقم 03-07 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع، المرجع نفسه.

[4]- أمر رقم 97-10 مؤرخ في 06-03-1997 المتعلق بحق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد 13 الصادر في 1997/03/12 معدل والمتمم بأمر 05/03 مؤرخ في 2003/07/19، المتعلق بحقوق المؤلف، والحقوق المجاورة، الجريدة الرسمية عدد 44، الصادر في 2003/07/23.

والذي يتبين من خلال استقراءها ما يلي:

- أن المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الاعلام الآلي ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي، التي تمكن من القيام بنشاط علمي أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وتترجم بانتفاعات الكترونية بالحاسوب. أما قواعد البيانات فهي مجموعة المصنفات والأساليب والقواعد ويمكن أن تشمل أيضا الوثائق المتعلقة بسير المعطيات.
- أن الحماية تحدّد من 25 إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية برن التي حددت كمدة دنيا للحماية 50 سنة، وبالتالي هذه المدة تشمل حتى مصنفات الاعلام الآلي.
- تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لا سيما مؤلفي المعلوماتية.

ثانيا: مكافحة الجريمة الالكترونية في ظل قانون العقوبات

لما كانت الحاجة ملحة وضرورية لحماية أنظمة المعالجة الآلية فلقد استقر الفكر القانوني على ضرورة وجود نصوص خاصة لهذا الغرض. ولهذا نجد المشرع الجزائري قد تدارك مؤخرا ولو نسبيا الفراغ القانوني في مجال الإجرام الالكتروني وذلك باستحداث نصوص تجريمية لقمع الاعتداءات الواردة على المعلوماتية بموجب القانون 15/04[1] المتضمن تعديل قانون العقوبات لكن تجدر الإشارة إلى أن المشروع الجزائري قد ركز على الاعتداءات الماسة بالأنظمة المعلوماتية، وأغفل الاعتداءات الماسة بمنتوجات الإعلام الآلي والمتمثلة في التزوير الالكتروني. ولذلك ارتأينا وحتى لا تكون دراستنا لموضوع الحماية الجزائية ناقصة أن تتعرض للاعتداءات الواردة على المعلوماتية من خلال ما يلي:

1- جريمة المساس بأنظمة المعالجة الآلية للمعطيات

[1]– القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، المتضمن قانون العقوبات الجريدة الرسمية عدد 71، صادر 2004/11/10.

جريمة المساس بأنظمة المعالجة الآلية للمعطيات أو جريمة الغش المعلوماتي وهو الفعل المنصوص والمعاقب عليه في المواد 394 مكرر الى المادة 394 مكرر 07.

وبالعودة إلى قانون العقوبات الجزائري نجد أن الغش المعلوماتي يأخذ صورتان أساسيتان:

- الدخول في منظومة معلوماتية.
- المساس بالمنظومة المعلوماتية.

أ- **الدخول في منظومة معلوماتية:** ويشمل فعلين هما: الدخول والبقاء.

- **جريمة الدخول غير المشروع:**

تنص المادة 394 مكرر من قانون العقوبات الجزائري والتي تقابلها المادة 323 فقرة 01 قانون عقوبات فرنسي على معاقبة كل من يدخل عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك. وتضاعف العقوبة إذا ترتب على الدخول أو البقاء أو الحذف أو تغيير معطيات المنظومة أو تخريب النظام.

- **جريمة البقاء الغير مشروع:**

نص المشرع الجزائري على هذه الجريمة في المادة 394 مكرّر من قانون العقوبات الجزائري المقابلة لنص المادة 1/323 من قانون العقوبات الفرنسي. ويقصد بالبقاء الدخول الشرعي أكثر من الوقت المحدد وذلك بغية عدم اتاء إتاوة. وتقوم الجريمة مباشرة على الحاسوب أو سواء حصل الدخول مباشرة على الحاسوب أو حصل بعد كما يجرم القاء حتى ولو تم بصفة عرضية[1].

ب- المساس بمنظومة معلوماتية:

تنص المادة 394 مكرر 1 من قانون عقوبات جزائري والتي يقابلها في النص الفرنسي المادة 3/323 من قانون العقوبات الفرنسي: على ان " كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"[2].

[1]– أحسن بوسقيعة، الوجيز في القانون الجزئي، الطبعة السادسة، دار هومة، الجزائر، 2007، ص445.

[2]– مرزوق نسيمة جرائم الانترنيت مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء الجزائر، 2006–2009، ص 10.

2- جريمة التزوير المعلوماتي:

إن قانون العقوبات الجزائري لم يستحدث نصا خاصا بالتزوير المعلوماتي الذي يعتبر من أخطر صور الغش المعلوماتي نظرا للدور الهام والخطير الذي أصبح يقوم به الحاسوب الآن. ونجد أن المشرع الجزائري نص على التزوير الخاص بالمحررات في القسم الثالث والرابع والخامس من الفصل السابع من الباب الأوّل من الكتاب الثالث من قانون العقوبات في المواد من 214 إلى 229 التي تشترط المحرر لتطبيق جريمة التزوير. ولم يتخذ أي موقف لتوسيع مفهوم المحرّر من أجل إدماج المستندات المعلوماتية ضمن المحررات محل جريمة والتزوير.

ثالثا: مكافحة الجريمة الالكترونية في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

يعتبر قانون 04/09 المتعلق بالجرائم المتصلة بتكنولوجيات الاعلام والاتصال مكافحتها نطاقا شاملا في مجال مكافحة الجرائم الالكترونية. حيث جاء تجريمه للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال، وبالتالي فهو يطبق على كل التكنولوجيات القديمة والجديدة بما فيها شبكة الانترنيت على كل تقنية تظهر مستقبلا.

ولقد تبنى المشرع الجزائري بموجب هذا القانون تعريفا موسعا للجرائم الالكترونية بعدما كان النظام العقابي يقتصر فقط على تلك الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات، حيث أصبحت تشمل بالإضافة إلى هذه الأفعال أي جريمة أخرى أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الالكترونية، وبذلك لم يعد مفهوم الجريمة الالكترونية في التشريع الجزائري، يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء بل توسع نطاقها إضافة لتلك الأفعال التي تكون المعلومة.

وقد عرفت المادة 02 من القانون 04/09[1] الجرائم المتصلة بتكنولوجيات الاعلام والاتصال أن جرائم المساس بأنظمة المعالجة الآلية للمعطيات في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

رابعا: مكافحة الجريمة الالكترونية في قانون الاجراءات الجزائية الجزائري المعدل بموجب القانون 04-14 المؤرخ في 2004/11/10

تناول قانون الاجراءات الجزائية موضوع الجرائم الافتراضية من خلال:

- إحداث المحاكم الجزائية ذات الاختصاص الموسع التي أجازت لها تمديد اختصاصها للنظر في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و ذلك في المواد 37، 40، 329 من ق إ ج.
- نصت المادة 16 من هذا القانون على أن تمديد الاختصاص الإقليمي لضباط الشرطة القضائية لمعاينة الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات إلى كافة الإقليم الوطني.
- التنصيص على قواعد استثنائية للتفتيش في المواد 45-47[2].
- إمكانية استعمال أساليب خاصة للتحري في هذه الجرائم.
- التنصيص على إمكانية تمديد فترة التوقيف للنظر.

المطلب الثاني: المكافحة المؤسساتية للجريمة الإلكترونية

يمكن القول أن المحقق هو من يتولى التحقيق من رجال الضبطية القضائية، أو من أعضاء النيابة العامة، أو قضاة التحقيق ويلحق بالمحقق الجنائي الباحث الجنائي الذي يكون غالبا من الشرطية القضائية، الذين خول لهم القانون مهمة جمع الاستدلالات عن المشتبه بهم.

[1]- القانون رقم 04/09 المؤرخ في 2009/02/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، سنة 2009.

[2]- المادتين 45 و47 من القانون رقم 04-14 المؤرخ في 2004/11/10 المتضمن قانون الاجراءات الجزائية الجزائري المعدل.

حيث تم استعراض أبرز الهيئات المختصة في مجال مكافحة الجرائم الإلكترونية، ويتم تناول الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بالفرع الأول، إضافة لتلك الوحدات التابعة لسلك الأمن، وكذلك تلك التابعة لقيادة الدرك الوطني بما يسمى الضبطية القضائية في الفرع الثاني.

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

تتمثل جرائم الإعلام والاتصال في جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وكل الجرائم التي يتم ارتكابها أو يسهل ارتكابها عن طريق منظومة معلوماتية أو باستعمال نظام الاتصالات الإلكترونية وفقا لما ورد في نص الفقرة أ من المادة 2 من قانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

لذلك تم إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الموجب نص المادة 13 من القانون المشار إليه أعلاه والتي يتم تحديد تشكيلتها وتنظيمها وسيرها عن طريق التنظيم، وكان ذلك بهدف مساعدة السلطات القضائية ومصالح الأمن الوطني في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية[1]، وتعد الهيئة بمثابة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى وزير العدل بمدينة الجزائر وفقا لنص المادتين 03 و 04 من المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2].

---

[1]- حابت آمال الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزاري مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، يومي 16 و17 نوفمبر 2015، ص 11.

[2]- المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة تكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج، عدد 53 الصادرة في 08 أكتوبر 2015 جاء نص المادة

وقد نظم كل من ق. ر 09-04 السابق الذكر والمرسوم الرئاسي 15-261 تنظيم عمل الهيئة، أما بالنسبة لتشكيلتها وكيفية سيرها فقد تم إدراجهما في المرسوم السالف الذكر.

أولا: تشكيلة الهيئة وتنظيمها

حدد الفصل الثاني من المرسوم الرئاسي المشار إليه أعلاه تشكيلة الهيئة بحيث أنها تضم هياكل تقنية وإدارية.

1- الهياكل الإدارية

تشمل الهياكل الإدارية للهيئة على اللجنة المديرة والمديرية العامة تكلفان بإدارتها بحيث يرأس اللجنة المديرة وزير العدل وتتشكل من أعضاء حكوميين يتمثلون في الوزير المكلف بالداخلية، وزير البريد وتكنولوجيات الإعلام والاتصال وممثل عن رئاسة الجمهورية بالإضافة إلى مسئولين من مصالح الأمن الوطني وقاضيان من المحكمة العليا يعينهما المجلس الأعلى للقضاء وفقا لما نصت عليهم 07 من المرسوم المشار إليه أعلاه، وتكلف بكل ما يتعلق بتنظيم سير عمل الهيئة بصفة عامة وتقييم حالة الخطر بخصوص الجرائم الواقعة على أمن الدولة لتحديد عمليات المراقبة الإلكترونية وأهدافها.

أما بالنسبة للمديرية العامة فيديرها مدير عام يتم تعيينه وانهاء مهامه بموجب مرسوم رئاسي طبقا لنص م 09 من المرسوم الرئاسي 15-261 ويكلف مجموعة من المهام التي تدخل ضمن صلاحياته والمتمثلة أساسا في التسيير الإداري والمالي للهيئة وتنفيذ عملها مع تنسيق ومتابعة أعمال هياكلها ومراقبتها وتمثيلها على المستوى الوطني والدولي، وكذا القيام بإجراءات التأهيل وأداء اليمين بالنسبة للمستخدمين وممارسة السلطة السلمية عليهم، بالإضافة إلى سهرة على احترام

01 منه كما يلي "تطبيقا لأحكام المادة 13 من القانون رقم 09-04 المؤرخ في 14 شعبان عام 1430 الموافق 5 غشت سنة 2009 والمذكور أعلاه، يهدف المرسوم إلى تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تدعى في صلب النص الهيئة".

قواعد السر المهني للهيئة، زيادة على ذلك يقوم بإعداد تقرير سنوي لنشاطها وعرضه على اللجنة المديرة لتصادق عليه مع قيامه بتحضير اجتماعات هذه اللجنة[1].

2- الهياكل التقنية

تضم الهيئة هيكلين تقنيين يتمثلان في مديرية المراقبة الوقائية لليقظة الإلكترونية ومديرية التنسيق التقني يكلفان بمهام الوقاية من الجرائم الإلكترونية ومكافحتها.

تشمل مديرية المراقبة الوقائية واليقظة الإلكترونية كل من ملحقات جهوية تقوم بتشغيلها[2]، ومركز للعمليات التقنية الذي تشغله المديرية، والذي يتم تزويده بمجموعة من المنشآت والتجهيزات والوسائل للقيام بالمراقبة التقنية للاتصالات الإلكترونية وفقا لنص م 13 من المرسوم المذكور أعلاه، وتكلف المديرية بعدة اختصاصات والتي يمكن تلخيصها فيما يلي:

- تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية للكشف عن الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال بموجب رخصة مكتوبة من السلطة القضائية وتحت مراقبتها طبقا للتشريع الساري المفعول وارسالها إلى كل من هذه السلطة والشرطة القضائية.
- جمع كل المعلومات والبيانات المتعلقة بالكشف عن الجرائم الإلكترونية بهدف استغلالها وتقديمها تلقائيا أو بناءا على طلب لكل من السلطات القضائية ومصالح الأمن الوطني.
- تنفيذ توجيهات اللجنة المديرة وطلبات المساعدة القضائية الدولية بخصوص جمع المعلومات، المعطيات المتعلقة بالمجرمين وتحديد أماكن تواجدهم.
- القيام بعمليات التوعية حول استعمالات تكنولوجيات الإعلام والاتصال والمخاطر التي تنجر عنها بهدف الحد من الجريمة الإلكترونية.

[1]– المادة 10 من المرسوم الرئاسي 15–261 مرجع سابق، ص17.

[2]– المادة 14، المرجع نفسه، ص18.

- السهر على حسن سير عمل مركز العمليات التقنية وملحقاتها الجهوية مع الحفاظ على منشأتها وتجهيزاتها وما تحتويه من وسائل تقنية، وكذا الحفاظ على السر المهني في تأدية أعمالها[1].

أما فيما يخص مديرية التنسيق التقني فوفقا لنص م 12 من المرسوم الرئاسي رقم 15-261 تكلف باختصاصات تتمثل أساسا في مجموعة من المهام تتلخص في تسيير منظومة الإعلام للهيئة وادارتها، مع إنجاز الخبرات التي تدخل في مجال اختصاصاتها، بالإضافة إلى إنشائها لقاعدة معلومات لحفظ المعطيات والبيانات التحليلية الجنائية المتعلقة بالجرائم الإلكترونية واعداد إحصائيات وطنية هذه الجرائم، كما تقوم بكل دراسة أو تحليل أو تقييم لصلاحياتها إما من تلقاء نفسها أو يطلب من طرف اللجنة المختصة.

ثانيا: سير الهيئة

تضمن الفصل الثالث من المرسوم الرئاسي رقم 15-261 على كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث تقوم بعقد اجتماعات والمصادقة على النظام الداخلي لها، بالإضافة إلى تزويد مختلف هياكلها بالتشكيلة البشرية لضمان سير عمل الهيئة، لها صلاحية طلب أي معلومات أو وثائق تفيدها من مؤسسة أو مصلحة معينة بغرض تأدية مهامها وطلب المساعدة من موظفين تقنيين في محال تكنولوجيات الإعلام والاتصال العاملين في وزارات أخرى وفقا للشروط الواردة في التنظيم الساري المفعول، كما خول لها القيام بإجراءات التحقيق ومراقبة الاتصالات الإلكترونية مع تجميعها وحفظها من طرف التقنيين الموكل إليهم ذلك، وكذلك ضمان سرية هذه العملية، والحفاظ على السر المهني ومعاقبة كل موظف يستغل المعلومات والمعطيات المتحصل عليها في أغراض أخرى غير الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

ثالثا: مهام الهيئة

[1]- المادة 11 من الرسوم الرئاسي رقم 15-261، مرجع سابق، ص 18

تتجلى عموما مهام الهيئة في مجال الوقاية ومكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، حيث حددت م 14ق.ر 09-04 مهام الهيئة التي تتمثل في تنشيط وتنسيق عمليات الوقاية ومكافحة الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال بمساعدة السلطات القضائية وأجهزة الأمن الوطني، جمع المعلومات والخبرات القضائية وتبادل المعلومات مع نظيراتها في الخارج بغرض جمع كل البيانات ذات الصلة بأماكن تواجد مرتكبي الجرائم الإلكترونية.

بالإضافة إلى ذلك نجد المرسوم الرئاسي رقم 15-261 في م 04 منه تضمنت مزيدا من التفاصيل بشأن مهام الهيئة، بحيث يمكنها أن تجري جميع عمليات التحري والتحقيق في إطار الوقاية من الجرائم الإلكترونية، مساعدة السلطات القضائية وأجهزة الأمن الوطني في مجال مكافحة هذه الجرائم وتضمن تنفيذ طلبات المساعدة للدول الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي، والمساهمة في تكوين وتدريب المحققين في مجال التحقيقات التقنية في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

الفرع الثاني: الضبطية القضائية

نظرا لخصوصية الجريمة الإلكترونية كان محتما توفير كوادر، وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة الإلكترونية، وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني.

أولا: الوحدات التابعة لسلك الأمن الوطني

تعد الجريمة الإلكترونية وجه جديد للجرائم يستلزم استحداث هياكل جديدة وتدعيم الهياكل القديمة المختصة في مكافحة الجرائم على مستوى المديرية العامة للأمن الوطني، وعلى هذا الأساس قررت القيادة العليا للأمن الوطني استحداث مخابر وفصائل وخلايا مختصة في مكافحة الجرائم الإلكترونية، والقيام بعمليات التحسس والتوعية من خلال المشاركة في الملتقيات الوطنية والدولية

وجميع التظاهرات التي من شأنها توعية المواطن، بالإضافة إلى تنظيم دروس توعوية في مختلف الأطوار الدراسية[1].

1- النيابة المديرية للشرطة العلمية على المستوى المركزي

قامت المديرية العامة للأمن الوطني بتحديث بنيتها الهيكلية من خلال إنشاء وحدات متخصصة تعمل على مكافحة نوع معين من الجرائم دون سواها، وهذا باستحداث أربعة (04) وحدات نيابية متخصصة تتمثل في:

- نيابة الشرطة العلمية والتقنية.
- نيابة مديرية الاقتصادية والمالية.
- نيابة القضايا الجنائية.
- مصلحة البحث والتحليل[2].

وما يهم في دراستنا هي مديرية النيابة للشرطة العلمية والتقنية التي تتألف من مخير مركزي على مستوى الجزائر العاصمة وثلاثة (03) مخابر جهوية، ويتكون كل مخبر من دائرتين دائرة للشرطة العلمية وأخرى تقنية، وتتمثل المهمة الرئيسية للمخبر المركزي بالمساهمة إلى جانب أجهزة العدالة في إظهار الحقيقة عن طريق تقديم المساعدات التي تطلبها الهيئات الفضائية فيما يتعلق بتفسير وتحليل الآثار المادية التي يعثر عليها في مسرح الجريمة أثناء عملية التحري والتحقيق[3].

أ- دائرة الشرطة العلمية

---

[1]– حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، يومي 16-17 نوفمبر، 2015 ص ص08-09.

[2]– ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراه في الحقوق، فرع قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 2016، ص177

[3]– بهلول مليكة، دور الشرطة العلمية والتقنية في الكشف عن الجريمة، أطروحة لنيل شهادة الدكتوراه علوم، فرع الحقوق، كلية الحقوق، جامعة الجزائر، 2013، ص140.

تتكون مصلحة الشرطة العلمية من سنة (06) فروع[1]، تتولى تحليل وفحص الأدلة[2]، المتصلة بالمجال البيولوجي، الطب الشرعي، الكيمياء، المخدرات وكذلك تلك المتعلقة بمجال التسميم والحرائق والمتفجرات.

ب- دائرة الشرطة التقنية

تتولى دائرة الشرطة العلمية مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها القذائف بمختلف أنواعها، وكذلك جرائم التزوير، إضافة إلى الجرائم الإلكترونية حيث تقوم الشرطة التقنية بمباشرة الإجراءات الخاصة بكل جريمة على مستوى الفروع الخاصة بكل نوع من الجرائم.

2- دائرة الأدلة الرقمية والآثار التكنولوجية على المستوى الجهوي

بالإضافة إلى المخبر المركزي الذي يتواجد بالجزائر العاصمة يوجد أيضا مخبرين جهويين على مستوى كل من قسنطينة ووهران يتوليان أعمال البحث والتحري في الجرائم، بما فيها الجريمة الإلكترونية وهذا تحت تسمية دائرة الأدلة الرقمية والآثار التكنولوجية والتي لم تكن سوى قسم عند استحداثها سنة 2004. وبسبب الارتفاع المتزايد لقضايا الجرائم الإلكترونية باستعمال تقنية المعلومات تم ترقيتها إلى دائرة تضم ثلاثة (03) أقسام:

- قسم استغلال الأدلة الرقمية الناتجة عن الحاسوب والشبكات.
- قسم استغلال الأدلة الناتجة عن الهواتف النقالة.
- قسم تحليل الأصوات (يتواجد على مستوى المخبر المركزي بالجزائر العاصمة).

في سنة 2010 تم خلق ما يقارب 23 خلية لمكافحة الجرائم الإلكترونية موزعة على كل ربوع الوطن شرق، وسط، غرب وجنوب[3]، وتكلف الدائرة بعدة مهام، من بينها البحث والتحري بحيث

---

[1]– تتكون دائرة الشرطة العلمية من ستة (6) فروع تتمثل في: فرع البيولوجية والبصمة الوراثية، فرع الكيمياء الشرعية، فرع المتفجرات والحرائق، فرع التسمم الشرعي، فرع مراقبة النوعية الغذائية وفرع الطب الشرعي.

[2]– بهلول مليكة، المرجع السابق، ص147.

[3]– حملاوي عبد الرحمان، المرجع السابق، ص08.

أن أعضاء الدائرة عادة ما يستجيبون للطلبات التي يقدمها لهم أعوان الشرطة التابعون لخلايا مكافحة الجرائم الإلكترونية الموزعة على كل مديريات الأمن الوطني أو لطلبات وكيل الجمهورية، أو قاضي التحقيق التي تردهم في شكل إنابة قضائية من أجل دعمهم ومساعدتهم أثناء إجراء المعاينة لمسرح الجريمة لحجز الأدلة المتواجدة عليها، وكذلك ضمان الدعم التقني لمختلف مصالح الشرطة والأجهزة القضائية من طرف خبراء مؤهلين إذ أنه في مرحلة التحقيق لا يتعدى دورهم إعداد تقارير الخبرة التي يطلبها كل من قاضي التحقيق ووكيل الجمهورية على الأدلة التي تم ضبطها كتحليل محتوى الأقراص الصلبة أو المواقع التي تم اختراقها[1].

من الأمثلة الواقعة بالجزائر في هذا الصدد، جريمة تعود حيثياتها إلى جويلية 2013 إثر تلقي مصالح الأمن الوطني بالجزائر العاصمة شكوى من وزارتي التعليم العالي والبحث العلمي وبريد الجزائر، مفادها احتراق لمواقعها الإلكترونية والمعلوماتية من طرف هاكر جزائري ينتحل هوية الرئيس الراحل صدام حسين باسم مستعار "صدام 2013" وعلى إثرها باشرت الجهات المختصة في مكافحة الجرائم الإلكترونية لتحرياتها عن هذا الهاكر وتم تحديد هويته الحقيقية وتنقلت الضبطية القضائية إلى مسكنه في أولاد ميمون بتلمسان وهو شاب يبلغ 22 سنة[2].

ثانيا: الوحدات التابعة للدرك الوطني

اهتمت قيادة الدرك الوطني بمكافحة الجريمة الإلكترونية بمختلف أشكالها وأنواعها، وهذا من خلال استحداث هياكل تابعة لها من أجل التصدي للإجرام المعلوماتي الذي بات يشكل تهديدا خطيرا على أمن الدولة وسلامة المجتمع، وعليه تم إنشاء أربعة (04) وحدات تنشط في مجال الوقاية من الجريمة الإلكترونية ومكافحتها والتي سنعرضها في هذا الفرع لنبين أهم ما تقوم به في هذا المجال.

1- المعهد الوطني للأدلة الجنائية وعلم الإجرام

[1]– ربيعي حسين، المرجع السابق، ص180.

[2]– الموقع الرسمي لمديرية الأمن الوطني، www.dgsn.dz، تاريخ الإطلاع 2023/06/04 على الساعة 22:42.

تم إنشاء المعهد الوطني للأدلة الجنائية وعلم الإجرام بموجب المرسوم الرئاسي رقم 04-183 المتضمن إحداث المعهد الوطني للأدلة الجناية وعلم الإجرام للدرك الوطني وتحديد قانونها الأساسي[1]، وفقا لنص م 02 من هذا المرسوم يعتبر المعهد مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، ويوضع تحت وصاية وزارة الدفاع الوطني في بوشاوي بالجزائر العاصمة، فهو يخضع لجميع الأحكام التشريعية والتنظيمية العسكرية، وقد صنف من بين المعاهد الكبرى في العالم[2].

يشمل المعهد على إحدى عشر (11) دائرة متخصصة في مجالات مختلفة جميعها تضمن انجاز الخبرة، التكوين والتعليم بالإضافة إلى تقديم المساعدات التقنية والقيام ببحوث ودراسات وتحاليل في علم الجريمة[3]، نظرا لاحتوائه على تجهيزات ووسائل تكنولوجية جد متطورة، بالإضافة إلى بنك المعلومات ومخابر للأدلة الرقمية والخبرة الصوتية للوقاية من جرائم الإعلام الآلي والهاتف المحمول، ومن بين دوائره نجد دائرة الإعلام الآلي والإلكترونيك المكلفة بتحليل البيانات الرقمية وتقديم المساعدة للمحققين في محال التحري والتحقيق في الجرائم الإلكترونية.

تتكون دائرة الإعلام الآلي والإلكترونيك من ثلاثة (03) مخابر تتمثل في مخبر الإعلام، مخبر الفيديو ومخبر الصوت، وتكلف هذه الدائرة بمهمة رصد ومراقبة وتتبع عمليات الاختراق والقرصنة وكذلك اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية[4].

أ- مخبر الإعلام الآلي

---

[1]- المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلمة الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر ج ج عدد 41 الصادرة في 27 يونيو 2004، ص ص 21-22.

[2]- بهلول مليكة، المرجع السابق، ص 144.

[3]- هواري عياش، المعهد الوطني للأدلة الجنائية وعلم الإجرام، مسار التحقيقات الجمالية في مجال الجريمة المعلوماتية، مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، يومي 16 و17 نوفمبر، 2015، ص03.

[4]- بهلول مليكة، المرجع السابق، ص 144

يحتوي مخبر الإعلام الآلي على سبعة (07) قاعات تتمثل في مكتب التوجيه، فصيلة الأنظمة المشحونة، فصيلة تحليل المعطيات، فصيلة الهواتف، فصيلة اقتناء المعطيات، قاعة موزع وقاعة تخزين، وتم تزويده بأحدث التجهيزات والوسائل لإنجاز المهام المحولة له لاكتشاف الجرائم المتعلقة بالمجال المعلوماتي والإلكتروني وهذا بالاعتماد على:

- محطة ثابتة ومحمولة لإجراء خبرات الإعلام الآلي.
- جهاز اقتناء معلومات الهواتف والحواسيب.
- محطة ترميم وتصليح الأجهزة والحوامل المعطلة.
- الحبكات الإعلامية (خبرات الإعلام والتجهيزات البيانية)[1].

من أهم المهام التي تعهد للمخبر تحليل ومعالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب وذاكرة الفلاش) وتحديد التزوير الرقمي للبطاقات البنكية[2]، وبلا شك فإنه يقوم بتقديم المساعدة للمحققين في المجال التقني عن طريق إصلاح كل تلف في الأجهزة الإلكترونية التي يتم العثور عليها في مسرح الجريمة.

ب- مخبر الفيديو

يضم مخبر الفيديو أربعة (04) قاعات تتمثل في قاعتان للتحليل، قاعة التخزين وقاعة موزع، ولكي تباشر هذه القاعات مهامها تتوفر على أحدث الأجهزة من بينها:

- مجموعة أجهزة لقراءة مختلف حوامل الفيديو الرقمية والممغنطة.
- جهاز فيديو بوكس
- حبكات إعلامية (كونيتك ستوديو، ماكس ثلاثة أبعاد)
- موزع لحفظ شرائح الفيديو

[1]– بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني cyper security في الجزائر: الدور والتحديات، المجلة الجزائرية للأمن الوطني الإنساني، عدد 20، مخبر الأمن الإنساني: الواقع، الرهانات والآفاق، جامعة باتنة 1، 2017، ص436

[2]– هواري عياش، المرجع السابق، ص 06

من المهام التي تباشرها هذه القاعات إعادة بناء مسرح الجريمة بتشكيل ثلاثي الأبعاد، بالإضافة إلى تحسين نوعية الصورة (فيديو أو صورة) بمختلف التقنيات، ومقارنة الأوجه وشرعية الصور والفيديو[1].

ج- مخبر الصوت

يتشكل مخبر الصوت من خمسة (05) قاعات ثلاثة منها تختص في التحليل وقاعة موزع وأخرى للتخزين، ومن بين التجهيزات التي يتوفر عليها المخبر:

- أجهزة الازدواجية والسماع
- حبكات إعلامية (معالجة وتحسين التسجيلات الصوتية، نسخ الأقراص المضغوطة)
- أجهزة التصليح والتغيير

يكلف المخبر بمهام تدخل في إطار اختصاصه من تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة، معرفة وتحديد المتكلم وكذلك تحديد شرعية التسجيلات الصوتية[2].

2- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية

تم إنشاء مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، يعمل على تأمين منظومة المعلومات الخدمة الأمن العمومي، وأعتبر بمثابة مركز توثيق، ويتواجد مقره ببئر مراد رايس[3]، ويتجلى هدف المركز في اكتشاف الجرائم والمخالفات المرتكبة في حق الأفراد والمؤسسات وممتلكاتهم التي تنتشر بواسطة التكنولوجيا الحديثة للإعلام والاتصال عبر الانترنت، ومحاربة كل أنواع الجريمة الإلكترونية[4].

[1]– هواري عياش، المرجع السابق، ص 06

[2]– المرجع نفسه، ص 07

[3]– المرجع نفسه، ص 08

[4]– بارة سمير، مرجع سابق، ص 335

يعهد المركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية القيام بمجموعة من المهام التي تدخل في مجال اختصاصه لمكافحة الجريمة الإلكترونية بصفة عامة بحيث يكلف بما يلي:

- التعاون بشكل وثيق مع الهيئات الأجنبية على مكافحة الجريمة الإلكترونية.
- إجراء التحقيقات بالتعاون والتنسيق بين مخابر المركز والمعهد الوطني للأدلة الجنائية وعلم الإجرام
- جمع وحفظ الأدلة الرقمية على المستوى المركزي أو على المخابر التقنية.
- البحث عن أسباب حذف وثيقة أو ملف ما أو رسالة معينة وكيفية استخراجها واسترجاعها.
- القيام بإعادة تحليل وتتبع أرشيف الإبحار عبر الانترنت.
- تتبع مسار البريد الإلكتروني وتحديد مصدر الهجمات بالفيروسات أو الاحتراق غير القانوني للوثائق الشخصية.
- توفير الأدلة حول سرقة المعطيات والمعلومات وتزوير الوثائق واستعمالها
- البحث عن أدلة في وثيقة معينة أو رسالة إلكترونية باستخدام برمجيات خاصة ومفاتيح الكلمات[1].

لقد تمكنت قيادة الدرك الوطني من خلال التكوين المستمر لأفرادها والمشاركة في الملتقيات الوطنية والدولية وتبادل الخبرات مع الدول الأخرى من أن توفر القوى المؤهلة ذات كفاءة عالية من مهندسي الإعلام الآلي ورجال القانون من أجل الفهم الصحيح للجريمة الإلكترونية والتصدي لها[2]، كما قامت قيادة الدرك الوطني بإطلاق برنامج لوقاية القصر من هذه الجريمة وهذا بفتح مكتب على مستوى المركز الحماية القصر من خلال ترصد كل محاولات الإيقاع بهم عبر الانترنت.

[1]–د. إدريس عطية، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، مكانة الأمن السيبراني في منظومة الأمن الأولي الجزائري، مجلة الجيش، العدد 599، مؤسسة المنشورات العسكرية، الجزائر 2013، ص ص 15–16

[2]– المرجع نفسه، ص ص12–16.

فعلى هذا الأساس تكمن المهمة الأساسية للمركز في محاربة كل أنواع الجريمة الإلكترونية التي تتخذ من الانترنت وسيلة، فمن القرصنة المعلوماتية إلى الذم والتحقير أو الشتم إلى التهديد أو الابتزاز، مرورا بالتحرش بكل أنواعه وسرقة الهوية وانتحال الشخصية[1]، وغيرها من الجرائم الإلكترونية الأخرى التي تحدد سلامة المجتمع وأمن الدولة باستعمال شتى الأجهزة الإلكترونية لتنفيذ هذا النوع من الجرائم.

3- المصلحة المركزية للتحريات الجنائية

تعد المصلحة المركزية للتحريات الجنائية هيئة ذات اختصاص وطني من بين مهامها مكافحة الجريمة الإلكترونية[2]، وعليه يمكن القول بأنها جهاز تابع لقيادة الدرك الوطني له مهام عديدة في ميدان التحريات الجنائية والمساهمة في إجراء التحقيقات لمكافحة الجرائم بكافة أنواعها ومن بينها الجريمة الإلكترونية بكل أشكالها التي أضحت من جرائم العصر الفتاكة بالمجتمع في العالم الافتراضي.

4- مديرية الأمن العمومي والاستغلال

تعتبر بمثابة هيئة تعمل على التنسيق بين مختلف الوحدات الإقليمية والمركز التقني العلمي في مجال أعمال البحث والتحري في الجرائم الإلكترونية[3]، وقد بلغ عدد القضايا التي عالجتها قيادة الدرك الوطني لسنة 2018 وهذا بداية من شهر جانفي إلى غاية شهر نوفمبر 1140 قضية متعلقة بالجريمة الإلكترونية منها 136 قضية خاصة بالأطفال دون 18 سنة و30% من مجموع القضايا تتعلق بالابتزاز والتشهير.

وعلى ضوء ما سبق عرضه حول الأجهزة المكلفة بالوقاية من الجريمة الإلكترونية نجد بأن الجزائر من بين الدول التي سعت جاهدة إلى التصدي لهذه الجريمة بكل أشكالها من خلال مراقبة

[1]– د. إدريس عطية، المرجع السابق، ص13

[2]– ربيعي حسين، المرجع السابق، ص183

[3]– المرجع نفسه، ص183.

كل التحركات التي تتم عبر الانترنت من إبحار وتصفح للمواقع الإلكترونية، والحد منها بمكافحتها وذلك بالاعتماد على مختلف الوسائل والتقنيات الحديثة في مجال المعلوماتية التي تم تسخيرها للكشف عن هذا النوع من الجرائم.

المبحث الثاني: الحماية الإجرائية للجريمة الالكترونية

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أضرار على الأفراد وعلى المؤسسات الدولة من جهة، ومحاولة منه للتدارك الفراغ التشريعي عمد منذ الألفية الثانية إلى تعديلات لعديد من القوانين الوطنية، بما فيها التشريعات العقابية وعلى رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال التكنولوجيا الإعلام والاتصال.

كما تثير الجرائم المعلوماتية مشكلات عديدة متعلقة بالقانون الجنائي الإجرائي، حيث وضعت نصوص قانون الإجراءات الجنائية لتحكم القواعد المتعلقة بالجرائم التقليدية، لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها مع خضوعها لمبدأ حرية القاضي الجنائي في الاقتناع وصولا إلى الحقيقة بشأن الجريمة والمجرم. وعلى العكس تماما تبرز صعوبات جمة فيما يخص البحث والتحري واثبات الجريمة المعلوماتية والوقاية منها على أساس أنها تتم في وسط افتراضي لا حدود له، وهو ما حاول أيضا المشرع الجزائري التكيف معه في سياسته الجنائية الهادفة إلى مكافحة هذه الجرائم المستحدثة.

من هذا المنطلق تم تقسيم هذا المبحث إلى مطلبين حيث يتناول (المطلب الأول) القواعد الإجرائية للتحقيق في الجريمة الالكترونية، ثم عرض الجزاءات المقررة في الجريمة الإلكترونية في (المطلب الثاني).

المطلب الأول: القواعد الإجرائية للتحقيق في الجريمة الالكترونية

يعتبر التحقيق من أهم الإجراءات التي تتخذ بعد وقوع الجريمة لما له من أهمية في تثبت من الحقيقة من خلال كشف الغموض الذي يعتري الجريمة وإسناد الدليل على مرتكبيها بأدلة الإثبات لغرض الوصول إلى إدانة المتهم من عدمه[1].

تعد البيئة الرقمية مسرحا لارتكاب الجريمة الإلكترونية، والتي تستدعي كافة الإجراءات من أجل الوصول إلى الدليل بالنسبة الذي لا يخلو أي جريمة، مهما كانت طبيعتها مادية أو تقنية، كما

[1]– خالد ممدوح ابراهيم فن التحقيق الجنائي في الجرائم الإلكترونية، ط1، دار الفكر الجامعي، الإسكندرية، 2010، ص119.

هو الحال بالنسبة لهذا النوع المستحدث من الجرائم، الذي يقوم على الدليل الرقمي، ومن الإجراءات التي ساهمت إلى حد بعيد في كشف معالم الجريمة، نجد إجراءات عامة وإجراءات خاصة.

الفرع الأول: القواعد الإجرائية الكلاسيكية للتحقيق في الجريمة الإلكترونية

تعد الجريمة الإلكترونية من الجرائم التي لا يترك أثر مادي في مسرح الجريمة فضلا عن أن مرتكبيها يملكون القدرة على إتلاف أو تشويه أو إضاعة الدليل في فترة قصيرة، أي سهولة طمس معالم الجريمة، لذلك عمل المشرع الجزائري في هذا المجال على دعم الإجراءات العامة والتي تم التطرق إليها على النحو الآتي:

أولا: المعاينة

المعاينة من أهم مراحل التحقيق في الجرائم المستحدثة نظرا لما يمكن أن توفره من أدلة إثبات للجريمة، وتزداد أهميتها في إثبات الجرائم المرتكبة عبر الانترنت في أنها تقوم على معاينة جملة من البرمجيات أو الأقراص وكل ما يتعلق بجهاز الحاسب الآلي، وذلك راجع إلى الطبيعة الخاصة للمعاينة في هذا المجال، وبالتالي جوهر المعاينة هو الملاحظة وفحص حسي مباشر لمكان أو شخص أو أي شيء له علاقة بالجريمة لإثبات حالته والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة، يجوز الالتجاء إلى المعاينة في كافة الجرائم[1]، إلا أن غالبية التشريعات بما فيها التشريع الجزائري يقتصرها على الجنايات والجنح الهامة بحيث تعد إجراء وجوبيا في الجنايات وجوازيا في الجنح وهي قد تتم في مكان عام أو خاص فإذا كانت في مكان عام، مأمور الضبط القضائي لا يحتاج إلى إذن أو ندب سلطة تحقيق بإجرائها ، أما إذا كانت بمكان خاص لابد لصحتها إما رضا حائز المكان أو وجود إذن مسبق من سلطة التحقيق بإجرائها.

بخصوص أهمية هذا الإجراء في الجريمة المعلوماتية، يكمن في كشف غموض جرائم الانترنت، وضبط الأشياء التي قد تفيد في إثبات وقوعها وإسنادها إلى مرتكبيها[2].

[1]– خالد ممدوح إبراهيم، المرجع السابق، ص 111.

[2]– المرجع نفسه، ص 212.

ثانيا: التفتيش

لم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفتيش بقدر ما اعتبره إجراء من إجراءات التحقيق وأحاطه بضوابط صارمة نظرا لأهميته في كشف الأدلة من جهة وخطورته فيما قد يترتب عنه من مساس بالحرية الأشخاص وبكرامتهم من جهة أخرى، خير دليل على ذلك اهتمام الدستور الجزائري بأهمية هذا الإجراء من خلال نص المادة 40 منه والتي تنص على ما يلي: ((فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة))[1].

نستخلص من فحو المادة أن التفتيش يعتبر من الإجراءات المخولة لضباط الشرطة القضائية حسب نص المادة 1/5 قانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وكذلك قانون الإجراءات الجزائية.

ثالثا: الضبط

يتمثل الضبط في العثور على أدلة في الجريمة التي يباشر التحقيق بشأنها التحفظ عليها، ويعتبر الضبط هو الهدف من التفتيش والنتيجة المباشرة والمستهدفة، ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تطبق بشأن التفتيش ويؤدي بطلان التفتيش إلى بطلان الضبط.

يختلف الضبط في الجريمة المعلوماتية عن ضبط في الجرائم الأخرى من حيث المحل لأن الجريمة الإلكترونية يرد فيه الضبط على الأشياء ذات طبيعة معنوية من حيث البيانات والمراسلات والاتصالات الإلكترونية وعلى الأشياء ذات الطبيعة المادية، كالكمبيوتر وملحقاته والأقراص الصلبة الخارجية والمرنة[2].

الفرع الثاني: القواعد الإجرائية المستحدثة للتحقيق في الجريمة الإلكترونية

[1]- المادة 40 من قانون رقم 08-19 مؤرخ في 15 نوفمبر 2008، يتضمن تعديل الدستور، ج ر عدد 63، صادر في 16 نوفمبر 2008.

[2]- خالد ممدوح إبراهيم، المرجع السابق، ص 221.

نظرا لتطور الكبير الذي شهده العالم في ميدان التكنولوجيا الرقمية، وما أفرزه من أضرار وخيمة تمس بالنظام العام، والذي نتج عنه ظهور نوع مستحدث من الجرائم الذي أصبح يهدد كيان المجتمعات، الأمر الذي دفع بالمشرع الجزائري إلى استحداث أساليب أخرى للبحث والتحري عن الجريمة من خلال تعديله لقانون الإجراءات الجزائية وفقا لقانون رقم 22/06 المؤرخ في 2006/07/20 وهو ما: يسمى بأساليب البحث والتحري الخاصة.

أولا: اعتراض المراسلات

يعتبر إجراء من إجراءات التحري المستحدثة والذي يقصد به التتبع السري والمتواصل للمراسلات الخاصة بالمشتبه به ودون علمه ذلك باعتباره إجراء تحقيقي يباشر خلسة وتنهك فيه سرية الأحاديث الخاصة تأمر به السلطات القضائية في الشكل المحدد قانون بهدف الحصول على دليل مادي للجريمة والتي تستخدمها في مواجهة الإجرام الخطير، وتتم عبر وسائل الاتصال السلكية واللاسلكية[1].

نجد وفقا لنص المادة 65 مكرر 5 من ق إ.ج.ج[2] أن اعتراض لم يقتصر فقط على المكالمات الهاتفية، بل تم توسيعه إلى مختلف أنواع الاتصال السلكية واللاسلكية، أما بخصوص أداة الاعتراض، فإن المشرع لم يحدد وسيلة معينة فقد تكون تقليدية أو مستحدثة.

ثانيا: التسرب

لقد تطرق المشرع الجزائري إلى تعريف التسرب من خلال نص المادة 65 مكرر 12 من قانون ا.ج.ج بعد تعديله بالقانون 22/06 والتي تنص على ما يلي: ((يقصد بالتسرب قيام ضابط أو عون شرطة قضائية 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.

[1]– زبيحة زيدان، المرجع السابق، ص 55

[2]– المادة 65 مكرر 5 من قانون الاجراءات الجزائية أمر رقم 66–156 مؤرخ في 8 جوان 1966 يتضمن قانون الإجراءات الجزائية، ج ر، عدد 84 المعدل والمتمم

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 يحوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم)).

وبالتالي تستخلص طبقا لنص المادة، أن التسرب هو قيام ضابط أو عون الشرطة القضائية بمراقبة المشتبه في ارتكاب جناية أو جنحة بإيهامهم أنه فاعل أصلي بغرض كشف الحقيقة، ويبطل هذا الإجراء إذا كان الهدف من التحريض على ارتكاب الجريمة.

كما نص المشرع الجزائري على التسرب في قانون مكافحة الفساد[1].

نجد أن المشرع الجزائري من خلال قانون مكافحة الفساد لم يعرف لنا التسرب حيث استخدم مصطلح اختراق للدلالة عنه وبالإشارة إليه فقط باعتباره من إجراءات التحري.

ثالثا: مراقبة الاتصالات الإلكترونية

نجد المشرع الجزائري على غرار العديد من المشرعين لم يقم بتعريف عملية مراقبة الاتصالات الإلكترونية، لكن بعض التشريعات قد قامت بتعريفها مثل التشريع الأمريكي الذي عرفها على أساس أنها عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز إلكتروني أو أي جهاز آخر[2].

إلا أننا يمكن أن نعرفها على أساس أنها إجراء تحقيق يباشر خلسة، وتنتهك فيه سرية الأحاديث الخاصة تأمر السلطة القضائية في الشكل المحدد قانون يهدف الحصول على دليل غير مادي للجريمة المعلوماتية، ويتضمن من ناحية استراق السمع إلى الأحاديث ومن ناحية أخرى حفظه بواسطة أجهزة متخصصة لذلك.

---

[1]– القانون رقم 06-01 مؤرخ في 20 فيفري 2006 يتعلق بالوقاية من الفساد ومكافحته ج ر عند 14، صادر في 08 مارس 2006، المتمم بالأمر رقم 10-05 مؤرخ في 26 اوت 2010، ج ر عدد 50، صادر في 1 سبتمبر 2010 معدل ومتمم بالقانون رقم 11-15 مؤرخ في 02 أوت 2011، ج ر عدد 44 صادر في 10 أكتوبر 2011.

[2]– ربيحة زيدان، المرجع السابق، ص ص 126-127

ونجد أن المشرع من خلال قانون 06-01 قد أشار إلى هذا الإجراء دون تقديم تعريف له بينما في بينما في القانون 09-04 في المادة 3 منه قد حدد كيفية مراقبة الاتصالات الالكترونية على النحو الآتي ((مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في القانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية المراقبة الاتصالات الإلكترونية وتجميع و تسجيل محتواها في حينها والقيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية))[1].

وبالتالي فإن مراقبة الاتصالات حددها القانون على سبيل الاستثناء وفي الحالات المحددة حصريا في المادة 4 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

المطلب الثاني: الجزاءات المقررة في الجريمة الإلكترونية

بعد التطرق إلى إجراءات التحقيق وما شملته من وسائل مادية وبشرية للبحث والتحري والتحقيق في الجريمة الالكترونية وكذلك التفتيش ومدى قابلية نظام الحاسوب الآلي للتفتيش وكذلك ضمانات التفتيش الآن تم التطرق إلى الجزاءات المقررة للجريمة الالكترونية في القانون الجزائري تم دراسة العقوبات المقررة للشخص الطبيعي كفرع أول ويتناول الفرع الثاني العقوبات المقررة للشخص المعنوي.

الفرع الأول: العقوبات المقررة للشخص الطبيعي

نص المشرع الجزائري على مجموعة من العقوبات الأصلية والتكميلية المقررة للشخص الطبيعي والمتمثلة في:

أولا: العقوبات الأصلية

[1]- المادة 3 من قانون 09-04 المرجع السابق.

تمثل العقوبات الأصلية المطبقة على الشخص الطبيعي في إطار الجريمة الالكترونية المؤشر الصريح لخطورة هذه الجريمة والتي أقرها المشرع على الأفعال التي يجرمها قانون العقوبات والمتمثلة فيما يلي[1]:

1- العقوبات المقررة لجريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي

تعتبر هذه الجريمة من أهم الجرائم الالكترونية وأخطرها على المؤسسات والأفراد لكونها تشكل انتهاكا صارخا ومباشرا للحقوق والحريات ويختلف الفقه في طبيعة هذه الجريمة بين من يعتبرها جريمة واحدة تؤدي نفس النتيجة وبين من يقسمها إلى جريمتين بحيث يفصل رواد هذا المذهب بين الدخول إلى النظام المعلوماتي كجريمة أولى والبقاء غير المشروع في النظام كجريمة ثانية[2].

ويقصد بجريمة الدخول إلى الأنظمة تحقيق فعل الدخول إلى النظام وتشير الكلمة إلى كل "الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والسيطرة على المعطيات أو المعلومات التي يتكون منها". كما يقصد به " الدخول إلى محتويات جهاز الكمبيوتر والقيام بأي عملية اتصال بالنظام محل الحماية دون أي ترخيص أو وجه حق".

أما جريمة البقاء غير المشروع داخل النظام المعلوماتي فتعتبر من الجرائم المستمرة وتبقى قائمة مستوفية أركانها ما دام الجاني لا يزال على اتصال بنظام المعلومات الذي تم الدخول إليه بطريقة غير مشروعة ودون ترخيص[3].

ويقصد بالبقاء كفعل " التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام والتصرف فيه " واستقر أغلب الفقه على أن جريمة البقاء غير المشروع داخل النظام المعلوماتي تعتبر بشكل عام من الجرائم التي يصعب تقديم دليل على إثباتها وكثيرا

[1]– عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، المجلد 22، العدد 86، الشارقة، الإمارات، 2013، ص265

[2]– دمان ذبيح وعماد بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، 2020، ص 145

[3]– المرجع نفسه، ص146.

ما تقترن الجريمتان (أي الدخول غير المشروع والبقاء غير المشروع) ببعضهما البعض وهو الأمر الذي جعل الكثير من الفقه المقارن وأغلب التشريعات الجنائية تجمع الصورتين في جريمة واحدة تحت مسمى الدخول والبقاء غير المشروع في النظام المعلوماتي، وقد قرر المشرع في إطار قانون العقوبات وبموجب المادة 394 مكرر عقوبتين أصليتين لجريمة الدخول أو البقاء غير المشروع.

أ- العقوبة المقررة للجريمة في صورتها البسيطة

يعاقب القانون على هذه الجريمة في صورتها البسيطة بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من خمسين ألف (50.000) إلى مائة ألف (100.000) وفتح في هذا المجال للقاضي السلطة التقديرية بأن جعل له حدا أدنى وحدا أقصى في تقدير العقوبة بالعودة إلى الحيثيات والوقائع، وبالنظر للباعث الذي دفع الشخص لارتكاب الجريمة.

ب- العقوبة المقررة للجريمة في صورتها المشددة

تضاعف عقوبة الجريمة إذا ترتب عنها حذف أو تغيير في المعطيات، بحد أدنى يقدر بستة أشهر بعدما كان ثلاثة أشهر، وحد أقصى يقدر بسنتين بعدما كان سنة واحدة، ويعاقب على هذه الصورة بغرامة مالية تقدر بمائة ألف (100.000) دينار إلى مائتي ألف (200.000) دينار وفي حال ما تم القيام بتخريب نظام المعالجة الآلية فيعاقب عليها بالحبس من ستة أشهر إلى سنتين وبغرامة من خمسين ألف (50.000) دينار إلى مئة وخمسين ألف (150.000) دينار[1].

2- العقوبات المقررة لجريمة إفساد أو تعطيل سير النظام

وتسمى أيضا جريمة الاعتداء على سير نظام المعالجة الآلية للمعطيات " حيث أغفل المشرع الجزائري وضع نص صريح خاص بتجريم الاعتداء على جريمة سير نظام المعالجة الآلية للمعطيات، إلا أنه يمكن استخلاص التجريم من خلال النصوص القانونية المستحدثة في إطار تجريم الاعتداءات الواقعة على أنظمة المعالجة أو على معطيات الأنظمة الداخلية أو الخارجية.

[1]– دمان ذبيح وعماد بهلول سمية، المرجع السابق، ص 147.

وعلى الرغم من أن هناك من يذهب إلى جريمة الاعتداء العمدي على المعطيات مثل جريمة الاعتداء العمدي على نظام المعالجة الآلية للبيانات تهدف إلى القيام بأفعال تخريب وقرصنة، إلا أن هناك من يذهب إلى أن الفرق بينهما يكمن في أن جريمة الاعتداء العمدي على النظام وإن كانت لا تقع بصفة أساسية على البرامج والشبكات إلا أنها تصيب المعطيات كنتيجة لأفعال الإفساد والتوقيف في حين أن الاعتداء على المعطيات الذي تقوم عليه جريمة الاعتداء العمدي على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه سواء على البرامج أو شبكات النقل والاتصال، وفي سبيل التفرقة بين الجريمتين تم الاتفاق على أن المعيار الأساسي هو المحل الذي يقع عليه الاعتداء ففي حال وقوع الجرم على العناصر المادية للنظام فإن الجريمة هي جريمة الاعتداء العمدي على نظام المعالجة الآلية للمعطيات، أما إذا كان يقع على العناصر المعنوية فإننا نكون في هذه الحالة أمام جريمة الاعتداء العمدي على المعطيات[1].

3- العقوبات المقررة لجريمة الاعتداء العمدي على المعطيات

يقصد بالاعتداء على المعطيات " التجاوز الذي يهدف إلى الإضرار بمعلومات الكمبيوتر أو وظائفه سواء بالمساس بسريتها أو المساس بسلامة محتوياتها وتكاملها أو بتعطيل قدرة وكفاءة الأنظمة بشكل يمنعها من أداء وظيفتها بشكل سليم" ويتحقق الاعتداء على معطيات النظام عادة بعد تجاوز مرحلة الدخول والبقاء في نظام المعالجة الآلي للمعطيات، ويتخذ وفق ما نص عليه المشرع الجزائري صورتين " الاعتداء على المعطيات الداخلية للنظام " أو الاعتداء على المعطيات الخارجية للنظام".

تنص المادة 394 مكرر من قانون العقوبات أنه " يعاقب بالحبس من ستة أشهر (06) إلى ثلاث (03) سنوات وبغرامة مالية من 500.000 إلى 2.000.000 دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها" وما

[1]– المرجع نفسه، ص 147.

يسجل أن عقوبة الاعتداء العمدي على المعطيات تفوق عقوبة الدخول أو البقاء غير المشروع سواء في صورتها المشددة أو البسيطة ذلك أن جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة لا تؤدي إلى حدوث أضرار معينة تلحق بالمعطيات أو النظام، أما الصورة المشددة وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة الاعتداء العمدي على المعطيات وإن كانت تؤدي إلى نفس النتائج فإن عقوبتها أكبر لأنها جريمة عمدية يجب فيها توافر القصد الجنائي لدى مرتكب جريمة الدخول أو البقاء غير المشروع في صورتها المشددة[1].

ثانيا: العقوبات التكميلية

يقدر المشرع في العديد من الحالات عدم كفاية العقوبة الأصلية التي قررها كجزاء على اقتراف الجريمة في ردع الجاني أو في حماية المصلحة التي قرر حمايتها، فيأتي بالعديد من العقوبات الفرعية لتدعيم الحماية المقررة للمصلحة المعنية فالعقوبات التكميلية هي عقوبات تضاف إلى العقوبات الأصلية، وقد حددها المشرع في نص المادة 09 المعدلة بموجب القانون 23/06 المعدل والمتمم لقانون العقوبات، وإن كانت هذه العقوبات مرتبطة بالعقوبة الأصلية، إلا أنها لا يحكم بها على المحكوم عليه بقوة القانون، إذ لا توقع إلا بالنطق بها وتتمثل هذه العقوبات في المصادرة والغلق ونشر الحكم وستتم مناقشتها كالتالي[2]:

1- المصادرة

يقصد بالمصادرة تجريد الشخص من ملكية مال أو من حيازة شيء معين له صلة بجريمة وقعت أو يخشى وقوعها، ثم إضافتها إلى جانب الدولة بلا مقابل بناء على حكم من القاضي الجنائي كما عرفها المشرع الجزائري من خلال المادة 15 من قانون العقوبات.

[1]– دمان ذبيح عماد بهلول سمية، مرجع سابق، ص 148

[2]– رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة ابو بكر بلقايد، تلمسان، 2017/2018، ص246.

فأحيانا العقوبات الأصلية لا تكن كافية كما هو الشأن بالنسبة للجرائم الماسة بالسرية المعلوماتية، إذ أنه من الممكن أن يرتكب الجاني في هاته الجرائم جرائم أخرى بحيازته لبعض الوسائل التي ارتكب بها جرائمه ومنه يعاود ارتكاب جرائم أخرى تمس السرية أو سلامة أو وفرة المعلومات لهذا يكون بالنسبة لهؤلاء من الضروري اتخاذ تدابير عملية لمنع وقع جريمة أخرى من نفس الشخص ويتحقق ذلك بمصادرة تلك الوسائل وهذا ما نصت عليه المادة 394 مكرر 6 كالتالي " مع الاحتفاظ بحقوق الغير حسن النية يحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة والملاحظ على النص أن المشرع أخذ بعين الاعتبار حسن النية وبذلك يكون قد انسجم مع مبدأ الشرعية

2- الغلق

فإلى جانب عقوبة المصادرة نص المشرع على عقوبة تكميلية وجوبية أخرى هي الغلق وذلك بموجب المادة 394 مكرر 6 كما يلي " مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها، ويكون بذلك المشرع جعل لعقوبة الغلق محلين هما المواقع محل ارتكاب الجريمة ومحل أو مكان الاستغلال[1].

ولكن المادة لم تنص على مدة الغلق وبالتالي فإننا نرجع القواعد العامة لقانون العقوبات حيث تكون مؤبدة أو مؤقتة وذلك وفقا للمادة 16 مكرر 1 في فقرتها الأولى " يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي ارتكبت الجريمة

بمناسبته ويحكم بهذه العقوبة إما بصفة نهائية أو لمدة لا تزيد عن عشر سنوات في حالة الإدانة لارتكاب جناية أو خمس سنوات في حالة الإدانة لارتكاب جنحة...."[2].

الفرع الثاني: العقوبات المقررة للشخص المعنوي

[1]– رابحي عزيزة، المرجع السابق، ص 246

[2]– المرجع نفسه، ص 247

تبنى قانون العقوبات الجزائري مبدأ المسؤولية الجزائية للأشخاص المعنوية بموجب القانون 15/04 في نص المادة 18 مكرر ليعزز ذلك بالقانون رقم 23 لسنة 2006 بنص المادة 51 مكرر وفي مضمون هذا النص استثنى المشرع الأشخاص المعنوية العامة من الخضوع للمسؤولية الجزائية وعلى رأسها الدولة، ومن خلال استقراء المادة 18 مكرر فالعقوبات التي تطبق على الشخص المعنوي في الجنايات والجنح كالتالي[1]:

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

2- واحدة أو أكثر من العقوبات التكميلية التالية:

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

ومما تجدر الإشارة إليه في هذا المقام أن هذه العقوبات ليست خاصة بجرائم الاعتداء على نظم المعالجة الآلية فحسب، بل تقع على كل الجرائم التي يرتكبها الشخص المعنوي، بينما ما يتعلق بالجرائم ضد الأنظمة المعلوماتية المحددة في المواد 394 مكرر وما بعدها فإن الغرامة المطابقة

[1]– رابحي عزيزة، المرجع السابق، ص248.

على هذا الأخير هي 5 مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي وذلك تطبيقا للمادة 394 مكرر 4 في قانون العقوبات الجزائري.

حيث أن المشرع الجزائري شدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية وهي الطائفة التي تنتمي إليها جل جرائم الدراسة، غذ نصت المادة 394 مكرر 4 بمضاعفة قيمة الغرامة 5 أضعاف ما قررته للشخص الطبيعي ونصت على الآتي " بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

أما إذا ارتكبت إحدى الجرائم السابقة من شخص معنوي على إحدى الجهات العامة فتضاعف الغرامة في التشريع الجزائري مرتين، إذ تضاعف إلى خمس (05) مرات عما هو مقرر على الشخص الطبيعي لأن الجريمة ارتكبت من شخص معنوي، وثم يضاعف ذلك إلى ضعفين لأن الجريمة ارتكبت ضد إحدى الجهات العامة، وبالتالي فمجموع ذلك هو مضاعفة الغرامة عشرة (10) مرات أضعاف عما هو مقرر على الشخص العادي[1].

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

خاتمة الفصل الثاني

من خلال دراستنا لآليات مكافحة الجريمة الالكترونية في الفصل الثاني تعرفنا بأن الجريمة الالكترونية جريمة لا محدودة ومتطورة ومرنة لذلك أعطت لها التشريعات سواء العربية أو العالمية إجراءات تحقيق ومتابعة خاصة، فلقد تم عرض من خلال المبحث طرق مكافحة الجريمة الالكترونية تمثلت في الجهود التشريعية لمكافحة الجريمة الالكترونية سواء كانت على المستوى الدولي أو على مستوى التشريع الجزائري، كذلك مؤسسات مكافحة الجريمة الإلكترونية كذلك التحقيق في الجريمة الإلكترونية وفي نهاية الفصل ضمن المبحث الثاني تم تناول الحماية الإجرائية للجريمة الالكترونية متمثلة في القواعد الإجرائية الكلاسيكية والمستحدثة للتحقيق في الجريمة الالكترونية وكذا العقوبات المطبقة على الشخصين الطبيعي والمعنوي من عقوبات أصلية وأخرى تكميلية، واستنتجنا بأن الجرائم التي تتسم بالإلكترونية والمرتكبة بأحدث الوسائل التقنية والمعلوماتية أصبحت تشكل خطرا محدقا كل يوم يكبر ويهدد أمن البشرية بعدم الثقة في المواقع وفي المعلوماتية بشكل عام فلذلك كان لزاما على كل الدول في العالم بأسره بأن تكثف الجهود وتتخذ إجراءات صارمة وردعية بشأن هذه الجريمة الالكترونية.

خاتمـــــة

تعتبر الجريمة الالكترونية من بين أحدث وأخطر الجرائم التي عرفها العالم وذلك لما تتميز به من خصائص بخلاف الجريمة التقليدية، فهي نتيجة كل فعل يستهدف سوء استخدام التكنولوجيا الحديثة، ومع غزو الانترنيت دول العالم، أصبح من الصعوبة ضبط وكشف مكان هذه الجرائم كونها عابرة للحدود الوطنية وتتسم بسرعة فائقة دون رقابة من أي دولة.

تتفق كل النظريات والدراسات المنجزة حول نقطة أساسية تتمثل في الغاية المادية البحتة التي يسعى إليها المجرم الالكتروني من سطو على الأموال إلى الاعتداء على البيانات السرية وتدمير البرامج المعلوماتية لأية دولة لتهديدها في أمنها القومي وكذلك ظهور ما يعرف بالإرهاب الالكتروني الذي أصبح هاجسا حقيقيا يهدد سلامة وأمن المجتمع الدولي عن طريق التهديد بتدمير أساليب واستراتيجية الدفاعات الأمنية والاقتصادية للدول وعوائدها المالية.

في هذا الإطار سعت مختلف دول العالم إلى تحديث نصوصها التشريعية القائمة، وسن الجديد منها في مجال مكافحة الإجرام الإلكتروني. وعلى غرار دول العالم، تبنت الجزائر سياسة التصدي إلى الجرائم الإلكترونية، هذه الأخيرة ولو تأخرت في الظهور بسبب الظروف التي مرت بها الجزائر، إلا انها عرفت تطور وانتشار سريع وتزايد مستمر لذلك عملت الدولة الجزائرية على تعديل الجوانب الموضوعية من خلال تعديل قانون العقوبات واستحداث قسم خاص بهذه الجرائم، كما تم أيضا تعديل الجوانب الإجرائية من خلال تحديت قانون الإجراءات الجزائية. كما استحدث المشرع الجزائري قوانين أخرى مثل القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تماشيا مع طبيعة الجريمة الإلكترونية.

هذا التنوع التشريعي الذي أحدثه المشرع الجزائري من شأنه أن يساهم في القضاء، أو على الأقل عدم تفاقم ظاهرة الإجرام الإلكتروني، والحيلولة دون انتشارها أكثر.

ومما سبق ذكره استخلصنا من هذه الدراسة مجموعة من النتائج يمكن إجمالها فيما يلي:

- عدم وجود إجماع فقهي بخصوص تعريف الجريمة الالكترونية، حيث تباينت التعريفات بين المفهوم الواسع والمفهوم الضيق.

- مفهوم الجريمة الإلكترونية مفهوم يتغير ويتطور حسب تطور التكنولوجي، مما قد يعطي وصف جديد لبعض الجرائم التي يمكن أن تستجد بفعل واقعة إجرامية جديدة.
- الطابع التقني للجريمة الإلكترونية الذي يسهل إخفاء معالم الجريمة.
- الطبيعة الخاصة للجريمة الإلكترونية واعتبارها من الجرائم العابرة للحدود يصعب من مكافحتها وملاحقة مرتكبيها.
- تصنف جرائم الأنترنت ضمن جرائم التقنية العالية، التي تقع على شبكة الأنترنت أو بواسطتها من قبل شخص يتصف بالذكاء والسرعة كذلك يكون متميزا بالدقة والتخصص في مسائل تكنولوجيا المعلومات.
- عدم توفر أدلة مادية واضحة وصعوبة الوصول إليها في بعض الأحيان، وكثرة المعلومات التي يستوجب فحصها.
- أنواع الجرائم الإلكترونية يتغير بحسب الاستخدام ممكن أن تكون على الفرد، أو مؤسسات الدولة.
- إن هذه الجريمة مع تعدد أنماطها واحتراف مرتكبيها، فإن لها جوانب سلبية خطيرة تهدد أمن وسلامة الفرد والمجتمع، وهي تتسم بالغموض، حيث يصعب إثباتها والتحقيق فيها، مما يضع مسؤولية كبيرة على ضباط الشرطة والقضاء.
- وجود قصور تشريعي في القواعد والإجراءات الواجب اتباعها في مرحلة التحقيق ومرحلة المحاكمة في الجرائم الإلكترونية.
- تتم المحاكمة في الجرائم الإلكترونية ذات الإجراءات المتبعة في الجرائم التقليدية.
- رغم اجتهاد المشرع الجزائري للتصدي لهذه الجريمة، إلا أنه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة.
- غموض بعض النصوص الخاصة والتي تهدف لمكافحة الجريمة الإلكترونية، وهذا نظرا لكلاسيكية هذه النصوص وعدم شمولها لبعض الجرائم الحديثة.

على ضوء النتائج التي توصلنا إليها، يمكن تقديم بعض التوصيات والاقتراحات التي قد يكون تطبيقها مجدي لمكافحة هذه الجرائم الخطيرة:

- وجوب إعادة تكييف المفهوم العام للجريمة الإلكترونية لجعله شموليا أكثر، وقابلا لأن يشمل بعض الجرائم المستحدثة في هذا الجانب وهذا لتسهيل محاربتها.
- وجوب إعادة النظر في قانون العقوبات الجزائري، خاصة فيما يخص هذا النوع من الجرائم وهذا من أجل مكافحتها.
- سد الفراغ التشريعي في مجال مكافحة الجريمة الإلكترونية، على أن يكون شاملاً للقواعد الموضوعية والإجرائية.
- إن محاربة الجريمة الإلكترونية على المستوى الدولي أو الوطني لا تتم إلا بإيجاد أساس تشريعي موحد وتصور شامل لمفهوم هذا النوع من الجرائم من أجل تحديد الأفعال التي تشكل هذه الجرائم، إضافة إلى عقد اتفاقيات بين الدول يكون هدفها التنسيق وتوحيد الجهود لمكافحة هذه الجرائم، وتشكيل لجان مختصة في البحث والتحري والتحقيق يكون أعضاؤها من ذوي الكفاءات في المجال المعلوماتي.
- الحرص على تكوين كفاءات من القطاع الأمني متخصصة في مراقبة التجاوزات والكشف المبكر عن الجرائم الالكترونية خاصة وأنها جرائم غير مادية ولا ملموسة كما سبق ووضحنا، ونادرا ما يتم الكشف عنها في مراحل متقدمة من ارتكابها وإرسالهم للتكوين في كل من الولايات المتحدة الأمريكية وبريطانيا وفرنسا كدول ساهمت في مكافحة هذا النوع من الجرائم.
- وضع إجراءات كالتحقيق والمحاكمة للجريمة الإلكترونية تختلف عن الجريمة التقليدية.
- ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة على كيفية التعامل مع هذا النوع من الجرائم وتحقيق التعاون مع التقنيين من أصحاب الخبرة.
- ضرورة خلق ثقافة اجتماعية جديدة تندد بجرائم الأنترنت مع تفعيل أسلوب التوعية والتهذيب لدى مستخدمي شبكة الاتصالات العالمية وحثهم على الاستخدام الأمثل لهذه التقنيات.

- ضرورة نشر الوعي الرقمي بين المستخدمين وكيفية تفادي التعدي على بياناتهم الشخصية وتعريفهم بحجم الخطورة التي ترصدهم في حالة عدم اتخاذ الاحتياطات الوقائية اللازمة.
- تشجيع الجامعات والمراكز البحثية على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة الجريمة المعلوماتية والحد من أثارها.

قائمة المصادر والمراجع

I. المصادر

1- النصوص التشريعية

أ- الأوامر

- الأمر رقم 66-156 مؤرخ في 8 جوان 1966 يتضمن قانون الإجراءات الجزائية، ج ر، عدد 84 المعدل والمتمم.
- الأمر رقم 97-10 مؤرخ في 06-03-1997 المتعلق بحق المؤلف والحقوق المجاورة، الجريدة الرسمية، عدد 13 الصادر في 1997/03/12 معدل والمتمم بأمر 05/03 مؤرخ في 2003/07/19، المتعلق بحقوق المؤلف، والحقوق المجاورة، الجريدة الرسمية عدد 44، الصادر في 2003/07/23.
- الأمر رقم 03-06 المؤرخ في 19 جويلية 2003 المتعلق بالعلامات التجارية، ج ر عدد 44، صادر في 23 جويلية 2003.
- الأمر رقم 03-07 المؤرخ في 2003/07/19 المتعلق ببراءات الاختراع ج ر عدد 44 صادر في 23 جويلية 2003.

ب- القوانين

- القانون رقم 15/04 المؤرخ في 10 نوفمبر 2004، المتضمن قانون العقوبات الجريدة الرسمية عدد 71، صادر 2004/11/10.
- القانون رقم 04-14 المؤرخ في 2004/11/10 المتضمن قانون الاجراءات الجزائية الجزائري المعدل
- القانون رقم 06-01 مؤرخ في 20 فيفري 2006 يتعلق بالوقاية من الفساد ومكافحته ج ر عند 14، صادر في 08 مارس 2006، المتمم بالأمر رقم 10-05 مؤرخ في 26 اوت 2010، ج ر عدد 50، صادر في 1 سبتمبر 2010 معدل ومتمم بالقانون رقم 11-15 مؤرخ في 02 أوت 2011، ج ر عدد 44 صادر في 10 أكتوبر 2011.

- قانون رقم 08-19 مؤرخ في 15 نوفمبر 2008، يتضمن تعديل الدستور، ج ر عدد 63، صادر في 16 نوفمبر 2008.
- القانون رقم 04/09 المؤرخ في 2009/02/05 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، الجريدة الرسمية، عدد 47، سنة 2009

2- النصوص التنظيمية

أ- المراسيم الرئاسية

- المرسوم الرئاسي رقم 04-183 المؤرخ في 26 يونيو 2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلمة الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج ر ج ج عدد 41 الصادرة في 27 يونيو 2004.
- المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة تكنولوجيات الإعلام والاتصال ومكافحتها، ج ر ج ج، عدد 53 الصادرة في 08 أكتوبر 2015.

I. المراجع

1- الكتب

- أحسن بوسقيعة، الوجيز في القانون الجزئي، الطبعة السادسة، دار هومة، الجزائر، 2007.
- جهاد محمد البريزات، الجريمة المنظمة: دراسة تحليلية، ط01، دار الثقافة للنشر والتوزيع، عمان، 2008.
- خالد داودي، الجريمة المعلوماتية، دار الاعصار العلمي للنشر والتوزيع، الجزائر، ط1، 2008.
- خالد ممدوح إبراهيم، أمن الجريمة الإلكترونية، الدار الجامعية، الإسكندرية 2008.
- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2009.

- خالد ممدوح ابراهيم فن التحقيق الجنائي في الجرائم الإلكترونية، ط1، دار الفكر الجامعي، الإسكندرية، 2010.
- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية – شبكة الانترنت وشبكة الهواتف التقليدية والآليات والمطبوعات–، دار الثقافة للنشر والتوزيع، 2019.
- عامر محمود الكسواني، التزويز المعلوماتي للعلامة التجارية، دار الثقافة للنشر والتوزيع، ط2، الاردن، 2014.
- عباس أبو شامة عبد المحمود، عولمة الجريمة الاقتصادية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007.
- عبد الرحمن بن عبد الله السند، الأحكام الفقهية للمعاملات الالكترونية، الحاسب الآلي وشبكة المعلومات (الانترنيت)، دار الوراقين للنشر والتوزيع، بيروت، 2004.
- عمرو عيسى الفقي، الجرائم المعلوماتية. جرائم الحاسب الالي والانترنيت في مصر والدول العربية المكتب الجامعي الحديث، الاسكندرية، 2006.
- غانم مرضي الشمري، الجرائم المعلوماتية –ماهيتها، خصائصها، كيفية التصدي لها قانونا، دذدن، دذط.
- غنية باطلي الجريمة الالكترونية دراسة مقارنة – الدار الجزائرية للنشر والتوزيع، الجزائر، طبعة 2015 .
- كميت طالب البغدادي، الاستخدام غير المشروع لبطاقة الائتمان المسؤولية الجزائية والمدنية، ط01، دار الثقافة للنشر والتوزيع، عمان، 2008.
- محمد أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر، الأردن، 2005.
- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، ط 01، دار الثقافة للنشر والتوزيع، عمان، 2004.

- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت، دار النهضة العربية، القاهرة د.ت.ن.
- نائلة عادل محمد فريد قورة – جرائم الحاسب الالي الاقتصادية دراسة نظرية وتطبيقية منشورات الحاتي الحقوقية، 2005
- نبيلة هبة هروال، الجوانب الاجرائية لجرائم الأنترنات _في مرحلة جمع الاستدلالات_، د ذ ط، دار الفكر الجامعي الاسكندرية، 2006.
- نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 01، دار الثقافة للنشر والتوزيع، عمان، 2008.

2- المقالات العلمية

- بارة سمير، الدفاع الوطني والسياسات الوطنية للأمن السيبراني cyper security في الجزائر: الدور والتحديات، المجلة الجزائرية للأمن الوطني الإنساني، عدد 20، مخبر الأمن الإنساني: الواقع، الرهانات والآفاق، جامعة باتنة 1، 2017.
- حفيظ نقادي معالم الجريمة المعلوماتية في القانون الجزائري مجلة الحقوق والعلوم الانسانية، العدد 20 جامعة زيان عاشور بالجلفة، 2014.
- د. إدريس عطية، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها، مكانة الأمن السيبراني في منظومة الأمن الأولي الجزائري، مجلة الجيش، العدد 599، مؤسسة المنشورات العسكرية، الجزائر 2013.
- د. نياب سليمة بوترعة بلالا الجريمة الالكترونية الأسس والمفاهيم مجلة تطوير العلوم، المجلد 13 العدد 01 الجزائر. جامعة زيان عاشور الجلفة 2020.
- دمان ذبيح وعماد بهلول سمية، الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، 2020.

- سامية عزيز، مازيا عيساوي، الجريمة من منظور سوسيولوجي الأسباب الآثار، مجلة دراسات في سيكولوجية الانحراف، السنة 2021، المجلد 6، العدد 1.
- سمير إبراهيم حسن "الثورة المعلوماتية عواقبها و آفاقها"، مجلة جامعة دمشق، العدد الأول، 2002.
- صورية بوربابة، التعاون الدولي في مكافحة الجرائم المعلوماتية، مجلة القانون الدولي للدراسات البحثية، العدد 01، جامعة طاهري محمد، بشار، 2019.
- عادل عبد الله خميس المعمري، التفتيش في الجرائم المعلوماتية، مجلة الفكر الشرطي، المجلد 22، العدد 86، الشارقة، الإمارات، 2013.
- عبد الصديق الشيخ، الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، مجلة معالم للدراسات القانونية والسياسية، المجلد 4 العدد 1 لسنة 2020.
- علوي مصطفى "الضحية المنسية أمام لغة الكبار"، مجلة الشرطة المديرية العامة للأمن الوطني، العدد 87 جوان، 2008.
- مايا خاطر، الجريمة المنظمة العابرة للحدود الوطنية وسبل مكافحتها، مجلة جامعة للعلوم الاقتصادية والقانونية، جامعة دمشق، العدد 03، المجلد 27، 2011.

3- الأطروحات والرسائل الجامعية والمذكرات

أ- أطروحة دكتوراه

- بهلول مليكة، دور الشرطة العلمية والتقنية في الكشف عن الجريمة، أطروحة لنيل شهادة الدكتوراه علوم، فرع الحقوق، كلية الحقوق، جامعة الجزائر، 2013.
- تركي بن عبد الرحمان المويشر، بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فاعليته، أطروحة مقدمة للحصول على درجة دكتوراه الفلسفة الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2009.

- رابحي عزيزة، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة ابو بكر بلقايد، تلمسان، 2017/2018.
- ربيعي حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة لنيل شهادة الدكتوراه في الحقوق، فرع قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة باتنة 2016.
- محمد الحبيب عباسي، الجريمة المنظمة العابرة للحدود، أطروحة لنيل شهادة دكتوراه علوم، تخصص القانون العام، قسم الحقوق كلية الحقوق والعلوم السياسية، جامعة أبي بكر بلقايد تلمسان، 2017/2016.

ب- الرسائل الجامعية

- بن عقون السلوك الإجرامي للمحرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية تخصص علم الإجرام وعلم العقاب جامعة الحاج لخضر، باتنة، 2011-2012.
- خديجة دحمان صبايحية، جرائم السرقة والاحتيال عبر الانترنت دراسة مقارنة بين الفقه الإسلامي والقانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم الإسلامية، تخصص شريعة وقانون، قسم الشريعة، كلية العلوم الإسلامية، جامعة الجزائر، 2013/2012.
- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر باتنة 2012-2013.
- سفيان سوير، جرائم المعلوماتية، مذكرة ماجستير، تخصص العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2011/2010.
- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية دراسة مقارنة مذكرة ماجستير في القانون العام، جامعة الشرق الأوسط الأردن، 2014.

- محمد فوزي صالح، الجريمة المنظمة وأثرها على حقوق الإنسان، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي لحقوق الانسان كلية الحقوق جامعة يحي فارس المدية، 2009/2008.
- نجاري بن حاج علي فايزة، الآليات القانونية لمكافحة الإرهاب الالكتروني، مذكرة لنيل شهادة الماجستير في القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو.
- نسيم دردور، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الجنائي، كلية الحقوق، جامعة منتوري، قسنطينة 2012/2013.
- يوسف صغير، الجريمة المرتكبة عبر الإنترنت مذكرة ماجستير في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2013/2014.

ب- مذكرات التخرج

- سعيدة بعرة، الجريمة الإلكترونية في التشريع الجزائري مذكرة لنيل شهادة الماستر جامعة محمد خيضر بسكرة 2015-2016.
- مرزوق نسيمة جرائم الانترنيت مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء الجزائر، 2006-2009.

4- الملتقيات والمداخلات

- بن عمير امينة، بوحلايس الهام، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ورقة بحثية مقدمة ضمن فعاليات الملتقى الدولي القانون الجنائي للأعمال نمو توجه جديد للتجريم، المنعقد يوم 21 أكتوبر 2021، عبر التحاضر المرئي عن بعدzoom ، المجلد 7 العدد1، لسنة 2022.

- بوزيدي مختارية ماهية الجريمة الإلكترونية مورقة بحثية مقدمة ضمن ملتقى آليات مكافحة الجرائم الإلكترونية في التشريع، يوم 29 مارس 2017، الجزائر.
- حابت آمال الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، يومي 16 و17 نوفمبر 2015.
- حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، يومي 16-17 نوفمبر، 2015.
- خالد محي الدين أحمد، "الجرائم المتعلقة بالرغبة الاشباعية باستخدام الكمبيوتر"، الندوة الاقليمية حول الجرائم المتصلة بالكمبيوتر، المملكة المغربية، أيام 2018 جوان 2007.
- فاطمة الزهراء خبازي، جرائم الدفع الإلكتروني وسبل مكافحتها، أعمال الملتقى الوطني آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، المنعقد في الجزائر يوم 29 مارس 2017.
- فضيلة عاقلي، "الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية، المنعقد في طرابلس يومي 24 مارس 2017.
- هواري عياش، المعهد الوطني للأدلة الجنائية وعلم الإجرام، مسار التحقيقات الجمالية في مجال الجريمة المعلوماتية، مداخلة ألقيت في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، يومي 16 و17 نوفمبر، 2015.

5- الكتب الفرنسية

- KURBALIJA Jouan, GELBSTEIN Eduardo, Gouvernance de l'internet, actems et fractures, public par diplo fondation et global knowledge partnership, Suisse 2005.

6- المواقع الاكترونية

- محمد محمد صالح الألفي، "أنماط جرائم الانترنت"، مقال متوفر على الموقع التالي : http://www.eastlaws.com.
- www.oecd-ong.
- www.g8utorionto.com
- www.dgsn.dz.

فهـــرس المحتويات

فهـرس المحتويات

ملخص مذكرة الماستر

تعتبر الجرائم الإلكترونية واحدة من أعظم ويلات هذا القرن إذا أصبحت واقعا مفزعا للدول والأفراد، ويعود ذلك أساسا الى إمكانيات المتاحة للمجرم الإلكتروني وذلك بتقدم وسائل الاتصال وذيوع استعمال الحاسوب وسهولة استخدام الأنترنت.

في هذا الإطار سعت الجزائر إلى تبني سياسة لمكافحة الجرائم الإلكترونية من خلال استحدث قوانين خاصة تختص بعملية الوقاية والقمع، ولاسيما منها القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، والمهم في ذلك هو القضاء على هذا الإجرام الخطير أو على الأقل التقليل من حدته، ويتحقق عندها التنظيم الفعال للجريمة.

الكلمات المفتاحية

1/ الجريمة 2/ الجريمة الالكترونية 3/ المجرم الالكتروني 4/ الحماية الإجرائية للجريمة الالكترونية 5/ مكافحة الجريمة الالكترونية 6/ القانون رقم 09-04

Abstract of The master thesis

Cybercrime is considered one of the greatest scourges of this century if it becomes a frightening reality for countries and individuals, and this is mainly due to the capabilities available to the cybercriminal through the advancement of means of communication, the widespread use of computers and the ease of using the Internet.

In this context, Algeria has sought to adopt a policy to combat cybercrime through the introduction of special laws related to the process of prevention and repression, especially Law No. 04-09, which includes rules for prevention and combating information and communication technology, and the most important thing is to eliminate this serious crime, or at least Reducing its intensity, and then achieving the effective organization of the crime

Reintegration of detainees :

1/Crime 2/ Cybercrime 3/ Cybercriminal 4/ Procedural protection of cybercrime 5/ Fighting cybercrime 6/ Law No. 04-09