جامعة عبد الرحمان ميرة – بجاية
كلية الحقوق والعلوم السياسي
قسم القانون الخاص

عنوان المذكرة

التنظيم القانوني للجريمة الإلكترونية طبقا لأحداث التعديلات في القانون الجزائري

مذكرة لنيل شهادة الماستر في القانون الخاص

تخصص: علوم جنائية

إعداد الطالبتين:

- حرزون ليلة
- هدروق أسماء

إشراف الاستاذة:

الدكتورة تواتي نصيرة

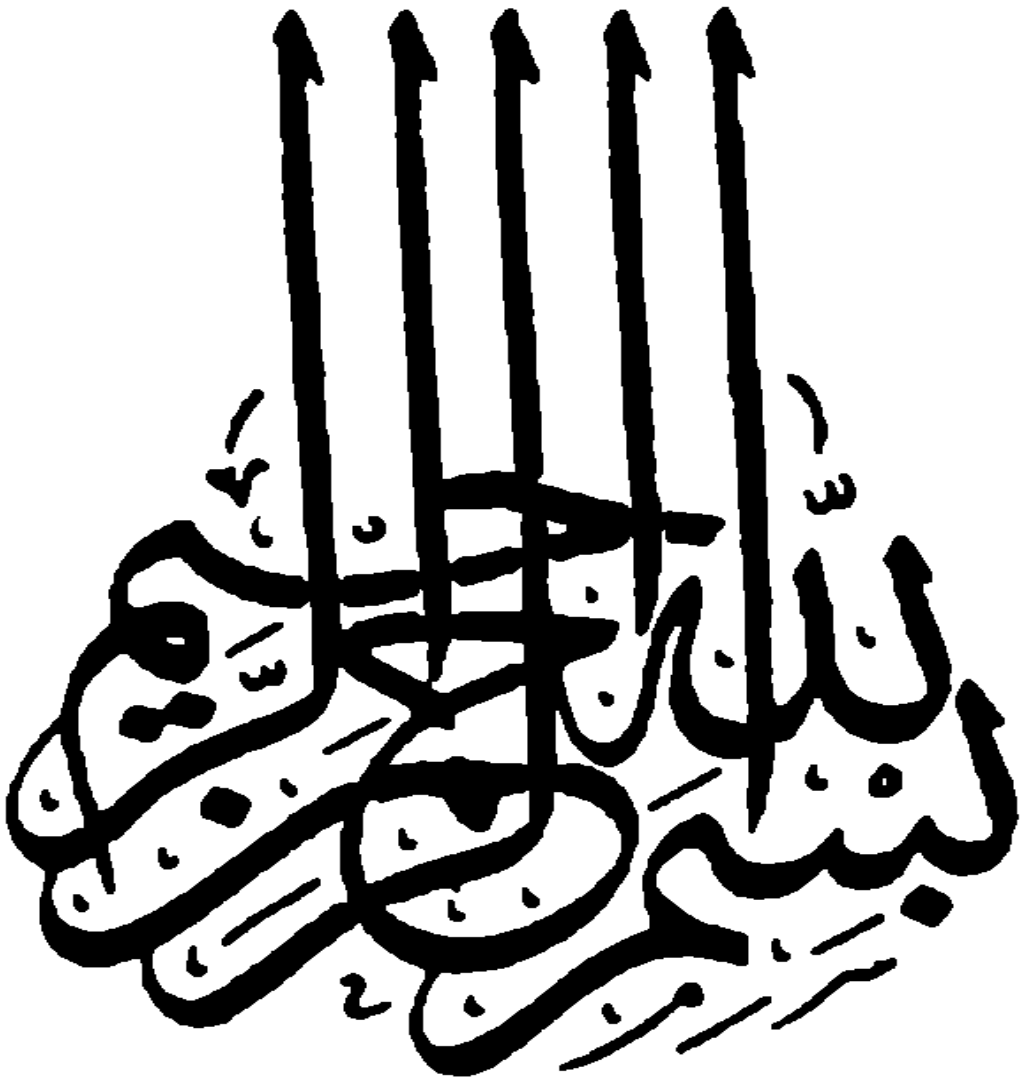
لجنة المناقشة

الأستاذ(ة):.....رئيسا

الأستاذ(ة): تواتي نصيرة.....مشرفا ومقررا

الأستاذ(ة):.....ممتحنا

السنة الجامعية: 2022/2021


بسم الله الرحمن الرحيم

قال تعالى:

بسم الله الرحمن الرحيم

"قَالُوا سُبْحَانَكَ لَا عِلْمَ لَنَا إِلَّا مَا عَلَّمْتَنَا إِنَّكَ أَنْتَ الْعَلِيمُ الْحَكِيمُ"

صدق الله العظيم

الآية -32- من سورة البقرة

الشكر والتقدير

نحمد الله تعالى حمد الشاكرين ونصلي ونسلم صلاة وتسليما يليقان بمقام أمير الأنبياء وإمام المرسلين سيدنا محمد وآله وصحبه أجمعين وبعد:

بداية نتقدم بجزيل الشكر والعرفان إلى كل من

ساعدنا في هذا العمل

ونتقدم بجزيل الشكر والعرفان إلى الأستاذة المشرفة

" **الدكتورة تواتي نصير**"

التي ساعدتنا كثيرا ولم تبخل علينا بالتوصيات والنصائح ونتمنى

لها مشوار مهني حافل بالنجاح وجزاها الله خيرا

ثانيا نتقدم بأعظم التقدير والثناء للسادة اعضاء المجلس العلمي من عمال الإدارة والأساتذة وأعضاء لجنة المناقشة على قبولهم مناقشة هذه المذكرة المقدمة للفحص.

إهـداء

إلى من تستنجد له كلماتي وتنحني له أحاسيسي إلى الذي علمني أن الحياة كفاح وأن عزة النفس كرامة إلى من دعاني فإستجبت إلى من علمني فأتقنت وانتظرني فقدمت له ثمرة جهدي هدية على ما وهبه لي

.... أبي الغالي.....

إلى من حملتني وهنا على وهن إلى من ولدت فربت فتعبت برغم الشقاء لم تبح يوما بآهات إلى نور لن ينحنى أبدا إلى سنفونية تتراقص على أهدابها كل عبارات الحب والإحترام والتقدير.

... أمي الغالية...

بأنامل تحيط بقلمي أعياه الأرق أترجم حبي وتقديري

*إلى كل من عائتي الاولى وعائلتي الثانية "**مداغ**" حفظهم الله لي.*

*إلى شموع لم تنطفئ أبدا في قلبي أولهم زوجي الغالي **يوسف***

*وثانيهم صديقي الغالية **تنهنان** حفظهم الله لي.*

وإلى كل من نسيهم قلمي ولم ينسهم قلبي وحفظتهم ذاكرتي.

إلى كل هؤلاء أهدى ثمرة جهدي هذه.

أسماء

إهـداء

الحمد اللّه الذي وفقنا، ولن نكن لنصل إلى ما نحن عليه الأن، أما بعد أهدي هذا العمل:

*إلى الينبوع الذي لا يميل العطاء، إلى من حاكت سعادتي بخيوط منسوجة في قلبها" **أمي العزيزة** "*

إلى من سعى وشقي لأنعم بالراحة والهناء الذي لم يبخل بشيء من أجل دفعي في درب النجاح الذي علمني أن أرتقى بسلم الحياة بحكمة وصبر

*" **أبي العزيز** "*

*إلى إخوتي وأصدقائي والأعزاء "**حرزون فرحات، يوبي ياسمين**"*

الى من سرنا ونحن نشق الطريق معا نحو النجاح والامل لحياة راقية مطمئنة

"زوجي"

ليلة

قائمة المختصرات

ط: الطبعة

ص: الصفحة

ص ص: من صفحة إلى صفحة

د.ط: دون طبعة

د.ب.ن: دون بلد النشر

ج.ر: جريدة رسمية

ط1: طبعة أولى

ط2: طبعة ثانية

ج.رج.ج.د.ش: الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية

مقدمة

إن مرور المجتمعات البشرية بمراحل عديدة ومتنوعة ضمن مسارها الحياتي والاجتماعي الصعبة خاصة في مجال التواصل بين الأفراد هذا ما جعل البشرية يسارعون إلى ايجاد وسائل تمكنهم من تخطى هذا الحاجز.

فتميز القرن العشرين باختراعات هائلة وذلك في ظل الثورة المعلوماتية الحديثة التي تلت الثورة الصناعية، حيث دخل المجتمع خظيرة الرقمية والمعلوماتية، فغزت الحواسيب الآلية والأنترنيت جميع مجالات الحياة، وأضحى استخدامها ضرورة لاغنى عنها بالنسبة للدول والحكومات ومؤسسات الدولة، ثم تطور الأمر ليصبح استعمال هذه التقنية متاحا للأفراد وذلك من خلال تبادل المعلومات والمراسلات و إبرام مختلف الصفقات، فأصبح بذلك العالم عبارة عن قرية صغيرة يمكن التواصل والتعامل بين مجتمعات مختلفة وأجناس متنوعة في مدة زمنية قصيرة واستطاعت هذه القفزة تقديم خدمات جليلة للأمم والشعوب، وبدأ العالم يدخل عصرا جديدا هو عصر المعلوماتية.

وعلى الرغم من أهمية الوسائل الالكترونية وايجابيات استعمالها على الفرد والمجتمع إلا أن هذا التقدم واكبه من جهة أخرى تطور الفكر والعقل البشري الإجرامي، إلا أن استخدامه لهذه التقنيات المتطورة ليس من الجانب الإيجابي كما يقال بل سارع إلى الإعتماد على هذه التكنولوجيا لتحقيق أغراضه الغير مشروعة، هذا ما أدى إلى ظهور نوع جديد من الجرائم سميت بالجرائم الالكترونية أو المعلوماتية هذا النوع الحديث من السلوكات الإجرامية الماسة بأمن الدولة وسلامة النظم المعلوماتية وبحقوق الغير تشكل خطر بالغا وذلك لتعدد أطرافها الإجرامية، كجرائم التحويل غير المشروع للأموال، وجرائم المعلومات المخزنة .

أن كل تطور في مجال دائما سلاح ذو حدين، هو ما ينطق على استخدام شبكة الأنترنت التي لها انعكاسات سلبية كبيرة في حال سوء استخدام الأنظمة المعلوماتية التي تحتويها فهذا النوع من الجرائم الجديدة التي لا تختلف عن الجرائم التقليدية إلا من حيث الوسيلة التي أصبحت متطورة.

وبتزايد معدلات الجريمة وتطور أشكالها وتهديداتها المباشرة التي مست مجتمعات العصر الراهن والخسائر الناجمة عن هذه الجرائم التي تستهدف الاعتداءات على المعطيات بدلالتها التقنية الواسعة وأ صبح، يواجه المؤلفون في البنية الرقمية المتشابكة العديد من المشاكل بسبب سهولة الوصول إلى مؤلفاتهم واستنساخها، في ظل تقاعس أو مواكبه التشريعات التقليدية للسرعة التي تتطور بها التكنولوجيا الحديثة وعصر المعلوماتية وعدم قدرتها على التكييف مع الوضع الحالي.

إذا كان القانون وليد فكرة المجتمع فهو يتطور بتطوره ومن أجل ذلك استوجب على التشريعات المختلفة للدول أن تواكب هذا التطور من خلال سن قوانين تتماشى مع هذه التطورات من أجل إيجاد سبيل وأليات للحد من استعمال التكنولوجيا في ارتكاب جرائمهم هذا ما دفع إلى بعض الدول إلى العمل مليا للحد من هذه الجريمة من خلال التوعية والوسائل الوقائية الأمنية وغيرها، بحيث بات لزما أن يواكب تطور الجريمة وأساليبها تطورا في المجال السياسة التشريعية عموما والسياسة الجنائية على وجه الخصوص بعد أن أصبح واضحا التهديد المباشر للمنظومة الحقوقية الذي يتسبب فيه إساءة استخدام شبكة الأنترنيت.

ومن بين الدول التي سارعت إلى سن وإصدار قوانين جديدة لمواجهة ومكافحة الجرائم المعلوماتية نجد الجزائر حيث قام المشرع الجزائري بتعديل بعض قوانينه القائمة كغيره من التشريعات الدولية الأخرى قد ساير هذا التطور الحاصل في ميدان التكنولوجيا، بحيث أجري تعديل لقانون العقوبات الجزائري بإصداره عدة قوانين كالقانون رقم 05- 15 المؤرخ في 10 نوفمبر 2004 والذي تم من خلاله استحداث نصوص خاصة متعلقة بالجرائم الماسه بأنظمة المعالجة الألية للمعطيات في المواد من 394 مكرر إلى 394 مكرر7، والأمر رقم 97-10 المؤرخ في 1997/3/6 المتعلق بحقوق المؤلف والحقوق المجاورة، والذي ألغي أحكام المواد 390 إلى 394 من قانون العقوبات، وقد أصدر كذلك القانون رقم 09-04 المؤرخ في 2009/8/5 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المعدل بالقانون رقم 21/11.

وعلى ضوء ما سبق تبرز أهمية دراسة هذا الموضوع في الرغبة الملحة لتحليل هذه الجريمة ودراستها من مختلف جوانبها بإبراز خطورتها على المجتمع كذلك التمعن في موقف المشرع الجزائري من هذه الجريمة الحديثة ومعرفة كيفية تصدى المشرع لها من خلال النصوص العقابية والتجريمة وبالتالي إظهاره مختلف السبل والأليات المستجدة للحد منها.

وككل بحث يعني بالبحث والدراسة نجده لا يخلو من بعض الصعوبات ولعل أبرزها قلة المراجع الوطنية الحديثة المعالجة للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكذلك بصفة أدق قانون العقوبات وهو الأمر الذي شدنا إلى الخوض فيه ومحاولة دراسة لكونه يتميز بكثير من المستجدات خاصة على الواقع العلمي.

وقد تم الاعتماد في دراسة موضوع البحث على منهجين أوليان أولهما المنهج الوصفي، للجانب الفني من الدراسة مع الاستعانة بالمنهج التحليلي في بعض مراحل البحث لمختلف القواعد والسنن القانونية المرتبطة بعناصر البحث.

وعليه سنحاول من خلال هذه الدراسة أن بين أبرز النقاط المهمة المتعلقة بهذه الجريمة الحديثة وذلك من خلال طرح الإشكالية التالية: "**إلى أي مدى تمكن المشرع الجزائري من ايجاد منظومة قانونية فعالة لمكافحة الجريمة المعلوماتية؟**"

وهاته الإشكالية العامة التي بدورها تتفرع عنها إشكاليات فرعية أو تساؤلات نذكر منها:

ما مفهوم الجريمة الإلكترونية؟

ما هي الحماية الجزائية للمعلوماتية التي أقرها المشرع الجزائري؟

من أجل الكشف عن مختلف خطايا الموضوع وكذا ايجاد أجوبة لكل التساؤلات المطروحة عبر الإشكال العام.

تم تقسيم الدراسة إلى فصلين أولهما عني بدراسة الجوانب الفنية والإيطارالمفاهيمي للجريمة الإلكترونية تم تقسيمه بدوره إلى مبحثين إثنين أولهما إلى مفهوم الجريمة الإلكترونية حيث تم

التطرق عبر مطالبه الإثنان إلى تعريفها ودوافع ارتكابها أما المبحث الثاني فقد خصص إلى دراسة خصائص وأنواع الجرائم الإلكترونية في القانون الجزائري.

بالنسبة للفصل الثاني تمت دراسة الجانب القانوني من خلال استعراض آليات مكافحة الجريمة الالكترونية والحد منها في التشريع الجزائري الذي قسم إلى مبحثين إثنينبالإعتماد على خطة ثنائية بسيطة حيث أوردنا في المبحث الأول القواعد الموضوعية لمكافحة الجريمة الالكترونية قسمناه بدوره إلى مطلبين تعرضنا في أولهما إلى الحماية الجزائية للمعلوماتية من خلال نصوص قانون العقوبات وأوردنا في الثاني الحماية الجزائية للجريمة الالكترونية من خلال القوانين والتنظيمات الأخرى.

أما في المبحث الثاني أظهرنا من خلاله مختلف القواعد الإجرائية لمكافحة الجريمة الالكترونية الذي تمت دراستها من خلال مطلبين أولهما يتمحور حول القواعد المنصوص عليها في قانون الإجراءات الجزائية والثاني تطرقنا فيه إلى الحماية الجزائية من خلال القانون 21/11 المتعلق بالوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال.

الفصل الأول

الإيطار المفاهيمي للجريمة الإلكترونية

لقد شهد العالم في الآونة الأخيرة تطور في مجال التكنولوجية خاصة المعلوماتية مما نتج عن استخدام الحواسيب الآلية وشبكة الأنترنات في مجالات متعددة ومختلفة، وعلى الرغم من أهمية الوسائل الإلكترونية وإيجابيات إستعمالها، إلا أن الإستخدام غير المشروع لها قد أدى إلى ظهور نوع جديد من الجرائم سميت بالجرائم الإلكترونية، ونظرا لحداثة هذه الجريمة فقد إختلفت آراء الفقهاء في تقديم تعريف موحد لهذه الجريمة، كما تميزت بمجموعة من الخصائص وظهور أنواع جديدة من المجرمين لهم عدة دوافع لإرتكاب هذه الجريمة، وسنحاول التطرق في هذا الفصل إلى مفهوم الجريمة الإلكترونية **(المبحث الأول)**، وبيان خصائص وأنواع الجريمة الإلكترونية **(المبحث الثاني)**.

المبحث الأول

مفهوم الجريمة الإلكترونية

من خلال هذا المبحث سنحاول تحديد التعاريف المختلفة للجريمة الإلكترونية وكذا الأركان التي ترتكز عليها ومنه الدافع المؤدية إلى إرتكابها باعتبارها تقع في العالم الإفتراضي على خلاف الجريمة التقليدية التي تقع في الواقع الملموس.

سنتعرض في هذا المبحث إلى مطلبين، نتعرض لتعريف الجريمة الإلكترونية وأركانها **(مطلب أول)**، وخصائص ودوافع الجريمة المعلوماتية **(مطلب ثاني)**.

المطلب الأول

تعريف الجريمة الإلكترونية وأركانها

لم يتفق الفقه الجنائي على تسمية موحدة للجريمة المعلوماتية، فهناك عدة تسميات لهذه الجريمة، منها الغش المعلوماتي والبعض الآخر يطلق عليها إسم جرائم الحاسوب الآلي والآخر

جرائم الكمبيوتر والأنترنيت أو الجريمة الإلكترونية، أما في الدول الأوروبية فيطلق عليها إسم: cyber criminalité[1]

ظهر إتجاهين من الفقهاء منهم من ينظر إلى الجريمة الإلكترونية بمفهوم ضيق ومنهم من ينظر إليها بمفهوم واسع، كما أن للجريمة المعلوماتية أركان لا تقوم إلا بتوافرها وهذا ماسنتطرق إليه من خلال هذين الفرعين المواليين.

الفرع الأول:

تعريف الجريمة الإلكترونية

بالرغم من الجهود المبذولة لمكافحة والتصدي لهذه الظاهرة الإجرامية المعلوماتية، إلا أنه لا يوجد تعريف شامل ومحدد ومتفق عليه بين الفقهاء، فقد إتجه جانب من الفقه إلى تناولها بالتعريف على النحو الضيق وجانب آخر على النحو الموسع.

أولا: التعريف الفقهي للجريمة المعلوماتية

يلاحظ في هذا الصدد أن التعريفات الفقهية جاءت بين مضيق وموسع لمفهوم الجريمة الإلكترونيةوسنتطرق إليها على النحو التالي:

1. التعريف الضيق للجريمة الإلكترونية

من التعريفات المضيقة لمفهوم الجريمة المعلوماتية على أنها " **كل فعل غير مشروع يكون العلم بتكنولوجيا الحواسيب الآلية بقدر كبير لازما لارتكابه من ناحية، ولملاحقته من ناحية أخرى**"،[2]وحسب هذا التعريف أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا التعريف يضيق بدرجة كبيرة من الجريمة المعلوماتية.

---

[1]–قربوز حليمة، الجريمة المعلوماتية في التشريع الجزائري والقانون المقارن، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الجزائر، 2006 – 2009، ص 1.

[2] – نائلة قورة، جرائم الحاسوب الإقتصادية، ط 1 ، دار النهظة العربية، القاهرة، 2003،ص 21.

كذلك تعرف هذه الجريمة على أنها " **الفعل غير المشروع الذي يتورط في ارتكابه الحاسب أو هي الفعل الإجرامي الذي يستخدم في اقترافه باعتباره أداة رئيسية** ".

وعرفت أيضا بأنها " **الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا هاما، أو هي كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية** " [1]

ما يآخذ على التعريفات السابقة أنها جاءت قاصرة عن الإحاطة بأوجه ظاهرة الإجرام الإلكتروني، فالبعض من فقهاء هذا الإتجاه ركز على معيار موضوع الجريمة، والبعض الآخر ركز على وسيلة إرتكابها والبعض على معيار النتيجة.

2. التعريف الواسع للجريمة الإلكترونية:

في المقابل هناك تعريفات حاولت التوسع في مفهوم هذه الجريمة ذلك نتيجة الإنتقاداتالموجهة للإتجاه الأول، فحاول الفقهاء تقديم تعريف واسع لهذه الجريمة لتفادي أوجه القصور التي شابت تعريفات الإتجاه المضيق للتصدي لظاهرة الإجرام المعلوماتي.

فعرفها البعض على أنها " **كل فعل أو إمتناع عمدي ينشأ عن الإستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الإعتداء على الأموال المادية والمعنوية** " وبأنها " **إستخدامالحاسوب كأداة لإرتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه وبياناته**"

كما قد تمتد هذه الجريمة لتشمل الإعتداءات المادية سواءا كانت على جهاز الحاسوب ذاته أو المعدات المتصلة به، وكذلك الإستخدام غير المشروع لبطاقات الإئتمان وانتهاك ماكينات الحسابات الآلية بما يتضمنه من شيكات تمويل الحسابات المالية بطريقة إلكترونية وتزييف المكونات المادية والمعنوية للحاسوب بل وسرقة الحاسوب في حد ذاته أو مكون من مكوناته [2]

[1] – حنان ريحان مبارك المضاحكي، الجرائمالمعلوماتية، ط 1، منشورات الحلبي الحقوقية، بيروت، 2014، ص 25.

[2] – ونوغي نبيل، زيوش عبد الرؤوف، "الجريمة المعلوماتية في التشريع الجزائري"، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشوربالجلفة، الجزائر، المجلد الرابع، العدد الثالث، سبتمبر2019، ص 131،130.

فتناول رأي آخر من الفقه تعريف الجريمة الإلكترونية بأنها "**عمل أو إمتناع يأتيه الإنسان إضرارا بمكونات الحاسوب وشبكات الإتصال الخاصة التي يحميها قانون العقوبات ويفرض لها عقابا**"

كما عرفت في إطار المنظمات الأوروبية للتعاون والتنمية الإقتصادية على أنها "**كل فعل أو إمتناع من شأنه أن يؤدي إلى الإعتداء على الأموال المادية والمعنوية، يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية**"[1]

لا شك أن هذا الإتجاه ينطوي على توسيع كبير لمفهوم الجريمة الإلكترونية لذا يآخذ عليه هذا التوسع الذي من شأنه أن يسقط وصف الجريمة الإلكترونية على أفعال قد لا تكون كذلك لمجرد مشاركة الحاسوب الآلي في النشاط الإجرامي، فبعض الجرائم كسرقة الحاسوب الآلي أو الأقراص مثلا لا يمكن إعطاءها وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسوب أو أحد مكوناته المادية كانت محل لفعل الإختلاس.

ثانيا: التعريف التشريعي للجريمة المعلوماتية

تأثر المشرع الجزائري بغيره من التشريعات الأجنبية الأوروبية منها والعربية فيما يخص القواعد التي إستند أو إعتمد عليها وأتى بها لمكافحة الجرائم المعلوماتية، حيث إتجه إلى خلق نصوص جديدة وخاصة تتعلق بهذا النوع من الجرائم رغبة منه في تأمين أنظمة المعلومات من إعتداءات المجرمين.

إذ نجد أنه ضمن موضوع الجريمة المعلوماتية في قانون العقوبات أو بموجب نصوص خاصة على السواء.

المشرع الجزائري على غرار المشرع الفرنسي لم يقم بتعريف نظام المعالجة الآلية للمعطيات بل أوكل مهمة تعريفه إلى الفقه والقضاء[2]، هذا الأخير فقد اصطلح تسمية الجريمة المعلوماتية

[1] – حنان ريحان مبارك المضاحكي، مرجع سابق، ص ص 130،131.

[2] – قارة أمال، الحماية الجنائية للمعلوماتية في التشريع الجزائري، ط 1، دار هومة، الجزائر،2006، ص101

بمصطلح الجرائم المتصلة بتكنولوجية الإعلام والإتصال، وتبنى في ذلك التعريف الذي ورد في الإتفاقيات الدولية للإجرام المعلوماتي بموجب المادة الثانية من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والإتصال ومكافحتها، وعرفها على أنها "**جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية**".[1]

وبالتالي تكون الجريمة المعلوماتية أيضا تلك الجرائم المرتكبة عن طريق أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين [2]، والمرتكبة عن طريق أي تراسل أو إرسال أو إستقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية [3].

يلاحظ على هذا التعريف ما يلي:

أن المشرع الجزائري قد إعتمد على الجمع بين عدة معايير لتعريف الجريمة المعلوماتية أولها معيار وسيلة الجريمة وهو نظام الإتصالات الإلكترونية، ثانيها معيار موضوع الجريمة والمتمثل في المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات [4].

كما اعتمد المشرع الجزائري على معيار رابع في تحديد نطاق الجريمة المعلوماتية كونه أقر أن هذه الجريمة ترتكب في نظام معلوماتي أو يسهل إرتكابها فيه، وهذا ما يوسع نطاق مجال الجرائم المعلوماتية في القانون الجزائري.

---

[1] – المادة الثانية الفقرة "أ" من القانون رقم 09-04 المؤرخ في 05 أوت 2009، ج ر عدد 47، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية الإعلام والإتصال ومكافحته، الصادرة في 16 أوت 2009.

[2] – المادةالثانية الفقرة "ب" من القانون نفسه.

[3] – المادة الثانية الفقرة "و" من القانون نفسه.

[4] – ونوغي نبيل، زيوش عبد الرؤوف، مرجع سابق، ص 132.

وترتيبا على كل هذه التعاريف الفقهية والتشريعية يمكننا القول أن الجريمة المعلوماتية هي كل سلوك غير مشروع يقع على النظام المعلوماتي أو بواسطته ويمس بالأشخاص أو الأموال أو أمن الدولة، وهي على غرار الجرائم التقليدية تعرف من خلال أركانها بتوافر القصد الجنائي لإرتكاب هذه الجريمة والركن المادي للجريمة وركنها المعنوي [1].

الفرع الثاني

أركان الجريمة الإلكترونية

تقوم الجريمة الإلكترونية شأنها في ذلك شأن أي جريمة على أركان أساسية، سنتناول هذه الأركان بصفة عامة من خلال الإشارة إلى كل ركن على حدى.

أولا: الركن المادي في الجريمة الإلكترونية

إن الركن المادي في هذه الجريمة يختلف من حال لآخر حسب التصنيف الذي يقع على الفعل، وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعدالتي ينطبق حكمها حتى على الجرائم الواقعة عن طرق جهاز الكمبيوتر، وهذا لا يسبب إشكالا، إذ تطبيق نصوص قانون العقوبات على هذه السلوكات التقليدية، إلا أنه هناك أنواعا أخرى من السلوك يتطلب التمييز بينها وبين سابقتها وهذا مايدعو للتدخل التشريعي[2].

[1] –أنظر المادة 02 فقرة "2" من القانون رقم 09-04، مرجع سابق.

[2] – بن غدقة شريفة والقص صليحة، الجريمة الإلكترونيةالممارسة ضد المرأة على صفحات الأنترنات وطرق محاربتها، أعمال الملتقى الوطني، " آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر، 29 مارس، ص 48.

فيتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها (مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة مناص من معاقبة الفاعل) [1].

يتخذ الركن المادي في هذه الجريمة عدة صور بحسب كل فعل إيجابي مرتكب وهو أغلب صور الجرائم الإلكترونية (مثلا: جريمة الغش الإلكتروني: الركن المادي فيها هو تغيير الحقيقة في التسجيلات الإلكترونية والمحررات الإلكترونية [2]، أو كأن يقوم باختراق شبكة الإتصالميحصل على بيانات سرية ويقوم بنشرها.

وقد يكون السلوك الإجرامي سلبيا وهو الإمتناع عن فعل كان من الواجب إتيانه مثل: إمتناع موظف أمن عن حماية بيانات ومعلومات الشركة التي يعمل بها وهو نادر الحدوث وفي الغالب يرتكب من قبل موظفين مختصين.

ثانيا: الركن المعنوي في الجريمة الإلكترونية

تعد الجرائم الإلكترونية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام (العلم والإرادة) لتحديد المسؤولية الجنائية، ولا يمكن تصور وجود قصد خاص بالجريمة دون أن يسبقه القصد العام، أما عن وجود قصد خاص في الجرائم في الجرائم المعلوماتية فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من وراء قيام بالفعل غير المشروع أو إرتكاب الجريمة.

فيكون الركن المعنوي للجريمة الإلكترونية من عنصرين العلم والإرادة، فالعلم هو إدراك الفاعل للجرم أو الفعل المجرم، أما الإرادة فهي توجه السلوك الإجرامي أي الرغبة لتحقيق النتيجة، وبالرجوع إلى المبادئ العامة في قانون العقوبات الجزائري قد يكون القصد الجنائي عاما أو خاصا،

[1] – بوضياف أسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، المسيلة، الجزائر، العدد 11، 2018، ص 354.

[2] – عاقلي فضيلة، "الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري"، المؤتمر الدولي الرابع عشر "الجرائم الإلكترونية"، طرابلس، بتاريخ 24– 25 مارس، 2017، ص 12.

فالقصد الجنائي العام هو: الهدف المباشر للسلوك الإجرامي، وينحصر في حدود إرتكاب الفعل[1]، أما القصد الجنائي الخاص هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارتكابه الجريمة بل يذهب إلى التأكد من تحقيق النتيجة (مثلا في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه).

أما فيما يتعلق بالجريمة الإلكترونية فالأصل أن الفاعل في هذه الجريمة يوجه سلوكه الإجرامي نحو إرتكاب فعل غير مشروع أو غير مسموح به مع علمه وقاصدا ذلك، ومهما يكن فلا يمكن إنتفاء علمه كركن للقصد الجنائي العام [2].

وعليه فالقصد الجنائي العام متوفر في جميع الجرائم الإلكترونية دون أي إستثناء، ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية يتوفر فيها القصد الجنائي الخاص (مثلا جرائم تشويه السمعة غبر الأنترنيت) ويبقى الأمر للسلطة التقديرية للقاضي في ذلك [3].

ثالثا: الركن الشرعي في الجريمة الإلكترونية

يقصد به إعتراف المشرع والنص القانونيعلى تجريم الفعل المرتكب، حيث أنه تطبيقا للقانون الجزائري لا جريمة ولا عقوبة إلا بنص، وتأكيدا على ذلك فإن المشرع الجزائري قد أحدث قسم في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص "بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات"[4]، ويشتمل على ثمانية (08) مواد تهتم بكل أنواع الإعتداءات على الأنظمة المعلوماتية، وإن كان من المستحسن أن يعتمد المشرع الجزائري على شكل هذا النمط من الجرائم المستحدثة بنص قانوني خاص بها وإلى غاية تكريس ذلك يبقى المنهج المعتمد من طرفه سليما ويتفق مع وجود ظاهرة إجرامية مستحدثة تستلزم ضرورة

---

[1] –بوضياف أسمهان، المرجع السابق، ص 354.

[2] –سوير سفيان، الجرائم المعلوماتية، مذكرة لنيل شهادة الماجيستير في العلوم الجنائية وعلم الإجرام، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، الجزائر،2001، ص 12.

[3] –محمود نجيب حسني، شرح قانون العقوبات، دار النهظة العربية، القاهرة، 1992، ص 4.

[4] –أنظرالمادة 394 مكرر من القانون رقم 04–15، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات، الجريدة الرسمية عدد 44.

التدخل وتجريمها وإفراد عقوبات مناسبة لها تطبيقا لمبدأ الشرعية وعدم جواز متابعة الشخص بأفعال غير محرمة قانونا، لذا فقد عمد المشرع على وضع نصوص خاصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات لتساير بذلك كل الإتجاهات التشريعية المعاصرة في هذا الشأن[1].

المطلب الثاني

دوافع ارتكاب الجريمة الإلكترونية

إن الباعث أو الدوافع هو العامل المحرك لإرادة توجيه السلوك الإجرامي وغالباً ما تتجه التشريعات العقابية إلى اعتبار الدافع عنصراً من عناصر التجريم إلاّ في الأحوال التي يحددها القانون صراحة، فالجريمة تقوم بتحقيق عناصرها وأركانها أيا كان الدافع من وراء ارتكبها، حيث أن دافع ارتكاب الجريمة هي مختلف العوامل والأسباب النفسية التي ترتبط بذاتية المجرموالتي تدفعه للقيام بالجريمة الإلكترونية، أين يكون إتيانه للسلوك الإجرامي الإلكتروني بسببها، كما أنها ترتبط بشخصية المجرم وطبيعة تكوينه النفسي وبنائه الذاتي التي تتمثل في الدوافع الشخصية(**الفرع الأول**) وأخرى موضوعية لارتكاب الجريمة الإلكترونية (**الفرع الثاني**).

الفرع الأول

الدوافع الشخصية لارتكاب الجريمة الإلكترونية

تعتبر الدوافع الداخلية الشخصية السبب التي تدفع الإنسان إلى الإقدام عن هذا السلوكالإجرامي، وهي تتعلق بشخصيته حيث يسعى من خلالها لتحقيق أهدافه الذاتية الخاصة والتي تتمثل في كل من الدوافع المادية (**أولاً**)وكذا الدوافع المعنوية (**ثانياً**).

[1] –بوخبزة عائشة، الحماية الزائية من الجريمة المعلوماتية في التشريع الجزائري، رسالة ماجيستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2012–2013، ص ص 61– 62.

أولاً: الدوافع المادية

يعدّ الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة المعلوماتية وذلك أن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم المعلوماتي إلى تطوير نفسه حتى يواكب كل حديث يطرأ على النفسية المعلوماتية واستغلال الفرص والسعي إلى الاحتراف بغية تحقيق مكاسب بأقل جهد دون ترك أي أثر وراءه[1].

فالإنسان بغية تلبية حاجياته الأساسية الفيزيولوجية كانت أو الاجتماعية فإنه يحتاج إلى المال الذي يعد عصب الحياة من أجل تحقيق وتلبية هذه الحاجيات مماّ يجعل مرتكبي الجريمة التكنولوجيا وفر الكثير من المعلومات التي يمكن لمرتكبي الجرائم الإلكترونية استغلالها واستخدامها عن طريق بيعها في ظل عصر بيع المعلومات والجوسية التي ساهمت في تطور سوق المعلومات باختراق أنظمة وبيانات الدول والهيئات والمؤسسات، وهذا ما مثل دافعاً أساسياً لارتكاب مثل هذه الجرائم بل يعد المحرك الأول والأساسي لأي جريمة إلكترونية في ظل عصر المعلومات اليوم[2].

ويجدر منا الإشارة في هذا المجال إلى أنّ هناك مجلة تسمى بالأمن الآلي التي تختص في الأمن المعلوماتي حيث أن الإحصائيات المعلن عنها في حالات الغش تتمثل في 43 بالمئة أما حالات اختلاس الأموال هي 23 بالمئة وكذا 15 بالمئة لاستغلال غير مشروع للحاسوب من أجل تحقيق منافع شخصية[3]، غير أنّ هذا لا ينكر أن هناك دوافع وأسباب أخرى تدفع الأفراد لارتكاب هذه الجريمة لتحقيق أهداف أخرى قد تكون مادية أو معنوية.

ثانياً: الدوافع المعنوية

تتمثل هذه الدوافع المعنوية في دافع الحصول على معلومات جديدة، كما أن هنالك من يرتكب جرائم الحاسوب بغية الحصول على الجديد من المعلومات، بالإضافة إلى أنه نجد أشخاص

[1]–وضاح محمود نشأت مقضي المجالي، جرائم الأنترنيت، دار المنارة للنشر، عمان، 2005، ص 30.

[2]–صابر بحري، خرموش منى، أهم الدوافع السيكولوجية وراء الجريمة الإلكترونية مجلة دراسات في سيكولوجية الانحراف، المجلد06، العدد01، جامعة محمد لمين دباغين سطيف، الجزائر، 2021، ص 48.

[3]–الرومي محمد أمين، الكمبيوتر والأنترنت، دار المطبوعات الجامعية الإسكندرية، مصر، 2004، ص 90.

يقومون بالبحث واكتشاف الأنظمة والعمل من خلال الجماعة وتعليم بعضهم، حيث يفضل هؤلاء القراصنة البقاء مجهولين أكثر وقت ممكن حتى يتمكنوا من الاستمرار في التواجد داخل الأنظمة، فالكثير من مرتكبي الجريمة الإلكترونية يكون دافعهم حب الاطلاع والحصول على المعلومة، ضف إلى دافع الاستلاء على المعلومة، كما نجد دافعاً أخر يتمثل في الرغبة على فهم النظام الإلكتروني والتغلب عليه، وذلك بسبب ميول هؤلاء الأشخاص بإبراز على تفوقهم على وسائل التكنولوجيا الحديثة، إذ أنّ هذه الرغبة وإثبات الذات وتحقيق الانتصار الشخصي على الأنظمة الإلكترونية من الدوافع النمطية لارتكاب الجريمة، فالمجرم الإلكتروني في حال تمكنه من الانتصار على النظام المعلوماتي يشعر بتقدير الذات وتعزيزالثقة لديه، حيث أنّ في ارتكابه للجريمة الإلكترونية يحقق دوافع نفسية، ومن الدوافع المعنوية دافع التسلية ولعل الكثير من مرتكبي الجرائم الإلكترونية يكون دافعهم الأول هو المزاح والتسلية وبمجرد احترافهم فيها يصبحون مجرد هاوين لهذه الجرائم إلى محترفين خطرين، كما يعتبر أيضا دافع الإثارة والمتعة دافعاً معنويلارتكاب الجريمة الإلكترونية.

الفرع الثاني

الدوافع الموضوعية لارتكاب الجريمة الإلكترونية

تتمثل الدوافع الموضوعية في تلك الدوافع الخارجية أي كل الأسباب والعوامل التي تكون خارج عن ذات الفرد والتي ليس لها علاقة بشخصيته، ولهذه الأسباب أهمية كبيرة في مجال الجريمة الإلكترونية، بحيث قد يتأثر المجرم الإلكتروني ببعض المواقف التي قد تكون دافعه لإتيان بالفعل الإجرامي الإلكتروني، كما أنه لا يسعى فيها المجرم الإلكتروني حينها لكسب المال ولا التسلية ولا حتى الإثارة والمتعة، ضف إلى أن هذه الدوافع تتعلق بدافع الانتقام وإلحاق الضرر بالغير **(أولاً)**، وكذا دافع التعاونوالتواطؤ **(ثانياً)**، بالإضافة إلى الضغوطات العامة**(ثالثاً)**.

أولاً: دافع الانتقام وإلحاق الضرر بالغير

يعد دافع الانتقام من أخطر الدوافع التي تدفع بالشخص إلى ارتكاب الجريمة، وغالباً ما يصدر هذا الفعل من شخص يملك معلومات كبيرة عن الشركة أو المؤسسة التي يعمل بها، إذ أن أسباب هذا الدافع متعلقة بالوظيفة التي يشغلها، وذلك حين يشعر بالحرمان من الحقوق المهنية أو التعرض للطرد من الوظيفة حيث يتولد لدى المجرم المعلوماتي الرغبة في الانتقام من رب العمل، و مثل ذلك فقد دفع الانتقام بالمحاسب بالتلاعب بالبرامج المعلوماتية أين جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحليه، وتحقق هذا الأمر في التاريخ المحدد من طرفه[1].

كما نجد كذلك أسباب تدفع المجرم الإلكتروني لإتيان الفعل الإجرامي بغية الانتقام من الضحايا كتشويه سمعة الضحية من خلال نشر معلوماته الشخصية السرية، تتبعه خلاف مع الضحية لأسباب شخصية أو مهنية، فشخصية المجرم الإلكتروني لها دور في تحديد البعد الانتقامي لديه، فالكثير من الجرائم يكون دافع الانتقام المنجز من المجرم الإلكتروني لا يستحق ذلك الانتقام، فالمجرم الإلكتروني حفظاً عنه عن ذاته وتحقيق لها هذا ما يدفع لإتيان السلوك الإجرامي هذا من جهة[2]، أما عن إلحاق الضرر بالغير يعتبر باعث لارتكاب الجريمة الإلكترونية كذلك، وهو إلحاق الضرر المادي أو المعنوي برب العمل انتقاما منه لأسباب شخصية تتعلق بطبيعة العلاقة التي تربط رب العمل بالمجرم الإلكتروني وفي ارتكاب الجريمة بكبد المؤسسة أو الشركة خسائر مادية على اعتبار أن تلك الخسائر تلحق المؤسسة، وبالتالي صاحب العمل يجعل من المجرم الإلكتروني أي مرتكب الجريمة فخوراً بما فعله بدافع الانتقام وبالتالي يرضى بنفسه محققاً بذلك انتصارا لذاته، فدافع إلحاق الضرر بالغير يعتبر دافعاً نفسياً عن طريق رغبة الإنسان

[1] سعيداني نعيم،"أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائر"، شهادة الماجستير في العلوم القانونية، تخصص علوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، الجزائر،2013، ص42.

[2] – صابر بحري، خرموش منى، المرجع سابق، ص ص 53– 62.

لإلحاق الأذى بالأخرين، بسبب مرض نفسي أو اضطراب نفسي أو بهدف إشباع حاجياته الاجتماعية والنفسية لإرضاء غروره، وتختلف هذه الأسباب لاختلاف طبيعة الجريمة الإلكترونية[1].

ثانياً: دافع التعاون والتواطؤ

إن الكثير من مرتكبي الجرائم الإلكترونية يشكلون جماعات لإجرام في هذا المجال بحيث يتعاونون من أجل إتيان الأفعال الإجرامية بدقة لتحقيق أهداف مشتركة بين هؤلاء المجرمين وتكون مرضية إما في الشخصية أو النفسية، هذا النوع يتكرر كثيراً في المجال الإلكتروني، حيث يكون ذلك بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي وأخر من المحيط أي خارج المعنى عليه، حيث يعطي عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة ودقيقة حول أنشطتهم[2].

ثالثاً: الضغوطات العامة

تتمثل في الضغوطات التي يتعرض لها المجتمع من بطالة وفقر وكذا ظروف اقتصادية صعبة، وتعتبر هذه العوامل من العوامل الضاغطة على المجتمع بصفة عامة وعلى الفئة الشيبانية بصفة خاصة وهذا ما يولد مشاعر سلبية عند شرائح كبيرة من الناس ضد المجتمع وكذا ضد الظروف، مما يدفع بهم إلى التأقلم السلبي مع هذه الظروف الصعبة منها الإتجار الإلكتروني بالبشر والجنس وغيرها[3]، ولارتكاب الجريمة الإلكترونية علاقة مباشرة مع الضغوطات النفسية لدى الشخص وهذا ما يدفعه لإتيان بالأفعال الإجرامية بجل صورها وفي حال تمكن هذا الشخص في المجال الإلكتروني وإتقانه لتقنية الإلكترونية، فقد تدفعه الضغوطات النفسية التي يعيشها من عوامل اجتماعية كالفقر والبطالة والتهميش الاجتماعي يدفع بالشخص إلى التفكير بالجريمة

[1]– المرجعنفسه، 54.

[2]– سعيداني نعيم، المرجع سابق، ص61–62.

[3]–ذياب موسى، الجرائم الإلكترونية المفهوم والأسباب الملتقى العلمي للجرائم المستحدثة في ظل التغيرات والتحولات الإقليمية والدولية، كلية العلوم الاستراتيجية، الأردن، 2014، ص15.

الإلكترونية، بهدف الوصول إلى حلول لمشكلته سواء المتعلقة منها بالجانب المادي بغية تلبية حاجياته المالية الأساسية أو ما يتعلق بالجانب المعنوي كمشكلة الفراغ، بحيث يضطر هذا الشخص لارتكاب هذه الجرائم بهدف ملأ فراغه هذا من جهة، ومن جهة أخربالتأثربالأخرين ومساندتهم لهم بحثاً عن السند والدعم، ما يعزز له السلوك الإجرامي الإلكتروني.

المبحث الثاني

خصائص وأنواع الجرائم الإلكترونية في القانون الجزائري

تعد الجرائم الإلكترونية من الجرائم المستحدثة حيث اختلف الفقه حول تصنيفها إلى عدة تقسيمات؛ إذ لم تراع أغلب التقسيمات خصائص الجرائم الإلكترونية وموضوعها، إذ نجد أهم ما يميز الجرائم الإلكترونية عن غيرها هو أن هذه الجريمة تستهدف البيانات المعنوية للحاسوب الألي وترتكب بواسطة جهاز الإلكتروني، كما اختلف الفقهاء في تقسيم الجرائم الإلكترونية نتيجة ظهور جرائم جديدة من حين إلى أخر، أي أن الجرائم الإلكترونية غير محصورة فلا يمكننا أن نجمل أصنفها وأشكالها وخصائصها فهي متغيرة ومتجددة، فكلما ظهرت وسيلة جديدة لاستخدام الحاسب الألي ظهرت معها جريمة جديدة، غير أن الفقهاء لم يستقروا على معيار واحد لتصنيف الجرائم الإلكترونية وهذا راجع إلى كثرة هذه الجرائم وسرعة تطورها، وهذا التصنيف يعود إلى الوسيلة التي يتم بها ارتكاب الجريمة أو على أساس محلها، ضف إلى ان المجرم المعلوماتي له تميزه معينة عن المجرم الذي يرتكب الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي ومعرفي للمجرم في عملية ارتكابها فإن الأمر يختلف بالنسبة للجرائم المعلوماتية، فهي جرائم فنية حيث يكون مرتكبها ذو قدرة في المجال الإلكتروني و مختص في مجال الشبكة الإلكترونية.

المطلب الأول

خصائص الجريمة الإلكترونية

نتج عن ارتباط الجريمة المعلوماتية بجهاز الحاسوب وشبكة الأنترنت مجموعة من الخصائص التي تجعلها منفردة عن غيرها من الجرائم التقليدية سواء من حيث الجريمة ذاتها أو من حيث مرتكبي هذه الجريمة وهذا ما سيتبين من خلال دراستنا.

الفرع الأول

السمات الخاصة بالجريمة الإلكترونية

بالرجوع للطبيعة المميزة للجريمة الإلكترونية بإعتبارها تمس المعلومات مما جعلها تتميز عن الجرائم التقليدية بمجموعة من الخصائص والمميزات وهذا ما يساعد على التعرف على خصائص الجريمة الإلكترونية للوصول إلى الحلول لمكافحة حيث يمكن أن نبرز أهم هذه السمات فيما يلي:

أولا-الجريمة المعلوماتيةمتعددة الحدود

فهي جريمة عابرة للحدود، فالمجرم المعلوماتي لا يعترف بالحدود الجغرافية ولا يعيرها اهتمام أذ هو مجتمع منفتح عبر شبكات تخترق المكان والزمان دون خضوعها لحرس الحدود، فبظهور شبكات الأنترنت لم يعد هنالك حدود مرئية أو ملموسة، ما جعل نقل المعلومات عبر الدول المختلفة سهلة في حركة المعلومات عبر أنظمة وبرامج تقنية حديثة مما سمح بإرتكاب الجريمة الإلكترونية عن طريق الحاسوب موجود في دول معينة بينما يتحقق الفعل الإجرامي في دول أخرى، فهذه المميزة التي تتسم بها الجريمة الإلكترونية خلقت العديد من المشاكل حول تحديد الدولة، ضف إلى صاحب الاختصاص القضائي وكذا تحديد القانون الواجب التطبيق، وكما نجد ظهور إشكاليات تتعلق بإجراء الملاحظة القضائية، غير أن ذلك من النقاط التي تسيرها الجرائم العابرة للحدود بصفة عامة[1].

ثانيا-صعوبة إكتشاف الجريمة الإلكترونية

تتميز الجرائم الإلكترونية بصعوبة اكتشافها، حيث الحالات التي يتم اكتشاف هذا النوع من الجرائم قليلة وبمحض بالصدفة، وترجع أسباب صعوبة اكتشاف الجريمة المعلوماتية إلى ترك هذه لأي أثر خارجي بصورة مرئية، فلا يوجد جثث لقتلى أو للدماء، كما أن المجرم المعلوماتي يمكن له ارتكاب

[1]-حمزة بن عقون، السلوك الإجرامي، المجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012/2011، ص 17-18.

هذه الجريمة في دول وقدرات مختلفة، ضف إلى صعوبة الحصول على الدليل المتوفر[1]، ولعل صعوبة كشف الدليل المتزايد بصورة خاصة من ارتكبت هذه الجرائم في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة بين هؤلاء يسهل عليهم اقتراف جرائمهم دون أن يتركوا أثار تدل عليهم[2].

ثالثا: صعوبة إثبات الجريمة المعلوماتية

يعتبر اكتشاف الجريمة الإلكترونية أمراً ليس سهلا، كما أشارنا إليه سالفا إلا أن في حالة اكتشافها والإبلاغ عنها، فإن إثباتها أمر يحيط بها الكثير من الصعاب، باعتبار أن الجريمة الإلكترونية في إطار غير تقليدي ووقوعها في إطار غير ملموس وغير مادي، لتقوم أركانها في بيئة الحاسوب والأنترنت مما يجعل الأمر يزداد صعوبة وتعقيداً لدى سلطات الأمن وأجهزة التحري والتحقيق والملاحظة كون البيانات والمعلومات في هذه البيئة عبارة عن نبضات إلكترونية غير مرئية، كما أن وسائل المعاينة وطرقها التقليدي لا تفلح في أغلب الأحيان في إثبات هذه الجريمة نظراً لطبيعتها الخاصة التي تتميز عن الجرائم التقليدية، فالمجرم الإلكترونية لا يخلق أثار مادية، كما أن هذه الجريمة يصعب فنياً الاحتفاظ بأثارها وإذا تركت أثاراً فإن هذه الجريمة الإلكترونية على التضليل والخداع في ارتكابها والتعرف على مرتكبها، كما أن الجريمة الإلكترونية تعتمد على قمة الذكاء في ارتكابها، إذ يصعب على المحقق التقليدي أن يفهم حدودها الإجرامية وما تخلفه من أثار غير مرئية.

رابعا: أسلوب ارتكاب الجريمة الإلكترونية

من سمات الجريمة الإلكترونية تبرز ذاتها بصورة أكثر وضوحاً في أسلوب ارتكابهاوطريقها، فالجرائم المعلوماتية تتسم بالهدوء بطبيعتها، لا تحتاج إلى العنف بل كل ما تحتاج إليه هي القدرة

[1]–عبد الناصر محمود فرغلي، محمد عبيد سيفالسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة مقارنة)، المؤتمر العربي الأول للعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007، ص 10.

[2]–موسى مسعود أرحومة، الإشكاليات الإجرائية التي تسيرها الجريمة المعلوماتية عبر الوظيفة، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظيمه أكاديمية الدراسات العليا، طرابلس، 26–2009/10/29، ص03.

على التعامل على جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الجريمة الأفعال غير المشروعة[1]، كما تحتاج أيضا إلى وجود شبكة الأنترنت مع وجود مجرم يوظف خبراته وقدراته على التعامل مع الشبكة للقيام بجرائم مختلفة كاختراق خصوصيات الغير أو التجسس، فكل ذلك دون الحاجة إلى سفك الدماء على عكس الجرائم التقليدية التي تتطلب نوعاً من الجهد العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء، كما هو الحال في جريمة القتل والاحتفاظ أو في صورة الكسر في جريمة السرقة[2].

خامسا: الجريمة الإلكترونية تتم بتعاون عدة أشخاص

تتم عادة بتعاون أكثر من شخص للإرتكابها حيث تتميز الجريمة الإلكترونية أنها ترتكبمن طرف شخصين أو أكثر حيث يقوم شخص متخصص في تقنيات الحاسوب والأنترنت بإخراج الجريمة إلى الواقع وحيز الوجود حيث يقوم بالجانب الفني من المشروع الإجرامي وشخص أخر من المحيط لتغطية عملية التلاعب وتحويل المكاسب إليه والاشتراك في الجريمة الإلكترونية له صورتين أولهما اشتراكا سلبياً المتمثل على من يعلم لتسهل لإتمام ارتكاب الجريمة أما الجانب الأخر فهو إيجابي الذي يتمثل في الكثير من الجرائم ويتمثل في المساعدة الفنية والمادية.

الفرع الثاني

السمات الخاصة بالمجرم المعلوماتي

المجرم المعلوماتي كإنسان يتمتع بالمهارة والمعرفة والذكاء بمعنى التعرف على كافة الظروف التي تحيط بالجريمة وتنفذها وإمكانية نجاحها وفشلها، فالجناة يمهدون لارتكاب جرمتهم بالتعرف على كافة الظروف المحيطة بهم، لتجنب الأمور غير المتوقعة والتي يمكن أن يتم يضبط أفعالهم والكشف عنهم من خلالها، كما أن المجرم الإلكتروني يتمتع بقدرة فائقة في مجال تقنية الحاسوب والأنترنت، فتنفيذ مثل هذه الجرائم يتطلب قدراً من المهارة لدى الجناة الذين يكتسبونها

[1]–نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة لنشر والتوزيع، عمان، 2008، ص55.

[2]– نفس المرجع السابق، ص55.

عن طريق الخبرة في المجال المعلوماتي، فالجريمة الإلكترونية تعد جريمة الأذكياء بالمقارنة مع الجرائم التقليدية التي تتسم بالميل إلى العنف، فالمجرم المعلوماتي دائم البحث والسعي إلى طرق جديدة وحديثة التي لا يعلم بها سواء بهدف اختراق كل الحواجز الأمنية في البيئة المعلوماتية لتحقيق أهدافه ونيل مبتغاه[1].

أولا: المجرم المعلوماتي إنسان اجتماعي

يمكن القول أن المجرم المعلوماتي بصفة إنسان ذكي فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل هو إنسان يستطيع التوافق والتصالح مع مجتمعه، باعتباره شخص مرتفع الذكاء الأمر الذي يساعده على تنفيذ عملية التكيف المجرم المعلوماتي في مجتمعه زادت بذلك خطورته الإجرامية مع توافر الشخصية الإجرامية لديه، فشعور المجرم المعلوماتي بأنه محل ثقة في مجتمعه ومجموعته وأنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا يتم الكشف عنها، وحتى إذا ما تم اكتشافها، أي أنها تواجه صعوبة الإثبات لسبب نقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء.

ثانيا: المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي

بمعنى بسلطة الحقوق والمزايا التي يتمتع بها المجرم الإلكتروني والتي من خلالها يستطيع من القيام بالسلوك الإجرامي، فالمجرم المعلوماتي يتمتع بالسلطة المباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة المتمثلة في الرقم السري الخاص للدخول إلى النظام يحتوي على المعلومات والتي تمتد للفاعل الجاني بمزاياً كفتح ملفات محو المعلومات أو تعديلها، وقراءة الملفات وكتابتها وقد تتمثل هذه السلطة في الحق في استعمال الأنظمة المعلوماتية أو القيام ببعض المعلومات، وكذا الدخول إلى الأماكن التي تحتوي على الأنظمة المعلوماتية، فإنه القيام بالتخطيط والتنظيم ففي علم الأنترنت والشبكات الإلكترونية، فيقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة، كما هو الحال في الواقع المادي حيث ترتكب أغلب الجرائم من طرف

[1]–سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات مذكرة هادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، جامعة بسكرة، 2013–2014، ص18.

مجموعات متكونة من عدة أفراد يحدد لكل شخص دوره، ويتم ذلك وفقاً لتنظيم وتخطيط مسبق على ارتكاب الجريمة حيث تتكون هذه المجموعة الإجرامية من متخصص في المجال الفني للحاسب الألي الذي يتولى، الجانب الفني من المشروع الإجرامي إلى جانب شخص أخر من المحيط أو من خال مؤسسة المجني عليها لتغطية التلاعب.

ثالثا: المجرم المعلوماتي يبرر ارتكابه للجريمة

يتولد لدى مرتكب فعل المجرم المعلوماتي إحساس وشعور بأن ما يقوم به لا يعتبر من عداد الجرائم[1]، حيث يميز مرتكبو هذه الجرائم بالإضرار بالأشخاص الأمر الذي يعدونه غاية من للأخلاقية وبين الأضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم[2].

رابعا: التطور في السلوك الإجرامي

يعني وجود المجرم الإلكتروني ضمن جماعة إجرامية تساعده في سرعة اكتساب المهارة الفنية التي تؤدي إلى المراد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى أعلى معدلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة، وبناءً على ما تقدم يمكن تقسيم المجرم الإلكتروني إلى عدة طوائف مختلفة متمثلة فيما يلي:

أ- **المخترقون أو المتطفلون:** نجد في هذا الإطار نوعين من المجرمين

1- القراصنة الهواة العابثون: هذا القسم من القراصنة يرون في اختراق الأنظمة المعلوماتية تحدياً لقدراتهم الذاتية، وهم يمثلون طائفة هواة الحاسوب فيقومون بأعمالهم هذه لمجرد إظهار قدراتهم على اقتحام المواقع الأمنية أحياناً أو مجرد ترك بصماتهم التي تثبت وصولهم إلى ذلك المواقع[3]،

[1]-نايريعائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار،2017/2016، ص12.

[2]- الزبدي وليد، القراصنة على الأنترنت والحاسوب، الطبعة الأولى، دار سامة للنشر، عمان، 2003، ص40.

3-www.tashreaat.com، تم الاطلاع على الموقع بتاريخ 2022/05/25 على الساعة 17سو35د.

ويدعون هؤلاء أنه لا يوجد هنالك دوافع تخزينية وراء أعمالهم، وأصحاب هذه الفئة لديهم الكفاءة الخاصة، المعرفة والمهارة المطلوبة في المجال الجواسيس والشبكات إلكترونية.

كما نجد كذلك النوع الثاني المسمى بقراصنة الأخلاقية ينتقلون أنهم يعملون من أجل المصلحة العامة، فقاموا بتشكيل منظمات خاصة مثل منظمة القراصنة ضد المواقع الإباحية للأطفال التي قامت واستطاعت بالقيام بحملات تحسيسية وتأديبية لإبطال وتعطيل قدرة بعض المواقع الإلكترونية عن عرض مواد غير أخلاقية[1].

ب-القراصنة المحترفون

تعرف هذه الطائفة بالمجرمين البالغين وأعمارهم تتراوح بين 25 و45 سنة فمن أهم نواتهم أنهم يتمتعون بمكانة بالمجتمع وأنهم غالباً من المتخصصين في المجالات التقنية أي أنهم يتمتعون بمهارات فنية في مجال الأنظمة الإلكترونية.

ج-طائفة الموظفون العاملون في مجال الأنظمة المعلوماتية

بحكم ارتباط هؤلاء بالنظام المعلوماتي كونه مجال عملهم الأساسي، ونظراً لمهاراتهم التقنية، فإنهم يرتكبون الجرائم المعلوماتية بهدف تحقيق أهدافهم الشخصية، وتكمن غايتهم القصوى هو تحقيق الكسب المادي فهنا نستنتج أنه بسبب العلاقة الوظيفية التي تربط بين المجني عليه والموظف ولحكم الثقة بينهما، هذا ما يسهل عملية ارتكاب الجريمة المعلوماتية، هذا من جهة ومن جهة أخرى نجد أن هنالك فئة من الحاقدين على عملهم وعلى شركات التي يعملون فيها، فإن هنا تكون العمليات الإجرامية ليس بهداف تحقيق الكسب المادي وإنما بدافع الثأر والانتقام، ويطلق على هذه الفئة بمجرمي المعلوماتية الحاقدين.

[1]-محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركزا لإعلام الأمنية الأكاديمية للشرطة، الجزء الأول، د ص.

د- مجرمون ذوي دوافع سياسية

هذه الفئةلها ميول ودوافع سياسية، لاختراق نظم الحاسب الآلي غير المصرح بالدخول إليها، والتي تتضمن بيانات ومعلومات سرية تخص الدفاع والأمن، ويعد المساس بها غاية في الخطورة.

هـ-صغار السن:

يمثلون فئة من صغار السن دون سن الأهلية، تتسم هذه الفئة بأنهم متحمسين بالحاسوب ودافعهم التحدي لكسر الرموز السرية لتركيبات الحاسوب.

فالإجرام الإلكتروني يتسم بالذكاء دون الحاجة إلى استخدام القوة والضعف والذكاء لديهم هو مفتاح المجرم الإلكتروني لاختراق البرامج المحصنة ومن المميزات التي تشترك فيها مجرمو المعلوماتية أن أعمارهم تتراوح بين 18 و45 سنة والثقة الزائدة بالنفس، كما يتسمون بالمهارة التقنية والإلمام والقدرة بالنظام المعلوماتي ضف إلى الإلمام التام بالمسرح الجريمة.

المطلب الثاني

أنواع الجرائم الالكترونية في القانون الجزائري

لقد اختلف الفقه في تقسيم وتصنيف الجرائم الالكترونية وذلك نتيجة ظهور جرائم جديدة ومستحدثة من حين لأخر، فكلما ظهرت وسيلة جديدة لاستخدام الحاسوب الآلي والانترنيت ظهرت معه جريمة جديدة[1]، فهناك من يصنفها بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية[2]، حيث أن البعضيصنفها بالرجوع إلى وسيلة ارتكاب الجريمة، أو على أساس محل الجريمة، أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الالكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها وبالتالي: تتمثل في كل من الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والاتصال، أما النوع الأخر يتمثل في الجرائم الواقعة

[1]- يوسف خليل يوسف العفيفي، الجرائم الالكترونية في التشريع الفلسطيني "دراسة تحليلية مقارنة"، رسالة لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون" الجامعة الإسلامية"، غزة، 2013، ص 13.

[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، ط1، الجزائر، 2002، ص 24.

على النظام المعلوماتي حددها المشرع الجزائري بموجب قانون العقوبات وهذا ما سيتم تناوله في الفروع الموالية.

الفرع الأول

الجرائم المرتكبةبإستخدام النظام المعلوماتي

تتنوع الجرائم التي ترتكب بواسطة النظام المعلوماتي ما بين جرائم اقتصادية أوقرصنة المعلومات أو ذات طابع سياسي أو متعلقة بالأمن القومي وقد تقع هذه الجرائم على الأشخاص الطبيعة أو الإعتبارية [1]والجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار، سنوضح كل نوع منها في البنود الآتية:

أولا: الجريمة الإلكترونية الواقعة على الأشخاص

وهي من الجرائم المتعلقة بإتلاف وتعطيل الممتلكات الخاصة بالناس على الانترنيت، ويطلق بعض الفقهاء على هذا النوع من الجرائم مصطلح الاعتداء على جريمة الحياة الخاصة للأفراد باعتبار حق حماية الحياة الخاصة من أهم الحقوق وذلك لما له من ارتباط وثيق بحرية الفرد، وقد جاء تجريم هذا النوع من الأفعال كحماية من التهديد الحقيقي الذي تشكله تكنولوجيات المعلومات لحق الأفراد في احترام حياتهم الخاصة مع انتشار ما يسمى ببنوك المعلومات بمختلف أنواعها (الأمنية، المالية، السياسية، الطبية، العسكرية...إلخ).

وعليه يمكن أن يستخدم النظام المعلومات في الاعتداء على حرمة الحياة الخاصة أو على الحريات العامة للفرد بصور متعددة من أهمها [2]:

- ✓ جمع البيانات وتخزينها على نحو غير مشروع.
- ✓ إساءة استعمال البيانات أو المعلومات الإسمية.

---

[1]– المادة 394 مكرر 3 من قانون العقوبات.

[2]– سوير سفيان، جرائم المعلوماتية، مذكرة ماجيستر في العلوم الجنائية، جامعة أبو بكر بلقايد، تلمسان، 2010، ص 35.

- ✓ الإفشاء غير المشروع للبيانات والمعلومات الإسمية.
- ✓ الاعتداء على سرية الإتصالات والمراسلات.

سنحاول من خلال هذا العنصر التعرض إلى بعض الجرائم التي ترتكب بواسطة النظام المعلوماتي عن طريق الانترنيت من بينها ما يلي:

1. جرائم السب والقذف عبر الانترنيت

عرفت المادة 297 من قانون العقوبات الجزائري السب بقولها:"**يعد سبا كل تعبير مشين أوعبارة تتضمن تحقيرا، أو قدحا لا ينطويعلى إسناد واقعة**".

كما يعرف القذف على أنه: " إسناد واقعة محددة تستوجب عقاب من تنسب إليه أو احتقاره إسنادا علينا يفيد نسبة الأمر إلى الشخص على سب التوكيد". ويتضح من النصوص السابقة أن السب والقذف يتطلبان بكل وضوح العلانية كما نص القانون على ذلك صراحة أي نشر السب والقذف عن طريق الانترنيت تتحقق به العلانية.

لقد اعتبر المشرع الجزائري صراحة من بين مكونات الركن المادي لارتكاب هذه الجريمة أن تكون موجهة لشخص الرئيس لاعتبار هذا الأخير من رموز السيادة الوطنية وهذا ما نصت عليه المادة 144 مكرر [1]، يعاقب بغرامة من 100.000دج إلى 500.000دج كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان عن طريق الكتابة أو الرسم أو التصريح أو بأية آلة لبث الصوت أو الصورة أوبأية وسيلة الكترونية أو معلوماتية أو إعلامية".

2. جرائم الإعتداء على الحياة الخاصة

فقد عني المشرع الجزائري بإضفاء الحماية على الحياة الخاصة سواء بالدستور، أو بالقانون، وقد يستخدم النظام المعلوماتي في الاعتداء على حرمة الحياة الخاصة كما لو قام شخص بعمل

[1]– المادة 144 من القانون 11–14، المؤرخ في 2 غشت 2011 يعدل ويتمم الأمر رقم 66–156 المتضمن قانون العقوبات ج، ر، العدد 44.

بالنظام المعلوماتي بإعداء ملف يحتوي على معلومات تخص شخص بدون علمه وبغير إذنه وقام هذا الشخص بإطلاع الغير عليها بدون إذن صاحبها كما في حالة الأسرار المودعة لدى المحاسبين أو لدى الأطباء. فكل هذه الأسرار يحميها القانون ويجرم إفشاءها غير المشروع وبدون موافقة صاحبها، وجريمة التعدي على الحياة الخاصة والاطلاع على الأسرار أو إفشاءها قد تتم بنشر المعلومات على الكومبيوتر وفتح السجلات الالكترونية والإطلاع عليها من خلال شاشة الكمبيوتر.

ويدخل كذلك في نطاق جرائم التعدي على الحياة الخاصة جريمة تسجيل المحادثات الشخصية أو مراقبتها بأية وسيلة حيث نجد بعض المتسللين يستطيعون اختراق شبكة الأنترنيت بطرق غير مشروعة والتنصت على هذه المكالمات.

وعلى هذا فقد نص المشرع الجزائري في المادة 303 مكرر [1]، "يعاقب بالحبس من ستة (6) أشهر إلى 3 سنوات وبغرامة من 50.000دج إلى 30.000دج، كل من تعمد المساس يحرمه الحياة الخاصة للأشخاص بأية تقنية كانت وذلك:

أ- بإلتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.

ب- بإلتقاط أو تسجيل صورة الشخص في مكانه خاص، بغير إذن صاحبها أو رضاه".

3. الجريمة الالكترونية الواقعة على حقوق الملكية الفكرية

إن استخدام معلومة معينة دون إذن صاحبها يعتبراعتداء على حق معنوي، إضافة إلى أنه يصنفكإعتداء على قيمته المالية كون أن المعلوماتية ذو قيمة أدبية ومادية، كما تندرج براءات الاختراع ضمن الحقوق الفكرية، فقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال

[1]- المادة 303 مكرر من القانون 06-23 المعدل والمتمم لقانون العقوبات.

نصوص قانونية خاصة في الأمر رقم 03-05 الصادر في 2003 المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 الصادر في 2003 المتعلق ببراءات الاختراع.

مع هذا التطور فقد ظهرت مشاكل التعامل مع نوع جديد منأنواع الملكيةالفكرية يمكن وصفها بالملكية الرقمية وهي تلك الملكية التي تنصب على برامج الحاسوب وبيانتها والمصنفات الرقمية المنشورة على شبكة الأنترنيت فقد أشار المشرع الجزائري إلى مفهوم المصنفات الرقمية في الأمر رقم 08/03 المؤرخ في 2013/07/19 في نصوص المواد 02-03-04-05[1]إضافة إلى نص المادة 03 والمادة 27 من الأمر 05/03 المؤرخ في 2003/07/19[2] إن جرائم المعلوماتية هي من أكثر الجرائم التي تمس بحق المؤلف من خلال ما يعرف بجرائم التقليدية (La contrefaçon)مثل جرائم التحميل غير المشروع عبر شبكة الانترنيت، فملايين المتصفحين لشبكة الانترنيت اعتادو على تحميل الأفلام والموسيقى دون شرائها من مصدرها الأساسي، معتمدين في ذلك على برامج متخصصة في فك شفرات الحماية وذلك إما بغرض استعمالها الشخصي أو بعرض إعادة نشرها وطرحها للغير على شبكة الانترنيت أو للبيع على وسائط تخزين خارجية كالأقراص المضغوطة[3].

ثانيا: الجرائم الواقعة على النظم المعلوماتية الأخرى

تتحقق هذه الجريمة باستخدام أداة إلكترونية معينة تسمح بإلتقاط المعلومات والتنصت عليها لدى النظم المعلوماتية الأخرى، بالإضافة إلى إساءة استخدام البطاقة الإئتمانية [4].

---

[1]-الأمر رقم 03-08، المتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، صادر في تاريخ 2003/07/23، الجريدة الرسمية، عدد 36، ص 44.

[2]- الأمر رقم 03-05، مؤرخ في 19 جمادى الأول عام 1424، الموافق لـ 19 يوليو 2003، المتعلق بحماية المؤلف من الحقوق المجاورة، ج، ر، عدد44.

[3]- فليح نور الدين، الجريمة الالكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة مولاي الطاهر، سعيدة، 2018-2019، صص 40، 41، 43.

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

بالنسبة للجريمة الولوج غير المشروع للمعلومات المعالجة أليا تنقسم إلى الولوج المباشر بها يستطيع الجاني الإستلاء على المعلومات المخزنة بعدة طرق هي:

1- بإستخدام آلة طباعة لاستخراج المكتوب على ورق.

2- استخدام شاشة النظام والإطلاع بالقراءة على ما هو مكتوب عليها.

3- بإستخدام مكبر الصوت أو سماعات لإلتقاط المعلومات والبيانات المعالجة كما هناك كذلك الولوج غير المباشر ويكون ذلك بإستعمال شبكات الاتصال البعيدة والمعالجة عن بعد إلى مخاطر تتمثل في التقاط والتسجيل غير المشروع للمعلومات أثناء بثها وحركتها[1].

أما الحالة الثانية تكون في حالة إساءة استخدام العميل البطاقة الإئتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الإئتمانية وشروط العقد المبرم بينه وبين البنك، كإستعماله بطاقة الإئتمانية انتهت مدة الصلاحية أو تم إلغائها أو بعد الإبلاغ بضياعها، وكذلك إساءة استخدام الغير لهذه البطاقات كإستعماله لبطاقة مسروقة للحصول على الخدمات والسلع أو سحب مبالغ بموجبها، أو السحب بإستخدام بطاقة مزورة[2].

ثالثا: الجريمة الإلكترونية الواقعة على الأسرار

إن المعلوماتي أصبحت أيضا تستخدم في إفشاء الأسرار خاصة تلك التي تخص الدولة فيها سواء كانت أسرار مالية أو عسكرية أو اقتصادية أو أسرار مهنية مثل الأسرار المتعلقة بالمحامين والقضاة فكل موظف يباشر النظام المعلوماتي.

[1]-أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، (دون بلد النشر)، 2006، ص 190، 191.

[2]- أحمد خليفة الملط، المرجع السابق، ص 197.

يدرك قيمتها السرية فهو مطالب بحمايتها وكل إفشاء يعتبر جريمة[1]، في حين تكون هذه الأسرار إما أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات الخاصة، فيتخذ هذا النوع من الجرائم صورتين، هما الأولى تتعلق بالجرائم الواقعة على أسرار الدولة، من بينهاالإطلاع على مختلف الأسرار خاصة العسكرية منها والاقتصادية، خاصة فيما يتعلق بالدول التي تكون فيها النزاعات وذلك عن طريق التجسس بأنواعه السياسي، العسكري والاقتصادي وذلك بإختراق الأنظمة للعبث بمحتوياتها وإتلافها، هذا مامكنالعدد من الدول من الحصول على أسرار معلومات دولة ما وإفشاؤها لدولة أخرى، أو استغلالها بما يضر المصلحة الوطنية للدولة ضحية التجسس[2]، والثانية متعلقة بالجرائم الواقعة على الأسرار المهنية، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات الغير قصد التشهير أو بيع هذه المعلومات لتحقيق المصلحة الخاصة، مثال ذلك كالحصول على عائد مادي ممن يهمه الأمر أو أن يستعملها للضغط على أصاحبها من أجل القيام بعمل أو الامتناع عن القيام بعمل[3].

فإرتباط الاقتصاد خاصة والسياسة الجزائرية في جزئها الكبير بالتقنيات الإلكترونية الحديثة يعتبر هدفا دائما لهجمات القراصنة الالكترونيين وعصابات الجريمة الإلكترونية المنظمة التي تستهدف البنية الأساسية التي تعمل بهدف إضعاف الدولة ككل والتي يعتبر الاقتصاد شريانها الحيوي هذا ما جعل المشرع الجزائري حريص على حماية هذه لأسرار من خلال نصوصه في الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر من قانون العقوبات وذلك بالإضافة إلى المادة 394 مكرر 03 التي تنص على: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة القانون العام، دون إخلال بتطبيق عقوبات أشد"[4].

---

[1]– المرجع نفسه، صص 198–199.

[2]– صغير يوسف، الجريمة المرتكبة عبر الانترنيت، مذكرة لنيل شهادة الماجستير، في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013، ص 57.

[3]– سوير سفيان، المرجع السابق، ص 38.

[4]– الأمر 04–15، مؤرخ في 10 نوفمبر 2004، المعدل والمتمم الأمر رقم 66–156 الصادر في 8 جوان 1966، المتضمن قانون العقوبات، ج، ر، العدد 71.

الفرع الثاني

الجريمة الإلكترونية الواقعة على النظام المعلوماتي

تعتبر هذه الصورة بدون شك أكثر الصور خطورة وانتشارا حيث يتم بواسطة الاحتيال إدخال معطيات في نظم المعالجة الآلية للمعطيات أو إتلافها أو حذفها أو تغيير المعطيات المدرجة فيها[1].

وقد عالج المشرع الجزائري هذا النمط من الجرائم من خلال القانون رقم 04-15 الصادر في 10 نوفمبر 2004، المتضمن قانون العقوبات، وذلك بتجريم كل أنواع الاعتداءات التي تمس بالأنظمة المعالجة الآلية للمعطيات، وقد ورد نص التجريم في القسم السابع مكرر من قانون العقوبات، وذلك بعنوان المساس بأنظمة المعالجة الآلية للمعطيات ذلك في المواد 394 مكرر إلى 394 مكرر07، فالإعتداء يأخذ صورتين هما: الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية وأفعال إجرامية أخرى، وهذا ما سنتناوله فيما يلي:

أولا: جريمة الدخول أو البقاء في منظومة معلوماتية

إن قانون العقوبات الجزائري من القوانين العربية السباقة إلى دراسة هذا الموضوع، خطى المشرع الجزائري هذه الخطوة بتعديل قانون العقوبات، وذلك بإضافة القسم السابع مكرر. بمحتوى المواد 394 مكرر إلى 394 مكرر 7، وقد نصت المادة 394 مكرر منه على ما يلي: (يعاقب بالحبس من ثلاث (3) أشهر إلى سنة (1) وبغرامة من 50000دج إلى 100000دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك)[2].

---

[1]- سومية عكور، الجرائم المعلوماتية وطرق مواجهتها قراءة في المشهد القانون والأمني، المتلقى العلمي "حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية"، كلية العلوم الاستراتيجية، الأردن، 02-04-09-2016، ص 12.

[2]- زبيدة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص 46.

فالملاحظ على هذا النوع من الجرائم، أنها ليست من الجرائم التي يطلق عليها جرائم ذو الصفة، مثل الرشوة أو الاختلاس أو الزنا. بل تقع وترتكب عن كل شخص أي كانت صفته سواء كان يعمل في مجال الأنظمة أم لا، سواء كان يفهم أم لا طريقة تشغيل النظام، وسواء كان يستطيع أن يستفيد من الدخول أم لا[1].

1. فعل الدخول إلى النظام

أن مدلول كلمة الدخول تنصرف إلى كل الأفعال التي تسمح بالولوج إلى النظام المعلوماتي، أو السيطرة على المعطيات والمعلومات التي يتكون منها[2]، لم يحدد المشرع الوسيلة التي يتم بها الدخول إلى النظام، ولذلك تقع الجريمة بأية وسيلة أو طريقة، فقد يلجأ الجاني إلى التلاعب بعناصر النظام المادي لكي يصل إلى هدفه وهو الدخول أو يربط بجهاز تنصت يستطيع من خلاله اختراق النظام واستقبال المعلومات، كما قد يكون عن طريق فيروس مثل (فيروس حصان طروادة)[3] أو عن طريق استخدام أرقام سرية لشخص أخر أو عن طريق تجاوز نظام الحماية، ويتم بطرق غير مباشرة أم مباشرة، كما هو الحال في الدخول عن بعد من خلال شبكات الهاتف النقال ويكون الدخول غير مشروع مثال ذلك الأنظمة المتعلقة بأسرار الدولة أو دفاعتها وكذلك إذا كانت فعل يتطلب الدخول إليه دفع المال، وتم الدخول إليه دون دفع المال.

ففعل دخوليتسع ليشمل كل فنيات الدخول الاحتيالية في منظومة محمية كانت أو غير محمية، كما يشمل استعمال من لاحق في ذلك المفتاح للدخول إلى المنظومة.

1– قورة نائلة، جرائم الحاسب الاقتصادية، دار النهضة العربية، القاهرة، 2004، ص 343.

2– محمد حماد مرهج الهيبتي، جرائم الحاسوب، دار المناهج للنشر والتوزيع، عمان، 2005، ص 183.

3– فيروس حصانة طروادة، وهو برنامج فيروس لديه قدرة على الاختفاء في البرنامج الأصلي للمستخدم، وعندما يتم تشغيل البرنامج الأصلي ينشط هذا الفيروس وينتشر ليبدأ في نشاط التدمير، وهو ما يؤدي إلى تعطيل البرنامج وتزويد المعلومات ومحو بعضها وقد يصل إلى تدمير النظام بأكمله.

2. فعل البقاء داخل النظام

هو كل تواجد غير عادي داخل نظام المعالجة الآلية للمعطيات ضد إدارة من له حق في السيطرة على هذا النظام، أي الدخول والنظر فيه وفي المعطيات التي يتضمنها وغيرها من التصرفات الغير المسموح بها والتي تشكل بدورها بقاء احتياليا[1].

يتحقق الركن المادي لهذه الجريمة في الحالة التي يجد فيها الشخص نفسه داخل النظام المعلوماتي عن طريق الخطأ أو الصدفة إلا أنه يقرر البقاء، داخل النظام وعدم قطع الاتصال به ويمكن تصور ذلك في الحالة التي يكون فيها الشخص يريد الدخول إلى نظام معلوماتي له الحق في الدخول إليه إلا أنه يجد نفسه لسبب ما دخل نظام أخر، كما لا يشترط لقيام هذه الجريمة حدوث نتيجة جرمية معينة، فيكفي البقاء غير المصرح به داخل النظام المعلوماتي ليقوم الركن المادي[2].

أما الركن المعنوي لا يتوفر متى كان دخول الجاني أو بقاءه داخل النظام مسموح به أي مشروعا، كما يمكن أن تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يجرم البقاء حتى ولو حصل الدخول بصفة عرضة[3].

ثانيا: جريمة المساس بمنظومة معلوماتية

جرم المشرع الجزائري كل فعل يهدف إلى إعاقة أو تحريف أو إفساد تشغيل نظام معالجة البيانات وذلك في نص المادة 394 مكرر 01 قانون العقوبات رقم 15/04 ويشرط بالإضافة إلى فعل الدخول للنظام أو البقاء فيه، إحداث استمرار في تخريب نظام تشغيل معالجة المعطيات،

---

[1]– عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنيت، دار الكتب، القاهرة، 2002، ص 235.

[2]– نهلا عبد القادر المومني، مرجع سابق، ص 161.

[3]– حمزة بن عقون، مرجع سابق، ص ص 183–184.

سواء بتعطيله، بإفسادهأو وتغيبه، ويكون ذلك بأية طريقة تكن، سواء بالإعاقة المادية كإتيان أعمال عنف على أجهزة، الحاسوب، أو بالإعاقة المعنوية كإدخال فيروس على البرامج[1].

كما أن المشرع لميشترط اجتماع هذه الصور بل يكتفي أن يصدر من الجاني إحداهما فقط لكي يتوافر الركن المادي.

تجدر الإشارة إلى أن المشرع الجزائري جرم كل من الاشتراك والشروع في ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وجعل العقوبة لها تساوي العقوبات المقررة للجريمة ذاتها.

ثالثا: أفعال إجرامية أخرى

جرمت المادة 394 مكرر 2 من قانون العقوبات الأفعال التالية: تصميم أو بحث أو تجميع أو الاتجار أو توفير أو استعمال أو نشر في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية، يمكن أن ترتكب بها إحدى جرائم الغش المعلوماتي السابق الذكر[2].

يقصد بفعل التوفير ومفاد ذلك تقديم المعطيات لمن يريدها وجعلها في متناول الجميع إلى جانب فعل التوفير نجد النشر المتمثل في إذاعة المعطيات محل الجريمة ويعتبر هذا السلوك خطيرا جدا كونه ينقل المعطيات إلى عدد كبير الأشخاص مما يزيد احتمال وقوع الجريمة، كما جرمت المادة سالفة الذكر فعل الاتجار بمعطيات لها علاقة بالجرائم الماسة بنظام المعالجة الآلية للمعطيات، ويتم ذلك عن طريق تقديمها للغير.

[1]– حمودي ناصر، "التنظيم القانوني لظاهرة المعلوماتية في الجزائر الانجازات والتحديات"، المجلة النقدية للقانون والعلوم السياسية، عدد2، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012، ص 210.

[2]– حمزة بن عقون، مرجع سابق، ص 184.

ويشترط للعقاب على هذه الأفعال أن تقع على معطيات مخزنة داخل أقراص أو ما شابه، أو معالجة في نظام للمعالجة أو مرسلة عن طريق إحدى المنظومات المعلوماتية، مع إمكانية أن ترتكب بهذه المعطيات جرائم بها هذه الجرائم فلا تقوم الجريمة[1].

قد يقوم الجاني بإستعمال هذه المعطيات ويشمل للتجريم كل استعمال للمعطيات السالفة الذكر مهما كان الهدف منها، ومثال ذلك قيام شركة ما بإستعمال معلومات أو معطيات متحصل عليها بطريقة غير شرعية بإحدى الجرائم المذكورة، آنفا تتعلق بشركة منافسة للإضرار به[2].

[1]– الهادي حضراوي، تجربة الجزائرفي مكافحة الجريمة الالكترونية، المؤتمر الدولي لمكافحة الجرائم المعلوماتية ICACC، كلية علوم الحاسب والمعلومات، جامعة الإمام محمد بن سعود الإسلامية، السعودية، 2015، ص 161.

[2]– نفس المرجع، ص ص 161، 162.

الفصل الثاني

آليات مكافحة الجريمة الالكترونية والحد منها في القانون الجزائري

بعد أن تطرقنا في الفصل الأول إلى ماهية الجريمة الإلكترونية من خلال تقديم تعريفها وأنواعها والدوافع لارتكابها، نتعرض في الفصل الثاني إلى بيان كيفية مكافحة الجريمة الإلكترونية وذلك من طرف المشرع الجزائري، وذلك عن طريق ما أقره المشرع من وسائل قانونية وقضائية لمكافحة هذه الجريمة بإصداره قوانين عامة وخاصة وهياكل وأجهزة للتصدى للجرائم الإلكترونية وتوفير الحماية للأنظمة المعلوماتية ومستخدميها، وذلك من خلال مختلف النصوص التشريعية خاصة المستحدثة منها والتي تناولت الجريمة المعلوماتية، وهذا سوف يتم توضحه .

المبحث الأول

القواعد الموضوعية لمكافحة الجريمة الإلكترونية

أمام صعوبة تتبع والكشف عن الجرائم المعلوماتية التي تعرف على أنها كل فعل أو امتناع من شأنه الإعتداء، على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة في تدخل التقنية المعلوماتية، وأمام قصور القواعد التقليدية في التصدى لهذه الجريمة التي باتت في تطور سريع مسايرة التطور المعلوماتي، فكان لابد من المشرع الجزائري التدخل بنصوص آمرة لتجريم هذه الظاهرة من جهة وإصدار قوانين خاصة تتلائم مع طبيعة الجريمة ومستلزمات المكافحة التي تستدعي التعاون بين الجهات القانونية والمتخصص في المعلوماتية زيادة على التعاون الدولي.

وعليه سنتناول في المطلب الأول الحماية الجزائية المعلوماتية من خلال نصوص قانون العقوبات وفي المطلب الثاني الحماية الجزائية للمعلوماتية من خلال القوانين والتنظيمات الأخرى.

المطلب الأول

الحماية الجزائية للمعلوماتية من خلال نصوص قانون العقوبات

لم تعرف الجزائر قبل 2004 قوانين تطبق على الأنظمة المعلوماتية لكن أمام التزايد السريع للمعلوماتية والإجرام خاصة، كانت لابد على المشرع الجزائري من إيجاد الإطار القانوني المناسب الذي يمنع هذا الإعتداء ولسد الفراغ القانوني و الإقتداء بأغلب دول العالم لذا قام بإصدار قوانين

معدلة ومتممة لقانون العقوبات تارة واصدار قوانين خاصة أهمها القانون رقم 09-04 المؤرخ المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته(1) في نصوص متعلقة بجرائم الأموال المقررة في قانون العقوبات.

الفرع الأول

الحماية الجزائية للمعلوماتية من خلال نصوص جرائم

الأموال المقررة في قانون العقوبات الجزائري

إن التطور المعلوماتي واستخداماته المتعددة أدى إلى ظهور مشاكل مستحدثة وهذا ما يسمى بأزمة القانون الجنائي أي عدم القدرة على مواجهة الواقع المعلوماتي لذلك فرض البحث في مدى ملائمة الأوضاع القانونية في التصدي لهذه المشاكل، بإعتبارها تهتم بالجانب المادي المعلوماتي، من هنا يجب البحث عن مدى امكانية القاضي الإستعانة بقانون العقوبات لتوفير الحماية لهذه القيمة الإقتصادية الجديدة ألا وهي أموال الإعلام في ظل النصوص التقليدية، وهل يستطيع هذا الأخير من خلال النصوص الحالية لجرائم الأموال تحقيق حماية جزائية معلوماتية دون الإطاحة بالمبادئ الراسخة التي يرتكز عليها القانون الجنائي؟ ولهذا الغرض قررنا التركيز على نقطتين أساسيتين وهما:

أولا- مدى اعتبار المعلوماتية موضوع لجرائم الأموال

ثانيا- مدى خضوع المعلوماتية للنشاط الإجرامي من الجرائم الأموال

أولا: مدى اعتبار المعلوماتية موضوع لجرائم الأموال

لمعرفة مدى امكانية اخضاع الاعتداءات الواردة على أموال الإعلام الألي للنصوص التقليدية لجرائم الأموال وجب أولا تحديد ما يلي:

1- مدى انطباق وصف المال على المعلوماتية

نعني بالمال المعلوماتي للحاسوب كل مكوناته والذي هو عبارة عن مجموعة من الكيانات التي تسمح بدخول المعلومات وتخزينها ومعالجتها وإعادة استرجاعها عند الحاجة إليها وهو يتكون من كيانين هما:

الكيان المادي الذي يشتمل على الأجهزة المادية المختلفة ومن بينها جهاز الإدخال وجهاز الإخراج ووحدات التشغيل المركزية التي يتم من خلالها معالجة المعلوماتية وتخزينها و إخراجها، أما فيما يخص الكيان المعنوي فيضم كل البرامج المختلفة التي تتحقق من خلالها قيام الحاسب بوظائف مختلفة بالإضافة إلى المعلومات المطلوب معالجتها بالفعل[1].

فإذا كانت الأجهزة المادية للحواسيب لا تحتاج إلى نصوص خاصة لحمايتها جزائيا، فهذا الأمر يختلف بالنسبة للكيان المعنوي لتلك الحواسيب. الأن في جرائم الاعتداء على الأموال يجب عادة أن يكون موضوعها شيئا ماديا، وطبيعة الكيان المعنوي ليست مادية، وعليه ما يجب التساؤل عنه حول مدى اعتبار الكيان المعنوي للحاسوب مالا [2].

يعتبر المال كل ما يصلح أن يكون محلا لحق ذو قيمة مالية، ويعتبر الشيء هو محل الحق، وتقسم هذه الأشياء إلى أشياء مادية وآخرى معنوية، وبما أن الأموال بالنسبة النصوص التقليدية لا ترد على الأشياء ولهذا فقد تم تعريف المال بصدد جرائم الأموال على أنه: "كل شيء مادي يصلح لأن يكون محلا لحق من الحقوق المالية"[3].

لكن مع التطور إزدادت الأشياء المعنوية عددا وتفوق بعضها من حيث قيمتها على الأشياء المادية هذا ما استدعى البحث لإيجاد معيار أخر الذي يرد عليه الحق المالي غير طبيعة الشيء حتى يمكن إسباغ صفة الشيء المعنوي.

---

[1]- محمد فتحي عبد الهادي، مقدمة في علم المعلومات، مكتبة عزيب، القاهرة، 1984، ص 217.

[2]- أمال قورة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، مرجع سابق، ص 12.

[3]- أحمد عبد الرزاق السنهوري، الوسيط في شرح القانون المدني، حق الملكية، الجزء الثاني، دار أحياء التراث العربي، بيروت، 1952، ص 09.

ومن بين هذه الأشياء المعنوية ذات القيمة الاقتصادية العالية برامج الحاسب الألي، تكون هذه البرامج مثبتة على دعامة أو حامل مثال ذلك الأقراص أو الشرائط الممغنطة من البلاستيك أو الورق المقوى وغيرها.

فيعتبر البرنامج المستقل عن دعامته في أنه شيء معنوي وبالتالي لا يصدق عليه وصف المال، أما إذا سجل البرنامج أو نقش على دعامته فإن تلك الدعامة بما عليها من برامج تصلح لأن تكون محلا لجرائم الأموال على الرغم من أن الدعامة منفصلة عن البرامج تعتبر ضئيلة القيمة إذ ما قيست بقيمة البرامج وعلى الرغم أيضا من أن الإعتداء عليها ليس في غاية في ذاته، وإنما الباعث على ذلك هو البرنامج نفسه لا دعامته ومع ذلك لا تأثير لهذه البواعث في القانون الجنائي[1].

2- مدى اعتبار المعلوماتية مالا بصدد جرائم الأموال

أ- مدى اعتبار البرنامج كمحل لجريمة السرقة

نبدأ أولا في دراسة مدى اعتبار البرنامج مالا بصدد جريمة السرقة هذا ما ذهبت إليه المادة 350 من قانون العقوبات الجزائري على أنه " **كل من إختلس شيئا غير مملوك له يعد سارقا**" فالمادة 350 لم تشترط ضرورة أن يكون المال موضوع للجريمة ماديا مما يجعل وقوع جريمة السرقة على مال معنوي أمر لا يصطدم بمبدأ شرعية الجرائم والعقوبات، ولكن يبقى اعتبار البرنامج كمحل للسرقة غير قطعي ومن باب الإمكان لا غير.

ب- مدى اعتبار البرامج كمحل لجريمة النصب

حسب المادة 372 من قانون العقوبات فإن: "كل من توصل إلى إستلام أو تلقى أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية ووعود أو مخالصات أو إبراء من إلتزامات أو الحصول على أي منها أو الشرع وكان ذلك بالإحتيال لسلب كل ثروة الغير أو بعضها أو الشروع

[1]- د. علي عبد الله القهوجي، الحماية الجنائية لبرامج الحاسب الألي، مرجع سابق الذكر، ص 7.

فيه إما بإستعمل أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي أو بإحداث الأمل في الفور بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع الشيء منها يعاقب بالحبس من سنة على الأقل إلى خمس سنوات على الأكثر بغرامة من 20.000 إلى 100.000دج.

ما يمكن استنتاجه من نص هذه المادة أنه ليس كل شيء مادي ومنقول يصلح أن يكون محلا لجريمة النصب بل يجب أن يكون ضمن الأشياء التي حصرتها المادة 372.

فالنص على المنقول في هذه المادة ورد دون تحديد طبيعته ودون أن يقيده المشرع بأن يكون ماديا هذا ما يسمح بإدخال برامج الحاسوب ضمن الأشياء التي تقع عليها جريمة النصب[1].

ج- مدى اعتبار البرنامج كمحل لجريمة خيانة الأمانة

طبقا للمادة 376 من قانون العقوبات "كل من اختلس أو بدد بسوء نية أوراقا تجارية أو نقودا أو بضائع أو أوراقا مالية أو مخالصات أو أية محررات أخرى تتضمن أو تثبت إلتزاما أو إبراء لم تكن قد سلمت إليه على سبيل الإجازة أو الوديعة أو الوكالة أو الرهن أو عارية الإستعمال أو لأداء عمل بأجر أو بغير أجر يشرط ردها أو تقديمها أو لإستعمالها أو لإستخدامها في عمل معين وذلك إضرار بمالكيها أو واضعي إليه اليد عليها أو حائزيها يعد مرتكبا لجريمة خيانة الأمانة...".

وما يمكن استنتاجه من هذا النص أن الإختلاس يقع على الأموال المنقولة سلمت إلى الجاني وذلك بعقد من عقود الأمانة، وعليه لا تقع جريمة خيانة الأمانة على غير المنقولات المادية، كما حددت المادة الأشياء التي تصلح محلا لهذه الجريمة وهي مذكورة على سبيل الحصر هي الأوراق التجارية، النقود أو أوراقا مالية، مخالصات، محررات تتضمن أو تثبت التزاما أو إبراء وعليه فإن اخضاع الاعتداءات الواردة على المال المعلوماتي إلى نصوص للأمانة يثير بعض

[1]- فشار عطاء الله، "مواجهة الجريمة المعلوماتية في التشريع الجزائري"، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، المنعقد بأكاديمية الدراسات العليا ب ليبيا في أكتوبر 2009، ص 5-6.

المشاكل القانونية وذلك لطبيعة الغير المادية للقيم المعلوماتية وعليه فإن تطبيق نصوص خيانة الأمانة في مجال المعلوماتية يكون في نطاق محدد ومن باب الإمكان لا غير[1].

د- مدى اعتبار البرنامج كمحل لجريمة الاتلاف

فحسبما نصت عليه المادة 407 من قانون العقوبات الجزائري "كل من خرب أو أتلف عمدا أموال غير المنصوص عليها في المادة 396 بأية وسيلة أخرى أو جزئيا يعاقب بالحبس من سنتين إلى خمس سنوات وبغرامة 500 إلى 5000دج".

كما تنص المادة 412 من قانون العقوبات الجزائري "كل من أتلف عمدا بضائع أو مواد أو محركات أو أجهزة أيا كانت مستعملة في الصناعية وذلك بواسطة مواد من شأنها الإتلاف أو بأية وسيلة أخرى يعاقب بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من 500دج إلى 5000دج". بالرجوع إلى نص المادة 412 نجدها قد حددت الأشياء الخاضعة للإتلاف وبالتالي فإنها تشمل المكونات المادية للحاسوب سواء بوصفها أجهزة أو بضائع.

ثانيا: مدى خضوع المعلوماتية للنشاط الإجرامي في جرائم الأموال

ما يجب البحث عنه حول مدى خضوع برامج الحاسب الآلي أو المعلومات بصفة عامة للسلوك الإجرامي الذي يتحقق به الركن المادي في جرائم السرقة والنص وخيانة الأمانة والإتلاف.

1- مدى خضوع المعلوماتية للنشاط الإجرامي في جريمة السرقة

إن النشاط الاجرامي المكون للسرقة هو الإختلاس، فنلاحظ أن الجاني وإن كان يدخل في ذمته ما استولى عليه من برامج إلا أنه في نفس الوقت تخرج هذه البرامج من ذمة صاحبها الشرعي إذ تظل رغم مباشرة الاختلاس تحت سيطرة هذا الأخير دون إنقاص من محتواها، ما

[1]- فشار عطاء الله، مرجع سابق، ص 6.

يمكن ملاحظته أن الإستلاء على البرامج بإعتبارها معلومات لا يتصور من الوهلة الأولى إلا إذا انتقلت هذه المعلومات ذهن أو من الحرة إلى ذاكرة[1].

كما يلاحظ أيضا أن المعلومات التي تحتويها البرامج من طبيعة غير مادية أي أنها شيء معنوي فلا يمكن تصور فعل الإختلاس على شيء معنوي وهذه تعتبر عقبة ثالثة، فحسب هذه العقبات فليس من السهل بسط أحكام السرقة على برامج الحاسب الآلي وخاصة في الحالات الأتية.

أ- سرقة المعلومات عن طريق النسخ غير المشروع للبيانات المخزنة إلكترونيا

ويتم ذلك بإعادة إنتاج الوثيقة أو الدعامة التي تحتويها، ولشرح حالات النسخ غير المشروع يمكننا الإعتماد إلى الإجتهاد القضائي الفرنسي وذلك عن طريق إعلانه أن المعلومات التي نسخت أو أعيد إنتاجها هي التي سرقت، لذلك حافظ على مبدأ مادية الاختلاس وعلاوة على ذلك فإن قرار الحكم بإختلاس المعلومات عن طريق إعادة إنتاج المستند الذي يحصر بها يحمل في طياتة ثروة مستمرة، ولكنها عميقة لأنها تسمح بالعقاب على إعادة الإنتاج الذي لا يمكن أن يقع تحت طائلة الجريمة التقليدية.

فهناك اختلاف بين جريمة سرقة المعلومات عن طريق النسخ غير المشروعة وبين الجريمة التقليدية لأن السرقة تحتوي على بيانات في ذاتها بينما الحماية التي يكيفها المشرع للمصنفات بتجريم تقليدها على طريقة التعبير عن أفكار المؤلف[2].

ب- سرقة وقت الآلة

يكيفها فقهاء القانون الجنائي على أنها سرقة، وفي هذه الحالة ليس من السهل بسط أحكام جريمة السرقة على وقت الآلة لذلك فالمشرع الجزائري يأخذ بما يسمى سرقة الخدمة وعليه تتطلب تدخلا تشريعيا على غرار ما فعل المشرع الفرنسي بتجريمه البقاء غير المشروع في نظام معالجة الألية

[1]- د. علي القادر القهوجي، مرجع سابق، ص 95.

[2]- أمال قورة، مرجع سابق، ص 26.

للمعطيات فإذا كانت هذه الجريمة تهدف أساسا إلى حماية نظام المعالجة الألية للمعطيات بصورة مباشرة إلا أنها تحقق أيضا وبصورة غير مباشرة حماية للمعلومات ذاتها.

ج- الإلتقاط الذهني للبيانات

وذلك بأن يقوم شخص بإلتقاط معلومات ظهرت على شاشة الحاسوب وقام بذلك بتخزينها وحفظها في ذاكرته، فهذا الفعل يمكن أن يكون إختلاسا رغم أنه يرد على ذات المادة المستند وإنما اقتصر الشيء المختلس على مضمون المستند مع بقائه في حيازة صاحبه، الأن هذا المضمون شيء منقول مملوك للغير، إلا أن المشرع الجزائري لا يأخذ بسرقة الإستعمال وعليه ضرورة تدخل تشريعي يشمل حالتي الالتقاط الذهني وحالة سرقة المعطياتدون استنساخها ودون المساس بسلامتها وأصالتها [1].

د- تكييف الإلتقاط الهوائي للبيانات المعالجة أو المنقولة إلكترونيا

أن الطاقة والقوة الطبيعية أو الصناعية تعد من الأموال المنقولة وتصلح لأن تكون محلا للسرقة إلا أنه لا يمكننا أن نطبق أحكام سرقة الطاقة على الإشعاعات والموجات والنبضات المنبعثة من الحواسيب الآلية أثناء تشغيلها رغم أنها كهربائية قابلة للقياس والتقدير الكمي.

فما يمكن ملاحظته عدم وقوع السرقة في الحالات السابقة لأن طبيعة هذه البرامج لا تحقق الأخذ و الإختلاس بمعناه الدقيق في جريمة السرقة والذي يعني الإستلاء على الحيازة الكاملة لشيء بدون رضا صاحبها أو حائزه السابق لأنه إذا تصورنا وقوع الإختلاس من خلال النسخ والتصوير على المعلومات الأصلية ذاتها تظل في نفس الوقت كما كانت من قبل تحت سيطرة صاحبها الأصلي ولا تخرج من حيازته، لما كان قانون العقوبات الجزائري لا يجرم سرقة الإستعمال بصفة عامة، فإن الحل الوحيد لا يكون إلا بتدخل صريح من هذا الأخير، لتفادي الجدال موضوع سرقة المعلومات وقت الآلة أو سرقة، استعمال الأصل وتحقق الحماية للبرامج المعلوماتية.

[1]- المرجع نفسه، ص 23.

2- مدى خضوع برامج الحاسب الآلي للنشاط الإجرامي في جرائم النصب وخيانة الامانة

أ- بتطبيق النشاط الإجرامي لجريمة النصب في المجال المعلوماتي

إن لجوء الجاني إلى إحدى الطرق الإحتيالية وحمل الجاني عليه على تسليمة دعامة مادية مثبة عليها أحد البرامج ثم استلاء الجاني عليها فإن النشاط الإجرامي في هذه الحالة يتحقق، لكن الأمر الذي يطرح إشكال هو هل يمكن تصور أن يتحقق النشاط الإجرامي في جريمة النصب من خلال الطرق الإحتيالية التي يقوم بها الجاني والتي يترتب عليها توقيع المجني عليه في غلط الذي يتم من خلاله نقل محتويات برامجه شفويا والتي يلتقطها الجاني ويحفظها في ذاكرته؟ وهل النقل حسب المادة 376 يعادل التسليم بناء على الغلط في قانون العقوبات؟ وهل الإلتقاط أو سماع الجاني للمعلومات يعادل الإستلاء؟

لا وجود لنشاط مادي يتحقق به التسليم والإستلام في جريمة النصب، ولو فرضنا إمكانية وقوع التسليم فإنه لن ينتج عن ذلك حرمان المجني عليه من المعلومات التي نقلها بالقول بل تظل تحت سيطرة من نقلها، إلا أنه لا يتفق هذا مع طبيعة النشاط الإجرامي في جريمة النصب وهذا يعني عدم صلاحية البرامج للخضوع للنشاط الإجرامي في جريمة النصب[1].

ب- بتطبيق النشاط الإجرامي لجريمة خيانة الأمانة في المجال المعلوماتي

لا جدال في وقوع جريمة خيانة الأمانة بالنسبة للدعامات المثبتة عليها البرامج والمعلومات وذلك في الحالة التي يقوم فيها الأمين بنسخ البرامج لحسابه متجاوز الاتفاق الذي يربطه مع صاحب البرنامج إذ يتحقق هذا النسخ فعل الإستعمال والذي يقصد به إستخدام الأمين مال إستخداما يستنزف قيمته كلها أو بعضها من بقاء المادة على حالها، وهذا يصعب قيام جريمة الأمانة في حالة البرامج والمعلومات المستقلة عن الدعامة وذلك لعدم قيام النشاط الإجرامي وهو

[1]- فشار عطاء الله، مرجع سابق، ص 10.

التسليم بناء على عقد الأمانة لعدم وجود النشاط المادي مجسم به يتحقق فعل الإستلام، مما يحول دون صلاحية البرامج والمعلومات للخضوع للنشاط الإجرامي في جريمة خيانة الأمانة[1].

ج- بتطبيق النشاط الإجرامي لجريمة الإتلاف في المجال المعلوماتي

نجد المشرع الجزائري لا يقيد النشاط الإجرامي في جريمة الإتلاف بوسيلة معينة إذ هي من الجرائم ذات القالب الحر ولهذا لا يوجد ما يحول دون لوقوع جريمة الإتلاف على برامج الحاسب الآلي خاصة وأن المشرع الجزائري لم يحدد طريقة بعينها لقوع الجريمة ولم يحدد نتيجة وحيدة محددة لقيامها، فإنه من المتصور أن يتجه الجاني بنشاطه الإجرامي إلى البرامج والدعاية المسجل عليهما معا، أو إلى البرامج فقط دون الدعامة وقد تقع الجريمة عن طريق الإتصال المباشر بالجهاز كما قد تقع من خلال الإتصال عن بعد.

وعليه فإن جريمة الإتلاف المنصوص عليها في قانون العقوبات تحقق حماية جنائية كاملة لبرامج الحاسب الألي على خلاف جرائم الأموال التي توفر حماية نسبية[2].

الفرع الثاني

الحماية الجزائية الإلكترونية من خلال النصوص المتعلقة

بجرائم المساس بأنظمة المعالجة الألية للمعطيات

تدارك المشرع الجزائري الفراغ القانوني في مجال الإجرامي المعلوماتي وذلك ما أدى به إلى استحداث نصوص تجريمية لقمع الإعتداءات الواردة على لمعلوماتية، وذلك بموجب القانون رقم 05 -15 المتضمن تعديل قانون العقوبات، لكن المشرع الجزائري ركز على الإعتداءات الماسة بالأنظمة المعلوماتية، وأغفل الإعتداءات التي تخص المنتوجات الإعلام الألي والمتمثلة في التزوير المعلوماتي.

[1]- أمال قورة، المرجع نفسه، ص 45-60.

[2]- فشار عطاء الله، مرجع سابق، ص 10.

نص المشرع الجزائري من خلال القانون رقم 04-15 على العقوبات المقرر للجرائم التي تمس الأنظمة المعلوماتية وهي كما يلي:

أولا: العقوبات المقررة لشخص الطبيعي

أ- العقوبات الأصلية

نص المشرع الجزائري في القانون رقم 04-15 على عقوبات أصلية لجريمتي الدخول البقاء غير المشروعان للنظام المعلوماتي وكذا جريمة المساس بمنظومة معلوماتية وفق الأتي:

-عقوبة الدخول أو البقاء غير المشروعان للنظام

في حالة الدخول غير المشروع من طرف المجرم المعلوماتي للنظام كله أو جزء منه أو متى كان مسموح له الدخول إلى جزء معين من ذلك النظام وتجاوزه، ومتى كان دخوله لنظام مخالف لإدارة صاحب ذلك النظام، تكون العقوبة المقررة في هذا الشأن الحبس من ثلاثة أشهر إلى سنة وغرامة مالية تقدر بقيمة 50.000دج إلى 100.000دج وذلك طبقا للمادة 394 مكرر من قانون العقوبات رقم 15/04.

إن العقوبة تضاعف في حالة إذا ترتب عن هذه الأفعال تغيير أو حذف لمعطيات منظومة معلوماتية مما يشكل ظرفا مشددا، وتكون العقوبة بالحبس من ستة أشهر إلى سنتين وغرامة من 50.000دج إلى 150.000دج، وذلك وفقا للمادة 394 مكرر من قانون العقوبات السابق الذكر.

-عقوبة المساس بمنظومة معلوماتية

نص المشرع الجزائري في المادة 394 مكرر 01 من قانون العقوبات على عقوبة الإعتداء العمدي على المعطيات الموجودة داخل النظام، وذلك بالحبس من 06 أشهر إلى 03 سنوات وغرامة من 500.000دج إلى 2.000.000دج، وذلك في حالة ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وفي حالة حيازة وإفشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى

الجرائم الماسة بالأنظمة المعلوماتية تكون العقوبة بالحبس من شهرين إلى 03 سنوات وغرامة من 1.000.000دج إلى 5.000.000 دج[1].

ثانيا: العقوبات المقررة للشخص المعنوي

لقد نص المشرع الجزائري في المادة 51 مكرر من القانون العقوبات بعد تعديله بموجب القانون 04-15 على موضوع الشخص المعنوي فيما يخص ارتكابه لهذه الجرائم وذلك وفقا لشروط منها:

- أن ترتكب إحدى الجرائم المنصوص عليها قانون أن تكون بواسطة أحد أعضاء أو ممثلي الشخص المعنوي، أن ترتكب الجريمة لحساب الشخص المعنوي. كما نصت المادة 394 مكرر 04 من نفس القانون على العقوبات الواجبة على الشخص المعنوي في حالة ارتكابه لأي جريمة إعتداء على نظام المعالجة الألية للمعطيات وبغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[2].

ثالثا: عقوبة الاشتراك والشروع في الجريمة

أ- عقوبة الاشتراك

نصت المادة 394 مكرر أن عليه من القانون العقوبات على أنه: "كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، وكان هذا التحضير مجسدا بفعل أو عدّة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها".

[1]- ختير مسعود، الحماية الجنائية لبرامج الكومبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر، 2010، ص 99-100.

[2]- المرجع نفسه، ص 100-101.

ب- عقوبة الشروع

نصت عليها المادة 394 مكرر 07 من القانون العقوبات على أنه" يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقرر للجنحة ذاتها".

رابعا: العقوبات التكميلية

لقد نصت المادة 394 مكرر 07 من نفس القانون على مجموعة من العقوبات التكميلية يعتمد عليها في حكمه إلى جانب العقوبات الأصلية وهي كالتالي:

المصادرة: تشتمل على الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية[1] مع مراعاة حقوق الغير حسن النية أي مصادرة الأجهزة وهذه البرامج التي إستخدمهاالإرتكاب هذه الجرائم.

إغلاق المواقع: تلك التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية[2]، أي إغلاق مواقع الأنترنيت أو الموقع الإلكتروني بصفة عامة التي كانت وسيلة لإرتكاب هذه الجرائم أو ساهمت في ارتكابها.

إغلاق المحل أو مكان الإستغلال: تكون في حالة إرتكاب الجريمة بعلم مالك المحل أو مكان الإستغلال كإغلاق مقهى إلكتروني.

ومن الملاحظ أن هذه العقوبات جاءت ردعية حيث تضاعف عند الضرورة، كما اشتملت على عقوبات تكميلية، وحتى عقوبات الشخص المعنوي.

[1]- صالح شنين: " الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري"، المجلة الأكاديمية للبحث القانوني، عدد 01، الجزائر، 2010، ص 74.

[2]- سوير سفيان، مرجع سابق، ص 99.

المطلب الثاني

الحماية الجزائية للجريمة الإلكترونية من خلال القوانين والتنظيمات الأخرى

نص المشرع الجزائري على بعض القوانين والتنظيمات من شأنها إضافة نوع من الحماية الجزائية للمعلوماتية، وذلك من خلال استحداث قواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية وهو ما سنفصله من خلال الفرع الأتي:

الفرع الأول

القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية

بإستقراء القانون الذي حدد القواعد العامة المتعلقة بالبريد والاتصالات لاحظنا أن هناك تسارع في مواكبة التطور الذي شهدته التشريعات العالمية مسايرة للتطور التكنولوجي، لذلك بات من السهولة إجراء التحويلات المالية عن طريق البريد الإلكتروني، ذلك ما نصت عليه المادة 87 منه، كما نصت المادة 84- 02 منه على استعمال حولات دفع عادية أو إلكترونية أو برقية، كما نصت المادة 105 من نفس القانون على احترام المراسلات[1]، وقد تناول المشرع في الفصل الثاني من القانون رقم 2000-03 المؤرخ في 5 أوت 2000[2]، تعريفات تتعلق بالمواصلات السلكية واللاسلكية منها الأمواج اللاسلكية واللاسلكية الشبكة الخاصة، والشبكة العامة وخدمة الهاتف وخدمة التلكس، والخدمات البريدية وأطرافها عن مرسل ومرسل إليه وغيرها من المصطلحات التي تم استعمالها في هذا القانون، كما تضمن الجرائم المعلوماتية والعقوبات وخصصت المواد 127 من إلى المادة 144 لنص على العقوبات للمقررة للجرائم المتعلقة بها ومن السلوكات المجرمة بنص هذا القانون نذكر ما يلي:

---

[1]- فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، مرجع سابق، ص131.

[2]- قانون رقم 2000-03 المؤرخ في أوت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالواصلات السلكية واللاسلكية، العدد 48، الصادر في 06 أوت 2000، (ملغي).

فتح وتحويل أو تخريب البريد أو انتهاك سرية المراسلات أو المساعدة على ارتكاب هذه الأفعال من قبل كل شخص يقوم بتقديم خدمة البريد السريع لدولة أو كل عون يعمل لديه وفي إطار ممارستهم لمهامهم، يعاقب من قام بهذه الأفعال بالحبس من شهرين إلى سنة وبغرامة من 50.000دج إلى 1.000.000دج أو بإحدى هاتين العقوبتين (المادة 127 فقرة 03).

فكل شخص يقوم بقطع عمدا كابل بحريا أو يسبب له تلفا قد يوقف المواصلات السلكية واللاسلكية كلياأو جزئيا، يعاقب بالحبس من 03 أشهر إلى 05 سنوات وبغرامة مالية 100.000دج إلى 1.000.000دج فحسب المادة 130 من القانون للسابق الذكر.

يعاقب بالحبس من سنة إلى سنتين وبغرامة من 100.000دج إلى 500.000دج أو بإحدى هاتين العقوبتين، كل من ينشئ أو يستغل شبكة عمومية للمواصلات السلكية واللاسلكية دون الرخص القانونية والمنصوص عليها[1].

إشهار بغرض بيع التجهيزات أو معدات للمواصلات السلكية واللاسلكية دون الحصول على الإعتماد المسبق (المادة 133 من القانون 03 -200).

[1]- فليح نور الدين، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في الحقوق تخصص القانون الجنائي، جامعة مولاي الطاهر، سعيدة، 2018-2019 ص106.

المبحث الثاني

القواعد الإجرائية لمكافحة الجرائم الإلكترونية

سعى المشرع الجزائري إلى التصدي لظاهرة الإجرام الإلكتروني وما يصاحبها من أثار وأضرار معتبرة على الأفراد وعلى مؤسسات الدولة من جهة، إذ نجد المشرع قام بإصدار نصوص قانونية لقمع الجريمة المعلوماتية وذلك بسبب التزايد للإعدادات على الأنظمة في الجريمة، كذا استعمال المنظومة المعلوماتية للأغراض إجرامية.

المطلب الأول

القواعد الإجرائية المنصوص عليها في قانون الإجراءات الجزائية

إن الطبيعة الخاصة للجرائم الإلكترونية لابد أن تنعكس على قانون الإجراءات الجزائية، الأمر الذي يتطلب على المجتمع المعلوماتي في مجال قانون الإجراءات الجزائية من إنشاء قواعد إجرائية حديثة إلى جانب القواعد الموضوعية ونظراً لإتسام هذه الجرائم الإلكترونية بصعوبة اكتشافها وإثباتها وتحتاج إلى خبرة فنية عالية للتعامل معها، فإن ذلك أثار العديد من المشكلات الإجرائية والتي جعلت القواعد الإجرائية التقليدية قاصرة في مواجهة تلك المشاكل، لهذا قام المشرع الجزائري بتعديل بعض القواعد الإجرائية لجعلها قادرة على مواجهة تلك المشاكل الإجرائية خاصة المتعلقة بالاختصاص المحلي وإجراءات البحث والتحري[1].

الفرع الأول

قواعد الاختصاص المحلي

إن الاختصاص المحلي هو ذلك المجال الإقليمي الذي يمارس فيه ضابط الشرطة القضائية مهامه في البحث والتحري عن الجريمة، ذلك في حدود الدائرة التي يباشر وظيفته وذلك يتعين أن

[1]– أحمد شوقي الشلفاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء 2، طبعة 5، ديوان المطبوعات الجامعية الجزائر، ص 159.

يكون في مكان وقوع الجريمة أو محل القبض على المتهم أو مكان إقامته[1]، حيث عالج المشرع الجزائري الاختصاص المحلي للجهات القضائية وذلك بتحديد لكل جهة قضائية مجالها الجغرافي الذي لا يجوز الخروج عنه، وقام بالاعتماد على عناصر تربط من الاختصاص الجهات القضائية بالنظر في الخصومة الجزائية وتتمثل في المجال الجغرافي هو مكان وقوع الجريمة أو إقامة المتهم أو القبض عليه، و نظرا لإعتبار أن الجريمة الإلكترونية جريمة عابرة للحدود فغالبا ما يكون الجاني في بلد والمجني عليه في بلد آخر، كما قد يحصل الضرر في بلد ثالث في الوقت نفسه، لهذا السبب نجد المشرع الجزائري قد أجرى بعض التعديلات المتعلقة بالاختصاص المحلي في الجريمة الإلكترونية بموجب القانون 22/06 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 155/66 المتضمن قانون الإجراءات الجزائية، لهذا سنتطرق في هذا الفرع إلى دراسة هذه القواعد.

أولاً: الاختصاص المحلي للنيابة العامة

وفقاً لنص المادة 37 من قانون الإجراءات الجزائية الجزائري فإنه يتحدد الاختصاص المحلي للنيابة بمكان وقوع الجريمة ومحل القبض أحد الأشخاص المشتبه في مساهمتهم في الجريمة أو القبض على هؤلاء الأشخاص حتى ولو تم القبض عليهم ليس لسبب أخر، وبالتالي فإن اختصاص وكيل الجمهورية لا يتعدى مكان وقوع الجريمة أو مكان القبض على الأشخاص المشتبه في مساهمتهم في الجريمة أو محل إقامة أحد هؤلاء الأشخاص، لما كانت الجريمة المعلوماتية جريمة قد ترتكب في مكان معين وتكون أثارها في مكان أخر، فإن المشرع الجزائري أجاز بتمديد الاختصاص المحلي لوكيل الجمهورية بموجب المادة 37 فقرة 2 من قانون الإجراءات الجزائية إلى دائرة الاختصاص المحاكم الأخرى مع ترك كيفية ترك تطبيق ذلك عن طريق التنظيم الذي سيحدد المحاكم التي يمتد إليها الاختصاص.

كما أن المشرع قضى في أحكام نص المادة 40 مكرر فقرة 2 من قانون الإجراءات الجزائية على أنه يتعين على ضابط الشرطة القضائية إخبار وكيل الجمهورية لدى المحكمة الكائن في

[1]- فليح نور الدين، مرجع سابق، ص ص107-108.

مكان الجريمة ويبلغونه بأصل ويستحسن بإجراءات البحث ويرسل هذا الأخير فوراً بنسخة ثانية إلى النائب العام لدى محكمة المجلس القضائي التابعة له المحكمة المختصة، والذي يطالب وفق المادة 40 مكرر فقرة 2 من قانون الإجراءات الجزائية التي تتعلق بإجراءات تحريك الدعوى العمومية أو مباشرتها أو رفعها بمجرد أن يتبين للنائب العام أن الجريمة ضمن المحكمة المختصة التابعة لها وهذا ما نصت عليه المادة 40 في الفقرة 03 من نفس القانون[1].

ثانياً: الاختصاص المحلي لقاضي التحقيق

الاختصاص المحلي لقاضي التحقيق يقصد به التحقيق في المجال الذي يباشر فيه قاضي التحقيق مهامه والذي يتحدد طبقاً للمادة 40 من قانون الإجراءات الجزائية بمكان وقوع الجريمة أو محل إقامة أحد هؤلاء الأشخاص المشتبه في مساهمتهم على اقترافها أو محل القبض على أحد من هؤلاء الأشخاص حتى ولو كان هذا القبض حصل لسبب أخر، غير أن المشرع الجزائري قام بإلغاء في التعديل الجديد الفقرة 2و3 من المادة 40 وأصبحت تنص الفقرة 2 على جواز تمديد الاختصاص لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، ونستخلص من هذا أن المشرع أجاز إمكانية تمديد الاختصاص المحلي لقاضي التحقيق في الجرائم المعلوماتية إلى دائرة اختصاص محاكم أخرى مع ترك كيفية تطبيق تلك الإجراءات لتنظيم الذي سيصدر بعد ذلك.

ثالثاً: الاختصاص المحلي لمحاكم الجنح

يتحدد الاختصاص المحلي للمحاكم الجنح طبقاً للمادة 329 من ق، إ، ج، ج، بمكان وقوع الجريمة أو محل إقامة أحد الأشخاص المتهمين أو شركائهم أو بمكان الذي في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو تم القبض لسبب أخر وبعد التعديل الصادر بموجب القانون 14/04، كما أضاف المشرع الجزائري فقرة أخرى أجاز فيها في حالة الجرائم الماسة بأنظمة

[1]–أمر رقم 66–155، مؤرخ في 18 جوان 1966، يتضمن قانون الإجراءات الجزائية، ج. ر. ج. ج. ر. ش، عدد 48، صادر في 11 جوان 1966، معدل ومتمم بموجب أمر رقم 15–02، مؤرخ في 23 جويلية 2015، ج. ر. ج. ج. د. ش، عدد 40، صادر في 23 جويلية 2015.

المعالجة الألية للمعطيات تمديد الاختصاص المحلي للمحاكم إلى اختصاص محاكم أخرى عن طريق التنظيم. وبالتالي فإن المشرع الجزائري أجاز في حالة ارتكاب جريمة من جرائم الماسة بأنظمة المعالجة الألية للمعطيات تمديد الاختصاص لوكيل الجمهورية واختصاص قاضي التحقيق واختصاص محاكم الجنح ولكنه ترك ذلك للتنظيم الذي سيصدر لاحقاً والذي يحدد تلك المحاكم الذي يمتد إليها الاختصاص وتطبيق القواعد المتعلقة بالدعوى العمومية والتحقيق والمحاكم أمام الجهات القضائية في المادة 40 مكرر[1]، والتي تم توسيع اختصاصها المحلي طبقاً للمواد 37، 40، 329 من ق. إ، ج، ج.

تعد مشكلة الاختصاص القضائي في الجريمة المعلوماتية من المشكلات التي تصعب الحصول على الدليل، ذلك أن هذه الجريمة قد ترتكب في مكان معين وتنتج أثارها في مكان أخر داخل الدولة أو خارجها، وإذا كانت مشكلة الإجراءات الجنائية في داخل إقليم الدولة تحل على أساس معيار القبض على المتهم أو محل إقامة أو مكان وقوع الجريمة، فأي مكان من هذه الأماكن ينعقد الاختصاص الجنائي لسلطات التحقيق والمحاكمة في الجريمة المعلوماتية، لكن على المستوى الدولي فإن الأمر بحاجة إلى اتفاقيات دولية، فقد شرعت بعض الدول في عقد اتفاقيات قضائية لتسهيل مهمة التحقيق في جرائم الحاسوب الألي،غير أنهبالرغم من ذلك لم يتحقق تقدماً في معالجة الاختصاص القضائي بهدف الحاجة الماسة إلى قانين جنائية أكثر مرونة حتى تواكب سرعة تقدم الحاسوب الألي في كل المجالات[2].

الفرع الثاني

إجراءات البحث والتحري

يقصد بإجراءات التحقيق الإبتدائية على أنها مجموعة من الأعمال التي تباشرها سلطة مختصة للتحقيق في مدى صحة الاتهام الموجه من طرف النيابة العامة بشأن واقعة جنائية

[1]–فليح نور الدين، مرجع سابق، ص 110.

[2]–محمد الأمين البشري، "التحقيق في جرائم الحاسوب الآلي والأنترنت، المجلة العربية للدراسات الأمنية والتدريب"، العدد 30 نوفمبر 2000، ص373.

معروضة عليها ويكون ذلك بالبحث عن الأدلة الثبتة لذلك، أما التحقيق فهو مرحلة لاحقة لإجراءات جمع الاستدلالوتسبق مرحلة المحاكمة والتي تكون اختصاص جهة الحكم، فالتحقيق يهدف إلى تمهيد الطريق أمام القضاء باتخاذ جميع الإجراءات الضرورية للكشف عن الحقيقة[1].

أما أهداف التحقيق الابتدائي فهي تكشف عن الحقيقة للوصول إلى هذا الغرض يلجأ المحقق إلى مجموعة إجراءات بعضها بهدف للحصوا على الدليل ويطلق عليها تسمية إجراءات جمع الدليل لتفتيش والضبط والمعاينة والشهادة والخبرة، وبعضها الأخر يمهد للدليل ويؤدي إليه وتعرف بالإجراءات الاحتياطية ضد المتهم كالقبض والحبس المؤقت.

أما بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية كالتفتيش والمعاينة واستجواب المتهم والضبط والشهادة والخبرة، حيث أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من ق، إ، ج، ج، كما نص على التفتيش في المادة 45 في الفقرة 07 من نفس القانون المعدلة، حيث أعتبر التفتيش الذي يكون على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية من حيث الشروط الشكلية والموضوعية، فالتفتيش وإذ كان إجراء من إجراءات التحقيق قد أحاطه المشرع بقواعد صارمة ولهذا لا تطبق الأحكام الواردة في المادة 44 من نفس القانون إذ تعلق الأمر بالجرام الإلكترونية، ضف إلى ذلك نص على التوقف بالنظر في جريمة المساس بأنظمة المعالجة في المادة 51 من الفقرة 06 بالإضافة إلى " **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور** "، إذ نجد أن المشرع الجزائري مدركا بأن المواجهة الفعالة للإجرام الإلكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها أن تفادي وقوع الجريمة الإلكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها وهو ما

[1]–عبد الله أوهابية، محاضرات في قانون الإجراءات الجزائية، ألقيت على طلبة سنة ثانية حقوق، جامعة، الجزائر، 2009، 2010، د.ص.

استدركه المشرع يتضمن القانون رقم 22/06 المعدل بقانون الإجراءات الجزائية مستحدثة تتعلق بالتحقيق في الجرائم الإلكترونية تتمثل في مراقبة الاتصالات الإلكترونية بتسجيلها والتسرب [1].

يقصد باعتراض المراسلات أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها[2]، فهنا قام المشرع الجزائري بالإشارة إلى ظروف وكيفية اللجوء لهذا الإجراء في المادة 65 مكرر 05 من قانون الإجراءات على النحو الاتي " **إذا اقتضت ضروريات التحدي في الجريمة المتلبس بها أو التحقيق الابتدائي في... الجرائم الماسة بأنظمة المعالجة الألية للمعطيات... يجوز لوكيل الجمهورية المختص أن يأذنباعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكي وضع الترتيبات التقنية دون موافقة المعنين من أجل التقاط وتثبيت وتسجيل الكلام المتفوه به، بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص** "

نستخلص من هذه المادة أن المشرع الجزائري يسمح لسلطات التحقيق والاستدلال إذ استدعت ضرورة التحري في الجريمة المتلبس بها، أو التحقيق في الجريمة الإلكترونية اللجوء إلى إجراء اعتراض المراسلات السلكية واللاسلكية وتسجيل المحادثات والأصوات والصور، والاستعانة بكل الترتيبات التقنية اللازمة للوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضوابط المألوفة مع وضع المشرع الجزائري مجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامةوالحياةالخاصة للأفراد[3].

---

[1]–فضيلة عاقلي، مرجع سابق، ص364.

[2]–بوضياف إسمهان،" الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، المرجع السابق، ص364.

[3]–براهيمي جمال، "مكافحة الجريمة الإلكترونية في التشريع الجزائري"، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية مولود معمري تيزي وزو، العدد 2، الصادر بتاريخ 11/15/ 2016، ص138–140.

المطلب الثاني

الحماية الجزائية المعلوماتية في ظل القانون رقم 11/21 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية لإعلام والإتصال

يعد الإجرام الإلكتروني من أخطر الظواهر الإجرامية المستحدثة في المجتمع الجزائري، نظراً لكثرة مثل هذه الجرائم في الأونة الأخيرة، مما أدى بالمشرع الجزائري إلى إصدار مجموعة من القواعد القانونية بغية ردع مثل هذه السلوكات الغير شرعية لما تشكل من خطورة ومساس بالنظام العام وأمن الدولة.

الفرع الأول

أسباب صدور القانون 11/21 ومضمونه

أولاً: أسباب صدور القانون 11/21

نظراً لخطورة الجرائم الإلكترونية باعتبارها جرائم حديثة ذات طبيعة خاصة لكونها ترتبط بوجود العالم الافتراضي الذي نعيشه والتي يصعب إثباتها هذا ما دفع بالمشرع الجزائري إلى التدخل بإصدار قواعد قانونية تحضر الفعل الإجرامي المعلوماتي التي يترتب عليها أثاراً خطيرة تمس بخصوصية الفرد والمجتمع، هذا ما يتطلب إلى وجود نصوص تجرمها وتعاقب مرتكبها، فكان إلزاماً سد الفراغ القانوني الذي عرفه المجال الإلكتروني بصدور قانون 11/21 المؤرخ في 25 غشت2021 [1]،من الباب السادس منه على إنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الذي ينص على الحماية الجزائية للأنظمة المعلوماتية وتجريم كل الأفعال المنصوص عليها في هذا الباب إذا كانت تشكيل جنحاً، بحيث يختص هذا القطب بالمتابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والمرتبطة بها، بمعنى أي جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات

[1]–أمر رقم 21–11، مؤرخ في 16 محرم عام 1443، الموافق ل 25 غشت سنة 2021، المتعلق بجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ج. ر. ج. ج. د. ش، العدد 65، صادر في 26 غشت 2021.

الإلكترونية أو أي وسيلة أخرى أولية ذات صلة بتكنولوجيات الإعلام والاتصال، ويكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية وبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبها، كما يختص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيداً وهي الجريمة المستحدثة وفقاً لهذا القانون هي الجريمة التي يتعدد فيها الفاعلين أو الشركاء أو المتضررين أو بسبب الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة أثارها أو الأضرار المترتبة عليها أو لطابعها المنظم أو العابر للحدود الوطنية أو لمساسها بالنظام والأمن العمومين، وتتطلب وسائل تحري خاصة وخبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي.

ثانياً: مضمون القانون11/21

يقضي الدستور الجزائري[1] الذي يعتبر القانون الأسمى في البلاد واستنادا إلى احكام التي صدرت بموجب اتفاقية الأمم المتحدة بتاريخ 05 فبراير 2000 المصادق عليها بالتحفظ وفق المرسوم الرئاسي، كما أنه حسب الأمر رقم 155/66، كذلك في هذا المسار نجد ما جاء في الأحكام المتواجدة في الأمر رقم 156/66 المتضمن قانون العقوبات[2]، كما نجد العديد من القوانين كقانون 04/09 المتعلق بالقواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجياً الإعلام والاتصال ومكافحتها، بالإضافة إلى القانون رقم 18/ 04 [3] الذي يحدد القواعد العامة المتعلقة

[1]–دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر بموجب المرسوم الرئاسي رقم 36–498، مؤرخ في 01 ديسمبر 1996، ج. ر. ج. ج. د. ش، عدد 76، صادر في 08 ديسمبر 1996، معدّا ومتمم بالقانون رقم 03–02، مؤرخ في 10 أفريل 2002، ج. ر. ج. ج. د. ش، عدد 25، صادر في 14 أفريل 2002، معدّل بموجب القانون رقم 08–09، مؤرخ في 15 نوفمبر 2008، ج. ر. ج. ج. د. ش، عدد 76، صادر في 16 نوفمبر 2008 معدل ومتمم بالقانون رقم 16–01 مؤرخ في 06 مارس 2016، ج. ر. ج. ج. د. ش، عدد14، صادر في 07 مارس 2016.

[2]–أمر قم 66–156، مؤرخ في 08 جوان 1966، يتضمن قانون العقوبات، ج. ر. ج. ج. د. ش، عدد 49، صادر في 10 جوان 1966، معدل ومتمم بالقانون رقم 16–02، مؤرخ في 16 جوان 2016، ج. ر.ج. ج. د. ش، عدد 37، صادر في 22 جوان 2016.

[3]–القانون رقم 18–04، المؤرخ في 24 شعبان 1439، الموافق ل 10مايو 2018، المتعلق بالقواعد العامة المتعلقة بالبريد والاتصالات الإلكترونية.

بالبريد والاتصالات الإلكترونية، وبمقتضى القانون رقم 05/20 [1] والمتعلق بالوقاية من التميز والكراهية ومكافحتها.

عمد المشرع الجزائري على إصدار أمر رقم 11/21 الذي يهدف إلى إتمام الأمر رقم 155/66 المتضمن قانون الإجراءات الجزائية، وذلك بإنشاء القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المتواجد مقره على مستوى محكمة مجلس قضاء الجزائر الذي يختص في متابعة والتحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والمرتبطة بها، كما يختص بالحكم فبي الجرائم المنصوص عليها في هذا الباب إذا كانت تشكل جنحاً، حيث يقصد بمفهوم هذا القانون بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، إذ تتمحور الحماية الجزائية من خلال هذا القانون بمكافحة ومعاقبة كل شخص يرتكب أو تشترك في ارتكاب الجريمة التي تمس بأمن الدولة والدفاع الوطني كجرائم النشر والترويج بأخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع، وكذا جرائم الإتجار بالأشخاص والأعضاء البشرية أو تهريب المهاجرين، بالإضافة إلى جرائم التميز وخطاب الكراهية، ضف إلى المساس بأنظمة المعالجة الألية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية، بمعني أنه أي جريمة ترتكب أو يسهل ارتكبها باستعمال منظومة معلوماتية أو نظام الاتصالات الإلكترونية أو أي وسيلة أخرى أولية ذات صلة بتكنولوجيا الإعلام والاتصال، فقد استحدث المشرع الجزائري نوعاً ثانياً من الجرائم المتصلة بتكنولوجياً الإعلام والاتصال في القانون 21/ 11 وأطلق عليها اسم الجرائم المتصلة بتكنولوجيا الإعلام والاتصال الأكثر تعقيداً والتي ينظر لها من حيث تعدد الأشخاص الفاعلين والشركاء في ارتكابها وكذا اتساع الرقعة الجغرافية لمكان ارتكابها، بالإضافة إلى مدى جسامة أضرارها، وما مدى مساسها بالنظام والأمن العمومين حيث أعطى المشرع الجزائري للضبطية القضائية استعمال وسئل خاصة للتحري فيها.

[1]– القانون رقم 20–05 المؤرخ في 05 رمضان 1441، الموافق ل 28 أبريل 2020، المتعلق بالوقاية من التميز وخطاب الكراهية ومكافحتها.

الفرع الثاني

الإجراءات المستحدثة بموجب القانون 11/21

حرص المشرع الجزائري على استحدث عدة إجراءات بموجب القانون رقم 11/21 تزامناً مع كثرة الجرائم الإلكترونية داخل المجتمع الجزائري حيث تم استحداث في الباب السادس من هذا القانون " قطب الجزائي المتخصص في الجرائم المتصلة بتكنولوجياً الإعلام والاتصال والتوسيع من اختصاص من هذا القطب، بمعني أي وسيلة تستحدث فيما بعد تكون من اختصاص القطب الجزائي، والتي تكون لها علاقة بالاتصال والإعلام وهذا ما يظهر لنا من خلال ما يلي

أولاً: من حيث الاختصاص المحلي

إن اختصاص القطب الجزائي المتخصص بالجرائم المتصلة بالإعلام والاتصال والجرائم المرتبطة بها، فإن الاختصاص، يمارس وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا قاضي التحقيق ورئيس محكمة جنح القطب صلاحيتهم في كامل الإقليم الوطني وفق نص المادة 211 مكرر 23 من هذا القانون[1].

ثانياً: الاختصاص النوعي للقطب الجزائي الوطني

يختص هذا القطب حصرياً بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وكذا الجرائم المرتبطة بها وفق نص المادة 211 مكرر 24[2] من نفس القانون حيث يختص هذا القطب في:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.

- جرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع.

[1]-أنظر المادة 211 مكرر 23 من الأمر رقم 21-11، المتعلق بجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

[2]-أنظر المادة 211 مكرر 24 من الأمر 21-11، المتعلق بجرائم المتصلة بتكنولوجيات الإعلام والإتصال.

– جرائم نشر وترويج أنباء معرضة تمس بالنظام والأمن العمومين ذات الطابع المنظم أو العابرة للحدود الوطنية.

– جرائم المساس بأنظمة المعالجة الألية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.

– جرائم الإتجار بالأشخاص أو الأعضاء البشرية أو تهريب المهاجرين.

–جرائم التميز وخطاب الكراهية وخير دليل قضية اغتيال جمال بن سماعيل

كما يختص أيضا القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بالإعلام والاتصال الأكثر تعقيداً والجرائم المرتبطة بها وفق لنص المادة 211 مكرر 25، حيث يختص هذا القطب بالمتابعة والتحقيق والحكم في القضايا الموصوفة بالجرائم الإلكترونية الأكثر تعقيداًن ففي هذه الجرائم أعطى المشرع الجزائري للضبطية القضائية ووكيل الجمهورية استعمال وسائل خاصة للتحري أو خبرة فنية متخصصة أو اللجوء إلى تعاون قضائي دولي وهذا في مثل هذه الحالات:

ثالثا: حالة الاشتراك في الاختصاص

– تطبيق في هذه الحالة الإجراءات المنصوص عليها في المادة 211 مكرر4 إلى 211 مكرر 14 من هذا القانون أمام القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

– يمارس هذا القطب الجزائي الوطني اختصاصا مشتركاً مع الاختصاص الناتج من تطبيق المواد 37 و40 و329 من ق، إ، ج، ج[1] بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها المتعلقة في الجرائم المتمثلة في المخدرات، الفساد، تبيض الأموال،

[1]– أنظر المواد 37، 40، 329، من القانون رقم 66–155، المتعلق بقانون الإجراءات الجزائية، معدل ومتمم.

الجريمة التي تمس بمعالجة الألية للمعطيات، جريمة الصرف، فالاختصاص هنا مشترك بين هذه الأقطاب وهذا ما قضت به المادة 211 مكرر 27 من هذا القانون.

– إذا تزامن اختصاص القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال مع اختصاص القطب الاقتصادي والمالي، يتنازل القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال حيث يؤول الاختصاص للقطب الاقتصادي والمالي وجوباً حسب نص المادة 211 مكرر 28 من قانون 11/21.

أما في حال ما إذا كان الاختصاص مشتركاً بين القطب الجزائي الوطني مع الجرائم التييختص بها القطب الجزائي الاقتصادي والمالي.

– الجرائم المنصوص عليها في المواد 119 مكرر1 و389 مكرر 2و3 من قنون العقوبات.

– الجرائم المنصوص عليها في القانون 01/06 المتعلقة بالوقاية من الفساد ومكافحته[1].

– الجرائم المنصوص عليها في الأمر رقم 22/96 المتعلقة بقمع مخالفة التشريع والتنظيم الخاصبالصرف وحركة رؤوس الأموال من وإلى الخارج[2].

– الجرائم المنصوص عليها في المواد 11، 12، 13، 14، 15 من الأمر رقم 06/05 المتعلق بمكافحةالتهريب.

– إذا كان الاختصاص مشتركا بين القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها مع اختصاص محكمة مقر مجلس قضاء الجزائر طبقاً للأحكام المواد 211 مكرر 16 إلى 211 مكرر 21 من هذا القانون، فإن

[1]–قانون رقم 06–01، مؤرخ في 20فيفري 2006، يتعلق بالوقاية من الفساد ومكافحته، ج. ر. ج. ج. د. ش، عدد 14، صادر في 08 مارس 2006، معدل ومتمم بأمر رقم 10–05، مؤرخ في 26 أوت 2010، ج. ر. ج. ج. د. ش، عدد50، صادر في 01 ديسمبر 2010.

[2]–أمر رقم 96–22، مؤرخ في 23 صفر 1386، الموافق ل 09 يوليو 1966، المتعلق بقمع مخالفة التشريع والتنظيم الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، المعدل والمتمم.

الاختصاص يؤول لمحكمة مقر المجلس قضاء الجزائر وفق المادة 211 مكرر 29 من القانون 11/21.

نستنتج مما سبق أن الاختصاص الوطني يكفل كامل القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والجرائم المرتبطة بها، ولتخفيف العبء عمد المشرع الجزائري بالتعاون مع الأقطاب الأخرى ماعدا في الاختصاص الحصري المنصوص عليه في المواد 211 مكرر 25 والجرائم الأكثر تعقيداً المنصوص عليه في المادة 211 مكرر 25.

خاتمة

أخيرا وعلى ضوء ما سبق يتضح لنا بأن الجرائم الإلكترونية تعد من الأنماط الإجرامية المستحدثة التي إنفجرت حديثا من الثورة المعلوماتية والاتصالات عن بعد التي تمس للأمن العام من جهة والحق في الخصوصية من جهة أخرى.

حيث اتسمت هذه الجريمة بطبيعة خاصة فوجدت صعوبة في وضح تعريف عام جامع وموحدلها، فإختلفت المفاهيم حولها بإختلاف الزاوية التي ينظر إليها كما تجسدت كذلك طبيعتها الخاصة في خصائصها المختلفة عن خصائص الجرائم التقليدية المتمثلة في أنها جريمة عابرة للحدود لكونها ترتكب بواسطة الحاسوب وفي مجال الحاسب الآلي، كما أنها تتميز بالسرعة في تنفيذها. ويغلب عليها طابع التطور المستمر والمتسارع من حيث ارتكابها وإلى جانب هذه الخصائص هناك خصائص يتميز بها المجرم المعلوماتي وصفاته، وهذه الطبيعة المتميزة للجريمة الإلكترونية جعلت المشرع الجزائري يدرك مدى خطورة هذه الجريمة على الفرد والمجتمع خاصة، فكان لابد له من وضع حد لهذه الجريمة بالأخص أن المجتمع الجزائري يشهد استعمال واسع للتقنيات المعلوماتية في جميع القطاعات ، وبعد الفراغ التشريعي الذي كانت تعاني منه الجزائر في هذا المجال، فإنها سعت إلى تعديل قانون العقوبات رقم 04-15 وكذلك ما أوردة في أمر 03-05 المتعلق بحقوق المؤلف والحقوق المجاورة، كما قام بالتعديل الجانب الجزائي، حيث قام بتعديل قانون الإجراءات الجزائية عن طريق إضافة إجراءات جديدة تطبق على جرائم المساس بأنظمة المعالجة الألية المعطيات وقام من جهة ثانية بإستحداث قوانين أخرى خاصة أكثر تجاوبا مع الطبيعة الخاصة للجرائم المعلوماتية وذلك القانون رقم لما يتناسب والظاهرة المستحدثة وبالإضافة إلى استحداث وحدات وهيئات خاصة لمواجهة الجريمة وردع المجرمين التي تم وضعها بموجب المرسوم الرئاسي رقم 15-261 والمحدد فيه تشكيلية وكيفية سير هذه الهيئة، وكيفها المشرع الجزائري على أنها سلطة إدارية مستقلة.

رغم كل المحاولات التي بذلها المشرع الجزائري في محاربة هذه الجريمة إلا أنها تعتبر غير كافية وذلك بسبب التطور السريع والكبيرة في مختلف الأجهزة الإلكترونية، ومن خلال ما سبق يمكن تقديم الإقتراحات التالية:

- العمل على وضع بروتوكولات تعاون مشترك بين الهيئة الوطنية للوقاية ومكافحة من جرائم الإعلام والإتصال وباقي الهيئات المتخصصة، كالهيئة الوطنية للوقاية ومكافحة جرائم الفساد، الديوان الوطني لقمع الفساد، المجلس الوطني الحقوق الإنسان.
- التأكيد على وجوب الحصول على إذن مسبق من طرف القاضي المكلف بإجراءات المراقبة عند تحديد المراقبة.
- توفير الإمكانات البشرية والمادية والتقنية الحديثة للمراكز والأجهزة المتخصصة في مكافحة الجرائم الإلكترونية.
- وضع قواعد واضحة حول سرية البيانات المتحصل عليها أثناء التفتيش وحجز الأدلة.
- ضرورة تكثيف الجهود الوطنية لنشر المعرفة وزيادة الوعي بالجرائم الإلكترونية ومدى خطورتها ووسائل الوقاية منها وسبل مواجهتها.
- من الأفضل أن سن المشرع قانون موحد لمكافحة الجرائم المعلوماتية، بلم بكل النصوص الموضوعية والإجرائية والتنظيمية، وهو يسهل عمل ضابط الشرطة القضائية ووكلاء الجمهورية وقضاة التحقيق والحكم، ويساعد رجال القانون من الإلمام بكل ما يخص هذه النوع المستحدث من الجرائم.
- ضرورة استقطاب هذا النوع من المجرمين ومحاولة الاستفادة من خبراتهم.
- ضرورة اعتماد نظام المرشد الجنائي وفتح مواقع لتلقي الشكاوي لتسهيل عملية القبض على هؤلاء المجرمين.
- ضرورة تكثيف الدراسات حول طبيعة المجرم المعلوماتي، ونرى أنه حان الوقت لميلاد علم جديد وهو علم الإجرام المعلوماتي.
- 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 الاجرام المعلوماتي وكيفية مكافحته والحد منه.

- على المشرع الجزائري تسليط الضوء على الجرائم المستحدثة التي تمارس ضد المرأة على صفحات الأنترنيت ووضع حد لها وحماية المرأة من هذه الجريمة والوقوع فيها.

{تبقى الوقاية خير من ألف مادة قانونية}.

قائمة المراجع

أولا :الكتب

أ-المؤلفات العامة

1-**أحمد شوقي الشلفاني**، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء2، ط05، ديوان المطبوعات الجامعية، الجزائر، (دن ص).

2- **أحمد عبد الرزاق السنهوري**، الوسيط في شرح القانون المدني، حق الملكية، الجزء الثاني، دار إحياء التراث العربي، بيروت، 1952.

3-**الرومي محمد أمين**، الكمبيوتر والأنترنيت، دار المطبوعات الجامعية، الإسكندرية، 2004.

4- **الزيدي وليد**، القراصنة على الانترنيت والحاسوب، ط1، دار النشر، عمان، 2003.

5- **أوهابية عبد الله**، محاضرات في قانون الإجراءات الجزائية، ألقيت على طلبة السنة الثانية حقوق، جامعة الجزائر، الموسم الجامعي 2009-2010.

6-**حنان ريحان، مبارك المضحاكي**، الجرائم المعلوماتية، ط1، منشورات الحلبي الحقوقية، بيروت، 2014.

7-**خثير مسعود**، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر،2011.

8- **زبيد زيدان**، الجرائم المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر،2011.

9- **قورة نائلة**، جرائم الحاسب الإقتصادية، دار النهضة العربية، القاهرة، 2004.

10- **محمد علي قطب**، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، الجزء الأول، (د س ن).

11- **محمدفتحي عبد الهادي**، مقدمةفي علم المعلومات، مكتبة غريب، القاهرة، 1984.

12-**محمد نجيب حسني**، شرح قانون العقوبات، دار النهضة العربية، القاهرة، 1992.

13-**وضاح محمود، نشأت مقضى المجاني**، جرائم الأنترنيت، دار المنارة للنشر، عمان، 2009.

ب-المؤلفات المتخصصة

1- **أحمد خليفة الملط،** جرائم المعلوماتية، ط2، دار الفكر الجامعي، مصر، 2006.

2- **عبد الفتاح بيومي حجازي،** الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنيت، دار الكتب، القاهرة، 2002.

3- **قارة أمال،** الحماية الجنائية للمعلوماتية في التشريع الجزائري، ط1، دار هومة، الجزائر، 2006. 4- **محمد حماد مرهج الهيبتي،** جرائم الحاسب، دار المناهج للنشر والتوزيع، عمان، 2005. 5 - **نهلا عبد القادر المومني،** الجرائم المعلوماتية، دار الثقافة، عمان، 2008.

ثانيا: المذكرات الجامعية

أ-مذكرات الماجيستر

1- **بن عقون حمزة،** السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة لحاج لخضر، باتنة، 2011-2012.

2-**بوخبزة عائشة،** الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري، رسالة ماجستير في القانون الجنائي، كلية الحقوق، جامعة وهران، 2012-2015.

3- **سعيداني نعيم،** آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة لحاج لخضر، باتنة، 2013.

4-**سويسر سفيان،** جرائم المعلوماتية، مذكرة ماجستير في العلوم الجنائية، جامعة أبو بكربلقايد، تلمسان، 2010.

5- **صغير يوسف،** الجريمة المرتكب عبر الأنترنيت، مذكرة تخرج لنيل شهادة الماجستير في القانون، تخصص قانون الدولي للأعمال، كليم الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.

6- **يوسف خليل يوسف العفيفي**، الجرائم الإلكترونية في التشريع الفلسطيني"دراسة تحليلية مقارنة"، رسالة لنيل شهادة الماجستير في القانون العام، كلية الشريعة والقانون، الجامعة الإسلامية، غزة، 2013.

ب-مذكرات الماستر

1-**فليح نور الدين**، الجريمة الإلكترونية وآليات مكافحتها في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي والعلوم الجنائية، جامعة مولاي طاهر، سعيدة، 2018-2019.

2- **مزغيش سمية**، جرائم المساس بأنظمة المعلوماتية، مذكرة مكملة من متطلبات لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2013-2014.

3-**نايري عائشة**، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، 2016-2016.

ثالثا- المقالات العلمية والمداخلات

أ- المقالات العلمية

1- **البشري محمد الأمين**،"التحقيق في جرائم الحاسوب الآلي والأنترنيت"، المجلة العربية لدراسات الأمنية والتدريب، العدد 30 نوفمبر 2000، ص ص353-349.

2-**بحري صابر، حزموش منى**، "أهم الدوافع السيكولوجية وراء الجريمة المعلوماتية"، مجلة الدراسات في سيكولوجيا الإنحراف، مجلد06، العدد 01، جامعة محمد لمين دباغين، سطيف، 2021، ص ص59-36.

3-**براهيمي جمال**، "مكافحة الجريمة الإلكترونية في التشريع الجزائري"، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية مولود معمري، تيزي وزو، العدد2، الصادر بتاريخ 2016/11/15، ص ص 138-140.

4-**بوضياف إسمهان**، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف، مسيلة، لعدد الحادي عشر،2018، ص ص374-358.

5-**شنين صالح**، "الحماية الجنائية لبرامج الحاسوب في التشريع الجزائري"، المجلة الأكاديمية للبحث القانوني، عدد 01، الجزائر، 2010، ص ص64-71.

6-**حمدي ناصر**، "التنظيم القانوني لظاهرة المعلوماتية في الجزائر: الإنجازات والتحديات"، المجلة النقدية للقانون والعلوم السياسية، عدد 02، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2012، ص ص179-242.

7- **محمد سليمان مصطفي**، "جرائم الحاسوب وأساليب مواجهتها"، مجلة الأمن والحياة، المجلد19، العدد 210، 1999، ص ص 48-50.

8-**ونوغي نبيل**، **زيوش عبد الرؤوف**، "الجريمة المعلوماتية في التشريع الجزائري"، مجلة العلوم القانونية والإجتماعية، جامعة زيان عاشور الجلفة، الجزائر، المجلد الرابع، العدد الثالث، سبتمبر 2019.

ب- المداخلات

1- **أرحومة موسى مسعود**، "الإشكاليات الإجرائية التي تسيرها الجريمة المعلوماتية عبر الوظيفة"، ورقة مقدمة الى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا، طرابلس،26-2009/10/29.

2-**بن غدقة شريفه والقص صليحة**، "الجريمة الإلكترونية الممارسة ضد المرأة على صفحات الأنترنيت وطرق محاربتها"، أعمال الملتقى الوطني، "آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري، الجزائر،29 مارس 2017.

3-**ذياب موسى**، "الجرائم الإلكترونية: المفهوم والأسباب"، ملتقى علمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، الأردن، خلال الفترة من 2 الى 4 سبتمبر 2014.

4-**عبد الناصر محمود فرغلي، محمد عبيد سيف السماري**، "الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة مقارنة)"، المؤتمر العربي الأول، للعلوم الأدلة الجنائية والطب الشرعي، الرياض،2007، ص ص 01-45.

5-**عاقلي فضيلة**، "الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري"، المؤتمر الدولي الرابع عشر،" للجريمة الإلكترونية"، طرابلس، بتاريخ 24-25 مارس2017، ص ص115-136.

6-**فشار عطاء الله**، "مواجهة الجريمة المعلوماتية في التشريع الجزائري"، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية، المنعقد بأكاديميةالدراسات العليا بليبيا، في أكتوبر 2009، ص ص01-10.

7- **عكور سومية**،" الجرائم المعلوماتية وطرق مواجهتها في المشهد القانوني والأمني"، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحويلات الإقليمية والدولية، كلية العلوم الاستراتيجية،02-04-2016.

رابعا- النصوص القانونية

أ- الدستور

1- دستور الجمهورية الجزائرية الدمقراطية الشعبية، الصادر بموجب المرسوم الرئاسي رقم 36-498، المؤرخ في 01 ديسمبر 1996، معدل ومتمم بالقانون رقم 03-02، مؤرخ في 10 أفريل 2002، ج، ر، ج، ج، د، ش، عدد25، صادر في 14 أفريل 2002، معدل بموجب القانون رقم 08-09، مؤرخ في 15 نوفمبر 2008، ج، ر، ج، ج، د، ش، عدد 76، صادر في 16 نوفمبر 2008، معدل ومتمم بالقانون رقم16-01، مؤرخ في 06 مارس 2016، ج، ر، ج، ج، د، ش، عدد 14، صادر في 07 مارس 2016.

ب- القوانين والأوامر

1-القانون رقم 2000-03، المؤرخ في 5 أوت 2000، يحدد القواعد المتعلقة بالبريد والمواصلات السلكية واللاسلكية، العدد 48، صادر في 06 أوت 2000، (ملغى).

2- القانون رقم 04-15، المؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، ج، ر، العدد 71، الصادر في 10 جوان 2004.

3-القانون رقم 06-01، المؤرخ في 20 فيفري 2006، يتعلق بالوقاية من الفساد ومكافحته، ج، ر، عدد 14، صادر في 08 مارس 2006، معدل ومتمم بأمر رقم 10-05، مؤرخ في 26 أوت 2010، ج، ر، عدد 50، صادر في 01 ديسمبر 2010.

4- القانون رقم 09-04، المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحته، عدد 47، الصادر في 16 أوت 2009.

5- القانون رقم 18-04، المؤرخ في 24 شعبان 1439، الموافق ل 10 مايو 2018، المتعلق بالقواعد البريد والإتصالات الإلكترونية، عدد 27، مؤرخ في 13 ماي 2018.

6-القانون رقم 20-05، المؤرخ في 05 رمضان 1441، الموافق ل 28 أفريل 2020، المتعلق بالوقاية من التميز وخطاب الكراهية ومكافحته، عدد 25، صادر في 29 أفريل 2020.

7- أمر رقم 66-156، المؤرخ في 8 يونيو، يتضمن قانون العقوبات، ج، ج، د، ش، ج، ر، عدد 49، مؤرخ في 19 جوان 1966، المعدل والمتمم بالقانون رقم 16-02 المؤرخ في 19 يونيو 2016، ج، ر، العدد 37، الصادر بتاريخ 22 يونيو 2016.

8- أمر رقم 66-155، المؤرخ في 18 جوان، يتضمن قانون الإجراءات الجزائية، ج، ج، د، ش، ج، ر، عدد 48، صادر في 11 جوان 1966، معدل بموجب الأمر رقم 15-02، مؤرخ في 23 جويلية 2015، ج، ر، ج، ج، د، ش، عدد 40، صادر في 23 جويلية 2015.

9- أمر رقم 29-22، مؤرخ في 23 صفر الموافق ل 09 يوليو 1966، المتعلق بقمع مخالفة التشريع والتنظيم الخاص بالصرف وحركة رؤوس الأموال من وإلى الخارج، المعدل والمتمم.

10- أمر رقم 03-08، المتعلق بحماية التصاميم الشكلية للدوائر المتكاملة، صادر في تاريخ 23 جويلية 2003، الجريدة الرسمية، عدد 36.

11- أمر رقم 03-05، مؤرخ في 19 جمادي الأول عام 1424، الموافق ل 19 يوليو 2003، المتعلق بحماية المؤلف والحقوق المجاورة، ج، ر، عدد 44.

12-أمر رقم 21-11، المؤرخ في 16 محرم 1443، الموافق ل 25 غشت 2021، المتعلق بجرائم المتصلة بتكنولوجيا الإعلام والإتصال، ج، ر، ج، ج، د، ش، العدد 65، صادر في غشت 2021.

ج- المراسيم التنظيمية

1- المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، المحدد تشكيلية وتنظيم وكيفيات سير الهيئة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، ج، ر، عدد 53، الصادر في 8 أكتوبر 2015.

2- المرسوم الرئاسي رقم 19-172، المؤرخ في 06 يونيو، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام وتنظيمها وكيفيات تسيرها، الجريدة الرسمية عدد 37، الصادرة في 09 يونيو 2019.

خامسا- الموقع الإلكتروني

Www.tashreaat.com، تم الإطلاع على الموقع بتاريخ 2022/05/25 على الساعة 17 سا و35 د.

الفهرس

الفهرس

الشكر والتقدير

إهـداء

قائمة المختصرات

مقدمة 1

الفصل الأول: الإيطار المفاهيمي للجريمة الإلكترونية

المبحث الأول: مفهوم الجريمة الإلكترونية 5

المطلب الأول: تعريف الجريمة الإلكترونية وأركانها 5

الفرع الأول: تعريف الجريمة الإلكترونية 6

أولا: التعريف الفقهي للجريمة المعلوماتية 6

1. التعريف الضيق للجريمة الإلكترونية 6

2. التعريف الواسع للجريمة الإلكترونية:..... 7

ثانيا: التعريف التشريعي للجريمة المعلوماتية..... 8

الفرع الثاني: أركان الجريمة الإلكترونية..... 10

أولا: الركن المادي في الجريمة الإلكترونية..... 10

ثانيا: الركن المعنوي في الجريمة الإلكترونية..... 11

ثالثا: الركن الشرعي في الجريمة الإلكترونية 12

المطلب الثاني: دوافع ارتكاب الجريمة الإلكترونية..... 13

الفرع الأول: الدوافع الشخصية لارتكاب الجريمة الإلكترونية 13

أولاً: الدوافع المادية 14

ثانياً: الدوافع المعنوية 14

الفرع الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية 15
أولاً: دافع الانتقام وإلحاق الضرر بالغير 16
ثانياً: دافع التعاون والتواطؤ 17
ثالثاً: الضغوطات العامة 17
المبحث الثاني: خصائص وأنواع الجرائم الإلكترونية في القانون الجزائري 19
المطلب الأول: خصائص الجريمة الإلكترونية 19
الفرع الأول: السمات الخاصة بالجريمة الإلكترونية 20
أولا–الجريمة المعلوماتيةمتعددة الحدود 20
ثانيا–صعوبة إكتشاف الجريمة الإلكترونية 20
ثالثا: صعوبة إثبات الجريمة المعلوماتية 21
رابعا: أسلوب ارتكاب الجريمة الإلكترونية 21
خامسا: الجريمة الإلكترونية تتم بتعاون عدة أشخاص 22
الفرع الثاني: السمات الخاصة بالمجرم المعلوماتي 22
أولا: المجرم المعلوماتي إنسان اجتماعي 23
ثانيا: المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي 23
ثالثا: المجرم المعلوماتي يبرر ارتكابه للجريمة 24
رابعا: التطور في السلوك الإجرامي 24
المطلب الثاني: أنواع الجرائم الالكترونية في القانون الجزائري 26
الفرع الأول: الجرائم المرتكبة بإستخدام النظام المعلوماتي 27
أولا: الجريمة الإلكترونية الواقعة على الأشخاص 27
1. جرائم السب والقذف عبر الانترنيت 28

2. جرائم الإعتداء على الحياة الخاصة..... 28
3. الجريمة الالكترونية الواقعة على حقوق الملكية الفكرية..... 29
ثانيا: الجرائم الواقعة على النظم المعلوماتية الأخرى..... 30
ثالثا: الجريمة الإلكترونية الواقعة على الأسرار 31
الفرع الثاني: الجريمة الإلكترونية الواقعة على النظام المعلوماتي..... 33
أولا: جريمة الدخول أو البقاء في منظومة معلوماتية..... 33
1. فعل الدخول إلى النظام 34
2. فعل البقاء داخل النظام 35
ثانيا: جريمة المساس بمنظومة معلوماتية..... 35
ثالثا: أفعال إجرامية أخرى 36
الفصل الثاني: آليات مكافحة الجريمة الالكترونية والحد منها في القانون الجزائري
المبحث الأول: القواعد الموضوعية لمكافحة الجريمة الإلكترونية..... 38
المطلب الأول: الحماية الجزائية للمعلوماتية من خلال نصوص قانون العقوبات 38
الفرع الأول: الحماية الجزائية للمعلوماتية من خلال نصوص جرائم الأموال المقررة في قانون العقوبات الجزائري..... 39
أولا: مدى اعتبار المعلوماتية موضوع لجرائم الأموال..... 39
1- مدى انطباق وصف المال على المعلوماتية 40
2- مدى اعتبار المعلوماتية مالا بصدد جرائم الأموال 41
ثانيا: مدى خضوع المعلوماتية للنشاط الإجرامي في جرائم الأموال 43
1- مدى خضوع المعلوماتية للنشاط الإجرامي في جريمة السرقة 43
2- مدى خضوع برامج الحاسب الآلي للنشاط الإجرامي في جرائم النصب وخيانة الامانة..... 46

الفرع الثاني: الحماية الجزائية الإلكترونية من خلال النصوص المتعلقة بجرائم المساس بأنظمة المعالجة الألية للمعطيات..... 47
أولا: العقوبات المقررة لشخص الطبيعي 48
ثانيا: العقوبات المقررة للشخص المعنوي 49
ثالثا: عقوبة الاشتراك والشروع في الجريمة 49
المطلب الثاني: الحماية الجزائية للجريمة الإلكترونية من خلال القوانين والتنظيمات الأخرى ... 51
الفرع الأول: القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية 51
المبحث الثاني: القواعد الإجرائية لمكافحة الجرائم الإلكترونية 53
المطلب الأول: القواعد الإجرائية المنصوص عليها في قانون الإجراءات الجزائية 53
الفرع الأول: قواعد الاختصاص المحلي 53
أولاً: الاختصاص المحلي للنيابة العامة..... 54
ثانياً: الاختصاص المحلي لقاضي التحقيق 55
ثالثاً: الاختصاص المحلي لمحاكم الجنح 55
الفرع الثاني: إجراءات البحث والتحري..... 56
المطلب الثاني: الحماية الجزائية المعلوماتية في ظل القانون رقم 11/21 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجية لإعلام والإتصال..... 59
الفرع الأول: أسباب صدور القانون 11/21 ومضمونه..... 59
أولاً: أسباب صدور القانون 11/21..... 59
ثانياً: مضمون القانون11/21 60
الفرع الثاني: الإجراءات المستحدثة بموجب القانون 11/21 62
أولاً: من حيث الاختصاص المحلي 62

ثانياً: الاختصاص النوعي للقطب الجزائي الوطني 62

ثالثا: حالة الاشتراك في الاختصاص..... 63

خاتمة 66

قائمة المراجع 69

الفهرس 76

ملخص

يعتبر الإجرام الإلكتروني من أخطر الظواهر الإجرامية المستحدثة التي يشهدها العالم والمجتمع الجزائري خاصة، التي من شأنها المساس ببعض الأفراد والجماعات وأمن الدولة، فنظرا لقلة الآثار المادية التي تخلفها وكثرة الأشخاص الذين يترددون على مسرح الجريمة ويثير البحث والتحرى عنها الكثير من الإشكالات القانونية هذا ما جعل المشرع الجزائري يتدخل لتقيد هذه الإجراءات على نحور يعزز الحريات الشخصية الأفراد وذلك من خلال التدخل عبر عديد من النصوص القانونية الموضوعية والإجرائية لمواجهة الجريمة والمجرم المعلوماتي وكذلك اللجوء إلى إنشاء أجهزة متخصصة تستطيع التعامل مع هذا النوع من الجرائم.

Résumé

La cybercriminalité est l'un des phénomènes criminels émergents les plus dangereux que connaît le monde et la société algérienne en particulier, ce qui porterait préjudice à certains individus, groupes et à la sécurité de l'État. Le législateur algérien a fait l'intervention pour restreindre ces procédures d'une manière qui renforce la liberté individuelle des individus, en s'immisçant à travers plusieurs textes juridiques de fond et de procédure pour faire face à la délinquance et au délit d'information, ainsi qu'en recourant à la mise en place de dispositifs spécialisés pouvant faire face à ce type de délinquance.