وزارة التعليم العالي والبحث العلمي
المركز الجامعي الشيخ المقاوم آمود بن مختار– اليزي –
معهد الحقوق

مذكرة تخرج لنيل شهادة ماستر في الحقوق
تخصص القانون الجنائي والعلوم الجنائية

بعنوان:

جرائم تكنولوجيا الإعلام والاتصال و ألليات مكافحتها في التشريع الجزائري

إعداد الطالبين :
– عبد العزيز لعروسي
– بلقاسم وردي

تحت إشراف الدكتور :
امين بن قردي

لجنة المناقشة

محمد بشير	**المركز الجامعي إيليزي**	رئيسا
امين بن قردي	**المركز الجامعي إيليزي**	مشرفا ومقررا
يوسف مرين	**المركز الجامعي إيليزي**	مناقشا

السنة الجامعية 2022 /2023


بسم الله الرحمن الرحيم

شكر

قال الله تعالى: {ولئن شكرتم لأزيدنكم} قبل كل شيء نشكر الله تعالى ونحمده على توفيقه ورعايته وإلهامه لنا في انجاز هذا العمل المتواضع حمدا يليق بعظمته وجلالته، حيث سهّل لنا الطريق وأتانا من العلم والمعرفة، فالحمد والشكر لله والصلاة والسلام على نبيّنا رسول الله.

ونتقدم بجزيل الشكر للدكتور المشرف: بن قردي أمين

الذي لم يبخل علينا بنصائحه وتحفيزاته التي تبث الثقة والاستمرار.

جزاه الله كل خير وسدد خطاه.

كما نتوجه بالشكر الخالص إلى جميع أساتذة معهد الحقوق

والشكر موصول إلى كل ساندنا ووقف بجانبنا ومد لنا يد العون من قريب أو بعيد.

إهداء

يا من خلقتني فأحسنت، ورزقتني وعلمتني فنفعت، إليك أتقرب بشيء من جزيل عطائك، فاجعله لقلبي ضياء ولبصري جلاء واكتبه في ميزاني حسناتي إليك يا من تشوق الأنفس الطاهرة للقياك وتقر العيون الفياضة لرؤياك يا رسول الله صلى الله عليه وسلم .إلى نبع الحب والحنان أمي الحبيبة، أبي الغالي، إلى أجمل ما أملك في الوجود اخوتي إلى صديقي الذي تقاسمت معه هذا البحث: وردي بلقاسم

لعروسي عبد العزيز

إهداء

إلى كل معلمي وأساتذتي من الطور الابتدائي إلى الطور الجامعي والشكر الجزيل للدكتور بن قردي محمد امين الذي ساندني منذ بداية العمل أهدي ثمرة جهدي هذا وما توفيقي إلا بالله وصلت رحلتي الجامعية إلى نهايتها بعد تعب ومشقة إلى من أفضلها على نفسي ولم لا فلقد ضحت من أجلي ولم تدخر جهدا في سبيل إسعادي على الدوام (أمي الحبيبة (نسير في دروب الحياة ويبقى من يسيطر على أذهاننا في كل مسلك نسلكه صاحب الوجه الطيب والأفعال الحسنة فلم يبخل علي طيلة حياته (والدي العزيز (إلى أصدقائي وجميع من وقفوا بجواري وساعدوني بكل ما يملكون وفي أصعدة كثيرة أقدم لكم هذا البحث وأتمنى أن يحوز على رضاكم

وردي بلقاسم.

قائمة المختصرات :

م : المادة

ع : العدد

مج : مجلد

ط : طبعة

ص : صفحة

ج.ر.ج.ج. :الجريدة الرسمية الجمهورية الجزائرية

ق.ع.ج :قانون العقوبات الجزائري

ج:الجزء

ف:فقرة

ص.ص:من الصفحة الى الصفحة

مقدمة

شهدت الجريمة بمختلف أنواعها تطورا سريعا، ساير من خلاله المجرمون تطور الوسائل التكنولوجية، إذ لم يعد استعمال التكنولوجيا مقتصرا على الجوانب التي وجدت من أجلها، بل أصبحت سلاحا ذا حدين، وجد فيها هواة الإجرام ضالتهم، خصوصا في ظل العولمة أين أصبح العالم كقرة صغيرة، نتيجة للثورة الرقمية وما أسهمت فيه الأنترنيت من تقريب للمسافات أين ظهرت ما يعرف بالجرائم المستحدثة والتي يعد الحاسب الآلي والأنترنيت أداتها الأولى، والتي من بينها جرائم تكنولوجيا الإعلام والاتصال.

هاته الجرائم ونظرا لطبيعتها التي تتميز بها، أصبحت ملاذا للمجرمين من فئة خاصة والذين لا يحبذون العنف، ويملون الى التستر وعدم إظهار سلوكهم الإجرامي للعلن، معتمدين في ذلك على مالهم من خبرات وكفاءات في هذا المجال خصوصا في ظل الجهد الذي يكاد منعدما في هذا النوع من الجرائم فيكفي القيام بنقرات محدود على لوحة المفاتيح أو إنشاء رابط بمجرد أن يضغط عليه الضحية تتحقق رغبة الجاني.

فجرائم تكنولوجيا الإعلام والاتصال تعد من الجرائم المميزة والسريعة التطور، الأمر الذي جعل من الصعب الحصول على مفهوم متفق عليه لها، وجعل المشرعين يقرون العديد من القوانين الردعية للحد منها.

وفي هذا السياق فلد سعى المشرع الجزائري الى مسايرة هذا الأمر من خلال إصدار ترسانة من القوانين لعلها تساهم في الحد من هذا الصنف من الجرائم.

ولهذا جاءت دراستنا هذه لتتناول جرائم تكنولوجيا الإعلام والاتصال والبحث في غمار هذا الموضوع لعلنا نسهم ولو بالقليل في إثراه.

أهمية البحث:

تبرز أهمية الموضوع من خلال المكانة التي تحتلها جرائم تكنولوجيا الإعلام والاتصال سواء على الصعيد الوطني أو الصعيد الدولي.

دوافع اختيار الموضوع:

من بين الأسباب التي دفعتنا لاختيار هذا الموضوع نذكر ما يلي:

رغبتنا الشخصية في تناول الموضوع وإثرائه توافق رغبتنا مع ما اقترحها الأستاذ المشرف

الميول الشخصي لدراسة الموضوع والذي يندرج ضمن تخصصنا

باعتبار جرائم تكنولوجيا الإعلام والاتصال من الجرائم المستحدثة والتي لازالت بحاجة لمزيد البحث والتعمق.

أهداف الموضوع:

نهدف من خلال دراستنا هذه الى:

1.عرض مختلف المفاهيم المتعلقة بجرائم تكنولوجيا الإعلام والاتصال

2.إبراز الخصائص التي تتميز بها جرائم تكنولوجيا الإعلام والاتصال والتي يتميز بها المجرم المعلوماتي

3.عرض الجهود الدولية والإقليمية المبذولة لمكافحة جرائم تكنولوجيا الإعلام والاتصال

4.عرض ما بذله المشرع الجزائري من جهد في سبيل التصدي لهذه الجرائم

صعوبات الدراسة:

لعل من أبرز الصعوبات التي واجهتنا هي أن الموضوع رحب و متشعب لذلك يصعب حصره، إضافة الى ضيق الوقت وكذلك صعوبة الاطلاع على مختلف المراجع.

إشكالية الدراسة:

ما مدى فعالية الجهود المبذولة في التصدي لجرائم تكنولوجيا الإعلام والاتصال؟

وانطلاقا من الإشكالية الرئيسية نطرح التساؤلات الفرعية التالية:

- ما المقصود بجرائم تكنولوجيا الإعلام والاتصال؟
- ماهي خصائص جرائم تكنولوجيا الإعلام والاتصال؟
- ما هي الإجراءات المتخذة بشأن مكافحة جرائم تكنولوجيا الإعلام والاتصال؟

مناهج وأدوات الدراسة:

اقتضت منا طبيعة الموضوع اتباع المنهج الوصفي والمنهج التحليلي، وذلك جرائم تكنولوجيا الإعلام والاتصال، ثم تحليل نصوص قانون العقوبات والقوانين التي تخصه من حيث أركان الجريمة والعقوبات الخاصة بمرتكبيها.

خطة الدراسة:

تضمنت دراستنا مقدمة، تلاها فصلين حيث تضمن الفصل الأول

الإطار المفاهيم لجرائم تكنولوجيا الإعلام والاتصال وضم مبحثين كالاتي:

المبحث الأول: تحديد مدلول جرائم تكنولوجيا الإعلام والاتصال

المبحث الثاني: نطاق جرائم تكنولوجيا الإعلام والاتصال

أما الفصل الثاني فعرضنا من خلاله آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال واحتوى كذلك على مبحثين كالاتي:

المبحث الأول: الجهود الدولية والوطنية لمكافحة جرائم تكنولوجيا الإعلام والاتصال

المبحث الثاني: الآليات الإجرائية لمكافحة جرائم تكنولوجيا الإعلام والاتصال

وأخيرا خاتمة تضمنت ما توصلنا اليه من نتائج.

تمهيد:

في ظل التقدم السريع الذي تشهده تكنولوجيا الإعلام والاتصال، وجد صنف من المجرمين ضالتهم الإجرامية، أين أتاحت لهم شبكة الأنترنيت وتوفر أجهزة الحواسيب ملاذا لتنفيذ جرائم متعددة الأضرار فمنها الماسة بالأفراد ومنها الماسة بالجانب المادي، الأمر الذي كل جعل الاهتمام ينصب حول دراسة هذا الصنف من الجرائم والتي تدخل في اطار ما يعرف بالجرائم المستحدثة، نظرا لتميزها عن الجرائم التقليدية، وعليه من خلال هذا الفصل سنحاول الإحاطة بالاطار المفاهيم لجرائم تكنولوجيا الإعلام والاتصال وذلك من خلال مبحث أول نسعى من خلاله لتحديد مدلول جرائم تكنولوجيا الإعلام والاتصال، ومبحث ثان نتناول فيه نطاق جرائم تكنولوجيا الإعلام والاتصال .

المبحث الأول: تحديد مدلول جرائم تكنولوجيا الإعلام والاتصال

أدّى التقدم التكنولوجي الهائل للمعلومات إلى ظهور ما يُعرف بجرائم تكنولوجيا الإعلام والاتصال أو بجرائم تكنولوجيا الإعلام والاتصال، ويرجع ذلك إلى استخدام التكنولوجيا المتمثلة بالحواسيب الآلية وبشبكة الإنترنت في كامل مجالات الحياة اليومية للأفراد، وبحيث أصبح لا يمكن الاستغناء عنها، لتسهيل وتسيير الحياة بشكل عام ،حيث إنّ المعلومات أصبحت في متناول الجميع بصورة يمكن معها القول بأن العالم صار أشبه بقرية صغيرة تترابط بها الحاسبات وشبكات المعلومات، ونتيجة لارتباط جرائم تكنولوجيا الإعلام والاتصال بالتطور التكنولوجي ،ظهرت هناك اتجاهات فقهية متعة قامت بتحديد مفهوم هذه الجرائم وخصائصها التي تتميز بها نظرا لحداثتها[1] وهذا ما سنتناوله في (مطلب أول) على أن نتطرق الى أطرافها في (مطلب ثان) .

المطلب الأول: ماهية جرائم تكنولوجيا الاعلام والاتصال

سنتناول في هذا المطلب مفهوم وخصائص جرائم تكنولوجيا الإعلام والاتصال حيث سنتطرق في (الفرع الاول) مفهوم جرائم تكنولوجيا الإعلام والاتصال اما (الفرع الثاني) تناولنا خصائص جرائم تكنولوجيا الإعلام والاتصال.

الفرع الأول: مفهوم جرائم تكنولوجيا الإعلام والاتصال

جاءت الجريمة في اللغة لمعنيين:

الأول: الذنب، نقول جرم وأجرم وأجترم بمعنى واحد.

[1] – ميرفت محمد حبابية، مكافحة الجريمة الالكترونية، دار اليازوري للنشر والتوزيع، ط1، بيروت، لبنان، 2022، ص21.

[2] – خالد حسن احمد لطفي، الدليل الرقمي ودوره في اثبات الجريمة المعلوماتية، دار الفكر الجامعي، ط1، الإسكندرية، مصر ،2020، ص13.

الثاني: الجناية، كقولهم جرم إليهم وعليهم جريمة أجرم جني جناية وجرم إذا عظم جرمة أي أذنب.[1]

الجريمة لغة: الجريمة والجرم معناها في اللغة الذنب، ومن اشتقاقاتها جرم وأجرم واجترام، وتجرم عليه معناها ادعى عليه ذنباً لم يفعله، وكلمة لا جرم تعني القسم، والجرم هو الذنب أو الجناية.[2]

والجريمة تأتي بمعنى الجناية وبمعنى الذنب، وجاء في لسان العرب: "وجرم إليهم وعليهم جريمة وأجرم: جنى جناية.[3]

تكنولوجيا الإعلام والاتصال: يُقصد بها المعالجة الآلية للمعلومات وهي ترجمة للمصطلح الفرنسي (Informatiqa) وهي اختصار للكلمتين الفرنسيتين (Information)معلومات (Automatique) ذاتياً، وصاحب هذا المصطلح هو قليب داريفوس الذي أراد أن يعني به العلم الذي يربط علم الحاسوب (Computer Science) والمعلومات (Information) والاتصالات (Telecommunication)[4]

الجريمة في معناها العام، فعل يخالف نصاً قانونياً، وذلك لخطورة السلوك المكون لها ويرتب لمن يرتكبه عقوبة جنائية وقد اختلفت الاتجاهات الفقهية حول تحديد جوهر الجريمة، فمنهم من يرده إلى الأخلاق، ومن هؤلاء العلامة (GATOFALO) الذي يعرف الجريمة بأنها جرح لعاطفتي الاستقامة والإحسان، فهي عدوان على شعور أخلاقي ومنهم من يرد هذا الجوهر إلى العدالة، فيعرفها بأنها فعل غير عادل لم يكن كذلك قبل تجريم المشرع له ومنهم من يعرفها بأنها سلوك يهدر مصالح الجماعة ويخالف أهدافها في الاستقرار والعدل.[5]

والجريمة بشكل عام هي: كلُّ أَمْرٍ إيجابي أو سَلِبي يُعاقب عليه القانون، سواء أكان مخالفة أم جُنحة أم جناية أما الإلكتروني في اللغة فهي المنسوب إلى الإلكترون،[6] ومنها الكمبيوتر وأجهزة الاتصال الحديثة التي تعتمد على الإلكترون لتشغيلها، وكما جاء في معجم المعاني هي: آلَةُ الحَاسُوبِ تَعْتَمِدُ عَلَى مَادَّةِ الإلكترُونَ لإجْرَاءِ أَدَقِّ الْعَمَلِيَّاتِ الحِسَابِيَّةِ وَبِأَسْرَعِ وَقْتٍ مُمْكِنٍ وَيُسَمَّى أَيْضاً كمبيوتر.

ونشير هنا الى أنه من الممكن أن تكون هذه الأداة وسيلة متصلة مع الإنترنت وبإمكانها الدخول إلى المواقع الإلكترونية، بمختلف أشكالها واتجاهاتها، ومن أشهر هذه الأدوات الحاسب الإلكتروني (الحاسوب، أو الكمبيوتر أو الآي باد) بمختلف أشكاله، والهواتف الذكية بمختلف أشكالها وأنواعها.[7]

---

[1] –ميرفت محمد حبابية، المرجع السابق، ص21.

[2] – ابن منظور أبي الفضل جمال الدين بن مكرم، لسان العرب، المج 12، دار صادر، ط3، بيروت، لبنان، 1993، ص 91

[3]– زين العابدين الكردي، جرائم الإرهاب المعلوماتية، منشورات الحلبي الحقوقية، ط 1، لبنان، 2018، ص 46.

[4] – عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، دار الحامد للنشر، ط1، عمان، الاردن، 2013، ص24.

[5]– زهراء عادل سلبي، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، دار الأكاديميون للنشر والتوزيع، ط1، الأردن، 2021، ص25.

وتكنولوجيا الإعلام والاتصال هي التكنولوجيا التي أنتجها اندماج تكنولوجيا المعلومات وتكنولوجيا الاتصالات، وهذه التكنولوجيا الحديثة الناشئة عن هذا الاندماج تختلف عن تكنولوجيا المعلومات ما قبل الاندماج، لأن تقنية الإعلام الحديثة ما هي إلا ثمرة المزاوجة بين تكنولوجيا الاتصالات وتكنولوجيا المعلومات (الأجهزة، الوسائط التكنولوجية) الذي أدى إلى ميلاد علم جديد هو علم انتقال المعلوماتية عن بعد télématiqueوهو مصطلح مركب من المقطع الأول لكلمة اتصال عن بعد (télécommunication)والمقطع الثاني من كلمة المعلوماتيةinformatique وهو يعني بذلك علم اتصال المعلوماتية عن بعد أو من مسافة أو بالأحرى موت المسافات[1].

كما أن هناك من يعرف جريمة تكنولوجيا الإعلام والاتصال بأنها ليست هي التي يكون النظام المعلوماتي أداة ارتكابها، بل هي التي تقع على النظام أو داخل نطاقه، ومن أنصار ذلك التعريف روزن بلاك وآخرين الذين يرون أن جرائم تكنولوجيا الإعلام والاتصال هي " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول للمعلومات المخزنة داخل النظام أو التي تحول عن طريقه ويندرج هذا النوع تحت جرائم المعالجة الآلية للبيانات" وفي هذا المعنى أيضاً عرفها البعض على أنها " السلوك السيئ المتعمد الذي يستخدم نظم المعلومات لإتلاف المعلومات أو إساءة استخدامها مما يتسبب أو يحاول التسبب) إما بإلحاق الضرر بالضحية، أو حصول الجاني على فوائد لاستحقها".[2]

وجريمة تكنولوجيا الإعلام والاتصال هي كذلك "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً، ويعبر عنها أيضا بأنها "كل نشاط إيجابي، أو سلبي من شأنه الاتصال دون وجه حق بالكيان المعنوي للحاسب الآلي، أو بنظام المعلومات، أو الإنترنت أو التأثير عليه بتعطيله، أو إضعاف قدرته على أداء وظائفه بالنسخ أو التعديل، بالإضافة أو الحذف، أو بالمناقلة للخصائص الأساسية للبرامج، أو مجرد النسخ أو الوصول إلى البرامج أو المعلومات المخزنة، أو الوصول إليها أثناء نقلها أو إرسالها أو الاتصال بها من غير وجه حق بأية وسيلة كانت".[3]

ومن خلال ما سبق يتبين لنا أن وضع تعريف للجرائم المتصلة بتكنولوجيات الإعلام والاتصال قد كان محلا لاجتهادات الفقهاء أين تناولوا تعريفها من عدة زوايا منها القانونية ومنها تقنية (فنية) والتي تعني بأنها (**نشاط**

[1] حفيظة رفاس، دور السياسة الجنائية للمشرع الجزائري في مكافحة جرائم التكنولوجيا الحديثة، أطروحة دكتوراه، سعيدة، الجزائر ، 2019 -2020 ، ص 13

[2] – خالد حسن احمد لطفي، مرجع سابق، ص25.

[3]– زهراء عادل سلبي، مرجع سابق، ص29.

إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي المقصود).

وهناك جانب من الفقه من يعتبر هذه الجريمة جريمة مستترة تتسم بالسرعة والتطور في وسائل ارتكابها، وهي اقل عنف في التنفيذ من الجرائم التقليدية، وعابرة للحدود ويصعب إثباتها وهناك اتجاه في الفقه يذهب إلى تعريفها اعتماداً على وسيلة ارتكابها.[1]

وتعرف جرائم تكنولوجيا الإعلام والاتصال كذلك، بأنها جميع الأفعال الإجرامية المرتكبة بواسطة الحاسب الآلي من خلال شبكة الأنترنت، ويشمل ذلك: الجرائم الجنسية والممارسات غير الأخلاقية، جرائم الاختراقات الجرائم المالية جرائم إنشاء أو ارتياد المواقع المعادية، جرائم القرصنة. وهي مسألة ذات أبعاد خاصة سيما إذا أدركنا أن العالم الافتراضي هو نتاج اجتماع الاتصالات والتكنولوجيا والمعلومات التي تتجاوز منطق الحدود الدولية هو بيئة مناسبة لارتكاب أفعال يعدها المجرى العادي للأمور في عالمنا المادي أفعال غير مشروعة تصل إلى التجريم في النظم الجنائية المعاصرة.[2]

أما منظمة التعاون الاقتصادي والتنمية OECD فقد عرفتها بأنها "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية.[3]

ومن خلال القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[4]، نجد أن المشرع الجزائري عرف جرائم تكنولوجيا الإعلام والاتصال

بأنها الجرائم الماسة بأنظمة المعالجة الألية للمعطيات، حيث نصت م 2 على المقصود بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي جاء في فحواها ما يلي: يقصد في مفهوم هذا القانون بما يأتي:

[1]- بخوش هشام، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ظل التشريع الجزائري، مجلة الحقوق والعلوم السياسية، مج04، ع01، جامعة خنشلة، الجزائر، 2017، ص196

[2]- علي جبار صالح الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، ط1، عمان، الأردن، 2018، ص34.

[3]- عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003، ص3.

[4] القانون 09-04 المؤرخ في 05 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجريدة الرسمية، ع 47 لسنة 2009.

– الجرائم المتصلة بتكنولوجيات الإعلام والاتصال:

جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.

– منظومة معلوماتية:

أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين.

– معطيات معلوماتية:

أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها.

ومن خلال الأمر 66- 156 المتضمن قانون العقوبات[1] وبالتحديد من م 394 مكرر إلى م 394 مكرر 2 نجد أن المشرع الجزائري حدد مفهوم المساس بأنظمة المعالجة الآلية للمعطيات، حيث حددها في م 394 مكرر بالآتي:

– الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو محاولة ذلك.

– حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو البقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة.

أما م 394 مكررا فقد أشارت إلى ما يلي:

– إدخال بطريق الغش معطيات في نظام المعالجة الآلية أو إزالة أو تعديل بطريق الغش المعطيات التي يتضمنها.

وبالنسبة للمادة 394 مكرر 2 فقد بينت المساس بأنظمة المعالجة الآلية للمعطيات من الآتي:

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

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

[1] الأمر 66-156 مؤرخ في 8 يونيو 1966 ، 49 ج ر المؤرخة في 11-06-1966 معدل ومتمم بموجب القانون 20-15 يتعلق بالوقاية من جرائم الاختطاف الأشخاص و الوقاية منها ، مؤرخ في 30ديسمبر 2020 ، 30 ج رج ج، ع مؤرخة في 30-12-2020

الفرع الثاني: خصائص جرائم تكنولوجيا الإعلام والاتصال

إن الجريمة التقليدية لا تثير أي مشكلة بالنسبة للجهات المكلفة بالبحث والتحري، أما بالنسبة لجريمة تكنولوجيا الإعلام والاتصال فإنها تثير العديد من المشاكل الإجرائية وهذه المشاكل تبدأ من طبيعة البيئة الافتراضية التقنية التي ترتكب فيها فهي لا تخلف أي آثار مادية محسوسة، كما أن هذه الجريمة تتم في الخفاء فكثيراً ما يعمد المجرم المعلوماتي من إخفاء نشاطه الإجرامي عن طريق التلاعب في البيانات والذي غالباً ما يتحقق في غفلة من المجني علية سواء بتدمير أو محو الدليل من مسرح الجريمة، مما يؤدي بصورة عامة الي صعوبة اكتشاف مرتكبها.

ولهذه الأسباب، ولأن جريمة تكنولوجيا الإعلام والاتصال لها طبيعة خاصة بعناصرها ووسائل ارتكابها، فقد تدفع المشرع الجنائي إلى إعادة النظر في الكثير من المسائل الإجرائية خاصة فيما يتعلق بمسألة الإثبات باعتبارها من أهم موضوعات هذا القانون.

والأمر لا يقف عند الاعتماد على الوسائل الاجرائية التقليدية، وانما ينبغي البحث عن دليل يقوي على إثبات هذا النوع من الجرائم.[1]

تختلف جريمة تكنولوجيا الإعلام والاتصال عن الجريمة التقليدية التي تتسم بطابع خاص هو أنها جرائم عابرة للحدود فهي تتم داخل الدولة ويكون تأثيرها منحصراً في تلك الدولة وإنما تلك الجرائم ترتكب عبر ع من الدول لتتم في دولة أخرى وتكون آثارها ممتدة لتصل إلى ع غير محدود من الدول. كما أن هذه الجريمة وفي جميع الأحوال يكون الحاسب الآلي هو أداة ارتكاب الجريمة وأن مرتكبها هو شخص ذو خبرة فائقة في مجال الحاسب الآلي ومحل هذه الجريمة هو دائما المعطيات إما بذاتها أو بما تمثله.[2]

ومن خلال ما سبق تتميز جرائم تكنولوجيا الإعلام والاتصال عن الجرائم التقليدية بمجموعة من الخصائص ولعل أبرز هذه الخصائص ما يلي:

أولاً: عابرة للدول والقارات

جرائم تكنولوجيا الإعلام والاتصال هي شكل من أشكال الجرائم العابرة للحدود، حيث أن جرائم تكنولوجيا الإعلام والاتصال لم تعد ترتكب محلياً، بل أصبحت إمكانية ارتكابها دولياً، حيث أصبح الجاني يقوم بالجريمة عن طريق الدخول الى ذاكرة الحاسب الآلي الموجود في بلد آخر، وهذا الفعل قد يضر شخصاً ثالثا في بلد آخر.

[1]- خالد حسن احمد لطفي، مرجع سابق، ص8.

[2]- علي جبار صالح الحسيناوي، مرجع سابق ،ص23.

ولعل ذلك أصبح بفعل ارتباط المجتمع المعلوماتي بشبكة الإنترنت التي تعبر الأزمنة والأماكن من دون أن تخضع في ذلك لحرس الحدود ونقاط التفتيش، حيث إنه وفق المجتمع الإلكتروني لا يوجد هناك اعتراف بالحدود الجغرافية للدول.

حيث إنه في المجتمع المعلوماتي تذوب الحدود الجغرافية بين الدول التي لا تعترف بالحدود الإقليمية وبالتالي أصبحت ساحتها العالم أجمع، ونتيجة للخسائر الكبيرة التي تتسبب في هذه الجرائم والتي أهمها تحديد الدولة صاحبة الاختصاص القضائي، وكذلك القانون الواجب التطبيق، إضافة إلى الإشكالات المتعلقة بإجراءات الملاحقة القضائية وصعوبة التعاون القضائي بين الدول نظراً لطبيعة هذه الجريمة.[1]

يمكن القول ان ميزة تخطيها للحدود الجغرافية ومن ثم اكتسابها طبيعة دولية، مردها أنه بعد ظهور المعلومات، لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالقدرة التي تتمتع بها الحاسبات الآلية في نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها ألاف الأميال، وقد أدت إلى نتيجة مؤداها أن أماكن متعة في دول مختلفة قد تتأثر بالجريمة الإلكترونية وحجم الأموال والمعلومات المستهدفة والمسافة التي قد تفصل الجاني عن هذه المعلومات والأموال، قد ميزت الجريمة الإلكترونية عن الجريمة التقليدية بصورة كبيرة.[2]

ثانياً: سهلة الارتكاب

لا تتطلب جرائم تكنولوجيا الإعلام والاتصال عنفاً أو مجهوداً كبيراً في ارتكابها، حيث إنها تتطلب نوعاً من الدراية الذهنية والتفكير المدروس القائم على معرفة بتقنية الحاسب الآلي وشبكة الإنترنت على عكس الجرائم التقليدية التي تحتاج إلى مجهود عضلي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، وكسر الأبواب، ولا تكلف الجاني شراء الأسلحة والذخائر وغيرها.

لذلك هذه الجريمة تمنح الجناة في الغالب فرصة لتخفيض تكاليف ارتكابهم لها. [3]

ثالثاً: ترتكب من خلال الوسائل التقنية:

نظراً للطبيعة الخاصة هذه الجريمة فإن هذه الجريمة ترتكب في بيئة إلكترونية، يستلزم التعامل معها استعانة الجاني لوسائل وأجهزة تقنية، كالحاسب الآلي، وكما أنها ترتكب عبر شبكة الإنترنت (العنكبوتية)، حيث تعتبر هذه الأدوات أنها الأساسية لارتكاب هذه الجريمة.

---

[1]- ميرفت محمد حبابية، المرجع السابق ، ، ص41.

[2]- غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، ط 1، القاهرة، مصر ، 2017، ص35.

[3]- ميرفت محمد حبابية، المرجع السابق ، ص43.

ويعد الحاسب الألى أداه لارتكابها حيث تعتبر هذه الخاصية من أهم الخصائص التي تميز جرائم تكنولوجيا الإعلام والاتصال عن غيرها من الجرائم الأخرى ولا سيما الجرائم التقليدية، ذلك لأن شبكة الإنترنت هي إحدى التقنيات الحديثة التي أفرزها تطور الحوسبة، ولذلك فإن ارتباطها بالحاسب الآلي هو أمر لا مفر منه، باعتباره النفذة التي تطل بها تلك الشبكة على العالم الخارجي وإن كنا اليوم نعاصر إمكانية استعمال الإنترنت عبر الهاتف الخلوي. [1]

رابعاً: جريمة يصعب اكتشافها

توصف جرائم تكنولوجيا الإعلام والاتصال بأنها خفية ومستترة في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة، لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، كإرسال فيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم. [2]

تتسم جرائم تكنولوجيا الإعلام والاتصال بانها مستترة خفية في أغلبها، حيث أن المجني عليه لا يلاحظها غالبا مع أنها تقع أثناء وجوده على الشبكة ولكن لا يكون عالما بها ولا ينتبه إليها إلا بعد فترة من وقوعها وفي بعض الأحيان لا يكتشف أمرها.

كما أن توافر المعرفة والخبرة التقنية لدى الجاني في هذا المجال يؤدى إلى صعوبة اكتشاف جريمته وذلك باتباعه الطرق وأساليب لا يفطن إليها المستخدم العادي الشبكة مثل ارسال فيروسات مدمرة، سرقة أموال وبيانات، تجسس وغيرها".[3]

تعتبر جرائم تكنولوجيا الإعلام والاتصال التي لا تترك أثر لمتابعتها وملاحظتها بل وقد يستخدم الجاني برامج تقنية من خلالها تعرقل الوصول إليه أو معرفة التقنية للجريمة المرتكبة أياً كان نوعها، وكما أن المجني عليه لا يكتشفها مباشرة ولا يشعر بها إما لضعف قدرته الفنية على ذلك بالمقارنة بمرتكب الجريمة أو للمهارات الفنية التي استخدمها الجاني عند ارتكابه للجريمة، أو لعدم رغبة المجني عليهم بالتبليغ عن وقوع الجريمة حفاظاً على السمعة وفقد الثقة فيهم، حيث تلجأ (الشركات والمصانع والجمعيات والمؤسسات، والبنوك، والجامعات) ذات السمعة المرموقة إلى التستر على هذه الجريمة، ويفضلون حلها من خلال موظفي تكنولوجيا المعلومات لديها.[4]

تتميز هذه الجريمة بقلة ع الحالات التي يتم اكتشافها بالفعل إذا ما قارنا ذلك في ضوء ما تم اكتشافه من الجرائم التقليدية، ويرى البعض أن من بين الأسباب وراء صعوبة اكتشاف هذه الجرائم يرجع إلى تميزها بأنها لا يشوب

---

[1]- غادة نصار، مرجع سابق ، ص35.

[2] رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة ، ع41، جامعة احمد دراية ،ادرار ، 2017،ص441.

[3]- غادة نصار، مرجع سابق ، ص37.

[4]- ميرفت محمد حبابية، المرجع السابق ، ص45.

ارتكابها أي عمل من أعمال العنف كما أنها لا تترك أثارا. وكذلك وسيلة تنفيذها التي تتسم في أغلب الحالات بالطابع التقني الذي يضفى عليها الكثير من التعقيد بالإضافة إلى الإحجام عن الإبلاغ عنها في حالة اكتشافها لخشية المجنى عليهم من فقد ثقة عملائهم، فضلا عن إمكانية تدمير المعلومات التي يمكن أن تستخدم كدليل في الإثبات مدة لا تقل عن الثانية الواحدة.[1]

خامساً: جريمة يصعب إثباتها

يعد إثبات جرائم تكنولوجيا الإعلام والاتصال من الصعوبة بمكان حيث يصعب تتبعها واكتشافها فهي لا تترك أثرا يقتفى، حيث تعتبر مجرد أرقام فمعظم جرائم تكنولوجيا الإعلام والاتصال تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أنها تفتقر إلى الدليل المادي التقليدي كالبصمات مثلا. ومن جهة أخرى فإن تعقبها يتطلب خبرة فنية يصعب تواجدها لدى المحقق العادي للتعامل معها، زيادة على ذلك يعمد مرتكب الجريمة الالكترونية إلى ممارسة التمويه عند ارتكابها والتضليل والتحايل بغاية عدم التعرف على مرتكبيها.[2]

وذلك نظرا للأسباب التالية : [3]

- أنها جريمة لا تترك أثر لها بعد ارتكابها.
- صعوبة الاحتفاظ الفني بأثارها إن وجدت.
- أنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها.
- أنها تعتمد على الخداع والتضليل في التعرف على مرتكبيها.
- أنها تعتمد على الذكاء في ارتكابها.
- ترتكب من قبل شخص ذو دراية فائقة بالإنترنت.
- سهولة اخفاء معالم الجريمة والتخلص من أثارها.
- يلعب البعد الزمنى (اختلاف المواقيت بين الدول). والبعد المكاني (تنفيذ الجريمة عن بعد)، والبعد القانوني اي تطبيق القانون دورا مهما في تثبيت جهود التحري والتنسيق الدولي لتعقب مثل هذه الجرائم.

وعليه فجرائم تكنولوجيا الإعلام والاتصال نظرا لأنها تقع في بيئة إلكترونية فإن الأدلة التي تخلفها تكون أدلة إلكترونية حيث يستطيع المجرم الإلكتروني التخلص من الآثار المادية لجريمته بفضل التقنيات المعلوماتية، وإخفاء

---

[1]- غادة نصار، مرجع سابق ، ص36.

[2] نعيمة دوادي، الجريمة الالكترونية (خصائصها ومجالات استخدامها وأهم سبل مكافحتها)، مجلة مهد اللغات، مج 2، ع 1، جامعة حسيبة بن بوعلي، الشلف، الجزائر - 2020، ص49.

[3]- غادة نصار، مرجع سابق ، ص36.

الدليل الرقمي الإلكتروني حيث يستخدم المجرم تقنية لارتكاب الجريمة ويستخدم تقنية اخرى لإخفاء العمليات التقنية التي تم استخدامها لارتكاب الجريمة، وهذا بدوره يجعل التحري عن الدليل الرقمي الإلكتروني للجريمة من قبل المختبر الجنائي الإلكتروني والخبراء المختصين صعباً للغاية. [1]

وبالتالي فإن هذه الجرائم وفي الغالب لا تترك اثر لها بعد ارتكابها، كما يصعب الاحتفاظ الفني بآثارها إن وجدت وهذا كله يصعب من مهمة المحقق العادي في التعامل معها، حيث يستخدم فيها وسائل فنية غير عادية تعتمد التمويه في ارتكابها والتضليل في التعرف على مرتكبيها، وفي كل الأحوال تحتاج مواجهة هذه الجريمة إلى خبرة فنية عالية متخصصة لإثباتها. [2]

سادساً: عدم وجود تعريف متفق عليه لجرائم تكنولوجيا الإعلام والاتصال على الصعيد الدولي

من خلال بحثنا وجدنا أنه لا يوجد تعريف موحد لجرائم تكنولوجيا الإعلام والاتصال، وأنه يوجد عدة تسميات جريمة الحاسب الآلي، الجريمة المعلوماتية، جرائم تكنولوجيا الإعلام والاتصال، جرائم الإنترنت وتعود هذه التسميات إلى المعايير والأسس التي استند عليها الفقهاء والخبراء القانونيون، مما جعل قراصنة تكنولوجيا المعلومات يستغلون هذا الاختلاف واعتباره أرضية خصبة للاستمرار بارتكاب جرائم تكنولوجيا الإعلام والاتصال واعتداءاتهم غير المشروعة وأيضا ابتكار أساليب وتقنيات جديدة لذلك.[3]

سابعاً: جريمة تسبق الخبرة التقنية لدى الجهات القضائية والخبراء الأمنيين لدى الأجهزة الأمنية في الدولة

إن التطور السريع الذي تشهده تكنولوجيا المعلومات أضفى بظلاله على الجرائم الناشئة عن الإنترنت حيث ان أساليب ارتكابها دائما في تطور مستمر، وأن المجرمين في مختلف أنحاء العالم يستفيدون من الشبكة في تبادل الأفكار والخبرات الإجرامية فيما بينهم. [4]

وهذا ما جعل جرائم تكنولوجيا الإعلام والاتصال تتميز بأنها تسبق الخبرة لدى الجهات المختصة بملاحقتها ومتابعتها ونظرا لما تطلبه هذه الجرائم من تقنية لارتكابها فهي تتطلب أسلوباً خاصاً في التحقيق والتعامل، الأمر الذي لم يتحقق في الجهات الأمنية والقضائية لدينا، ونظراً لنقص المعرفة التقنية وهذا الأمر يتطلب تخصص في تقنية لحماية الجهاز الأمني والقضائي من هذه الظاهرة وتمكنه من الحصول على الأدلة وكشف جرائم تكنولوجيا الإعلام والاتصال.

---

[1]- ميرفت محمد حبابية، المرجع السابق ، ص46.

[2] رحموني محمد، مرجع سابق، ص441.

[3]- ميرفت محمد حبابية، المرجع السابق ، ص46.

[4]- غادة نصار، مرجع سابق ، ص37.

حيث إن هناك فروقات معرفية وتقنية ما بين مرتكب الجريمة الفاعل وما بين الخبراء الجنائيين والسلطة القضائية بفرعيها القضاء والنيابة لا وعليه لا بد من العمل على تدريب هذه الجهات بشكل كاف ليتمكنوا من الإلمام والقدرة على الربط ما بين الدليل الإلكتروني والنص القانوني، حيث إن جرائم تكنولوجيا الإعلام والاتصال سبقت التشريعات فمنها مازال غير منصف في ملاحقة المجرم، حيث إن الأمر يتطلب تدخل المشرع لسن القوانين الحديثة التي تتلاءم بشكل متطور مع تطور جرائم تكنولوجيا الإعلام والاتصال وزيادة التعاون الدولي لمكافحتها.[1]

ثامناً: جريمة قليلة المخاطرة

جرائم تكنولوجيا الإعلام والاتصال لا تحتاج إلى عنف عند تنفيذها، أو مجهودا كبيرا، وإنما تنفذ بأقل مجهود ممكن حيث يعتمد الجاني وبشكل رئيسي على الخبرة في المجال المعلوماتي. وهذا عكس الجرائم التقليدية التي تحتاج إلى عنف ودماء ومجهود كبير يقوم به الجاني غالبا في الوصول إلى غايته.[2]

وهذا ما جعل جرائم تكنولوجيا الإعلام والاتصال تتميز بأنها قليلة المخاطرة، نظرا لعدم وجود مواجهة مباشرة مع المجني عليه أو غيره ولا خطر لمواجهة الشرطة كما في الجرائم التقليدية.[3]

المطلب الثاني: أطراف جرائم تكنولوجيا الإعلام والاتصال وأركانها

وسنتناول في هذ المطلب اطراف الجريمة في(الفرع الاول) اما في (الفرع الثاني) أركان جريمة تكنولوجيا الإعلام والاتصال.

الفرع الأول: أطراف الجريمة

أولا: المجرم المعلوماتي

المجرم الإلكتروني ليس مجرماً عادياً، فهو يتميز بمميزات تجعله خبيراً في التقنيات الإلكترونية، فهو إنسان يمتلك نسبة ذكاء عالية جداً، يشكل بموجبها على المحقق التقليدي صعوبة في تتبع جرائم تكنولوجيا الإعلام والاتصال والكشف عنها وإقامة الدليل عليها،[4] وعليه سوف نبين المقصود بالمجرم في اللغة والاصطلاح وصولاً إلى معرفة المقصود بالمجرم الإلكتروني.

---

[1]- ميرفت محمد حبابية، المرجع السابق ، ص47.

[2]- غاد غادة نصار، مرجع سابق ، ص37.

[3]- ميرفت محمد حبابية، المرجع السابق ، ص47.

[4]- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان ، 2014 ، ص 41.

فالمجرم كلمة مشتقة من الفعل جرم ومضارعه يجرم ومصدره إجرام، وأجرم جرماً وتجرم عليه ادعى عليه قلباً لم يرتكبه. [1]

عرف المجرم بأنه الشخص الذي يرتكب جريمة بمفهومها القانوني وأصدر القضاء حكماً بإدانته وأصبح هذا الحكم نهائياً غير قابل للطعن فيه، حيث إن الدليل على أن المجرم هو ليس ذلك الشخص الذي يقع فقط تحت طائلة القانون وتثبت إدانته فهناك كثير من الأشخاص يرتكبون الجرائم وما يزالون طلقاء لم تطلهم يد العدالة بعد.

فهل تنتفي عنهم صفة الإجرام؟ كلا. [2]

المجرم الإلكتروني مجرم أو عا من المجرمين لا يرتكبون سوى جرائم الكمبيوتر أي أنهم يتخصصون في هذا النوع من الجرائم، دون أن يكون لهم أي صلة بأي نوع من الجرائم التقليدية الأخرى مما يبين أن المجرم الذي يرتكب الجريمة المعلوماتية مجرم في الغالب متخصص في هذا النوع من الإجرام.[3]

أما إذا جئنا إلى تعريف المجرم التقليدي مقارنة مع المجرم المرتكب للجرائم المستحدثة، فإننا نقول إن المجرم التقليدي هو الشخص العادي الذي اعتاد ارتكاب الجريمة العادية أو نوع محدد منها نظراً لظروف أحاطت به كونه غير متكيف اجتماعياً، مستخدماً بذلك أدوات تقليدية وصولاً إلى هدفه حتى لو اضطر إلى استخدام العنف على عكس المجرم الحديث الذي سخر التطور الهائل في تكنولوجيا المعلومات والاتصالات وصولاً لهدفه.[4]

ولعل هذه الخصائص على النحو الآتي:

1-المجرم الإلكتروني يتمتع بالمهارة والذكاء

القيام بجرائم تكنولوجيا الإعلام والاتصال يتطلب درجة من الدقة والمهارة والذكاء، لكي يتعامل مع الحاسب الآلي أو شبكة الإنترنت وكي يعمل على اختراق الشبكات ويتمكن من زرع الفيروسات والقنابل الزمنية والمنطقية التي من شأنها أن تعمل على تدمير وإتلاف برامج الحاسب الآلي.

ومن هؤلاء المجرمين من يشكل خطراً وتهديداً لأمن المجتمع نتيجة لما يتمتعون به من قدرة ذكاء فائقة يتمكنون بموجبها من تجاوز جدران الحماية الأمنية لأنظمة المعلومات المختلفة في سبيل ارتكاب المجرم لجريمته الإلكترونية. [5]

---

[1]- ميرفت محمد حبابية، المرجع السابق ، ص58.

[2]- عبد الكريم الردايدة، مرجع سابق، ص34.

[3]- غادة نصار، مرجع سابق ، ص43.

[4]- عبد الكريم الردايدة، مرجع سابق، ص34.

[5]- ميرفت محمد حبابية، المرجع السابق ، ص61.

والسبب في ذلك أن هذا المجرم يمتلك من المهارات ما يؤهله للقيام بتعديل وتطوير في الأنظمة الأمنية الإلكترونية وكسر واختراق برامج الحماية، حيث بإمكانه أن يكون تصور كاملا لجريمته حتى لا يتم اكتشاف أفعاله الإجرامية من خلال الشبكات أو داخل أجهزة الكومبيوتر، وبالتالي تتم ملاحقته وتتبعه فالمجرم الإلكتروني عادة يمهد لارتكاب جرائمه بالتعرف على كافة الظروف المحيطة به، لتجنب ما من شأنه ضبط أفعاله والكشف عنه.[1]

2-المجرم الإلكتروني لا يميل إلى العنف ولا يستخدمه:

ينتمي الإجرام الإلكتروني إلى إجرام الحيلة، حيث أن المجرم الإلكتروني لا يلجأ إلى العنف في ارتكاب جرائم تكنولوجيا الإعلام والاتصال، حيث أن هذا النوع من الجرائم لا يستلزم أي قدر من العنف. [2]

يلجأ المجرم الخاص بهذا النوع من الجرائم إلى العنف في ارتكاب جرائمه، خاصة أنه لا يواجه عند ارتكابه هذه الجرائم شخصاً حقيقياً، بل يتعامل مع وسائل وأدوات تقنية متطورة يسخرها لتنفيذ جريمته. [3]

3-المجرم الإلكتروني مجرم متخصص:

أثبتت العديد من الدراسات في هذا المجال أن المجرم الإلكتروني يكون متخصصاً في هذا النوع من الجريمة، دون أن يكون له أية صلة بأي نوع من الجريمة التقليدية الأخرى.[4]

حيث أن الأشخاص المرتكبين للجرائم المستحدثة تجد أنهم ينفردون بتوعية معينة من الجرائم التي يرتكبونها، وهذا يعود إلى علمهم وثقافتهم السابقة والخاصة بطبيعة ومكونات م التي يقع عليها الفعل المجرم.

كما إنهم أيضاً يتميزون بأسلوب محدد في ارتكاب الجريمة، وهذا يعود إلى عوامل كثيرة تتعلق بثقافة ذلك الشخص وعلمه وخبرته السابقة، والتي أعطت لشخصيته أسلوباً ينفرد فيه عن غيره.[5]

4-المجرم الإلكتروني مجرم محترف:

يتمتع المجرم المرتكب للجريمة المستحدثة بقدر كبير من الذكاء، حيث يستخدم وسائل التقنية الحديثة من كمبيوتر وأجهزة اتصال وغيرها كوسائل مساعدة لتنفيذ جريمته، حيث يتميز بالاحتراف أثناء استخدامه لتلك الوسائل بطريقة تفوق الأشخاص العاديين المستخدمين لهذه

---

[1]- طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة، القاهرة، ط1، مصر، 2009، ص 177.

[2]- ميرفت محمد حبابية، المرجع السابق ، ، ص61.

[3]- عبد الكريم الردايدة، مرجع سابق، ص35.

[4]- ميرفت محمد حبابية، المرجع السابق ، ص62.

[5]- عبد الكريم الردايدة، مرجع سابق، ص35.

الوسائل. [1]

كما أنه يتمتع بقدرة ومهارة تقنية يستغلها في اختراق الشبكات وكسر كلمات المرور أو الشفرات بغاية الحصول على البيانات والمعلومات الموجودة في أجهزة الكومبيوتر ومن خلال الشبكات.[2]

وعليه فالمجرم الإلكتروني يتميز بمهارة فنية عالية لا يستطيع بموجبها الشخص العادي القيام بها، حيث يمتلك قدرة عالية على التلاعب بالحاسوب وكذلك بإمكانه التهرب من كشف الجريمة، وبإمكانه اختراق كافة جدران الحماية الأمنية لأنظمة المعلومات، وهذه الاختراقات يكتسبها المجرم الإلكتروني إما عن طريق دراسة تكنولوجيا المعلومات أو عن طريق الخبرة العملية أو التفاعل الاجتماعي مع الآخرين. [3]

5-يغلب عليه طابع التكيف الاجتماعي

يتميز بأنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به بل على العكس من ذلك نجده إنسان متوافق مع مجتمعه[4] ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو بغاية إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يتم تشغيله بها، أو بدافع الحصول على الأموال، أو بهدف الانتقام.[5]

حيث إن هذا النوع من المجرمين يرتكب جرائمه من خلال استخدامه لتلك الوسائل التقنية الحديثة، فهو لا يكون ظاهراً في الغالب، ويتعايش مع الوسط الاجتماعي الذي يعيش فيه، ولا يظهر لهم العداء ولا يشعرون منه ذلك، حيث إن هذا التكيف لا يقلل من خطورته الإجرامية بل قد تزداد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه".[6]

5-المجرم الإلكتروني مجرم عائد إلى الإجرام

يعود كثير من المجرمين الإلكترونيين إلى ارتكاب جرائم أخرى في مجال الحاسب الآلي، انطلاقاً من سد الثغرات التي أدت إلى التعرف عليهم وبعد ذلك كشف الجريمة وينتهي بهم الأمر في تقديمهم للمحاكمة.[7]

---

[2]- محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، عمان، الأردن، ص 14

[3]- ميرفت محمد حبابية، المرجع السابق، ص62.

[4]- عبد الصبور عبد القوي علي، الجريمة الالكترونية، الطبعة الأولي، دار العلوم للطباعة والنشر، القاهرة، مصر، 2007.ص13

[5]رحموني محمد، مرجع سابق، ص444.

[6]- عبد الكريم الردايدة، مرجع سابق، ص35.

[7]- ميرفت محمد حبابية، المرجع السابق، ص62.

ثانيا: (الضحية) الأشخاص الطبيعيون

يتعرض كثير من الأشخاص لأي شكل من أشكال الجريمة المعلوماتية فيما إذا كان من بين الأشخاص الذين يحفظون أسرارهم التجارية أعمالهم وشؤونهم داخل الحاسب الخاص بهم.

وينبغي لقيام الجريمة المعلوماتية هنا أن يكون الشخص العادي (المجني عليه) هنا من بين الأشخاص الذين قد ينجذب إليهم الجناة كأن يكون ذا منصب سياسي رفيع أو رجل أعمال مرموق أو صاحب شهرة عالمية في قطاع من القطاعات الاقتصادية أو الاجتماعية أو العسكرية.

ويلاحظ أن تحديد نطاق خاص يضم فئات المجني عليهم في جرائم تكنولوجيا الإعلام والاتصال يعد أمراً صعبا بسبب حقيقة أن المجني عليهم في هذه الجرائم غالياً يكتشفونها بعد حصولها، الأمر الذي يدفعهم في غالب الأحيان إلي السكوت أو الإذعان لها، وتفضيل الموقف السلبي عن القيام بالتصريح عن تعرض أجهزتهم ومعلوماتهم التي يفترض فيها الأمان والسرية الي الدخول غير المشروع والانتهاك، وهو الأمر الذي يشكل بحد ذاته سبباً في ازدياد معدل جرائم تكنولوجيا الإعلام والاتصال وصعوبة اكتشافها أو الحد منها، ومن ثم كثر مشكلاتها على الصعيد القانوني والعملي.[1]

الفرع الثاني: أركان جريمة تكنولوجيا الإعلام والاتصال

الجريمة مبدئيا هي كل فعل أو امتناع صادر من ارادة جنائية، يحظره القانون الجنائي ويعاقب عليه، بسبب ما يحدثه من اضطراب جماعي.

ولكن الجريمة لا تقوم الا إذا توافرت أركانها، التي تنقسم إلى ثلاثة أركان وهم:

أولا الركن الشرعي (القانوني):

ويقصد به أن يكون هناك نص قانوني أو شرعي يجرم الفعل أو يعاقب على إتيانه.

ويشترط في النص أن يكون نافذ المفعول وقت اقتراف الفعل، أن يكون ساريا على المكان الذي اقترف فيه الفعل وعلى الشخص الذي اقترفه.

وعلى هذا يعتبر الركيزة الأساسية لوصف السلوك جريمة معاقب عليها أم لا، وجود النص القانوني المحدد لنوع الجريمة، وهذا تطبيقا لمبدأ شرعية التجريم والعقاب أو ما يصطلح علية في المجال القانوني بمبدأ لا جريمة ولا عقوبة إلا بنص".[2]

– خالد حسن احمد لطفي، مرجع سابق، ص44.43

ثانيا: الركن المادي:

يتكون الركن المادي من عناصره الثلاثة السلوك المادي والنتيجة الإجرامية والعلاقة السببية ما بينهما، والركن المادي هو الفعل الظاهري الذي يبرز الجريمة ويعطيها وجودها وكيانها في الخارج.

1.السلوك الإجرامي:

إن ارتكاب جرائم تكنولوجيا الإعلام والاتصال يحتاج إلى منطق تقني يتمثل بسلوك مادي إيجابي مما يجعل جرائم تكنولوجيا الإعلام والاتصال ذات طابع موحد فهي تباشر من حيث السلوك أو النشاط المادي فيها بوصفه أحد عناصر الركن المادي يضاف إلى فلسفة الركن المادي فيها، تدارك هذا الأمر المشرع المقارن حين النص على جرائم يمكن أن ترتكب عبر الحاسوب ففي مثل هذه النصوص نجد المشرع يقرر صراحة عبارة ... إذا ارتكبت الجريمة باستخدام الحاسوب..." أو عبارة .... باستخدام المعالجة الآلية للبيانات... ويكون بهذه الحالات المشرع مدركا للقيمة الموحدة للشروع في ارتكاب جريمة عبر الأنترنت أو باستخدام الحاسوب المرتبط بالأنترنت.[1]

ضرورة استخدام الآلة وسيطاً لارتكابها مما يجعل جرائم تكنولوجيا الإعلام والاتصال خاصة والحاسوب عامة من نوعية جرائم الوسيلة، وهذا الأمر غير مقبول لمشروعية هذا الوسيط المستخدم لارتكاب الجريمة وهو هنا الحاسوب أو الشبكة أو الخادم... وهذه أدوات مشروعة بحسب الأصل.

من اللازم استخدام الحاسوب لكي يمكن ارتكاب الجريمة التي ترتبط بإمكانية استخدام ومدى تمتع الشخص بالتقنية الكافية في هذا الشأن لارتكاب الجريمة، وأن كل من الحاسوب والأنترنت يدخلان في طائلة المشروعية لا يمكن أن تقوم أي من الجرائم التي أشار إليها المشرع سوى باستخدامها وهذا يجعل مسألة استخدام الحاسوب والأنترنت جزءاً من النشاط المادي في الجرائم الناشئة عن استخدام أي من الحاسوب والأنترنت.

مما تقدم نرى أنّ النشاط المادي يبنى على العلاقة التقنية بين مرتكب جريمة الأنترنت وبين الآلة وفي كيفية تحديد حدوث السلوك الإجرامي باستخدام الأنترنت والحاسوب وجد المشرع الأمريكي أن استخدام الأنترنت ليس له هدف في ذاته فلا يستخدم الأنترنت لمجرد الاستخدام وإنما هو تحقق فوائد عظيمة في الوقت الذي يمكن أن تكون مهدا لارتكاب الجريمة أيضا لذلك لم يمانع في تحديد طرائق السلوك الاجرامي بشكل تفصيلي لكي يمكن القول بقيام النشاط الاجرامي بما يجعل هذا النص ينطبق مع مراعاة تحقيق النتيجة المشار إليها.[2]

- علي جبار صالح الحسيناوي، مرجع سابق ،ص27.26.

2.العلاقة السببية ما بين السلوك الإجرامي والنتيجة:

وهي إسناد ماديات إلى مصدرها بشكل تسلسلي وهي من طبيعة مادية كأصل عام، فالعلاقة السببية هي علاقة مادية وليست علاقة قانونية والمشرع يعترف بها قانونا صراحة أو ضمنا ولا يحيلها إلى الوصف القانوني بحيث تبرز.

3.النتيجة الإجرامية:

وتعني النتيجة الاجرامية ذلك التغيير الذي يحدث في العالم الخارجي.

كأثر للسلوك الإجرامي والذي يعتد به القانون فيجعله عنصر من العناصر المكونة لجريمة معينة فلا تقع الجريمة تامة إلا بتوافره مع بقية العناصر الأخرى. فالنتيجة الإجرامية هي إحدى عناصر الركن المادي في الجريمة.

تثير النتيجة الاجرامية في جرائم تكنولوجيا الإعلام والاتصال مشاكل متعة حيث مسألة مكان وزمان تحقق النتيجة الإجرامية، فهل تعد هذه الجريمة مرتكبة سلوكا ونتيجة في العالم الافتراضي أو أن هناك امتداداً للنتيجة لكي يتحقق منتهاها في العالم المادي بينما يتحقق أولها في العالم الافتراضي ومن ثم يكون هناك امتداد في النتيجة من العالم الافتراضي إلى المادي؟ مع الأخذ في الاعتبار أن هناك من الجرائم التي يكون لها وجود سواء عبر الأنترنت أم بمعنى أكثر وضوحا هي من ضمن جرائم التقنية التي لا يمتد أثرها إلى العالم المادي ويشمل ذلك بالطبع صعوبة اكتشافها وإقامة الدليل على ارتكابها ويتجه الفقه المقارن إلى محاولة إرساء رؤية الإفساد أو الإعاقة لكي تكون المحصلة في العمل الإجرامي ومن ثم فإن النهج هنا ينطلق نحو الاعتداء بالضرر في تقدير قيام المسئولية الجنائية حيث ينبغي وفقا لهذه النظرية الأخذ في الاعتبار ضرورة أن تكون كل علاقة وهمية على تعطيل الخدمات التي يقدمها الحاسوب للمستخدم الشرعي، كل ذلك يؤدي بالضرورة إلى الاهتمام بالنتيجة الاجرامية على حساب النشاط المادي للجريمة من حيث كونه الخلاصة النهائية التي ما تحرك المشرع المقارن إلا بسببها.[1]

ثالثا: الركن المعنوي في جرائم تكنولوجيا الإعلام والاتصال:

ويعني الجاني أو المجرم تحديدا فالركن المعنوي هو المسلك الذهني والنفسي للجاني باعتباره محور القانون الجنائي ذلك أنه في إطار هذا الركن تتوافر كافة مقومات المسئولية الجنائية من إسناد وإذناب مع إقرار حق الدولة في العقاب الذي يبنى على هذه المقومات، ويعرف الركن المعنوي بأنه العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها وهذه العلاقة هي محل الذنب في معنى استحقاق العقاب ومن ثم يوجه إليها لوم القانون وعقابه. واجهت جرائم تكنولوجيا الإعلام والاتصال مشكلات تتعلق بمدى تطلب القصد الجنائي فيها وبشكل يمكن أن يحقق غرض المشرع في هيكلة الإدانة.

إن تفهم موقف الركن المعنوي في جرائم تكنولوجيا الإعلام والاتصال يعد من الأمور الهامة في تحديد طبيعة السلوك المرتكب وتكييفه لتحديد النصوص العقابية التي يلزم تطبيقها إذ بدون الركن المعنوي لن يكون هناك سوى جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع لذلك فإن اتجاه القضاء المقارن في تطلب العمد بالنسبة لجريمة الولوج فقط يعد من الموضوعات المنتقدة هنا، فالتمييز بين جريمة الدخول غير المشروع على نظام المعالجة الآلية للبيانات وبين جريمة تجاوز الصلاحيات في الدخول على مثل هذا النظام يعد تمييزاً دقيقا.[1]

– علي جبار صالح الحسيناوي، مرجع سابق ،ص31.28

المبحث الثاني: نطاق جرائم تكنولوجيا الإعلام والاتصال

مما لا شك فيه أن مختلف التشريعات العقابية تصدت للعديد من الجرائم الواقعة على الأموال والأشخاص، ومنها قانون العقوبات الجزائري وذلك من خلال المواد من 254 إلى417 مكرر 3 ق ع.

لكن نظرا لإفرازات التقدم العلمي الذي حققه الإنسان، فقد تغيرت النظرة إلى الجريمة ذاتها، فبعد أن كانت تتسم في التقليدية في طرق ارتكابها، سرعان ما تطورت وظهرت صور مستحدثة تختلف عن نظيرتها التقليدية لاسيما في وسيلة ارتكابها أو محلها وكذلك درجة خطورتها.

فالثورة الرقمية أتاحت للمجرم المعلوماتي إمكانية تسخير وسائل تقنية المعلومات في ارتكاب وتسهيل ارتكاب أغلب الجرائم الواقعة على الأموال والأشخاص.[1]

وعليه سيتم التطرق من خلال هذا المبحث إلى أهم صور جرائم الاعتداء على الأموال بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية في المطلب الأول ومن ثم أستعرض أهم صور جرائم الاعتداء على الأشخاص بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية في المطلب الثاني.

المطلب الأول: الجرائم الماسة بالأفراد

نظرا لانتشار الوسائل التقنية في عصرنا الحالي، والتي وجد العابثون من ذوي النزعة الإجرامية ضالتهم في استغلال هذه التقنية وتحقيق مآربهم الإجرامية عن طريقها، فتحول بذلك الإنسان إلى هدف من أهداف مجرمي تقنية المعلومات، بعد أن أتاحت الوسائل التقنية تحقيق أغلب صور الاعتداء على الأشخاص وبأبسط الأساليب، فأصبح بإمكان هؤلاء الاعتداء على حق الإنسان في سلامة الجسم والحياة، وحقه في شرفه وسمعته وكذلك في حرمة حياته الخاصة، الأمر الذي جعل التوافق بين السياسة الجنائية وحق الفرد في سلامة شرفه وحرياته وبدنه من كل أذى يحيط به مطلبا أساسيا لمواجهة هذا النوع من الإجرام الذي تستخدم فيه الوسائل التقنية المستحدثة.

يقصد بجرائم الاعتداء على الأشخاص بصفة عامة :تلك الجرائم التي تنال بالاعتداء أو التهديد بالخطر حقوق ذات طابع شخصي بحت أي تلك الحقوق اللصيقة بشخص المجني عليه والتي تعبر عن المقومات الأساسية لشخصيته، وهي تخرج عن دائرة التعامل الاقتصادي؛ وأهمها الحق في الحياة وفي سلامة الجسم، والحق في الحرية وفي صيانة العرض والحق في الشرف والاعتبار"[2]

---

[1] حبيباتني بثينة، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أطروحة لنيل شهادة دكتوراه ل. م. د في القانون العام، كلية الحقوق، جامعة الجزائر1، 2020، ص 120.

[2]– هبة نبيلة هروال، جرائم الأنترنت دراسة مقارنة، أطروحة دكتوراه كلية أبي بكر بلقايد تلمسان، الجزائر ، 2013–2014، ص73.

وتعد الجرائم الماسة بالأفراد من جرائم تكنولوجيا الإعلام والاتصال واسعة الانتشار عبر الشبكات، حيث تستخدم أسلوب القذف والسب وتشويه السمعة وغيرها من الأفعال اللاأخلاقية بغرض المساس بشرف الشخص أو النيل من كرامته، وقد يكون عبر خطوط الاتصال أو عبر البريد الإلكتروني أو عبر صفحات الويب أو عبر غرف المحادثة والدردشة.[1]

وتعد هذه الطائفة من الجرائم والتي أوردها المشرع في الفصل الأول من الباب الثاني الوارد في قانون العقوبات وينصرف ذلك إلى الأقسام الخمسة المتضمنة في المواد من 254 إلى 303 مكرر 41 من قانون العقوبات الأكثر وقوعا وانتشارا في مجتمعاتنا مقارنة مع غيرها، وهناك أسباب كثيرة تجعل الأشخاص يقومون بها سواء بالنظر لسهولة ارتكابها أو لعدم استخدام وسائل يصعب تحصيلها أو لقرب الضحية من الجاني أو لطبيعة العلاقة التي تجمعها أو لأسباب أخرى، الأمر الذي جعل مختلف التشريعات العقابية تتصدى لها وتتناولها في منظومتها العقابية.

ولهذا سأحاول معالجة كل من جريمة السب والقذف عبر الوسائط الإلكترونية في القرع الأول، أما الفرع الثاني سأخصصه لجريمة الاعتداء على حرمة الحياة الخاصة. [2]

الفرع الأول: جريمة السب والقذف

تعد جرائم السب والقذف من أكثر الجرائم انتشار، وهي جرائم للمساس بشرف الغير وسمعتهم ويكون عن طريق القذف والسب كتابيا، أو عن طريق المطبوعات أو رسوم، عبر البريد الإلكتروني، صفحات الويب بعبارات تمس الشرف.[3]

ولقد عرف المشرع الجزائري القذف ولقد اعتبر المشرع الجزائري صراحة أن من بين مكونات الركن المادي لارتكاب هذه الجريمة أن تكون موجة لشخص.

ولقد خص المشرع الجزائري الرئيس باعتبار هذا الأخير من رموز السادة الوطنية وهذا ما نصت عليه م 144 مكرر[4] "يعاقب بغرامة من 100.000 دج إلى 500.000 دج، كل من أساء إلى رئيس الجمهورية بعبارات

[1]- محمد عبيد الكعبي، "الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت"، دار النهضة العربية القاهرة، مصر،2009، ص114.

[2] حبيباتني بثينة، مرجع سابق، ص 144.

[3]- خالد حسن أحمد لطفى، جرائم الانترنت "بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني"، دار الفكر الجامعي مصر، الطبعة الأولى، 2018، ص 31

[4]- قانون العقوبات الصادر بموجب الأمر 66-156 مؤرخ في 8 يونيو 1966 ، ج ر 49 المؤرخة في 11-06-1966 معدل ومتمم بموجب القانون 20-15 يتعلق بالوقاية من جرائم الاختطاف الأشخاص و الوقاية منها ، مؤرخ في 30ديسمبر 2020 ، ج، ر ،ج، ج، ع 30 مؤرخة في 2020-12-30

تتضمن إهانة أو سبا أو قذفا سواء كان عن طريق الكتابة أو الرسم أو التصريح أو بأية آلية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية ".

ومن خلال م 31 من القانون 20-05 نص على:[1]يعاقب على التمييز وخطاب الكراهية بالحبس من سنتين (2) إلى خمس (5) سنوات وبغرامة من 200.000 دج الى 500000 دج

-إذا كانت الضحية طفلا أو سهّل ارتكاب الجريمة حالة الضحية الناتجة عن مرضها أو إعاقتها أو عجزها البدني أو العقلي،

-إذا كان لمرتكب الفعل سلطة قانونية أو فعلية على الضحية أو استغل نفوذ وظيفته في ارتكاب الجريمة،

-إذا صدر الفعل عن مجموعة أشخاص سواء كفاعلين أصليين أو كمشاركين،

-إذا ارتكبت الجريمة باستعمال تكنولوجيات الإعلام والاتصال.

على الرغم من أن الدساتير والمواثيق الدولية والتشريعات كفلت حرية الرأي، وأن لكل إنسان حق التعبير عن رأيه ونشره بالقول أو الكتابة أو غيرها، ولكن هذه الحريات ليست مطلقة وإنما عليها عدة قيود، ومن بينها تجريم السب والقذف.

كما نصت م 32 من نفس القانون على: يعاقب على خطاب الكراهية بالحبس من ثلاث (3سنوات إلى سبع 7) سنوات وبغرامة من 300000 دج إلى 700000 دج إذا تضمن الدعوة إلى العنف.

ولقد أولى المشرع الجزائري أهمية كبرى لهذا النوع من الجرائم باعتبار حق الإنسان في شرفه واعتباره من الحقوق اللصيقة بالشخصية القانونية والمتفرغة عنها أيا كانت المكانة الاجتماعية التي يحتلها في المجتمع، وبالتالي لا يوجد شخص معدوم الشرف والاعتبار منذ أن اعترفت القوانين الحديثة لكل فرد بشخصيته القانونية، الأمر الذي جعل المشرع يقر الحماية الجنائية على هذا الحق، وأفرد قواعد خاصة في قانون العقوبات، لتنظيم الأحكام المتعلقة بالسب والقذف على اعتبارها جرائم تمس حق الإنسان في شرفه واعتباره.

ومن المعلوم أن المعلومات المتعلقة بالأفراد متداولة بكثرة في ظل شيوع استخدام الأنترنت، مما يجعلها عرضة للانتهاك والاستعمال من طرف هؤلاء المجرمين، فأصبحت بالتالي تكنولوجيات الإعلام والاتصال إحدى الوسائل الفعالة التي تستعمل للمساس بشرف الغير أو كرامتهم أو اعتبارهم.[2]

[1] القانون رقم 20-05 مؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما ج.ر.ج.ج ع 25 صادر في 6 رمضان عام 1441 الموافق 29 أبريل سنة 2020.

[2] حبيباتني بثينة، مرجع سابق، ص145.

الفرع الثاني: جرائم المساس بحرمة الحياة الخاصة

تعد حماية حرمة الحياة الخاصة، حقا مكرسا دستوريا، كفله المؤسس الدستوري الجزائري وذلك من خلال م 47 الدستور الجزائري لسنة 2020 والتي نصت على: لكل شخص الحق في حماية حياته الخاصة وشرفه، لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت، لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية، حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي يعاقب القانون على كل انتهاك لهذه الحقوق[1] وجرم المساس بحرمة الخاصة للأشخاص في م 303 مكرر و303 مكرر1.

إلا أنه على الرغم من ذلك لا نستطيع أن نغفل حقيقة ما تتعرض له حرمة الحياة الخاصة من أخطار كثيرة يكمن سببها الرئيسي في انتشار وسائل التقدم العلمي والتكنولوجي بجميع أنواعه.

فلقد أصبحت خصوصيات الأشخاص وأسرارهم ومعلوماتهم الخاصة بداخل الأجهزة الإلكترونية وشبكات المعلومات، نظرا لاعتبارهما وسيلة لتخزين المعلومات الشخصية المتعة والمختلفة، مما يشكل تهديدا وانتهاكا غير مسبق لخصوصيتهم.[2]

أولا: التهديد والمضايقة

يقصد بالتهديد والمضايقة زرع الخوف في نفس الإنسان من ضرر قد يلحق به شخصياً أو بمن تحت رعايته أو بمن لهم صلة به أو بماله...[3] حيث يقوم المجرم الإلكتروني بإرسال رسالة الكترونية للمجني عليه تنطوي على ما يرعبه كيفما كان شكله أو مضمونه، وذلك رغبة منه في التحكم في الضحية أو ابتزازه أو لأي سبب آخر.[4]

ثانياً: انتحال شخصية الغير والاستدراج

يتم ذلك من خلال استخدام المجرم الإلكتروني لشخصية الضحية أو المجني عليه بغرض الاستفادة من سمعته أو سلطته أو ماله أو غيره من الأسباب، فقد تتم بواسطة انتحال شخصية المجني عليه أو انتحال شخصية المواقع، ويكثر استخدام هذه النمط في الوسط التجاري.[5]

---

[1]- المرسوم الرئاسي رقم 20/442 والموقع في 15 جمادى الأولى عام 1442 الموافق الموافق لـ 30 ديسمبر سنة 2020 المتعلق بالتعديل الدستوري. ج ر ج ج ، ع 82

[2] حبيباتني بثينة، مرجع سابق، ص 156.

[3]- محمد عبيد الكعبي، مشار إليه، ص 88.

[4] نعيمة دوادي، مرجع سابق، ص49.

[5] رحموني محمد، مرجع سابق، ص445.

أما الاستدراج فغالب ضحاياه هم صغار السن، حيث يوهمون من قبل المجرم الالكتروني برغبته في تكوين صداقة عبر الشبكة تتحول إلى لقاء واقعي بينهما، وقد تتم الجريمة في إقليم الدولة الواحدة، وقد تكون مخترقة حدود الدولة أي أن المجرم الإلكتروني في دولة والضحية موجود بدولة أخرى.[1]

ثالثاً: نشر الإباحة

يقصد بنشر الإباحة كل إرسال أو نشر عمل إباحي أو بإعداد أو حفظ أو معالجة أو عرض أو طباعة أو نشر او ترويج أنشطة أو أعمال إباحية أو اتصل بالدعارة أو الأعمال الإباحية.[2]

ويتم ذلك من خلال المواقع الإلكترونية الموجودة على الشبكة، والتي تستخدم بغرض الإثارة الجنسية من خلال قيام المجرم الإلكتروني بنشر صور جنسية فاضحة وأفلام جنسية، وكثيرا ما تستهدف الأطفال والشباب لأن هذه الفئة أقل تحصيناً[3]

رابعاً: جريمة إلكترونية ماسة بشخص الإنسان وكرامته

تعد من جرائم تكنولوجيا الإعلام والاتصال واسعة الانتشار عبر الشبكات، حيث تستخدم أسلوب القذف والسب وتشويه السمعة وغيرها من الأفعال اللاأخلاقية، بغرض المساس بشرف الشخص أو النيل من كرامته، وقد يكون عبر خطوط الاتصال أو عبر البريد الإلكتروني أو عبر صفحات الويب، أو عبر غرف المحادثة أو الدردشة.[4]

المطلب الثاني: الجرائم الماسة بالأموال

إن ازدياد الاعتماد على التكنولوجيا الحديثة والتخلي عن الأساليب القديمة في المجال المالي بهدف تسهيل العمليات المصرفية، وإنجازها في وقت قصير وبكلفة أقل،[5] الأمر الذي مكن الجناة من إيجاد بيئة الكترونية خصبة وكافية لارتكاب العديد من جرائم الأموال بواسطة الوسائل الالكترونية المستحدثة بسهولة ويسر بالغين، ومن قبيلها جرائم السرقة، جرائم النصب والاحتيال وتبييض الأموال.[6]

---

[1] نعيمة دوادي،مرجع سابق، ص49

[2]- أحمد محمد اللوزي و محمد عبد المجيد الذنيبات، الجريمة الإباحية الإلكترونية كما نظمها قانون جرائم أنظمة المعلومات الأردني، مجلة دراسات، كلية علوم الشريعة والقانون، الجامعة الأردنية، مج 42، ع 03، 2015، ص853.

[3] نعيمة دوادي، مرجع سابق، ص50.

[4]- محمد الكعبي، مشار إليه، ص 114.

[5]- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، الاردن ، 2005، ص51.

[6] حبيباتني بثينة، مرجع سابق، ص121

وعليه فهذا التطور الذي شهته التعاملات المالية والاعتماد الكبير على الاتصالات الإلكترونية سايره تطور جرائم تكنولوجيا الإعلام والتي سنتطرق الى بعض صورها ضمن الفرعين المواليين[1]:

الفرع الأول: جريمتي النصب والاحتيال المعلوماتي

مع التطور في نوع الجريمة وأساليبها تبدو جريمة النصب من أهم الجرائم المتطورة، والتي تزداد وتختلف صورها بتنوع أساليب المحتالين، فالجاني في هذه الجريمة يخاطب ملكة الفكر والخيال وملكة الشعور وملكة الإرادة لدى من يتلقى هذه المخاطبة منه لإقناعه بتسليم المال.[2]

وقد عرف الفقه النصب بأنه" استيلاء بطريق الاحتيال على شيء مملوك للغير بنية تملكه"[3].

كما أنها في جريمة الاحتيال المعلوماتي يستخدم فيها الجاني كافة الوسائل التقنية للتوصل إلى البيانات المالية التي تتصل بحقوق مالية أو قيامه بأعمال احتيالية موجهة لنظام الكمبيوتر فيجني المنافع المادية عن طريق العبث بالبيانات أو البرامج أو حتى عمليات النظام ذاته، أو الاحتيال باستغلال مواقع الإنترنت لجني مبالغ ماليه عبر مشاريع وهمية لمنتجات أو خدمات أو من خلال الوصول إلى أرقام بطاقات ائتمان، وبسبب عدم نشاط وجود مادي مجسم يتحقق به فعل الاستلام في جرائم خيانة الأمانة لا يمكن خضوع البرامج والمعلومات للنشاط الإجرامي في هذه الجريمة وهذا ما نصت عليه م 376 من قانون العقوبات الجزائري وعليه لا تقع جريمة خيانة الأمانة على غير المنقولات المادية كما لا يوجد نشاط مادي يتحقق به التسليم والاستلام في جريمة النصب، وحتى لو تم ذلك فانه لن ينتج عنه حرمان المجني عليه من المعلومات التي نقلها بالقول بل تظل تحت سيطرة من نقلها وفي حوزته وهو أمر وان كان يتفق وطبيعة البرامج والمعلومات إلا انه لا يتفق وطبيعة النشاط الإجرامي في جريمة النصب وهذا يعني عدم صلاحية البرامج للخضوع للنشاط الإجرامي في جريمة النصب، وهذا ما نصت عليه م 372 ق ع.[4]

لقد حدد المشرع النتيجة الإجرامية للنصب في م 372 ق ع بأنها" :استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من التزامات".

[1] رحموني محمد، مرجع سابق، ص446.

[2]- رمسيس بهنام، القسم الخاص في قانون العقوبات، منشأة المعارف، الإسكندرية، مصر ، 1982، ص504.

[3]- أحمد خليفة ملط، الجرائم المعلوماتية، دراسة مقارنة، ط2، دار الفكر الجامعي، الإسكندرية، مصر ، 2006، ص297.

كما حدد المشرع الجزائري أيضا من خلال نص م 372 ق ع الطرق الاحتيالية التي من خلالها تتحقق جريمة النصب، وهذه الوسائل واردة على سبيل الحصر، وهي استعمال أسماء أو صفات كاذبة أو مناورات احتيالية فإذا وقع النصب بدون أي طريقة من تلك الطرق فإن الجريمة تنتفي.[1]

فذهب جانب من الفقه، إلى القول بأن النصب المعلوماتي هو تلاعب في البرامج والبيانات للتغيير فيها بما يترتب عليه إيهام المجني عليه بصحتها، الأمر الذي يجعله يسلم بها، وبالتالي يمكن انطباق النص المتعلق بجريمة النصب على النصب المعلوماتي باعتباره أحد أساليب الاحتيال وأن النظام المعلوماتي يستخدم كوسيط للتحايل.

وذهب رأي آخر إلى أنه يمكن أن يستخدم الجاني أحد الأساليب الفنية في الاحتيال على النظام المعلوماتي من ناحية استخدام النظام كأداة سلبية، أو كأداة إيجابية عن طريق التدخل المباشر في المعطيات والكيان المنطقي بإدخال معطيات وهمية أو تعديل البرامج أو خلق برامج صورية وهي جميعها طرق احتيالية.

ويذهب البعض الآخر إلى القول بعدم تحقق الاحتيال على المنظومة المعلوماتية، واعتبر أن استخدام وسائل الغش والخداع في أنظمة الحاسوب للاستيلاء على الأموال لا تدخل ضمن نطاق الطرق الاحتيالية، لأن هذه الأخيرة يجب أن ترتبط بين شخصين الخادع والمخدوع أي الجاني والمجني عليه وهو ما ينتفي في هذه الحالة.[2]

ولا يجوز النظر إلي التسليم هنا على أنه واقعة مادية تتمثل في مناولة مادية، ترد على شيء ينقله من حيازته إلى حيازة الجاني، بل يجب النظر إلى التسليم على أنه عمل قانوني، جوهره قيام إرادة المجني عليه المعيبة بتمكين المحتال من السيطرة على المال، سواء تحققت هذه السيطرة على الفور أو بعد وقت قصير.

إن الأخذ بهذا المعنى للتسليم، لا يثير مشكلة في مجال النصب المعلوماتي الذي لا ينطوي على تسليم مادي للمال محل النشاط الإجرامي، حيث أنه يمكن القول أن تسليم المال يتم في شكل عمليات متعة يقوم بها الحاسب الآلي بحيث لا يصل المال إلى يد الجاني بصورة مباشرة. لا يكفي لقيام جريمة النصب قيام الجاني بفعل الاحتيال، وحدوث واقعة التسليم، وإنما يلزم أن يكون التسليم وقع كأثر من آثار الطرق الاحتيالية المستخدمة من الجاني.

فالطرق الاحتيالية التي اتخذها الجاني تربط بينها وبين المال الذي حصل عليه علاقة هي السبب في هذه الجريمة، ولولا هذه الطرق الاحتيالية لما تمت الجريمة التي أوقعت المجني عليه في الخطأ نتيجة لها وجعلته يسلم ماله وسواء كان هذا الشخص ذاته أو النظام المعلوماتي أو جهاز التوزيع الآلي للنقود.[3]

---

[1]– أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج 1 ،ط14 ، دار هومة للطباعة والنشر والتوزيع، الجزائر 2012، ص 317 وما يليها .

[2]– حبيباتني بثينة، مرجع سابق، ص128.130

[3] حبيباتني بثينة، مرجع سابق، ص 132.

الفرع الثاني: جريمة تبييض الأموال

غسيل الأموال أو كما يسميها البعض إحدى الظواهر الإجرامية المعاصرة المصنفة ضمن الجرائم الاقتصادية الحديثة تحولن من تلك الجريمة التقليدية الى جريمة مستحدثة تستخدم لارتكابها التقنية العالية كالحاسب الالي والأنترنيت فظهرت بذلك ما يسمى بجريمة غسيل الأموال عبر الأنترنيت أو جريمة التبيض الإلكتروني.[1]

وفي هذا الصدد تنص م 389 مكرر ق.ع على الأفعال التي تشكل جريمة تبييض أموال، وتتضمن هذه الأفعال صور السلوك الإجرامي المكون للجريمة، حيث نصت على:

يعتبر تبيض للأموال:

– تحويل الممتلكات أو نقلها مع علم الفاعل بأنها عائدات إجرامية بغرض إخفاء أو تمويه المصدر غير المشروع لتلك الممتلكات .....

ان إخفاء أو تمويه الطبيعة الحقيقية للممتلكات: ويقصد بفعل الإخفاء كل ما من شأنه منع كشف الطبيعة الحقيقية للممتلكات أو مصدرها أو كيفية التصرف فيها أو حركتها أو ملكيتها أو الحقوق المتعلقة بها، وبأي شكل كان، وبأي وسيلة.[2]

أما فعل التمويه فيقصد به اصطناع مظهر المشروعية لممتلكات غير مشروعة كإدخال هذه الأموال القذرة في نتائج شركة قانونية ضمن أرباحها فتظهر وكأنها أرباحاً مشروعة ناتجة عن نشاط مشروع.[3]

– اكتساب أو حيازة أو استخدام الممتلكات المتحصلة من جريمة: هذه الصورة تتعلق بتجريم اكتساب أو حيازة أو استخدام لأموال، مع ضرورة علم مرتكب الفعل بأن تلك الممتلكات متحصلة من جريمة.

– المساهمة في ارتكاب الأفعال السالفة الذكر.[4]

[1] هروال هبة نبيلة مرجع سابق ، ص 228

[2]– أحسن بوسقيعة، المرجع السابق، 403.

[3]– نادر عبد العزيز شافي، تبييض الأموال دراسة مقارنة، منشورات الحلب الحقوقية، لبنان، 2001، ص45.

[4]– أحسن بوسقيعة المرجع السابق، ص 404 وما يليها.

تمهيد:

إن ما تتميز به جرائم تكنولوجيا الإعلام والاتصال من خصائص جعل مختلف الجهود تتكاتف لتحقيق هدف واحد آلا وهو كيفية الحد من انتشار هذه الجرائم والعمل على تنسيق الجهود الدولية والإقليمية في سبيل مكافحتها، سواء أكان ذلك من خلال عقد اتفاقيات دولية وإقليمية أو من خلال انشاء هيئات متخصصة في هذا الشأن.

والمشرع الجزائري ليس بمنأى عما يحدث في بقية أقطار العالم، لذا نجده قد ساير التطور الذي شهدته جرائم تكنولوجيا الإعلام والاتصال وذلك من خلال إقرار قوانين ردعية وزجرية، وإنشاء هيئة وطنية تعنى بالأمر. وعليه سنتطرق من خلال مبحث أول الى الجهود الدولية والوطنية لمكافحة جرائم تكنولوجيا الإعلام والاتصال، لنعرج بعد ذلك ضمن مبحث ثان للآليات الإجرائية لمكافحة جرائم تكنولوجيا الإعلام والاتصال.

المبحث الأول: الجهود الدولية والوطنية لمكافحة جرائم تكنولوجيا الإعلام والاتصال

كنتيجة للخسائر الكبيرة التي تسببها جرائم تكنولوجيا الإعلام والاتصال، بدأت أصوات تتعالى داعية إلى ضرورة التعاون الدولي وإبرام الاتفاقيات والمعاهدات الدولية. وفي هذا الشأن سارع المشرع الجزائري إلى التصديق على نصوص الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية وتدخل جرائم تكنولوجيا الإعلام والاتصال ضمن هذا الإطار أو ذاك لأنها تعد جريمة عابرة للدول والقارات.[1] وعليه من خلال هذ المبحث سنتناول الجهود الدولية والإقليمية العربية لمكافحة جرائم تكنولوجيا الإعلام والاتصال ضمن (مطلب أول)، على أن نتطرق الى الجهود الوطنية ضمن (مطلب ثان).

المطلب الأول: الجهود الدولية والإقليمية العربية لمكافحة جرائم تكنولوجيا الإعلام والاتصال

إن جرائم تكنولوجيا الإعلام والاتصال تتسبب في مخاطر كبيرة وآثارها لا تعترف بالحدود الدولية، الأمر الذي جعل الجهود الدولية والإقليمية تصب في اتجاه واحد بغية التصدي لها ومكافحتها وعليه سنستعرض ضمن (فرع أول) الجهود على المستوى الدولي ومن خلال (فرع ثان) على المستوى العربي.

الفرع الأول: على المستوى الدولي

نظرا لأن جرائم تكنولوجيا الإعلام والاتصال ذات طبيعة دولية فإن مجابتها تقتضي بكل تأكيد تضافر الجهود الدولية والإقليمية وعليه من خلال هذا الفرع سنتناول عينة من الاتفاقيات الدولية المتعلقة بهذا الشأن.

[1]- ميرفت محمد حبابية، مرجع سابق، ص42.

1 –جهود الأمم المتحدة: تبذل الأمم المتحدة جهودا لا يستهان بها في مجال محاولة التصدي لجرائم تكنولوجيا الإعلام والاتصال وتؤكد على وجوب تعزيز العمل المشترك بين أعضاء المنظمة من أجل التعاون للحد من انتشارها وتعاظم آثارها، وقد حظيت جرائم تكنولوجيا الإعلام والاتصال باهتمام مؤتمرات الأمم المتحدة، وأبرزها ما جاء في هذا المجال ما يلي:

–بند 01 القرار الصادر عن مؤتمر الأمم المتحدة الثامن لمنع الجريمة ومعاملة السجناء هافانا 1990 بشأن الجرائم ذات الصلة بالكمبيوتر.

بعد هذا القرار من الجهود الذي بذلتها الأمم المتحدة حيث عقد هذا المؤتمر في هافانا سنة 1990 حيث في قراراه المتعلق بالجرائم ذات الصلة بالكمبيوتر الدول الأعضاء وأن تكثف جهودها لمكافحة إساءة استعمال هذا الجهاز وبتجريم تلك الأفعال جنائيا، واتخاذ الإجراءات التالية متى دعت الضرورة لذلك: ضمان أن الجزاء والقوانين الراهنة بشأن سلطات التحقيق والإدانة في الإجراءات القضائية تنطبق على نحو ملائم، وإدخال تغيرات مناسبة عليها إذ دعت الضرورة لذلك. النص على الجرائم والجزاء والإجراءات تتعلق بالتحقيق والأدلة حيث تدعوا الضرورة للتصدي لهذا الشكل الجديد والمعقد من أشكال النشاط الإجرامي في حالة عدم وجود قوانين تنطبق على نحو ملائم.[1]

كما حث أيضا الدول الأعضاء على مضاعفة الأنشطة التي تبذلها على صعيد الدولي من أجل مكافحة جرائم تكنولوجيا الإعلام والاتصال بما في ذلك دخولها كأطراف في المعاهدة المتعلقة بتسليم المجرمين وتبادل المساعدات في المسائل الخاصة المرتبطة بهذه الجريمة، ونصح هذا القرار الدول الأعضاء بالعمل على أن تكون تشريعاتها ذات صلة بتسليم المجرمين وتبادل المساعدة في المسائل الجنائية تنطبق بكل ما هو تام على الأشكال الجديدة للإجرام مثال جرائم تكنولوجيا الإعلام والاتصال، وأن تتخذ خطوات محددة نحو تحقيق الهدف.

كما تكمل الأمم المتحدة رؤيتها بشأن الجريمة المعلوماتية بصفة عامة بضرورة وضع أو تطوير:[2]

1. معايير دولية لأمن المعالجة الآلية للبيانات.

2. اتخاذ تدابير ملائمة لحل الإشكالية الاختصاص القضائي التي تثيرها جرائم تكنولوجيا الإعلام والاتصال العابرة للحدود أو ذات الطبيعة الدولية.

---

[1] سعادة نور الايمان ، مكافحة الجريمة الالكترونية على مستوى التشريعات الوطنية و الدولية ، مذكرة ماستر ، كلية الحقوق و العلوم السياسية ، جامعة [1] محمد بوضياف المسيلة ، 2021- 2022 ،ص

[2] سعادة نور الايمان ، مكافحة الجريمة الالكترونية على مستوى التشريعات الوطنية و الدولية ، مذكرة ماستر ، كلية الحقوق و العلوم السياسية ، جامعة محمد بوضياف المسيلة ، 2021- 2022 ،ص 36 -37

4.إبرام اتفاقية دولية تنطوي على النصوص تنظيم وإجراءات التفتيش والضبط المباشر الواقع عبر الحدود على الأنظمة المعلوماتية المتصلة فيما بينها والأشكال الأخرى للمساعدة المتبادلة مع كفالة الحماية في الوقت ذاته لحقوق الأفراد وحرياتهم وسيادة الدول.

كما عقدت منظمة الأمم المتحدة المؤتمر الثالث عشر لمنع الجريمة والعدالة الجنائية من 12 إلى 19 أفريل 2015 بدولة قطر، وكان الموضوع الرئيسي للمؤتمر "إدماج منع الجريمة والعدالة الجنائية في جدول أعمال الأمم المتحدة الأوسع للتصدي للتحديات الاجتماعية والاقتصادية وتعزيز سيادة القانون على الصعيدين الوطني والدولي، ومشاركة الجمهور" وقررت الجمعية العامة قرارها (184/67) النظر في ما يلي: إنشاء حلقات عمل من بينها تعزيز تدابير منع الجريمة والعدالة الجنائية للتصدي للأشكال المتطورة للجريمة منها جرائم تكنولوجيا الإعلام والاتصال.

عقد منظمة الأمم المتحدة المؤتمر الثاني عشر من 12 إلى 19 أفريل 2010 بالبرازيل تحت عنوان "استراتيجيات شاملة لتحديات عالمية نظم منع الجريمة والعدالة الجنائية وتطورها في عالم متغير، وتضمن جدول أعمال المؤتمر ثمانية بنود: من بينها جرائم تكنولوجيا الإعلام والاتصال، حيث دعت لجنة منع الجريمة والعدالة الجنائية إلى عقد اجتماع لفريق من خبراء حكومي دولي مفتوح العضوية لدراسة شاملة لمشكلة الجريمة المعلوماتية وتدابير التصدي لها.

قرارات وتوصيات الجمعية العام للأمم المتحدة:

- القرار (121/45) العام 1990، وكذلك نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها في العام 1994.

- القرار رقم (63/55) المؤرخ في 2000/12/04، والقرار رقم (121/56) المؤرخ في 2001/12/19 بشأن «مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات». يدعو هذا القرار الدول الأعضاء، عقد وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات على أن تأخذ بالاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

- القرار رقم (239/57) في 2003/01/31 والقرار رقم (199/58) المؤرخ في 2004/01/30 بشأن إنشاء ثقافة عالمية للأمن السيبراني ودعوة الدول الأعضاء إلى التعاون وتعزيز ثقافة الأمن السيبراني.

– قرار لجنة مكافحة المخدرات (5/48) حول تعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب الجرائم المتصلة بالمخدرات".[1]

– التوصيات والمبادئ التوجيهية للهيئة الدولية لمراقبة المخدرات (INCB) التي نشرت العام 2005 توصيات للحد من انتشار المبيعات غير المشرعة من المواد الخاضعة للرقابة ولاسيما المستحضرات الصيدلانية، عبر الإنترنت.[2]

2–جهود الاتحاد الدولي للاتصالات

يوفر الاتحاد الدولي للاتصالات الذي يضم 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية منبرا استراتيجيا للتعاون بين أعضائه باعتباره وكالة متخصصة داخل الأمم المتحدة، وقد وضع الاتحاد الدولي للاتصالات مخططا لتعزيز الأمن الإلكتروني العالمي، ومن أهم أهدافه الرئيسية ما يلي: [3]

– وضع استراتيجيات لتطوير نموذج التشريعات السيبرانية يكون قابلا للتطبيق محليا وعالميا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

– وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهياكل التنظيمية والسياسات المتعلقة بجرائم تكنولوجيا الإعلام والاتصال.

3–جهود المنظمة الدولية للشرطة الجنائية الإنتربول:

تستهدف هذه المنظمة تأكيد وتشجيع التعاون بين سلطات البوليس في الدول الأطراف، وطبقا للمادة الثانية من ميثاق المنظمة تتمثل أهم أهداف هذه المنظمة في تحقيق الآتي:[4]

أ–جمع المعلومات المتعلقة بالجرائم والمجرمين، وذلك عن طريق المعلومات التي تتسلمها المنظمة المكتب الرئيسي في اليونان من المكاتب المركزية الوطنية للشرطة الجنائية في الدول الأعضاء، ويتم ذلك عبر شبكة اتصالات حديثة.

بالتعاون مع الدول الأعضاء في ضبط الهاربين والمطلوبين أيا كانت جنسياتهم والصادر ضدهم أحكام قضائية، أو أوامر بالضبط والإحضار لمثولهم أمام جهات التحقيق، وذلك من خلال إصدار النشرات الدولية المخصصة.

---

[1] سعادة نور الايمان ، مكافحة الجريمة الالكترونية على مستوى التشريعات الوطنية و الدولية ، مذكرة ماستر ،كلية الحقوق و العلوم السياسية ، جامعة محمد بوضياف المسيلة ، 2021– 2022 ،ص 37.

[2] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، مج03، ع02، جامعة محمد خيضر، بسكرة، 2015، ص12.

[3] فاروق خلف، مرجع سابق، ص12.

[4] – سليمان أبو نمر ، يوسف بوكشريدة ، مكافحة الجريمة المعلوماتية في اطار القانون الدولي ، مذكرة ماستر تخصص قانون دولي ،كلية الحقوق و العلوم السياسية ، جامعة محمد خيضر بسكرة ، 2020 -2021 ، ص 28

ج دعم جهود الشرطة في مكافحة الإجرام العابر للحدود، وتقديم الخدمات في مجال الأدلة الجنائية كبصمات الأصابع، والحمض النووي.

د –إنشاء وتنمية كافة المؤسسات القادرة على المساهمة الفعالة في الوقاية من جرائم القانون العام.

هـ –تأمين وتنمية التعاون المتبادل على أوسع نطاق بين كافة سلطات الشرطة الجنائية في إطار القوانين القائمة في مختلف البلدان، وبروح الإعلان العالمي لحقوق الإنسان.

4–جهود المنظمة العالمية للملكية الفكرية:

يهدف حماية حقوق المؤلفين على مصنفاتهم الأدبية بأكثر الطرق فعالية تم إبرام إتفاقية برن الدولية في 09 سبتمبر 1886 والمكملة بباريس في ماي 1896 والمعدلة في برلين في 13 سبتمبر 1908، والمكملة في 20 مارس 1914 والمعدلة بروما في جوان 1928 وبروكسل سنة 1948، وإستوكهم لهم في جويلية 1967، وباريس في جويلية ،1971، حيث تشكل الدول الأطراف في هذه الإتفاقية إتحاد لحماية حقوق المؤلفين على مصنفاتهم الأدبية والفنية.

وبموجب إتفاقية برن الدولية تتمتع برامج الحاسب الآلي الكمبيوتر" سواء كانت بلغة المصدر أو بلغة الآلة بالحماية بإعتبارها أعمالا أدبية وفقا لما جاء فيها المتعلقة بالجوانب المتصلة بالتجارة الدولية حيث تسعى الدول "TRIPIS" إضافة إلى إتفاقية الأطراف في الإتفاقية إلى تشجيع الحماية الفعالة وملائمة لحقوق الملكية الفكرية من أجل التخفيف العراقيل التي تعوق التجارة الدولية.

– جهود منظمة التعاون الاقتصادي والتنمية:

تضم هذه المنظمة في عضويتها 34 دولة وضعت المنظمة توصيات إرشادية بخصوص أمن نظم المعلومات ومن مجمل أعمال منظمة التعاون الاقتصادي والتنمية حول جرائم تكنولوجيا الإعلام والاتصال حصل اتفاق على ضرورة أن يغطي قانون العقوبات في كل دولة الأفعال التالية:

أ–التلاعب في البيانات المعالجة آليا بما في ذلك محوها.

ب–التجسس المعلوماتي.

ج–التخريب المعلوماتي.

د–قرصنة البرامج

هـ–الدخول غير المشروع على البيانات أو نقلها، واعتراض استخدام المعطيات أو نقلها.

6-جهود الاتحاد الأوروبي: أعلنت "يوروبول"[1] في 2014/09/01، وكالة تطبيق القانون الأوروبية، المتخصصة في مكافحة الجرائم والإرهاب في دول الاتحاد الأوروبي، عن إنشائها قوة خاصة لمحاربة جرائم تكنولوجيا الإعلام والاتصال في دول الاتحاد، كما أن عملها يمتد إلى دول أخرى.

وستكون مهمة القوة الجديدة التنسيق مع التحقيقات الدولية لاتخاذ التدابير اللازمة في مواجهة التهديدات الرئيسية على الإنترنت مثل البرمجيات الخبيثة وخاصة ما يستهدف منها القطاعات المالية ومكافحة عمليات الاحتيال المعلوماتية والمواقع التي تبيع الممنوعات وغير ذلك.

وستبدأ القوة التي أطلق عليها اسم "J-CAT" وسيكون مقرها ضمن المركز الأوروبي للجرائم تكنولوجيا الإعلام والاتصال "EC3" التابع لليوروبول.

ويتضمن فريق العمل المشترك ضد جرائم تكنولوجيا الإعلام والاتصال الأعضاء في الاتحاد الأوروبي بالإضافة إلى شركاء آخرين لا ينتمون إلى الاتحاد الأوروبي من وكالات تطبيق القانون.

وانضمت للتعاون مع هذه القوة الجديدة مجموعة من الدول منها كندا واستراليا وألمانيا وفرنسا وهولندة وإيطاليا وإسبانيا والمملكة المتحدة والولايات المتحدة الأمريكية.[2]

7-جهود اتفاقية المجلس الأوروبي:

إن الاتفاقية الأوربية جرائم تكنولوجيا الإعلام والاتصال هي المعاهدة الدولية الأولى التي تسعى لمعالجة جرائم تكنولوجيا الإعلام والاتصال عبر التنسيق بين القوانين الوطنية وقوانين الدول الأخرى. حيث عملت اللجنة الأوروبية لمشاكل الجريمة بين العامين 1997 و2000 على مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر أبريل 2001. وتم التصديق على الاتفاقية من قبل 30 دولة سنة 2010 وتهدف الاتفاقية إلى:[3]

- توحيد الأحكام المتعلقة بالجرائم الإلكترونية مع عناصر القانون الجزائي المحلي.
- تعيين نظام سريع وفعال للتعاون الدولي.

[1]- الموقع الإلكتروني لليوروبول www.eurpol.europa.eu تاريخ الاطلاع 22افريل 2023على ساعة 13.00

[2] فاروق خلف، مرجع سابق، ص13.

[2] حشيفة عبد الهادي ، التعاون الدولي في مجال مكافحة الجرائم الإلكترونية ، مذكرة ماستر ، كلية الحقوق والعلوم السياسية ، جامعة زيان عاشور الجلفة ، 2019-2020ص 31

8-جهود مجموعة الدول الثماني "G8": اعتمد وزارة العدل والداخلية لبلدان الثمانية في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم تكنولوجيا الإعلام والاتصال تستند إلى المبادئ التالية:

عدم إتاحة ملاذات آمنة للمعتدين على تكنولوجيا المعلومات التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم تكنولوجيا الإعلام والاتصال ومحاكمتهم تدريب الموظفين المكلفين تنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية، بالإضافة إلى ذلك دعت دول الثمانية إلى مواصلة العمل حتى التوصل إلى حلول دولية ناجحة من خلال عقد اتفاقات دولية لمعالجة الجريمة ذات التقنية العالية والاستفادة من عمل المنظمات الدولية المختلفة ومن توصيات مجموعة الدول الثماني بالنسبة للجرائم تكنولوجيا الإعلام والاتصال موجودة في إطار الباب "D" من المعاهدة وتتلخص بما يلي :[1]

- يتعين على الدول أن تجرم الانتهاكات على حقوق الغير على الشبكة العنكبوتية التي تستوجب العقوبات الجزائية وأن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال لمنع الجريمة، وإقامة تعاون دولي فيما يتعلق بمكافحة هذه الانتهاكات وينبغي للدول أن تتخذ خطوات لمنع الجريمة ذات التقنية العالية.

9-جهود الاتحاد الإفريقي: طلب المؤتمر الاستثنائي لوزارة الاتحاد الإفريقي المسؤولين عن تكنولوجيا المعلومات والاتصالات المنعقد في جنوب إفريقيا من 02 إلى 05 نوفمبر 2009 من مفوضية الاتحاد الإفريقي القيام بالاشتراك مع لجنة الأمم المتحدة الاقتصادية لإفريقيا بإعداد اتفاقية حول التشريع القضائي على أساس احتياجات القارة والالتزام بالمتطلبات القانونية والتنظيمية للمعاملات الإلكترونية والأمن الإلكتروني وحماية البيانات الشخصية.

كما أوصت بضرورة توفير الحماية القانونية لأنظمة المعلوماتية التي تعتبر قيمة بالنسبة للمجتمع مما يجعل من الضروري سن التشريعات ضد الجريمة الإلكترونية. وفي يونيو 2014، اجتمع مجموعة من قادة الاتحاد الإفريقي مكون من 54 حكومة أفريقية في القمة 23 للاتحاد الإفريقي، ووافقوا على اتفاقية الاتحاد الأفريقي فيما يتعلق بمجال الأمن السيبراني وحماية البيانات الشخصية.[2]

الفرع الثاني: على المستوى العربي

من أبرز ما يمكن أنت يقال عن الجهود العربية المبذولة على مستوى الدول العربية من أجل الحماية من جرائم تكنولوجيا الإعلام والاتصال التي تضررت منها تلك الدول وألحقت بها خسائر نجد:

[1] فاروق خلف، مرجع سابق، ص14.13.

[2] حشيفة عبد الهادي ، مرجع سابق ،ص 34

– الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتي:

تمت موافقة مجلس وزراء الداخلية والعدل العرب في اجتماعهم المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 2010/12/21 وتحتوي على (43) مادة وجاء في مضمون م الأولى منها "تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات لدرء أخطار هذه الجرائم حفاظا على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها ونجد في الفصل الثاني تفصيلا للأفعال التي تعد مجرمة، وفي الفصل الثالث تتعرض لنطاق تطبيق الأحكام الإجرائية، وفي الفصل الرابع تعرضت للتعاون القانوني والقضائي وفي الفصل الخامس تعرضت إلى أحكام ختامية. وهدفت هذه الاتفاقية الى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تكنولوجيا الإعلام والاتصال أخطارها وحفاظا على أمن الامة العربية ومصالحها وسلامة ومجتمعاتها وأفرادها [1]

2–المكتب الإقليمي العربي للاتحاد للاتصالات: عقد محضر الاجتماع الأول في الجزائر يومي 25 و26 فيفري 213 تم تشكيل فريق العمل حول حماية الأطفال على الإنترنت في المنطقة العربية ويهدف إلى تنسيق الجهود وتوحيد الرؤية في المنطقة العربية من أجل التوصل إلى وضع مبادئ توجيهية لإطار قانوني لحماية الطفل على الإنترنت في المنطقة العربية وتم الاتفاق على ان تكون مهمة الفريق كالتالي:

أ–تحديد الأفعال التي تشكيل خطرا على الأطفال في الفضاء السيبراني.

ب–وضع المبادئ التوجيهية للإطار القانوني الإقليمي لحماية الأطفال في الفضاء.

السيبراني في إطار التعاون والتنسيق الإقليمي في المنطقة العربية.

ج–تقديم توصيات عامة حول الاسترشاد بالمبادئ التوجيهية على المستوى الوطني لكل دولة عند صياغة قوانينها الخاصة.

3–القوانين النموذجية: اعتمدت جامعة الدول العربية عبر الأمانة العامة لمجلس وزراء العدل العرب ما سمي بالقوانين العربية الاسترشادية الخاصة بمكافحة جرائم تكنولوجيا الإعلام والاتصال ومنها:[2]

أ–القانون العربي الاسترشادي للإثبات بالتقنيات الحديثة: اعتمده مجلس وزراء العدل العرب بالقرار رقم (771/د24) بتاريخ 2008/11/27 يحتوي على سبعة فصول، و(24) مادة ونجد الفصل الخامس من م (23) إلى (32) وما يليه يحتوي على الجرائم والعقوبات الخاصة بالجرائم تكنولوجيا الإعلام والاتصال.

[1] حشيفة عبد الهادي ، مرجع سابق ،ص 35

[2] فاروق خلف، مرجع سابق، ص15.

ب–قانون الإمارات العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها: اعتمده مجلس وزراء العدل العرب في دورته (19) بالقرار رقم (495/د19) بتاريخ 2003/10/08 واعتمده مجلس وزراء الداخلية العرب في دورته (21) بالقرار رقم (417–د2004/21) ويحتوي على (27) مادة تخص العقوبات للجرائم تكنولوجيا الإعلام والاتصال.

ج– القانون العربي الاسترشادي لحماية حق الملكية الفكرية: اعتمده مجلس وزراء العدل العرب بقرار رقم (940/د28) سنة 2012 والذي يحوي في الجزء الأول على حماية حق المؤلف والحقوق المجاورة، ويتكون من (10) فصول ونجد الفصل الرابع في م (19) الذي يوضح المصنفات المشمولة بالحماية منها برامج الحاسوب مهما كانت لغتها بما فيها الأعمال التحضيرية" أما م (20) تتمتع بالحماية المقررة في هذا القانون المصنفات المشتقة والمتمثلة في قواعد البيانات، سواء أكانت مقروءة أم غير مقروءة من الحاسب وفي الفصل التاسع نجد الإجراءات التحفظية والجزاءات في م (74) وما يليها.

4– مجلس وزار العدل العرب: بموجب القرار رقم (229) سنة 1996 وباستعراض الباب التاسع الخاص ضد الأشخاص نجد القانون قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية وذلك في المواد (461 –464) حيث أشارت المواد (461–463) على وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيفية الاطلاع عليها وم (464) نصت على عقاب من يقوم بفعل الدخول الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات، وعرفة رقلة أو إفساد نظام التشغيل عن أداء وظيفته المعتادة وتغيير المعلومات داخل النظام وتزوير وثائق المعالجة الآلية وسرقة المعلومات.

المطلب الثاني: الجهود الوطنية لمكافحة جرائم تكنولوجيا الإعلام والاتصال

أنشأ المشرع الجزائري هيئة وطنية تعنى بالوقاية من جرائم تكنولوجيا الإعلام والاتصال ومكافحته والتي سنتعرف على مهامها من خلال الفرع الأول، على أن نتطرق الى الجهود التشريعية وذلك بتخصيص الفرع الثاني لقانون العقوبات أما الفرع الثالث للقوانين الأخرى.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

أصدر رئيس الجمهورية مرسوم رئاسي رقم 15–261[1] مؤرّخ في 8 أكتوبر سنة 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحة

1ج.ر.ع.53.ص16..مرسوم رئاسي رقم15–261 مؤرخ في8 اكتوبر سنة 2015 م1

نص في مادته الأولى على انه تطبيقا لأحكام م 13 من القانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها يهدف هذا المرسوم تحديد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تدعى في صلب النص الهيئة. وحسب نص المادة الثانية تعتبر هذه الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل[1] وهو نفس الأمر لما هو في فرنسا إذ أنشأت الوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال وهي هيئة تابعة للمديرية العامة للشرطة الوطنية الفرنسية وخاضعة للمديرية المركزية للشرطة القضائية[2].

تمارس الهيئة المهام المنصوص عليها في م 14 من القانون رقم 04/09 المؤرخ في 5 أوت سنة 2009 تحت رقابة السلطة القضائية طبقا لأحكام التشريع الساري المفعول لا سيما منها قانون الإجراءات الجزائية والقانون والمذكور أعلاه تكلف الهيئة في ظل احترام الأحكام التشريعية المبينة أعلاه على الخصوص بما يأتي:[3]

– اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

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

– مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وهو ما نصت عليه م 14 فقرة ب من القانون 04/09.

– تقوم الهيئة بإذن من السلطات القضائية بجميع إجراءات التحري والأعمال التقنية الخاصة بالتحقيقات كمساعدة لمصالح الشرطة القضائية المختصة بتحقيقات لجرائم خاصة ارتكبت أو سهل ارتكابها استعمال تكنولوجيات الإعلام والاتصال.

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

– تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها. [1]

[1]– م 1 من المرسوم الرئاسي رقم 15–261 المؤرخ في 8 أكتوبر سنة 2015 ج .ر.ع 53، ص 16.

[2]– م 2 من المرسوم الرئاسي رقم 15–261 المؤرخ في 8 أكتوبر سنة 2015 ج. ر. ع 53.ص16

[3] بخوش هشام، مرجع سابق، ص202

الفرع الثاني: الحماية من خلال قانون العقوبات

إن القانون الجنائي التقليدي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا الجديدة، لاسيما أن نصوصه وضعت في عصر لم يكن الأنترنت قد ظهر فيه ولم تظهر المشاكل القانونية الناتجة عن استخدامه لكن نجد أن المشرع الجزائري تدارك الفراغ القانوني في مجال الإجرام المعلوماتي ولو نسبيا، خصوصا بموجب القانون رقم 04-15[1] المتضمن تعديل قانون العقوبات، إذ بموجبه جرم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات [2]

يعتبر قانون العقوبات وسيلة ردعية للكف عن ارتكاب الجرائم بصفة عامة، وبما أن جرائم تكنولوجيا الإعلام والاتصال تلحق أضرار بالغير فقد أقر المشرع عقوبات ردعية لتلك الجرائم وهي كالتالي:

أولا: المساس بأنظمة المعالجة الآلية للمعطيات: وهي من أبرز الجرائم التي عالجتها المحاكم الجزائرية وهذا بموجب القانون رقم (15/04)[3] المتعلق بقانون العقوبات وذلك من خلال المواد (394 مكرر) إلى (394 مكرر 7)، فمن خلال استقراء نصوص المواد حاول المشرع الجزائري حصر هذه الجرائم والعقوبات المقرر لها فيما يلي:[4]

1-**جريمة دخول معالجة آلية للمعطيات عن طريق الغش** نصت عليها م (394 مكرر)[5] من قانون العقوبات، حيث تعاقب بالحبس والغرامة عند الدخول أو البقاء بالغش في المنظومة المعلومة وفرق المشرع في هذه الحالة بين ما إذا كانت الجريمة بسيطة ومضاعفة العقوبة إذا ترتب عنها حذف أو تغيير المنظومة، وبين ما إذا ترتب على ذلك تخريب لنظام اشتغال المنظومة.

2-جريمة إزالة أو تعديل معطيات في نظام المعالجة آلية بطرق تدليسية: نصت عليها م (394 مكرر1)[6] من قانون العقوبات، حيث اعتبر المشرع الجزائري أن إزالة أو تعديل المعطيات التي يتضمنها النظام بطريق الغش عملا إجراميان ويقصد بإزالة المعطيات سواء جزئيا أو كليا أما محوها أو إتلافها أو تخريبها من أجل منع النظام القيام بمهامه أو تعطيل النظام المعلوماتي، والطرق متع شرحناها في مبحث سابق مثل نشر الفيروسات، أما تعديل المعطيات ويقصد به إما إدخال معلومات وهمية أو تزويرها في النظام المعلوماتي.[7]

---

[1]- م 04من المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر سنة 2015 ج.ر.ع.53

[2] نايري عايشة ، الجريمة الإلكترونية في التشريع الجزائري ، مذكرة ماستر، كلية الحقوق و العلوم السياسية ، جامعة أحمد درارية ، أدرار ، 2016 - 2017 ص 36

[3]- القانون (15/04) المؤرخ في 2004/11/10 المتعلق بقانون العقوبات ج.ر.ع 71،المعدل و المتمم صادر في 2004/11/10.

[4]- مولود ديدان، قانون العقوبات، دار بلقيس للنشر، ط مصححة ومحينة ، الدار البيضاء، الجزائر، 2012، ص.ص135-137

[5]- م (364 مكرر) من القانون (15/04)، المرجع السابق.

[6]- م (394 مكرر1) المرجع نفسه.

[7] فاروق خلف، مرجع سابق، ص16.

4- جرائم نشر حيازة أو الاتجار بالمعطيات المخزنة أو المعالجة: نصت عليها م (394 مكرر2)[1] من قانون العقوبات، حيث تعد هذه الجريمة من أكثر الجرائم وقوعا في العالم الافتراضي ولقد اعتبر المشرع الجزائري عملية اصطناع برنامج مخصص لارتكاب فعل الغش المعلوماتي أو إعداد برنامج ناقص من الناحية الفنية وخاصة المبرمج من أجل خلق فجوات وثغرات فيه لممارسة فعل الغش أو تجميع أو التقاط البيانات بغرض استغلالها أو نشرها خاصة عن طريق الإنترنت أو الاتجار فيها من الجرائم المعاقب عليها، بحكم أن جريمة الإفشاء والنشر تتسم بخطورة على الحياة الخاصة.

5- جرائم المعالجة الآلية الماسة بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام طبقا للمادة (394 مكرر)[2] من قانون العقوبات: حيث اعتبر المشرع جرائم تكنولوجيا الإعلام والاتصال التي تستهدف الدفاع الوطني أو أي مؤسسة رسمية بمثابة ظرف تشديد ويستخلص من نص م (394 مكرر 3) من قانون العقوبات أن العقوبة المشددة على جميع الجرائم المنصوص عليها في م (394 مكرر) وم (394 مكرر1) و(مكرر2) من قانون العقوبات وحرص المشرع الجزائري على ضمان حماية مطلقة لهيئات الدفاع الوطني ولمؤسسات الدولة الجزائرية وتوسع في هذه الحماية وذلك بإدراج جميع الجرائم[3] المنصوص عليها في م (394 مكرر) من قانون العقوبات كلها.

6-الجرائم المعلوماتية للشخص المعنوي: نصت عليها م (394 مكرر4)[4] من قانون العقوبات حيث أقر المشرع الجزائري المسؤولية الجزائية للأشخاص المعنوية وشدد عقوبة الغرامة في جرائم الاعتداء على نظم المعالجة الآلية، حيث أن الغرامة المطبقة على الشخص المعنوي تتراوح بين واحد إلى خمس أضعاف الغرامة المقررة على الشخص الطبيعي.

7-جريمة تكوين جمعية أشرار المعلوماتيين لغرض التحضير للجرائم الماسة بأنظمة المعالجة الآلية طبقا للمادة (394 مكرر5)[5] من قانون العقوبات: ويتضح من خلال نص م أن العقوبات يطال من يشارك أي مجموعة أو في اتفاق الغرض منه التحضير أو الإعداد لارتكاب جرائم تكنولوجيا الإعلام والاتصال مع توفر القصد الجنائي،

---

[1]- م (394 مكرر2)من قانون 15/04

[2]- م (394 مكرر3 من قانون 15/04.

[3]- زيبحة زيدان، المعلوماتية في التشريع الجزائري، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2001، ص 100

[4]- م (394 مكرر4) من القانون رقم (15/04) المرجع السابق.

[5]- م (394 مكرر5) من قانون 15/04.

كما يستخلص أن مجرد المشاركة أو الاتفاق المجسد بفعل مادي يوحي بالتحضير للجريمة خاصة أن ذلك يمكن أن يتم عبر الشبكات المعلوماتية.

8-**العقوبات التكميلية وفقا للمادة (394 مكرر6)[1]من قانون العقوبات:** نص المشرع في هذه م على العقوبات التكميلية للجرائم السالفة الذكر وتمثل في المصادرة للأجهزة المستعملة والبرامج والوسائل المستعملة مع إلحاق ذلك بغلق المواقع وأماكن الاستغلال شريطة أن تكون بعلم صاحبها.

9-العقاب على الشروع في الجريمة المعلوماتية طبقا لنص م (394 مكرر7):[2] من قانون العقوبات أن فعل الشروع أو البدء في ارتكاب الجريمة يعاقب عليه بنفس العقوبة المقررة للجنحة ذاتها، ونظرا لكون جرائم الاعتداء على نظام المعالجة الآلية ذات وصف جنحي أقر المشرع العقاب لها بمثل الجريمة نفسها.

ثانيا: حماية حرمة الحياة الخاصة: من خلال التعديل الذي جاء في القانون رقم (06-23)[3] المتعلق بقانون العقوبات فم (303 مكرر)[4] من قانون العقوبات تعاقب بالحبس والغرامة كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت سواء بالتقاط أو تسجل أو نقل صور أو مكالمات خاصة أو سرية دون إذن رضا صاحبها أما م(303 مكرر1)[5] من قانون العقوبات، تعاقب بالعقوبة ذاتها على من يحتفظ أو يضع في متناول الجمهور الصور أو الوثائق بأية وسيلة كانت.

ثالثا: حماية حرمة رموز الدولة: من خلال التعديل الذي جاء في القانون رقم (14/11)[6] المتعلق بقانون العقوبات، حيث نصت م (144 مكرر)[7] منه، على عقوبة الغرامة المالية فقط كل من أساء لرئيس الجمهورية بأية وسيلة كانت أو بوسيلة إلكترونية وفي حالة العود تضاعف الغرامة.

رابعا: الحماية من خلال قانون الإجراءات الجزائية: حيث أن م (16) من قانون الإجراءات الجزائية[8] وسعت من الاختصاص المحلي لضباط الشرطة القضائية فيما يتعلق بالبحث ومعاينة الجرائم الماسة بأنظمة المعالجة الآلية

---

[1]- م (394 مكرر6) المرجع نفسه.

[2]- م (394 مكرر7)، المرجع نفسه.

[3]- القانون (06/23) المؤرخ في 2006/12/20، المتضمن قانون العقوبات، ج.ر.ع. 48، الصادرة في 2006/12/24.

[4]- م (303 مكرر)، المرجع نفسه.

[5]- م (303 مكرر1) من القانون (23/06)، المرجع السابق.

[6]- القانون (14/11) مؤرخ في 2011/08/02 المتضمن قانون العقوبات، ج.ر.ع.44، صادرة في 2011/08/10

[7]- م (144 مكرر)، المرجع نفسه.

[8]- القانون (22/06) المؤرخ في 2006/12/20 المتضمن قانون الإجراءات الجزائية، ج.ر.ع.84، صادرة في 2006/12/24.

للمعطيات ويمتد الاختصاص إلى كامل الإقليم الوطني، كما جاءت م (37) من قانون الإجراءات الجزائية[1] وم (40) منه لتمكن كل من وكيل الجمهورية وقاضي التحقيق على تمديد الاختصاص المحلي إلى دائرة اختصاص محاكم أخرى في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

الفرع الثالث: الحماية من خلال قوانين خاصة

وهذه القوانين الخاصة شملت الحماية في قانون التأمينات الاجتماعية، وكذلك الحماية من خلال نصوص الملكية الفكرية، وأيضا الحماية في نصوص التوقيع الإلكتروني بالإضافة إلى الحماية المتعلقة بالمواصلات السلكية واللاسلكية.[2]

أولا: الحماية المتعلقة بالموصلات السلكية واللاسلكية:

باستقراء القانون رقم (03/2000)[3] الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات بحيث لاحظنا أنه تسارع مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان إجراء التحويلات المالية عن الطريق الإلكتروني ذلك ما نصت عليه م 87 منه، كما نصت م 84 منه على استعمال حوالات دفع عادية أو إلكترونية أو برقية كما نص في م 105 منه على احترام المراسلات بينما أتت م 127 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من سنة إلى خمس سنوات.[4]

وأيضا تضمن الفصل الثاني من الباب الرابع من القانون رقم (03/2000) المتعلق بالبريد والمواصلات السلكية واللاسلكية الأحكام الجزئية المترتبة على مخالفة النظام القانوني، فالأشخاص المرخص لهم تقديم خدمة المواصلات السلكية واللاسلكية والعمال متعاملي الشبكات العمومية الذين ينتهكون سرية المراسلات السلكية واللاسلكية أو المساعدة على ذلك يعاقبون طبقا لنص م (137) من قانون العقوبات أم غيرهم ممن يرتكب هذه الأفعال يعاقب بالحبس والغرامة.

---

[1]- م (37) وم (40) من القانون رقم (14/04) مؤرخ في 2004/11/10 يعدل ويتمم الأمر (155/66) المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية، ج.ر.ع.71، صادرة في 2004/11/10.

[2] بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، كلية جيلالي اليابس، سيدي بلعباس، عدد 1، 2013، ص63

[3]- القانون (03/2000) المؤرخ في 2000/08/05 الذي يحدد القواعد العامة المتعلقة بالبريد السلكية واللاسلكية، ج.ر.ع.المؤرخة في 2000/08/06.

[4] فضيلة عاقلي ، الجريمة الإلكترونية و إجراءات مواجهتها من خلال التشريع الجزائري ،أعمال المؤتمر الدولي الرابع عشر : الجرائم الالكترونية / طرابلس 24-25 مارس 2017 ، ص 131

ثانيا: الحماية من خلال قانون الملكية الأدبية والفنية:

حاول المشرع الجزائري مواجهة الجريمة الإلكترونية من خلال قانون الملكية الأدبية والفنية المتعلق بحق المؤلف والحقوق المجاورة الصادر بموجب الأمر رقم (05/03)[1] المؤرخ في 2003/07/23 المتعلق بحقوق المؤلف والحقوق المجاورة، حيث وسع قائمة المؤلفات المحمية، وذلك بإدماج برامج المعلوماتية، ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج المعلوماتية، كما شدد العقوبات على المساس بحقوق المؤلفين خاصة المصنفات الرقمية التي تشملها الحماية. [2]

ثالثا: الحماية في نصوص التوقيع الإلكتروني:

أصدر المشرع الجزائري قانون رقم (03/15)[3] المتعلق بعصرنة العدالة، حيث تطرق في الفصل الثاني إلى المنظومة المعلوماتية المركزية لوزارة العدل والإشهاد على صحة الوثائق الإلكترونية وضمان حمايتها، أما الفصل الثالث تعرض إلى إرسال الوثائق والإجراءات القضائية بالطريق الإلكترونية، والفصل الخامس تعرض إلى الأحكام الجزائية لحماية التوقيع والتصديق الإلكترونيين، حيث أن م (17)[4] منه تعاقب على كل من يستعمل بطريقة غير قانونية العناصر الشخصية المتصلة بإنشاء توقيع إلكتروني يتعلق بتوقيع شخص آخر. أما م (18)[5] تعاقب كل شخص حائز على شهادة إلكترونية يستعملها بعد انتهاء صلاحيتها أو الغائها.

رابعا: الحماية في قانون التأمينات الاجتماعية

قد تطرق هذا القانون رقم (01/08)[6] المؤرخ في 2008/01/23 كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي، في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية حسب م 93 مكرر 3منه [7]

---

[1]- الأمر (05/03) المؤرخ في 2003/07/19، المتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر.ع.44، صادرة بتاريخ 2003/07/23.

[2] فاروق خلف، مرجع سابق، ص18.

[3]- القانون (03/15) المؤرخ في 2015/02/01، المتعلق بعصرنة العدالة ج.ر.ع.2، صادرة في 2015/02/10 .

[4]- م (17) المرجع السابق

[5]- م (18) المرجع نفسه.

[6]- القانون (01/08) المؤرخ في 2008/01/27 المتعلق بالتأمينات الاجتماعية، ج.ر.ع.04، صادرة في 2008/01/27.

[7] فضيلة عاقلي ، مرجع سابق ، ص 132

بمقتضى أحكام قانون التأمينات الاجتماعية شدد العقوبة فيما يتعلق بالمساس غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا وعاقب المشرع الجزائري كل من يسلك أو يستسلم بهدف الاستعمال غير المشروع للبطاقة الإلكترونية للمؤمن له اجتماعيا المفتاح الإلكتروني لهيكل العلاج أو المفتاح لمهني الصحة طبقا للمادة (93 مكرر2)[1] نفس القانون، كما يشمل العقاب التعديل أو الحذف الكلي أو الجزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية أو نسخ البرمجيات المتعلقة باستعمال البطاقة الإلكترونية، أو المحاولة على ارتكاب الفعل طبقا لنص م (93 مكرر3) منه،[2] كما أقر المشرع أيضا عقوبة للشخص المعنوي تتمثل في الغرامة ضعف المقررة للشخص الطبيعي طبقا لنص م (93 مكرر5)[3] من ذات القانون، ومصادرة الأجهزة والوسائل المستعملة وكذا غلق المحلات وأماكن الاستغلال التي تكون محل الجنح.

خامسا: الحماية من خلال قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

جاء هذا القانون(04/09)[4] منظما للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكل ما يتعلق بالمنظومة المعلوماتية والمعطيات المعلوماتية، ومقدمو الخدمات والمعطيات المتعلقة بتسيير الاتصالات الإلكترونية من مراقبة وتفتيش المنظومات المعلوماتية عند الضرورة، وحجز المعطيات المعلوماتية، وحفظ المعطيات المتعلقة بحركة السير على الالتزامات الخاصة بمقدمي خدمة الإنترنت، وأخيرا على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.[5]

وتكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية ويبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع لتحديد مصدرها والتعرف على مرتكبيها، وقد جرم الأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الإنترنت وعلى كل تقنية تظهر مستقبلا. وقد حدد القانون الحالات

[1]- م (93 مكرر2) من القانون رقم (01/08) المرجع السابق.

[2]- م (93 مكرر3)، المرجع نفسه.

[3]- م (93 مكرر5)، المرجع نفسه.

[4]- القانون (04/09) المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر.ع.47، الصادرة في 2009/08/16.

[5]- بشير حماني، خصوصية التحقيق في الجريمة الإلكترونية، مذكرة مقدمة لنيل شهادة الماستر أكاديمي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2019/2018، ص21.

التي يسمح فيها اللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أو في حالة توفر معلومات عن احتمال اعتداء منظومة معلوماتية. [1]

وقد تعرض الفصل الأول من القانون إلى أهدافه وتحديد مفهوم التقنية، أما الفصل الثاني فقد تعرض إلى أحكام خاصة بمراقبة الاتصالات الإلكترونية، والفصل الرابع تعرض إلى القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، والفصل الرابع تعرض إلى تحديد الالتزامات التي تقع على المتعاملين في الاتصالات الإلكترونية، ثم الفصل الخامس نص على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحتها والفصل السابع فقد نص على التعاون والمساعدة القضائية الدولية بخصوص مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال خاصة منها بالمساعدة وتبادل المعلومات.

المبحث الثاني: الآليات الإجرائية لمكافحة جرائم تكنولوجيا الإعلام والاتصال

إن التحقيق هو إجراء من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها من أجل استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه[2] وهناك تشابه بين التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وبين التحقيق في الجرائم التقليدية، فهي جميعا تحتاج إلى إجراءات تشابه في عمومها مثل المعاينة والتفتيش والخبرة والاستجواب والشهود وجمع وتحليل الأدلة، إلا أن التحقيق في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال له خصوصية خاصة؛ لأنه يتم في بيئة رقمية.

المطلب الأول: إجراءات وأساليب جمع الأدلة

جمع الأدلة في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يستخلص من البيئة الرقمية، والتي تعتبر مسرحا للجريمة، وبما أن الدليل يقوي على إثبات الجريمة، يستلزم أن يكون من ذات طبيعتها التقنية وتحيط بعملية جمع الأدلة العديد من الصعاب، إلا أنه لا مناص من مواصلة جمع الأدلة مع التطوير المستمر لوسائل البحث، وتكييف جمع الأدلة مع طبيعة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.[3]

[1] فاروق خلف، مرجع سابق، ص18.

[2]- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير علوم جنائية، كلية الحاج لخضر، باتنة 2013، ص.ص110 إلى120.

[3]فاروق خلف، مرجع سابق ،ص8

الفرع الأول: المعاينة

المقصود بالمعاينة في الجريمة المعلوماتية هو الوقوف على الآثار التي يخلفها مستخدم النظام المعلوماتي، حيث يعتبر الانتقال إلى عين المكان أولى الخطوات التي يقوم رجال الضبطية القضائية في تعاملهم مع مسرح الجريمة لمعاينة وإثبات الأثار والمخلفات المادية والمحافظة عليها، وإثبات حالة الأماكن والأشخاص عن طريق الكتابة والتخطيط والصور ويمنع إحداث أي تغيير في معالم مسرح الجريمة، كما يراعى تسجيل وقت وتاريخ التقاط الصور والفيديو، والسرعة في اتخاذ الإجراءات الكفيلة بإثبات هوية بعض الحضور وسماعهم، وفي بعض الحالات منعهم من مغادرة الأمكنة، وإخطار نيابة الجمهورية بذلك فورا. كما يجب التأكيد على ضرورة التقيد بالنصوص القانونية التي تنظم إجراءات المعاينة، من أجل إضفاء طابع الشرعية على الإجراءات، وعدم المساس بالحقوق والحريات الفردية أو التعرض لها إلا في حدود ما يسمح به القانون احتراما لمبدأ قرينة البراءة، وفي الأخير يجب تدوين المعاينة بكافة تفاصيلها في محضر لتمكين القاضي من الاطلاع عليها[1]

كما تعرف المعاينة بأنها ملاحظة وفحص حسي مباشر لأي شيء له علاقة بالجريمة لإثبات حالته، والكشف والتحفظ على كل ما قد يفيد من الأشياء في كشف الحقيقة وتكمن أهمية المعاينة في دورها لتصور كيفية وقوع الجريمة وظروف ملابساتها، وتوفير الأدلة والمعاينة في مسرح الجريمة تتيح أمام المحقق الكشف عن طريق معاينة الآثار المادية التي خلفها ارتكاب الجريمة، والتحفظ على الأشياء التي تفيد التحقيق، لكن بالنسبة للجرائم المتصلة بتكنولوجيات الإعلام والاتصال قلما تخلف آثار مادية، لذلك وجب مراعاة قواعد وإرشادات فنية خاصة مثل: تصوير الحاسوب وملحقاته إثبات التوصيلات عدم نقل مادة المعلوماتية من مسرح الجريمة.[2]

وينبغي التعامل مع مسرح الجريمة الإلكترونية على أنها مسرحان: [3]

1-مسرح تقليدي: ويقع خارج بيئة الحاسوب والأنترنت، ويتكون من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون إلى مسرح جريمة تقليدية يترك فيها الجاني آثار كالبصمات أو وسائط تخزين رقمية ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه.

[1] حليم رامي ، إجراءات استخلاص الدليل في الجرائم المعلوماتية، **دفاتر البحوث العلمية، مج9، ع 1،المركز الجامعي تيبازة ، 2021** ،ص 230

[2] فاروق خلف، مرجع سابق، ص8.

[3] فاطيمة دهان، كلثوم دهان ، إجراءات البحث و التحري في الجرائم المعلوماتية ، مذكرة ماستر ، كلية الحقوق و العلوم السياسية ، جامعة غرداية ، 2021-2022 ص 34

2-مسرح اقتراضي: يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله والتعامل مع الأدلة الموجودة في هذا المسرح يجب أن لا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية

و عند تلقي بلاغ عن وقوع إحدى الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، ويرى الفقه الجنائي ضرورة وضع عدة ضوابط في معاينة مسرح الجريمة المعلوماتية مثل تصوير الحاسب والأجهزة الطرفية وإخطار الفريق الذي يتولى المعاينة والذي يعد خطة موضوعية بالرسومات، كما عليه إثبات حالة التوصيلات والكابلات ليتمكن من إجراء المقارنة عند الع رض على المحكمة مع ضرورة عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل التأكد من خلو المحيط من أي قوى مغناطسية قد تتسبب في محو البيانات، كما يجب أن يتم التحفظ على محتويات سلة المهملات التي قد تكون ذات صلة بالجريمة، ومن الضروري أن تتم المعاينة من طرف المحققين ذوي الكفاءة العلمية والخبرة الفنية في مجال المعلوماتية وأن تتم وفق مبدأ المشروعية[1]

وقد نصت م 42 من قانون الإجراءات الجزائية الجزائري على المعاينة بشكل عام كإجراء يتم في مرحلة جمع الاستدلالات وهو مخول لجهاز الضبطية القضائية بعد إخطار وكيل الجمهورية بذلك وذلك طبقا للمادة 79 ق.إ.ج.ج، سواء في الحالة العادية أو حالات التلبس، ويترتب على تغيير أو تعديل يطرأ على مكان وقوع الجريمة الجزاءات المنصوص عليها في م 43 قانون إ.ج.ج.

وفيما يتعلق بإجراءات المعاينة التي يتم أمام مسرح الجريمة لجرائم تكنولوجيا الإعلام والاتصال فإنه ينبغي مراعاة ما يلي :[2]

- القيام بتصوير جهاز الحاسب الآلي وكل ما يتصل به من أجهزة ظرفية ومحتويات الذي بواسطته ارتكبت الجرائم.
- العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص التي يخففها ولوج النظام، والآثار الإلكترونية التي يخلفها ولوج النظام أو التردد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تم عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه في الحوار.

[1] فاطيمة دهان، كلثوم دهان ، مرجع سابق ، ص 35

[2] هروال أية نور الهدى، الأدلة الرقمية في إثبات الجريمة الإلكترونية، مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون- تيارت، 2021، ص ص25- 26.

– الاستعانة بأهل الخبرة عند الضرورة. ويسميها الخبراء "حقيقة الأدلة الرقمية وفي هذا السياق نص المشرع الجزائري من خلال نص م 05 في فقرتها الأخيرة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بأنه « يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية لعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات المعلوماتية التي تضمنتها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها».

– تأمين التيار الكهربائي من الانقطاع المفاجئ، لأن ذلك يسبب العديد من المخاطر تتمثل في محو المعلومات من الذاكرة من جراء غلق جهاز الكمبيوتر، وبالتالي فقدان كافة العمليات التي كان يتم تشغيلها واتصالات الشبكة والأنظمة الثابتة.[1]

الفرع الثاني: التفتيش

يعرف التفتيش بصفة عامة بأنه: "البحث في مكنون سر الأفراد على دليل الجريمة المرتكبة، أو هو البحث عن الدليل..."[2]

التفتيش في الجريمة المعلوماتية هو أحد إجراءات التحقيق التي تقوم بها الهيئات المنصوص عليها حسب تشريع كل دولة وتُعنى هذه الهيئات بالانتقال إلى محل وقوع هذه الجريمة "الحاسب الآلي"، فيكون التفتيش إما بشكل تقليدي عن طريق تفحص الجهاز ومكوناته وكل ما يحيط به أو بطريقة تقنية بالدخول إلى النظام الذي يشغله والبحث والتمحيص في كل البيانات، وهي إجراءات تساعد في تقفي آثار الجاني متى وجد لها المحققون سبيلاً ومنه تضييق دائرة الاشتباه إلى تسليم الجاني للمحاكمة".[3]

هو إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في محل يتمتع بحرمة، وذلك وفقا للضمانات والقيود المقررة قانونا، ويعد تفتيش نظم المعالجة الآلية من أخطر المراحل؛ لأنه يكون على طابع غير مادي ولا يعدو إلا أن يكون معلومات إلكترونية ليس لها مظهر محسوس خارجيا، والتفتيش ينصب على الجانب المادي والمنطقي للحاسوب معا وهذا ما سنفصل فيه فيما يلي :[4]

[1]– ممدوح عبد المطلب، البحث والتحقيق الجنائي الرقمي البحث في جرائم الكمبيوتر ، والإنترنت، دار الكتب القانونية، مصر، 2006 ص 115.

[2]– عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، دار هومة، الجزائر، ط4، ص 266.

[3] عبير بعقيقي، فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04، مجلة العلوم القانونية والسياسية، مج09، ع02، جامعة الوادي، الجزائر، 2018، ص45

[4] فاروق خلف، مرجع سابق، ص9.

1 – تفتش المكونات المادية للحاسوب: إن التفتيش الواقع على المكونات المادية للحاسوب لا توجد فيه مشكلة في التنفيذ؛ لأنه يرد على أشياء مادية، لا خلاف فيها لقواعد القانون؛ لأنه تطبق عليه القواعد التقليدية، لكن مع الأخذ بعين الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها، ونظام التفتيش تنطبق عليه الضمانات المقررة قانونا.

2 – تفتيش المكونات المنطقية للحاسوب: لقد اختلف الفقه الجنائي في مسألة مدى قابلية البيانات المعلوماتية؛ لأن تكون موضوعا للتفتيش من عدمه طبقا للنصوص التقليدية، وهو ما حذا بالمشرعين سن قوانين إجرائية جديدة تنص على إمكانية تفتيش المكونات المنطقية للحاسوب، وهذا ما ذهب إليه المشرع الفرنسي في تعديله للنصوص التي تحكم التفتيش، وكما نص المشرع الإنجليزي على جواز تفتيش نظم الحاسوب المادية والمعنوية، وقد صرحت الاتفاقية الأوروبية المتعلقة بجرائم تقنية المعلومات أنه يحق للدول الأعضاء تفتيش نظام الحاسوب أو جزء منه أو المعلومات المخزنة فيه ووسائط التخزين، والتفتيش في البيئة الرقمية يخضع لشروط شكلية وأخرى موضوعية تختلف عن شروط التفتيش في البيئة التقليدية.[1]

وبالنسبة للمشرع الجزائري فلقد نص صراحة على تفتيش انظمة الحاسب الآلي من خلال القانون رقم 09-04 المتعلقة بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، وذلك بموجب نص م 05 منه، بحيث يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد إلى المنظومة المعلوماتية أو جزء منها، وكذا المعطيات المعلوماتية المخزنة فيها، وكذا منظومة تخزين المعلوماتية.[2]

وكذلك من خلال م 06 من القانون 09-04 بحيث أنه: «عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها، وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث، وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية»

[1]– محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة ماجستير قسم علوم الشرطة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004، ص76-80.

[2] هروال أية نور الهدى، مرجع سابق، ص31.

الفرع الثالث: ضبط الأدلة

وهو وضع اليد على الشيء يتصل بالجريمة ويفيد في كشف الحقيقة وعن مركبيها، ويفيد في ضبط الأدلة في التحقيق الجاري بشأن الجريمة.[1]

وضبط الأدلة في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال يتصل بضبط المكونات المادية لأنظمة الحاسوب، وضبط المكونات المنطقية والبرمجيات، وكذا ضبط المعطيات التي تتناقل أو يجري تبادلها في نطاق شبكة المعلومات التي تربط الحواسيب وما يتصل بها،[2] وعلى هذا الأساس فإن من الأشياء التي يتم ضبطها والتحفظ عليها في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم هي جهاز الحاسوب وملحقاته، ضبط المعدات المستعملة في الشبكة كجهاز المودم، ووسائط تخزين البيانات والمعطيات، وضبط البرمجيات.

المطلب الثاني: حجية الأدلة في إثبات جرائم تكنولوجيا الإعلام والاتصال

الجريمة الإلكترونية ظاهرة إجرامية مستجدة تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها وأنماط السلوك الإجرامي المجسدة للركن المادي لكل جريمة على حدي، مع تطور أنماطها يوما بعد يوم وما أتاحته الشبكة من فرص جديدة لارتكابها، مما جعل إثباتها من العقبات التي يعمل الخبراء على كسرها من أجل إيجاد وسائل إثبات ناجعة على أساس أنها تتطلب خبرة فنية عالية واعتماد أسلوب واضح في التحقيق ومن الأسباب التي تصعب اكتشاف وإثبات الجرائم الإلكترونية نذكر ما يلي:[3]

1-تمتاز الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بصعوبة الاكتشاف وإثباتها وذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز والأرقام هي رموز دقيقة ويصعب اكتشافها وإثباتها لهذا عادة ما يتم اكتشافها بالصدفة

2-فالجريمة المعلوماتية لا تترك آثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات إلكترونية غير مرئية.

3-كذلك وسيلة التنفيذ فيها تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات.

---

[1]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2001، ص 170-171.

[2]- خالد عياد الحلبي، المرجع السابق، ص 281-282

[3] بشير حماني، مرجع سابق،ص 22

4-يصعب العثور على دليل مادي للجريمة وذلك راجع إلى استخدام الجاني وسائل فنية وتقنية معقدة لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل والتلاعب به.

5-تتطلب خبرة وتحكما في التكنولوجيا المعلوماتية عند متابعتها، ولذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري، لابد أن يكون المحقق متخصص حتى لا يتسبب في إتلاف الدليل الإلكتروني.

6-عدم وجود تعاون دولي، فكما بينا سابقا قد يتم السلوك الإجرامي في بلد معين ولكن النتيجة تحدث في بلد أخر ليس بالضرورة أن ينتج هذا السلوك أثاره في بلد المجرمين.

7-اختلاف النظم القانونية وبالتالي عدم الاتفاق على الفعل المجرم، فما هو محظور في الجزائر من الناحية الأخلاقية مباح في غيرها من الدول.

8-التطور السريع للجريمة والمعالجة البطيئة لقضايا، استفادة المجرم من هذه العقبات للعبث ولهذه الأسباب وكذا الطبيعة الخاصة التي تتسم بها الجريمة أدى ببعض التشريعات الى تبنى الخبرة والمعاينة كأسلوبين للإثبات والتحقيق وكشف الجريمة والتخريب والاستمرار في الجريمة[1].

[1]- بشير حماني، مرجع سابق، ص22.

الخاتمة

الخاتمة

من خلال دراستنا هذه تبين لنا أن موضوع جرائم تكنولوجيا الإعلام والاتصال موضوع رحب يصعب الإحاطة بكافة جوانبه، خصوصا في ظل التطور الكبير الذي تشهده وتعدد أثارها والجوانب الماسة بها، دون أن ننسى بأنها جرائم لا تعترف بالحدود الدولية بل هي جرائم يمكن أن ترتكب في أي منطقة في العالم في حيث يكون آثارها في منطقة أخرى.

- حيث أنه بالرغم ما حققته تكنولوجيا الإعلام والاتصال فوائد عديدة وتزايد الاعتماد عليها في مجالات الحياة كافة. وبقدر ما أفرزته الوسائل التقنية الحديثة في مجال الرقي والتقدم الإنساني، بقدر ما مهدت إلى بروز أنماط جديدة من الجرائم بالغة الخطورة.
- فلقد كان لهذا التقدم والتطور التكنولوجي أن ظهر هناك من يستغل هذه التكنولوجيا لغايات ومصالح شخصية أو مادية أو لغايات الانتقام وإلحاق الضرر بالأفراد أو المؤسسات أو غايات تدميرية، وهذا بدوره أدى إلى ظهور نمط جديد من المجرمين يُعرف بالمجرم الإلكتروني.

الأمر الذي استدعى العمل للحد من التهديدات التي تنجم من استعمال شبكة الإنترنت والتقنيات الحديثة لتحقيق الأمن المعلوماتي وحماية الأفراد من مخاطر جرائم تكنولوجيا الإعلام والاتصال، وذلك لا يأتي إلا من خلال العمل على الوقاية من مخاطر جرائم تكنولوجيا الإعلام والاتصال، الأمر الذي أدى إلى ظهور أساليب ووسائل للوقاية من الجريمة الإلكترونية والحد منها.

وذلك لأن لجاني يستخدم فيها كافة الوسائل التقنية للتوصل الى الغاية التي يسعى إليها كالبيانات المالية أو التي تتصل بحقوق مالية أو قيامه بأعمال احتيالية موجهة لنظام الكمبيوتر فيجني المنافع المادية عن طريق العبث بالبيانات أو البرامج أو حتى عمليات النظام ذاته، أو الاحتيال باستغلال مواقع الإنترنت للتعدي على الحياة الخاصة للأفراد أو لجني مبالغ ماليه عبر مشاريع وهمية لمنتجات أو غير ذلك

كما رأينا أيضا أنه لم يجمع الفقه على وضع تعريف جامع لجرائم تكنولوجيا الإعلام والاتصال، بل اختلف الفقه في تعريف هذا النوع من الجرائم، وكما أنهم لم يتفقوا على تسمية واحدة لهذا النوع من الجريمة

ورأينا أيضا أن المشرع الجزائري خص مكافحة جرائم تكنولوجيا الإعلام والاتصال بترسانة من القوانين، إلا أن هذا يتطلب المزيد من الجهود والعمل على نشر التوعية لدى الأفراد حتى لا يقعوا كضحايا.

اما بالنسبة للتوصيات فتتمثل فيما يلي:

- ايجاد ادلة اثبات جديدة تتلاءم مع طبيعة هذه الجرائم وذلك لعدم ملائمة ادلة الاثبات التقليدية في القانون الجنائي لإثباتها.
- تعد مراقبة الاتصالات الالكترونية وتفتيش النظم المعلوماتية من اهم وأخطر الاجراءات التي جاء بها قانون 04-09 لان هذين الإجراءين يمسان بشكل مباشر الحياة الخاصة للأفراد، فكان من الاحسن بالمشرع وضع قيود قانونية لتبرير اللجوء الى هذين الإجراءين.
- وجب اصدار نصوص جديدة او تعديل النصوص الجزائية القائمة لمواجهة الجرائم المعلوماتية وذلك بتقرير الجرائم وتحديد العقوبات المناسبة لها بغية حماية النظام المعلوماتي.

قائمة المصادر والمراجع

أولا: الكتب

1. ابن منظور أبي الفضل جمال الدين بن مكرم، لسان العرب، مج 12، دار صادر، ط3، بيروت، لبنان، 1993.
2. أحسن بوسقيعة، الوجيز في القانون الجزائي الخاص، ج 1 ،ط14، دار هومة للطباعة والنشر والتوزيع، الجزائر 2012.
3. أحمد خليفة ملط، الجرائم المعلوماتية، دراسة مقارنة، ط2، دار الفكر الجامعي، الإسكندرية، 2006،
4. حنان ريحان مبارك المضحكي، الجرائم المعلوماتية دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014.
5. خالد حسن احمد لطفي، الدليل الرقمي ودوره في اثبات الجريمة المعلوماتية، دار الفكر الجامعي، ط1، الإسكندرية، مصر ،2020.
6. خالد حسن أحمد لطفى، جرائم الانترنت "بين القرصنة الإلكترونية وجرائم الابتزاز الإلكتروني"، دار الفكر الجامعي مصر، الطبعة الأولى، 2018.
7. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، دار الثقافة للنشر والتوزيع، الأردن، 2001.
8. رمسيس بهنام، القسم الخاص في قانون العقوبات، منشأة المعارف، الإسكندرية، 1982.
9. زهراء عادل سلبي، جريمة الابتزاز الإلكتروني (دراسة مقارنة)، دار الأكاديميون للنشر والتوزيع، ط1، الأردن، 2021.
10. زيبحة زيدان، المعلوماتية في التشريع الجزائري، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2001.
11. زين العابدين الكردي، جرائم الإرهاب المعلوماتية، منشورات الحلبي الحقوقية، ط 1، لبنان، 2018.
12. طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتي)، دار الجامعة الجديدة، القاهرة، ط1، مصر، 2009.
13. عبد الصبور عبد القوي علي، الجريمة الالكترونية، الطبعة الأولي، دار العلوم للطباعة والنشر، القاهرة، مصر، 2007.
14. عبد الكريم الردايدة، الجرائم المستحدثة واستراتيجية مواجهتها، دار الحامد للنشر، ط1، عمان، الاردن، 2013.
15. عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، دار هومة، الجزائر، ط2، 2006.

16. عفيفي كامل عفيفي، جرائم الكومبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003.
17. علي جبار صالح الحسيناوي، جرائم الحاسوب والإنترنت، دار اليازوري للنشر والتوزيع، ط1، عمان، الأردن، 2018.
18. غادة نصار، الإرهاب والجريمة الإلكترونية، العربي للنشر والتوزيع، ط 1، القاهرة، مصر، 2017.
19. محمد عبيد الكعبي، "الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت"، دار النهضة العربية القاهرة، مصر،2009.
20. محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، عمان، الأردن، 2010.
21. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، الاردن، 2005.
22. ممدوح عبد المطلب، البحث والتحقيق الجنائي الرقمي البحث في جرائم الكمبيوتر، والإنترنت، دار الكتب القانونية، مصر، 2006.
23. مولود ديدان، قانون العقوبات، دار بلقيس للنشر، ط مصححة ومحينة، الدار البيضاء، الجزائر، 2012،
24. ميرفت محمد حبابية، مكافحة الجريمة الالكترونية، دار اليازوري للنشر والتوزيع، ط1، بيروت، لبنان، 2022.
25. نادر عبد العزيز شافي، تبييض الأموال دراسة مقارنة، منشورات الحلب الحقوقية، لبنان، 2001.

ثانيا: الرسائل العلمية

أ–الأطروحات:

1. هبة نبيلة هروال، جرائم الأنترنت دراسة مقارنة، أطروحة دكتوراه جامعة أبي بكر بلقايد تلمسان، الجزائر، 2013-2014.
2. حبيباتني بثينة، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، أطروحة لنيل شهادة دكتوراه ل. م. د في القانون العام، كلية الحقوق، جامعة الجزائر1، 2020،
3. حفيظة رفاس، دور السياسة الجنائية للمشرع الجزائري في مكافحة جرائم التكنولوجيا الحديثة، أطروحة دكتوراه قانون عام، كلية الحقوق والعلوم السياسية، جامعة مولاي الطاهر، سعيدة، الجزائر، 2019 – 2020.

ب–رسائل الماجستير:

4. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير علوم جنائية، جامعة الحاج لخضر، باتنة 2013.

5. محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والإنترنت، رسالة ماجستير قسم علوم الشرطة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

ج–مذكرات الماستر:

6. نايري عايشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة أحمد درارية، أدرار، 2016 -2017.
7. حشيفة عبد الهادي، التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، 2019-2020
8. بشير حماني، خصوصية التحقيق في الجريمة الإلكترونية، مذكرة مقدمة لنيل شهادة الماستر أكاديمي، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، المسيلة، 2019/2018.
9. سعادة نور الايمان، مكافحة الجريمة الالكترونية على مستوى التشريعات الوطنية والدولية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف المسيلة، 2021-2022

10.هروال أية نور الهدى، الأدلة الرقمية في إثبات الجريمة الإلكترونية، مذكرة تخرج تدخل ضمن متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون-تيارت، 2021،

11.سليمان أبو نمر، يوسف بوكشريدة، مكافحة الجريمة المعلوماتية في إطار القانون الدولي، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2020 -2021

12.فاطيمة دهان، كلثوم دهان، إجراءات البحث والتحري في الجرائم المعلوماتية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة غرداية، 2021-2022.

ثالثا: المقالات والمنشورات العلمية.

1. أحمد محمد اللوزي ومحمد عبد المجيد الذنيبات، الجريمة الإباحية الإلكترونية كما نظمها قانون جرائم أنظمة المعلومات الأردني، مجلة دراسات، كلية علوم الشريعة والقانون، الجامعة الأردنية، مج 42، ع 03، 2015.
2. بخوش هشام، الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في ظل التشريع الجزائري، مجلة الحقوق والعلوم السياسية، مج04، ع01، جامعة خنشلة، الجزائر، 2017.
3. بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، جامعة جيلالي اليابس، سيدي بلعباس، ع 1، 2013.

4. حليم رامي، إجراءات استخلاص الدليل في الجرائم المعلوماتية، دفاتر البحوث العلمية، مج9، ع 1، المركز الجامعي تيبازة، 2021.
5. عبير بعقيقي، فيصل نسيغة، الإثبات في الجرائم المعلوماتية على ضوء القانون 09-04، مجلة العلوم القانونية والسياسية، مج09، ع02، جامعة الوادي، الجزائر، 2018.
6. فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، مجلة الحقوق والحريات، مج03، ع02، جامعة محمد خيضر، بسكرة، 2015.
7. رحموني محمد، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، ع41، جامعة احمد دراية، ادرار، 2017.
8. فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، أعمال المؤتمر الدولي الرابع عشر: الجرائم الالكترونية / طرابلس 24-25 مارس 2017.
9. نعيمة دوادي، الجريمة الالكترونية (خصائصها ومجالات استخدامها وأهم سبل مكافحتها)، مجلة مهد اللغات، مج 2، ع 1، جامعة حسيبة بن بوعلي، الشلف، الجزائر، 2020.

رابعا: النصوص القانونية

أ-المراسيم:

1. المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر سنة 2015 ج.ر.ع.53.
2. المرسوم الرئاسي رقم 20/442 والموقع في 15 جمادى الأولى عام 1442 الموافق الموافق لـ 30 ديسمبر سنة 2020 المتعلق بالتعديل الدستوري. ج ر ج ج، ع 82

ب-القوانين والأوامر

3. القانون (15/04) المؤرخ في 2004/11/10 المتعلق بقانون العقوبات الرسمية، ع 71، صادر في 2004/11/10.
4. القانون (22/06) المؤرخ في 2006/12/20 المتضمن قانون الإجراءات الجزائية، ج.ر، ع 84، صادرة في 2006/12/24.
5. القانون (01/08) المؤرخ في 2008/01/27 المتعلق بالتأمينات الاجتماعية، ج.ر، ع 04، صادرة في 2008/01/27.
6. القانون (04/09) المؤرخ في 2009/08/05 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر، ع 47، الصادرة في 2009/08/16.
7. القانون (14/11) مؤرخ في 2011/08/02 المتضمن قانون العقوبات، ج.ر، ع 44، صادرة في 2011/08/10

8. القانون (03/15) المؤرخ في 2015/02/01، المتعلق بعصرنة العدالة ج.ر، ع 2، صادرة في 2015/02/10.
9. القانون (03/2000) المؤرخ في 2000/08/05 الذي يحدد القواعد العامة المتعلقة بالبريد السلكية واللاسلكية، ج.ر، ع المؤرخة في 2000/08/06.
10. القانون (06/23) المؤرخ في 2006/12/20، المتضمن قانون العقوبات، ج.ر، ع48، الصادرة في 2006/12/24.
11. قانون العقوبات الصادر بموجب الأمر 66-156 مؤرخ في 8 يونيو 1966، ج ر 49 المؤرخة في 11-06-1966 معدل ومتمم بموجب القانون 20-15 يتعلق بالوقاية من جرائم الاختطاف الأشخاص والوقاية منها، مؤرخ في 30ديسمبر 2020، ج رج ج، ع 30 مؤرخة في 30-12-2020
12. القانون رقم 20-05 مؤرخ في 5 رمضان عام 1441 الموافق 28 أبريل سنة 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، ج.ر.ج.ج ع 25 صادر في 6 رمضان عام 1441 الموافق 29 أبريل سنة 2020.
13. القانون رقم (14/04) مؤرخ في 2004/11/10 يعدل ويتمم الأمر (155/66) المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية، ج.ر، ع 71، صادرة في 2004/11/10.
14. الأمر (05/03) المؤرخ في 2003/07/19، المتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر، ع 44، صادرة بتاريخ 2003/07/23.

خامسا: المواقع الالكترونية:

1. www.eurpol.europa.eu تاريخ الاطلاع 22افريل2023 على الساعة13:00.

فهرس المحتويات

ملخص

لقد تطورت الجرائم تكنولوجيات الإعلام والاتصال في العصر الحديث تطورا ملحوظا سواء في أشخاص مرتكبيها أو في أسلوب إرتكابها وذلك باستخدام أخر ما توصلت إليه العلوم التقنية والتكنولوجية، ولما كانت هذه الجرائم حديثة النشأة لتعلقها بتكنولوجيا المعالجة الآلية للمعلومات فقد اكتنفها الغموض بالشكل الذي دعا إلى القول بأن لا وجود لها وأنه لا يوجد أي تهديدحقيقي منبعه الحاسبات الإلكترونية، وإن كان هناك أشكال للسلوك غير المشروع الذي يرتبط بالمجالات الإلكترونية فهي جرائم عادية يمكن تطبيق النصوص الجزائية التقليدية بشأنها.

ان تطبيق النصوص التقليدية على هذه الأنماط المستحدثة من الجرائم قد أسفر عن الكثير من المشكلات القانونية، وقد تضاربت أحكام القضاء منها من طبقت أحكام النصوص التقليدية على أي سلوك يتعلق بنظم معالجة المعلومات، ومنها من رأت أنه سلوكا مباحا لم يرد بشأنه نص يجرمه التزاما بمبدأ الشرعية الجزائية والذي يقضي بأن (لا جريمة ولا عقوبة الا بنص) .

abstract

In the last years the world witnessed a big development in the crimes of technology and communication . Criminals use a new and advanced methods in the electronic and technology science by, the way many opinions and doubts about these crimes because there are no real menace and threatening.However ,if there are kinds and types of behavior related to electronic Field means are normal crimes should apply the penal law on them.

The application of ancient articles on these new types of crimes brought plenty of problems in law . There are different sanctions applied by the ancient penal articles related to the system of informtion treatment,in other way law must be applied due to there is no crime without sanctions.THe creation of economical and financial pole and Cyber pole else in this last period decreased huge role of competent authoroties which made it's role narrow and leave the main role for the cyber Pole in stead the ancient competent authoroties because of the developped materials and capacities that push it to face and fight these crimes