وزارة التعليم العالي والبحث العلمي

Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة عبد الحميد ابن باديس مستغانم

كلية الحقوق والعلوم السياسية

المرجع:

قسم: القانون العام

مذكرة نهاية الدراسة لنيل شهادة الماستر

الآليات القانونية لمكافحة الجريمة الالكترونية في ظل التشريع الجزائري

ميدان الحقوق و العلوم السياسية

الشعبة : حقوق

التخصص : القانون الجنائي و العلوم الجنائية

من إعداد الطالب(ة) :

مدرك نريمان

تحت إشراف الأستاذ(ة):

ساجي علام

أعـــضاء لجنة الـــمناقـــشة :

الاستاذ (ة) : درعي لعربي رئيسا

الاستاذ (ة) : ساجي علام مشرفا و مقررا

الاستاذ (ة) : بن عودة نبيل مناقشا

السنة الجامعية 2022/ 2023.

نوقشت في : 2023/06/04.

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

شكر وعرفان

الشكر الأول والأخير لله عز وجل، والصلاة والسلام على سيدنا محمد ﷺ، الحمد لله حمدا كثيرا، على توفيقه لنا في انجاز هذا العمل المتواضع.

أتقدم بالشكر الجزيل إلى أستاذي الفاضل "**يوسفي محمد** "على نصائحه وتوجيهاته التي أنارت دربي والذي لم يبخل عليا بمعلوماته القيمة.

كما أتوجه بالشكر إلى كل أساتذتي من الطور الابتدائي إلى الجامعي وإلى كافة عمال وعاملات جامعة عبد الحميد بن باديس.

أتقدم بامتناني وشكري إلى كل **أساتذة كلية الحقوق والعلوم السياسية** "**مستغانم** "وخاصة **أساتذتي** اللذين قاموا بتدريسي من سنة أولى إلى يوم تخرجي.

كل الشكر إلى من ساهم سواء بمعلومة، أو نصيحة أو كلمة طيبة.

نريمان

الإهداء

إلى من قال فيهما الله عز و جل : « **و قضى ربك ألا تعبدوا إلا إياه و بالوالدين إحسانا إما يبلغن عندك الكبر احدهما أو كلاهما فلا تقل لهما أف و لا تنهرهما و قل لهما قولا كريما.** » "والديا".

إلى من أرضعتني الحب والحنان إلى رمز الحب وبلسم الشفاء إلى القلب الناصع **أمي الحبيبة.**

إلى من جرع الكأس فارغا ليسقيني قطرة الحب، إلى من كلت أنامله ليقدم لنا لحظة سعادة، إلى من حصد الأشواك عن دربي ليمهد لي طريق العلم **أبي العزيز**، والى من لا ينساهم القلب والروح إلى **أجدادي رحمهم الله.**

إلى القلوب الطاهرة الرقيقة و النفوس الصافية، إلى إخوتي:**فارس و محمد بدر** و خاصة خاصة أختي "**مريم**" التي ساعدتني في إنجاز هدا العمل، و إلى كافة عائلة "**مدرك**" كبيرا وصغيرا ، و إلى كل عائلة "**زويش**" كبيرا وصغيرا، خاصة خالاتي: **يمينة، جميلة، ذهيبة، سعدية، فاطمة.**

أهدي عملي هذا المتواضع إلى كل أصدقائي **دفعة التخرج 2023**، خاصة أصدقائي: **عبد الرحمان، جليل، نصرو، أليسيا، فيصل.**

وأهدي عملي هذا إلى أعز شخص في حياتي **سعيد.**

إلى من وسعتهم ذاكرتي ولم تسعهم مذكرتي لكم جميعا أهدي ثمرة هذا الجهد المتواضع.

نريمان

مقدمة

تعد جريمة الانترنت من الظواهر الجرمية الحديثة التي تنتشر بشكل متزايد في العصر الرقمي، وتتضمن العديد من الأنشطة الإجرامية التي تتم عبر الإنترنت، وهي تشكل تحديا أمنيا كبيرا للمجتمعات الحديثة، حيث أصبحت تقنية الحاسوب تستعمل كوسيلة لارتكاب الجرائم، حيث أصبح هذا النوع من الجرائم يرتكب في وسط افتراضي غير متعارف عليه، ولا يشبه الوسط التقليدي للجرائم التقليدية، وتعد مكافحة الجريمة من التحديات الرئيسية التي تواجه المجتمع العالمي في الوقت الحاضر. حيث يشكل الجرم الإلكتروني خطرا حقيقيا يستدعي التعامل معه بأساليب وآليات قانونية محكمة، تستطيع التصدي له والحد من تداعياته.

وتعد الجزائر من الدول التي تولي اهتماما كبيرا لمواجهة هذا التحدي، ومن خلال هذه المذكرة سيتم استكشاف الآليات القانونية التي تتوفر في التشريع الجزائري لمكافحة الجريمة الالكترونية، بما يشمل الآليات التقليدية والحديثة لمواجهة الجريمة الالكترونية والآليات المؤسساتية لمكافحتها.

وعليه فمن الأسباب التي دفعتني إلى دراسة هذا الموضوع، راجع إلى حداثته، والتزايد المستمر للجرائم الإلكترونية، وكذا الرغبة في التعمق في البحث ومواجهة النشاط الإجرامي الالكتروني.

و من هنا تكمن أهمية دراسة هذا الموضوع من خلال معرفة الجرائم المرتكبة ضد الحاسوب وشبكة الانترنت وإلقاء العبء على الدولة بوضع التشريعات اللازمة لحماية المجتمع منها، بالإضافة إلى أهمية معرفة مدى خطورة جرائم الحاسوب التي تطال المعلومات وتمس حياة الأفراد وتهديد الأمن القومي والسيادة الوطنية ، ولذلك يجب الإلمام بماهية الجريمة الالكترونية وخصائصها وأنواعها وكذا دوافع ارتكابها. والهدف من دراسة هذا الموضوع هو إثراء المكتبة وسد النقص في المراجع المتخصصة في هذا المجال، ومحاولة دراسة الظاهرة وتحليلها وبيان كيفية مكافحتها ، فقد واجهتني صعوبات في إنجاز البحث، لان الموضوع له علاقة بالجانب التقني والفني، وهذا ما يستدي التخصص للإلمام أكثر بالموضوع.

والاشكال الذي يطرح هو ما مدى فعالية الأليات القانونية لمكافحة الجريمة الإلكترونية في ظل التشريع الجزائري؟ وتندرج تحت هذه الإشكالية مجموعة من التساؤلات نذكرها فيما يلي:

-ما هو الإطار المفاهيمي للجريمة الإلكترونية ؟

- ما طبيعة الدليل المناسب لإثباتها ؟

- ما هي الصعوبات التي تحول دون مكافحتها ؟

- ما موقف المشرع الجزائري من الجريمة الإلكترونية، وما هي السبل التي أقرها لمكافحتها؟

- هل الآليات القانونية الإجرائية والمؤسساتية كفيلة لوحدها لمكافحة الجريمة الالكترونية؟

- أيمكن إيجاد آليات مساعدة على مكافحة الجريمة الالكترونية؟

ومن الأسباب الشخصية التي دفعتني لكتابة هذا الموضوع ، هو أنه مجرد اسمها يكتسي جانب من الغموض خصوصا في إطار مكافحتها، فتجعل العقل يفكر في شكل مسرح الجريمة ، و طريقة التفتيش و غيرها من الإجراءات، و هذا ما أعطاني دافع للبحث و التعرف عليها باعتبارها متعلقة بالعام الافتراضي، أما الأسباب الموضوعية تتمثل في كون أن الجريمة الإلكترونية موضوع حديث يمس الواقع المعاش، كما أن الجريمة الإلكترونية تمس كل القطاعات إذ أن الدولة تسعى إلى إنشاء إدارة إلكترونية ، حكومة إلكترونية ن و هذا ما يساعد على انتشار هذا النوع من الجرائم ، و للإجابة على الإشكالية المطروحة وتلك التساؤلات ، تم الاعتماد على مجموعة من المناهج، أولها المنهج التحليلي، والثاني المنهج الوصفي، واستعملنا كذلك المنهجين الاستقرائي والمقارن. ونظرا لتشعب البحث وما يشمله من مسائل قانونية متعددة ,انتهجت خطة بحث متكونة من فصلين مسبوقين بمبحث تمهيدي، تم التطرق فيه إلى ماهية الجريمة الالكترونية وبيان دوافع ارتكابها وكذا خصائصها وأنواعها أما الفصل الأول فقد خصصته للآليات القانونية الإجرائية لمكافحة الجريمة الالكترونية ،الآليات التقليدية(المبحث الأول)،والآليات الإجرائية الحديثة (المبحث الثاني)،أما الفصل الثاني فقد تناولت فيه الآليات القانونية المؤسساتية للجريمة الإلكترونية ،وتضمنت أيضا مبحثين ،مكافحة الجريمة الإلكترونية

بموجب القوانين والهياكل الخاصة (المبحث الأول) ، والآليات المساعدة على مكافحة الجريمة الإلكترونية (المبحث الثاني).

المبحث التمهيدي

المبحث التمهيدي: ماهية الجريمة الالكترونية

لقد شهد العالم في الآونة الأخيرة تطور ملحوظ في مجال التقنية، مما نتج عنه استعمال الحاسب الآلي وشبكة الإنترنت في جميع الميادين، لكن قد يتم استخدام هذه الوسائل بطرق غير مشروعة، الأمر الذي قد ينحدر عنه ارتكاب جرائم لها علاقة بهذا المجال، وهو ما يعرف بالجريمة الإلكترونية، ونظر الحداثة هذه الجريمة، فقد اختلف الفقهاء في وضع تعريف موحد لها، كما اتسمت بمجموعة من الخصائص، والدوافع لارتكاب هذه الجريمة، ومن خلال هذا الفصل سأحاول التطرق إلى مفهوم الجريمة الالكترونية ودوافعها في المبحث الأول، وبيان خصائصها وأنواعها في التشريع الجزائري في المبحث الثاني.

المبحث الأول: ماهية الجريمة الإلكترونية:

قبل إرادة مختلف تعريفات الجريمة الإلكترونية تجدر الإشارة إلى أنه لا توجد تسمية موحدة للدلالة على هذه الظاهرة الإجرامية، فهناك تباين في التسميات التي أطلقت عليها، ومن تسميات هذه الظاهرة جرائم الكمبيوتر والإنترنت، الجريمة المعلوماتية، الاحتيال المعلوماتي، جرائم أصحاب الياقات البيضاء، وغيرها من التسميات[1] وهناك جانب يرى أن هذه الجريمة ناشئة أساسا من التقدم التكنولوجي ومدى التطور الذي يطرأ عليه، فهو متجدد بصفة دائمة ومستمرة وخاصة في مجال تكنولوجيا المعلومات، ويفضل أن يطلق عليها اصطلاحا ' جرائم التكنولوجيا الحديثة ' التي تعتمد أساسا على الحواسيب وغيرها من الأجهزة التقنية قد تظهر في المستقبل، وهي كذلك جرائم حديثة نظرا لحداثتها النسبية من جهة، وارتباطها الوثيق بما قد يظهر من أجهزة حديثة تكون ذات طاقة تخزينية وسرعة فائقة ومرونة في التشغيل[2].

تعتبر التكنولوجيا الحديثة لاسيما تحديدا التكنولوجيا المتعلقة بتقنيات الحاسوب والإنترنت متطورة ومسارعة النمو، الآمر الذي يجعل من الصعب حصر صور الجرائم الإلكترونية

[1] نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الأولى ، دار الثقافة للنشر و التوزيع ، الأردن ، 2008 ، ص 46

[2] حمزة بن عقون ، السلوك الإجرامي للمجرم المعلوماتي ، مذكرة لنيل شهادة الماجستير ، قسم الحقوق ، كلية الحقوق و العلوم السياسية ، جامعة الحاج لخضر ، باتنة ، 2012 ، ص 13

وأنواعها، ومن هذا الإطار أثر المشروع الانجليزي في قانون إساءة استخدام الحاسوب عام 1990، عدم وضع تعريف محدد لجرائم الحاسوب بغية عدم حصر القاعدة التجريمية في إطار أفعال معنية، تحسبا للتطور العلمي والتقني في المستقبل.[1]

المطلب الأول: مفهوم الجريمة الإلكترونية:

يراد بمصطلح الجرائم المعلوماتية Les crimes d'Informationعموما مجموعة الجرائم المتصلة بعلم المعالجة المنطقية للمعلومات[2]،ويمكن القول بأن شبكة المعلومات (الإنترنت) تمثل بحق، قمة ما وصل إليه ذلك العلم من التطور. لذلك فإن للجرائم المعلوماتية الواقعة عليها طبيعة قانونية خاصة تميزها عن غيرها من الجرائم التقليدية فضلا عن الخصائص والمميزات الأخرى المتعددة والمترتبة عليها.[3]

وفي هذا المطلب سنقوم بالتطرق إلى تعريف الجريمة الإلكترونية بين الموسع لمفهوم الجريمة الإلكترونية والمضيق.

الفرع الأول: التعريف الضيق:

من التعريفات الضيقة لمفهوم الجريمة الإلكترونية:

- التعريف الذي جاء بين الفقيه الألماني تيدمان Tiedemannt بأنها :" كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب".[4]

وأيضا التعريف الذي جاء به الأستاذ Rosenblantt بأنها " نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو أخذها أو حذفها أو التي تحول عن طريقه".[5] ومن الواضح فإن هذه التعاريف تضيق من مفهوم الجريمة الالكترونية، إذ يخرج من نطاقها العديد من الأفعال غير المشروعة التي يستخدم الحاسب أداة لارتكابها.

---

[1] حمزة بن عقون، المرجع السابق، ص 13.

[2] انظر د.هدى حامد قشقوش، جرائم الحاسب الالكتروني، دار النهضة العربية، القاهرة 1992. ص8.

[3] د. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، منشورات الحلبي الحقوقية، الطبعة 1 2011، ص292

[4] حمزة بن عقون، المرجع النفسه ، ص13.

[5] نهلا عبد القادر المومني، المرجع السابق ، ص 48 .

الفرع الثاني: التعريف الموسع: لقد حاول جانب آخر من الفقه التوسع في مفهوم الجريمة الإلكترونية، وجاء ذلك على شكل عدة تعريفات نذكر منها:

تعريف خبراء المنظمة الأوروبية للتعاون الاقتصادي الذين عرفوا الجريمة على أنها:" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[1] أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد تبنى التعريف الآتي للجريمة الإلكترونية:" أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية".[2]

ما يمكن ملاحظته من هذه التعريفات أنها حاولت الإلمام بجميع الأشكال الإجرامية للجريمة الإلكترونية وعدم حصرها في شكل معين، فهي لم تركز على مرتكب الجريمة أو وسيلة ارتكابها أو على قدراته التقنية، ومنه نقول أن الجرائم الكترونية لم يرد فيها تعريف شامل ومانع، وهذا راجع إلى أن هذا النوع من الجرائم معقد وصعب وفي تطور دائم، إذ أنها تختلف فعلا عن بقية الجرائم، سواء بالنظر إلى طبيعتها الخاصة أو إلى دوافع ارتكابها. وبالنسبة للمشرع الجزائري على غرار الدول الأخرى فقد قام بتجريم أفعال المساس بأنظمة الحاسب الآلي، نتيجة للتأثر بالثورة المعلوماتية، وهذا الآمر دفع بالمشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون15/04المؤرخ في2004/11/10 المتمم للأمر رقم 156/66 والمتضمن قانون العقوبات، ونص عليها في القسم السابع مكرر بعنوان " المساس بأنظمة المعالجة الآلية للمعطيات " الذي يتضمن ثمانية مواد، من المادة 394 مكرر حتى المادة 394 مكرر7 وقد نص المشرع الجزائري على عدة جرائم منها ما جاء في المادة 394 مكرر، التي جاء فيها ثلاثة أنواع من الجرائم والتي تنص: يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50.000 إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. وإذا ترتب على الأفعال المذكورة أعلاه

[1] حمزة بن عقون، المرجع السابق ، ص 15 .

[2] حمزة بن عقون، المرجع نفسه ، ص 16 .

تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من50.000 دج إلى150.000 دج[1].كما أقر المشرع الجزائري بمسؤولية الشخص المعنوي بموجب المواد(18مكرر،18مكرر1) من القانون04/15،وعاقب على الاشتراك في هذه الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر 5).كما أدخل تعديل آخر على قانون العقوبات الجزائري في2006بموجب القانون 23/06 المؤرخ في2006/12/20الذي قام فيه بتشديد عقوبة الحبس والغرامة المقررة لهذه الأفعال فقط دون لمساس بالنصوص التجريمية الواردة في هذا القسم (القسم 7مكرر) من قانون رقم 15/04.

المطلب الثاني: الدوافع الشخصية لارتكاب الجريمة الإلكترونية:

في هذا المطلب سنقوم بدراسة دوافع أو الأسباب الدافعة إلى ارتكاب الجريمة الإلكترونية.

الفرع الأول: الدوافع الشخصية لارتكاب الجريمة الإلكترونية: تصنف هذه الدوافع إلى دوافع مادية وأخرى ذهنية، وذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب الجريمة الإلكترونية، أو تأثير العنصر الذهني المعنوي على المجرم الإلكتروني ودفعه لارتكاب جريمته، هذا ما سنقوم بدراسته في ما يلي:

أولا: الدوافع المادية: يعتبر الدافع المادي من أكثر الدوافع التي تترك الجاني لاقتراف الجريمة الإلكترونية، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الإلكتروني الى تطويرنفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويشتغل الفرص ويسعى إلى الاحتراف الآلية لها من خلال اكتشافه لفجواتها الأمنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه، أو لحساب شركائه، أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة. كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها، بطريق الاختلاس من جهاز الحاسوب، وقد أشارت إليه مجلة"Securiteinformatique"وهي مجلة متخصصة في الأمن المعلوماتي، أن43%من

[1] المادة (394 مكرر من الأمر155/66 من قانون العقوبات المؤرخ في 8 جوان 1966، المعدل والمتمم بالقانون 15/04 المؤرخ في 10 نوفمبر 2004، ج ر 71 بتاريخ 10 نوفمبر 2004 ص 11، 12.

حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، و23%من أجل سرقة معلومات، و19% أفعال إتلاف، و15%الاستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية. وفي حال نجاح المجرم الإلكتروني في ارتكاب جريمته فإن ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادة التي يحققها المجرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الالكترونية، حيث تبين أن 85% من المشاركين في الدراسة تعرضوا للاختراقات بالنسبة للأنظمة المعلوماتية، وأن 64% لحقت بهم خسارة مادية جراء هذه الاعتداءات.[1]

ثانيا: الدوافع الذهنية لارتكاب الجريمة الإلكترونية:

المتعة والتحدي والرغبة في فهم النظام المعلوماتي وإثبات الذات. وقد تكون هذه الدوافع مجرد شغف بالإلكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الأنظمة الإلكترونية وكسر الحواجز الأمنية المحيطة بهذه الأنظمة قد يشكل متعة كبيرة لمرتكبيها وتسلية تغطي أوقات فراغه، وعلى صعيد آخر قد يكون إقدام المجرم الإلكتروني على ارتكاب جريمته بدافع الرغبة في قهر الأنظمة الإلكترونية والتغلب عليها، إذ يصير المجرم هنا إلى إظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب لا تكون لديهم دوافع حاقدة أو تخريبية، وإنما ينطلق من دافع التحدي وإثبات المقدرة.[2]

---

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة الالكترونية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة لخضر، 2012- 2013، 620-61 نقلا عن نهلا عبد القادر المومني الجرائم المعلوماتية، ط02، 2010، ص90، ونقلا عن ضاح محمود الخمود ونشأت مقضي المجاني، جرائم الإنترنت، دار المنار للنشر والتوزيع، 2005ص31.

[2] سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص61-62.

الفرع الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية:

قد يتأثر المجرم الإلكتروني ببعض المواقف قد تكون دافعة له على اقتراف الإجرام الإلكتروني ولا يسعى في ذلك حينها للمتعة والتسلية ولا لكسب المال، وفي هذا الفرع سنقوم بإبراز أهم هذه الدوافع:

أولا: دافع الانتقام وإلحاق الضرر برب العمل: ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقية، فهذه الأمور تجعله يقدم على ارتكاب جريمته[1]، كما يعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك أنه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة أو الشركة التي يعمل فيها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المجرم الإلكتروني الرغبة في الانتقام من رب العمل، ومثال ذلك أن الانتقام دفع بمحاسب إلي التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

ثانيا: دافع التعاون والتواطؤ: هذا النوع يتكرر كثيرا في الجرائم الإلكترونية، وغالبا ما يحدث بالتعاون

بين متخصص في الأنظمة المعلوماتية، أين يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسها لتلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم.[2]

الفرع الثالث: الدافع القومي والوطني:

وهو أن يقوم الهاكرز بالهجوم على مواقع معادية تختلف مع قيم وعادات مجتمع ما بتدمير أو

---

[1] صغير يوسف. الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013/03/06 ص42.

[2] سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص62.

تغيير هذه المواقع، مما يؤدي إلى منعها من تهديد فكر وسلوك أفراد ذلك المجتمع (أحمد 2010) وإذا كانت هذه أبرز الدوافع لارتكاب الجريمة الإلكترونية، مع ذلك فهي ليست ثابتة ومتعددة لدى الفقهاء والباحثين لأن السلوك الإجرامي والدوافع لارتكاب الجريمة الإلكترونية قد تتغير وتتحول بسرعة من حالة العبث ومحاولة التحدي والتغلب على الأنظمة، إلى تدميرها أو على الأقل حيازتها للقيام بعملية الابتزاز والحصول على الأموال، لذلك فإن هذه الدوافع قد لا تتوقف عن هذا الحد، إذ نجد في كل جريمة جديدة دوافع جديدة، بكل كثيرا ما نحد الجريمة الواحد لها دوافع متعددة خاصية ما إذا اشترك فيها أكثر من شخص أو أكثر من جهة بحيث يسعى كل منهم لتحقيق أهدافه الخاصة.[1]

المبحث الثاني: خصائص وأنواع الجريمة الإلكترونية في التشريع الجزائري:

بعد التطرق لمفهوم الجريمة الإلكترونية، وبيان الدوافع المؤدية لارتكابها من طرف المجرم الإلكتروني، سأحاول من خلال هذا المبحث بيان خصائص هذه الجريمة وأنواعها في التشريع الجزائري بحسب ما إذا ارتكبت باستخدام النظام المعلوماتي، أو كانت موجهة ضده، وهذا ما يتم بيانه في المطلبين الآتيين:

المطلب الأول: خصائص الجريمة الإلكترونية:

لما كانت الجريمة الإلكترونية هي نتائج التطور العلمي والتكنولوجي، وبالتالي فهي تختلف عن الجريمة التقليدية التي ترتكب في الواقع المادي الملموس، لذا تجد لها مجموعة من الخصائص والتي سنقوم بدراستها في هذا المطلب. مع تبيان أثر خصوصية الجريمة الإلكترونية على الإثبات.

الفرع الأول: الجريمة الإلكترونية متعددة الحدود:

المجتمع المعلوماتي مجتمع لا يعترف بالحدود الجغرافية، فهو منفتح عبر شبكات تخترق الزمان والمكان دون خضوعها لحرس الحدود، فبعد ظهور شبكات المعلومات الدولية لم يعد

[1] سعيداني نعيم، رسالة الماجستير نفسها، ص62.

هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات حيث أن القائم على النظام المعلوماتي في أي دولة يمكنه أن يحول مبلغا من المال لأي مكان في العالم.[1]

الفرع الثاني: صعوبة اكتشافها وإثباتها:

تتميز الجريمة الإلكترونية بكونها لا تترك آثار ماديا لها بعد ارتكابها، وصعوبة الاحتفاظ الفني بآثارها إن وجدت، إذ ليست هناك أموال أو مجوهرات مفقودة، إنما هي أرقام تتغير في السجلات لذا نجد أن معظم جرائم الانترنت تم اكتشافها بالمصادفة، بل وبعد وقت طويل من ارتكابها.[2]

الفرع الثالث: الجريمة المعلوماتية تتم عادة بتعاون أكثر من شخص:

تتميز الجريمة الإلكترونية أنها تتم عادة بتعاون أكثر من شخص على ارتكابها فغالبا ما يشترك في إخراج الجريمة إلى حيز وجود شخص متخصص في تقنيات الحاسوب والانترنت، يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو خارج مؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب إليه.

إذ أن الأشخاص الذين يقومون بارتكابها عادة يكونون من ذوي الاختصاص في مجال تقنية المعلومات، والاشتراك في إخراج الجريمة المعلوماتية إلى حيز الوجود وقد يكون اشتراكا سلبيا وهو الذي يتضح بالصمت من جانب من يعلم بالجريمة في محاولة منه لتسهيل إتمامها، وقد يكون اشتراكا إيجابيا وهو الغالب في الكثير من الجرائم ويتمثل في المساعدة الفنية أو المادية.[3]

***أثر خصوصية الجريمة الإلكترونية على الإثبات:**

تتميز الجريمة بطبيعة خاصة جعلتها تثير العديد من المشكلات، مما صعب إلى درجة كبيرة إثبات الجريمة الإلكترونية وهذا راجع إلى العديد من الأسباب منها:

أن الجريمة الإلكترونية تتم في بيئة غير تقليدية، فهي تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل أمر طمس الدليل ومحوه كليا سهل جدا

[1] نهلا عبد القادر المومني، المرجع ص50.

[2] سمير معاشي" ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني، العدد السابع، جامعة محمد خيضر كلية الحقوق والعلوم السياسية، بسكرة2010 ، ص284.

[3] نهلا عبد القادر المومني، المرجع السابق، ص58.

ومن ثم يكون من الصعب ملاحقة المجرم أو كشف شخصيته، لذلك يرى جانب من الفقه ضرورة تدخل المشرع بإضافة حالة ارتكاب الجريمة الإلكترونية كظرف استثنائي، يسمح لرجال السلطة العامة بالقيام بضبط الأدلة عند وقوع الجريمة، وبدون إذن مسبق من النيابة العامة، وهذا حماية للأدلة من المحو والتعديل من قبل الفاعل. كما أن المجني عليه له دور في هذه الصعوبة، بسبب دوره السلبي وعدم إبلاغه عن وقوع هذا النوع من الجرائم، فالكثير من الجهات التي تتعرض أنظمتها للانتهاك تعمد إلى عدم الكشف عنها تجنبا لعدم الإضرار بسمعتها ومكانها وتكتفي باتخاذها الإجراءات الإدارية، وفي هذا الخصوص أوص المؤتمر الدولي الخامس عشر للجمعية العامة، والذي عقد في " ريو دي جانيرو " بالبرازيل في الفترة من 4 إلى 9 سبتمبر 1994، بضرورة تشجيع المجني عليهم في هذه الجرائم على الإبلاغ عنها فور وقوعها، وهذا بهدف تحقيق الرقم الأسود للجرائم الإلكترونية في الفضاء الافتراضي. كما أن نقص الخبرة الفنية والتقنية لدى سلطات الاستدلال والتحقيق والقضاء، يشكل عائقا أساسي أمام إثبات الجريمة الإلكترونية، ذلك أن هذا النوع يتطلب تدريب، وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة، والملاحقة في بيئة الحاسوب والانترنت، ونتيجة لنقص الخبرة والتدريب كثيرا ماتخفق أجهزة القانون في تقدير أهمية هذه الجرائم، فلا تبذل لكشف غموضها وضبط مرتكبيها جهودا تتناسب وهذه الأهمية، بل إن المحقق قد يدمر الدليل عن خطأ منه أو إهمال أو بالتعامل بخشونة مع مختلف الوسائط التي تتضمن الدليل الإلكتروني كالأقراص المرنة وغيرها.[1]

ومنه نقول أن الجريمة الإلكترونية تنشأ عنها عدة معيقات تعيق إثباتها، وهذا في إطار الإثبات الجنائي، وهذا نظرا للطبيعة الخاصة لهذه الجريمة المستحدثة كصعوبة جمع أدلتها نظرا لسهولة محوها وتغييرها بعد ارتكاب الجريمة مباشرة، وهذا الأمر كما رأينا يترتب عليه صعوبة الوصول إلى الفاعل ومرتكب الجريمة.

[1] عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي: دار الجامعة الجيدة، مصر2010، ص46، 49.

المطلب الثاني: أنواع الجريمة الإلكترونية في التشريع الجزائري:

إن أنواع الجرائم الإلكترونية كثيرة حيث لم يوضع لها معايير محددة من أجل تصنيفها وهذا راجع إلى التطور المستمر للشبكة والخدمات التي تقدمها.

الفرع الأول: الجرائم المعلوماتية الواقعة بواسطة النظام المعلوماتي:

أولا: الجرائم الواقعة على الأشخاص:

فرغم الإيجابيات والقواعد التي جاءت بها الشبكة المعلوماتية والتسهيلات المقدمة للفرد، إلا أنها جعلته أكثر عرضة للانتهاك، ومنها:

1_جريمة التهديد: يقصد به زرع الخوف في النفس، بالضغط على إرادة الإنسان، وتخويفه من أضرار ما ستلحقه أو ستلحق أشخاص له صلة بها، ويجب أن يكون التهديد على قدر من الجسامة المتمثلة بالوعيد بإلحاق الأذى ضد نفس المجني عليه أو ماله أو ضد نفس أو مال الغير.

2_انتحال شخصية: وهو استخدام شخصية فرد للاستفادة من ماله أو سمعته أو مكانته، ولقد تميزت بسرعة الانتشار خاصة في الأوساط التجارية. وتتم بجمع قدر كبير من المعلومات الشخصية المراد انتحال شخصيته، للاستفادة منها لارتكاب جرائمه عن طريق استدراج الشخص ليدلي بمعلوماته الشخصية الكاملة، كالاسم، العنوان الشخصي، رقم بطاقة الائتمان للتمكن من الوصول لماله أو سمعته.....عن طريق الغش.

3_انتحال شخصية أحد المواقع: ويتم ذلك عن طريق اختراق أحد المواقع للسيطرة عليه، ليقوم بتركيب برنامج خاص به هناك، باسم الموقع المشهور.[1]

4_جرائم السب والقذف: المساس بشرف الغير وسمعتهم، واعتبارهم ويكون القذف والسب كتابيا أو عن طريق مطبوعات أو رسوم، عبر البريد الإلكتروني أو الصوتي، صفحات الويب، بعبارات تمس الشرف. فيقوم المجرم بنشر معلومات تكون مغلوطة عن الضحية، وقد يكون شخصا طبيعيا أو معنويا، لتصل المعلومات المراد نشرها إلى عدد كبير من مستخدمي شبكة الإنترنت.

[1] محمد عبد الله بن علي المنشاوي، جرائم الإنترنيت في المجتمع السعودي، ماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2003، ص55.

5_المواقع الإباحية والدعارة: وجود مواقع على شبكة الانترنيت تحرض على ممارسة الجنس للكبار والقصر، وذلك بنشر صور جنسية للتحريض على ممارسة المحرمات، والجرائم المخلة بالحياء عن طريق صور، أفلام، رسائل..... بالإضافة إلى انتشار الصور ومقاطع الفيديو المخلة بالآداب على مواقع الإنترنيت من قبل الغزو الفكري لكي بتداولها الشباب وإفساد أفكارهم وإضعاف إيمانهم. وتوفير الشبكة تسهيلا للدعارة، عبر آلاف المواقع الإباحية، وتسويق الدعارة وتستثمر لها مبالغ ضخمة مع استخدام أحدث التقنيات.

6_التشهير وتشويه السمعة: يقوم المجرم بنشر معلومات قد تكون سرية أو مظللة أو مغلوطة عن ضحيته، والذي قد يكون فردا أو مؤسسة تجارية أو سياسية.

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي كلفها القانون وفي مقدمته الدستور الجزائري حيث تنص المادة 40 منه: " تضمن الدولة عدم انتهاك حرمة الإنسان."[1]

وعليه فإن استخدام الشبكة المعلوماتية في الاعتداء على حرية الفرد وحياته الخاصة وحرمته، والحريات العامة للأفراد، مخالف للقانون ومعاقب عليه.

ثانيا: الجرائم الواقعة على الأموال:

أصبحت معاملات الشراء، البيع والإيجار تتم عبر الشبكة المعلوماتية، وما أنجز عليه من وسائل الدفع والوفاء، فابتكرت معه طرق ووسائل للسطو على هذا التداول المالي بطريق غير مشروع، كالتحويل الإلكتروني، السرقة، القرصنة وغيرها.

1_السرقة الواقعة على البنوك: يتم سرقة المال بالطرق المعلوماتية، عن طريق اختلاس البيانات والمعلومات الشخصية للمجني عليهم، والاستخدام لشخصية الضحية ليقوم بعملية السرقة المتخفية، ما يؤدي بالبنك إلى تحويل البنكي للأموال الإلكتروني أو المادي إلى الجاني. حيث يستخدم الجاني الحاسب الآلي لدخول شبكة الإنترنيت والوصول إلى المصاريف والبنوك،

[1] بنظر المادة 1/40 من دستور 1996، ج. ر رقم 76 المؤرخة في 8 ديسمبر 1996، المعدل والمتمم بالقانون رقم 16- 01 المؤرخ في 6 مارس 2016، ج. ر رقم 14 المؤرخة في 07 مارس 2016.

وتحويل الأموال الخاصة بالعملات إلى حسابات أخرى.[1] مثال: كالاستيلاء على ماكينات الصرف الآلي والبنوك، ينتم فيها نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ومن ثم استخدامها لصرف أموال من حساب الضحية.

2_تجارة المخدرات عبر الإنترنيت: تتعلق بالترويج للمخدرات وبيعها، والتحريض على استخدامها، وصناعتها بمختلف أنواعها.

3_غسيل الأموال: تمارس عبر الإنترنيت، حيث استفاد الجناة ما وصلت إليه عصر التقنية المعلوماتية لتوسيع نشاطهم الغير مشروع في غسيل أموالهم، بتوفير السرعة وتفادي الحدود الجغرافية، والقوانين المعيقة لغسيل الأموال، وكذا لتشفير عملياتهم وسهولة نقل الأموال واستثمارها لإعطائها الصيغة الشرعية.[2]

4_قرصنة البرمجيات: هي عملية نسخ وتقليد لبرامج إحدى الشركات العالمية على اسطوانات وبيعها لناس بسعر أقل، وجريمة نسخ المؤلفات العلمية والأدبية بالطرق الإلكترونية المستحدثة، حيث أن المعلومة الأدبية والفكرية ذات قيمة أدبية ومادية بالإضافة إلى براءات الاختراع التي تحول لمالكها حق معنوي وآخر مالي، نص عليها المشرع في الدستور في المادة 44: " حقوق المؤلف يحميها القانون[3]. " بالإضافة إلى قوانين متعلقة بحقوق المؤلف والحقوق المجاورة، وبراءات الاختراع[4].

ثالثا: الجرائم الواقعة على آمن الدولة:

تقع هذه الجرائم باستعمال النظام المعلوماتي سواء لإفشاء الأسرار التي تخص مصالح الدولة ونظام الدفاع الوطني أو الإرهاب، التجسس...

---

[1] عباس أبو شامة، التعريف بالظواهر الإجرامية المستحدثة: حجمها، أبعادها، ونشاطها في الدول العربية، الندوة العلمية للظواهر الإجرامية المستحدثة وسبل مواجهتها، تونس، أيام 29-30 جوان 1999، ص20.

[2] صالحة العمري، جريمة غسيل الأموال وطرق مكافحتها، مجلة الاجتهاد القضائي، العدد الخامس، مخبر أثر الاجتهاد القضائي على حركة التشريع، جامعة محمد خيضر، بسكرة د.س.ن، ص179.

[3] انظر المادة 2/44 من الدستور المرجع السابق.

[4] ينظر الأمر 03-05 المؤرخ في 2003، المتعلق بحقوق المؤلف و الحقوق المجاورة، و كذلك الأمر 03-07 المؤرخ في 19 جويلية2003 المتعلق ببراءت الاختراع ،ج،ر رقم 44 المؤرخة في 23 جويلية 2003.

نصت عليها المادة 394 مكرر2: " تضاعف العقوبة المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد".[1]

_الإرهاب: تستخدم المجموعات الإرهابية حاليا تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية. وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات والتنسيق، وبث الأخبار المغلوطة، وتوظيف بعض صغار السن.

2_التجسس: يقوم المجرمون بالتجسس على الدول والمنظمات والشخصيات والمؤسسات الوطنية أو الدولية، وتستهدف خاصة، التجسس العسكري، السياسي، الاقتصادي، وذلك بإستخدام التقنية المعلوماتية، وتمارس من قبل دولة على دولة، أو من شركة على شركة.... وذلك بالاطلاع على المعلومات الخاصة المؤمنة في جهاز آلي، وغير مسموح الاطلاع عليه، كأن تكون من قبيل أسرار الدولة.

الفرع الثاني: الجرائم المعلوماتية الواقعة على النظام المعلوماتي:

وهي الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف سواء المكونات المادية لنظام المعلومات أو برامج النظام المعلوماتي، أو المعلومات المدرجة بالنظام المعلوماتي على النحو التالي:

أولا: الاعتداء على برامج النظام المعلوماتي:

ويتوجب هنا معرفة ودراية ذات درجة عالية في مجال البرمجة، وتقع هذه الجرائم إما على البرامج التطبيقية أو برامج التشغيل.

1_البرامج التطبيقية: وهنا يقوم الجاني بتحديد البرامج ثم التلاعب فيها للاستفادة منه ماديا، وذلك بتعديل البرنامج: ويكون الهدف من تعديل البرامج اختلاس النقود، حتى ولو كان باستقطاع مبالغ قليلة لكن لفترات زمنية طويلة لتحقيق الفائدة، بدون إثارة الشبهات. أما التلاعب: فيأخذ عدة أشكال، فقد يكون عن طريق زرع برنامج فرعي في البرنامج الأصلي مثلا يسمح له

[1] ينظر المادة 394 مكرر2 من الأمر 66- 156، المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، المعدل المتمم.

الدخول غير المشروع في العناصر الضرورية للنظام المعلوماتي، حيث يصعب اكتشاف هذا البرنامج لدقته وصغر حجمه.[1]

2_برامج التشغيل: وهي البرامج المسؤولة عن عمل نظام معلوماتي من حيث قيامها بتنظيم وضبط ترتيب التعليمات الخاصة بالنظام.

وتقوم الجريمة هنا عن طريق تزويد البرامج بمجموعة تعليمات إضافية ليسهل الوصول إليها بواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي.[2] شكلين هما وتأخذ المصيدة وهو إعداد برنامج به ممرات وفراغات في البرنامج وتفرعات إضافية، وهنا يمكن للمبرمج استخدام البرنامج في أي وقت، ويصبح المهيمن على النظام وعلى صاحب العمل. أما تصميم البرنامج هو القيام ببرنامج خصيصا يصعب اكتشافه لارتكاب الجريمة ومراقبة تنفيذها.

ثانيا: الجرائم الواقعة على المكونات المادية للنظام المعلوماتي:

ويقصد به الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات، الكابلات والاعتداء عليها يكون بالسرقة لهذه المعدات، أو عن طريق الإتلاف العمدي كإحراقها، ضرب الآلات بشيء ثقيل، العبث بمفاتيح التشغيل خربشة الأسطوانات لكي لا تصبح صالحة للاستعمال.[3]

ثالثا: الجرائم الواقعة على المعلومات المدرجة بالنظام المعلوماتي:

إن المعلومات المعالجة آليا هي أساس عمل النظام المعلوماتي، لأنها ذات قيمة مادية واقتصادية، لذلك تعد هدفا للجرائم الإلكترونية من خلال التلاعب فيها أو إتلافها.

1_التلاعب: يكون في المعلومات الموجودة على النظام المعلوماتي بطريقة مباشرة أو غير مباشرة، فيتم التلاعب المباشر عن طريق إدخال معلومات بمعرفة المسؤول عن القسم

---

[1] Le rapport du conseil du l'Europe. 15، 18 novembre 1976.

[2] أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، الطبعة الثانية 2006، ص87.

[3] ذكي ذكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي، المؤتمر السادس للجامعة المصرية للقانون الجنائي، القاهرة أيام 25-28 أكتوبر 1993، ص471.

المعلوماتي، كضم مستخدمين غير موجودين بالعمل بهدف الحصول على مرتباتهم، أو الإبقاء على مستخدمين تركوا العمل للحصول على مبالغ شهرية، أو عن طريق تحويل مبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك، وتسجيلها وإعادة ترحيلها وإرسالها لحساب آخر في بنك آخر، بهدف اختلاس الأموال.[1]

أما التلاعب الغير مباشر، فيتم عن طريق التدخل لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين، أو التلاعب عن بعد بمعرفة أرقام وشفرات الحسابات،[2] قصد التلاعب في الشرائط الممغنطة، أو باستخدام الجاني كلمة السر أو مفتاح الشفرة، وإمكانية تسلل الجاني إلى المعلومات المخزنة والحصول على المنفعة المالية من مسافات بعيدة.

2_إتلاف المعلومات: في مجال المعلوماتية بالاعتداء على الوظائف الطبيعية للحاسب الآلي، وذا بالتعدي على البرامج والبيانات المخزنة والمتبادلتين الحواسب وشبكاته، وتدخل ضمن الجرائم الماسة بسلامة المعطيات المخزنة ضمن النظام المعلوماتي، ويكون الإتلاف العمدي للبرامج والبيانات كمحوها أو تدميرها الكترونيا، أو تشويهها على نحو يجعلها غير صالحة للاستعمال.

[1] محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الثانية دار النهضة العربية، القاهرة،1994، ص7.

[2] Voir I 'information nouvelle, mai 1976.N°73.

الفصل الأول

الفصل الأول: الآليات القانونية الإجرائية للجريمة الإلكترونية:

كرس المشرع جملة من الإجراءات القانونية التي من شأنها مساعدة جهات التحقيق في الكشف عن الجريمة المعلوماتية ومن ضمن هذه الإجراءات تجد الآليات التقليدية نذكر الدليل الالكتروني الذي بموجبه يمكن متابعة مرتكب الجريمة، ونجد أيضا إجراء التفتيش ويمكن تطبيقه على البيئة الرقمية مع مراعاة خصوصية هذه البيئة وطبيعتها واعتراض المراسلات وتسجيل الأصوات والتقاط الصور. بالإضافة إلى هذه الإجراءات نجد الآليات الإجرائية الحديثة التي استحدثها المشرع للكشف عن الجريمة الالكترونية سنذكر فيها: التسرب الالكتروني والذي يقوم به ضباط الشرطة القضائية.

المبحث الأول :الآليات التقليدية:

في هذا المبحث سنتطرق إلى الآليات التقليدية لمكافحة الجريمة الإلكترونية الدليل الإلكتروني، التفتيش والمعاينة (المطلب الأول) واعتراض المراسلات وتسجيل الأصوات والتقاط الصور (المطلب الثاني).

المطلب الأول: الدليل الالكتروني والتفتيش والمعاينة.

في هذا المطلب سنتطرق إلى الدليل الإلكتروني ثم التطرق إلى تعريف التفتيش والمعاينة.

الفرع الأول: الدليل الالكتروني:

أولا: تعريف الدليل الإلكتروني:

إن التعاريف التي جاءت فيما يخص الدليل الإلكتروني، كانت متباينة، فمنها ما جاء واسعا ومنها ما جاء ضيقا، وهذا راجع للعلم الذي ينتمي إليه هذا الدليل، فاختلفت بين أولئك الباحثين في مجال التقنية، والباحثين في المجال القانوني.

وعليه سنورد فيما يلي التعاريف الفقهية للدليل الالكتروني وتعريفه من قبل المنظمة الدولية لأدلة الحاسوب. عرفه البعض على أنه : "كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما"[1].

[1] عائشة بن قارة مصطفى، المرجع السابق ص53.

وأيضا هناك من يعرفه بأنه: "معلومات يقبلها المنطق والعقل ويعتمدها العلم يتم الحصول عليها بإجراءات قانونية وعلمية ، بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة أو جان أو مجني عليه"[1].

من معدات وأدوات الحاسب الآلي من خلال إجراءات قانونية وفنية بهدف تحليلها علميا لتقديمها للقضاء في شكلها النهائي.

كما نجد التعريف الذي جاء به الأستاذ " كيسي" الذي عرفه بأنه: يشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هنالك جريمة قد ارتكبت أو توجد علاقة بين الجريمة والجاني أو بين الجريمة والمتضرر منها.

والبيانات الرقمية هي مجموعة من الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات ، الخرائط، الصوت والصورة[2].

الملاحظ على هذه التعاريف الفقهية أنه هناك خلط بين الدليل الالكتروني وبرامج الحاسب الآلي حيث تم اعتبار هذا الدليل كبيانات يتم إدخالها إلى جهاز الحاسوب، وهذا التعريف ينطبق تماما مع مفهوم برامج الحاسب الآلي.

فكلا المصطلحان يعد آثار المعلوماتية، وباعتبار أن البيانات الموجودة داخل الكمبيوتر مهما كانت صورته نصوص أو أرقام أو صور وغيرها تتحول إلى طبيعة رقمية، لان تكنولوجيا المعلومات الحديثة ترتكز على تقنية الترقيم، إلا أن الفرق بين الدليل الإلكتروني داخل الكمبيوتر وبرامج الحاسوب يكمن في الوظيفة التي يؤديها كل واحد منهما ، حيث يتمحور دور برامج هذا الجهاز في تشغيله، وتوجيهه إلى حل المشاكل ووضع الخطط المناسبة، وإلا كان مجرد آلة صماء، والملاحظ أن هناك برامج خاصة تساهم في استخلاص الدليل الالكتروني

[1] عائشة بن قارة مصطفى، المرجع نفسه ص53.

[2] محمد الأمين البشرى، التحقيق في الجرائم المستحدثة الطبعة الأولى دار الحامد للنشر والتوزيع الأردن 2014ص233.

كبرنامج معالجة الملفات مثل: (XTRA PRO GOLD) وبرنامج النسخ (la PLINK) أما الدليل الالكتروني له دور أساسي في التعرف على كيفية حدوث الجريمة الالكترونية بغرض إثباتها ونسبتها لمرتكبيها، خاصة في البيئة الافتراضية، حيث يمكن تفتيش محتوى القرص الصلب لمعرفة كل المراحل التي مر بها المجرم في سبيل تحقيقه للهدف الإجرامي .

ومن جهة أخرى نجد أن التعريفات قد حصرت الأدلة الإلكترونية في أجهزة الحاسب الآلي وملحقاته، إلا أنه نجد أن هناك نظم أخرى مدمجة بالحواسب كالهواتف المحمولة والبطاقات الذكية والمساعد الرقمي الشخصي[1].

التعريف الصادر من المنظمة الدولية الأدلة الحاسوب (LOCE) ، وقد عرفته المنظمة لأول مرة في مارس سنة 2000 وهذا بقولها:

بأنه:" المعلومات المحزنة أو المتنقلة في تشكل ثنائي، والتي يمكن الاعتماد عليها أمام المحكمة[2].

ثم عرفته في أكتوبر سنة2001، على أنه المعلومات ذات القيمة المحتملة، والمخزنة والمنقولة في صورة رقمية[3].

ثانيا: خصائص الدليل الالكتروني:

للدليل الالكتروني خصائص تميزه عن الأدلة الجنائية التقليدية، وهذا راجع للبيئة التي يحيا فيها وهي البيئة الافتراضية، وما يمكن أن يقال عن هذه البيئة.

أنها متطورة بطبعتها، بحيث تشمل على أنواع متعددة من البيانات الرقمية التي قد تكون منفردة أو مجتمعة حتى تكون دليلا للإدانة أو البراءة ومنه فان هذه البيئة انعكست على هذا الدليل، مما جعله يتصف بعدة خصائص لا تتوافر في باقي الأدلة الجنائية.

---

[1] عائشة بن قارة مصطفى المرجع السابق ص55،60.

[2]أحمد مسعود مريم، آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم04/03 مذكرة لنيل شهادة الماجستير، قسم الحقوق والعلوم السياسية، جامعة قاصدي مرباح الجزائر 2010 ص02.

[3] المرجع نفسه، ص82.

وهذا ما سنوضحه من خلال العناصر التالية بالتكلم عن كل خاصية على حدا، وسيكون الحديث في البدء عن الخاصية العلمية للدليل الالكتروني، ثم خاصيته التقنية، بعدها ما يتميز من تنوع وتطور وكذا الحديث عن أنه دليل يصعب التخلص منه وقابل للنسخ.

1: الدليل الالكتروني دليل علمي :الدليل الإلكتروني هو الواقعة التي تتنبئ عن وقوع الجريمة أو فعل مشروع ، وهذه الواقعة مبناها علمي، من حيث أن مبنى العالم الافتراضي علمي، وهذه الخاصية مفادها أن الدليل لا يمكن الحصول عليه ولا الاطلاع على فحواه إلا باستخدام الأساليب العلمية[1].

وتفيد هذه الخاصية أيضا أنه عند قيام رجال الضبط القضائي أو سلطات التحقيق، بالتعامل مع هذا الدليل سعيا لإثبات الحقيقة بطريقة علمية، أي يكون البحث على أسس علمية، وهذا مرده إلى أن الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقاً لقاعدة القانون المقارن هي قاعدة "أن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة"، وعلى الرغم من الانتقادات التي توجه إلى هذه القاعدة من حيث الالتزام الذي يلقيه القانون المقارن على أعضائه بضرورة توافر معرفة علمية، لكي يمكن إقامة بنيان التمييز بين ما هو قانوني وما هو علمي.

كذلك تفيد هذه الخاصية وجوب حفظ الدليل الإلكتروني على أسس علمية، ومنه ضرورة البحث على تحديث أسلوب تحرير المحاضر في هذا الشأن، فتحرير محضر يتناول دليلا علميا يختلف عن المحاضر المتناول اعتراف شخص بجريمة قتل أو انتهاك حرمة مسكن و غيرها فالمحضر بالدليل العلمي يعني وجوب توافر مسلك علمي يتوافق مع ظاهرة الدليل العلمي أثناء تحريره بحيث يجب ألا يتخذ صورة المحضر التقليدي[2].

[1] فتحي محمد أنور عزت الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، الطبعة الأولى دار الفكر والقانون، مصر 2010، ص648.

[2] فتحي محمد أنور عزت، المرجع نفسه، ص649.

2: الدليل الإلكتروني دليل تقني: جاءت التقنية بناءا على ميزته العلمية، باعتبار أن العلم يبنى على أساس التقنية، ولا يمكن أن تتواجد هذه التقنية بدون أسس علمية، ومفاد هذه الخاصية أن يتم التعامل مع الدليل الإلكتروني من قبل تقنيين مختصين في العالم الافتراضي وفي الدليل الإلكتروني، لأن الدليل الإلكتروني ليس كالدليل العادي، فما تتجه إليه التقنية هو نبضات إلكترونية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب في أي شكل يكون عليه، فقام المشرع البلجيكي على إثره بمقتضى القانون 28نوفمبر2000،بتعديل قانون التحقيق الجنائي بإضافة المادة 39،التي سمحت بضبط الأدلة الإلكترونية، كنسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية[1].

فهذه الخاصية دعوة إلى سلطات الضبط القضائي والتحقيق لكي يمكنهم الشروع في بناء منطق لا يقوم على أساس الخبرة، فمثلا سلطات التحقيق الجنائي في العديد من الدول وعلى رأسها الولايات المتحدة الأمريكية تتوفر على مقومات الاستدلال والتحقيق التقنية الكاملة، وهو ما يستفاد منه الفصل بين الخبرة وسلطات الاستدلال والتحقيق فيما يتعلق بالدليل الإلكتروني مع توافر هذه السلطات على عناصر ذات خبرات عالية الكفاءة فيما يخص هذا الدليل.

كما تظهر أهمية تقنية الدليل الإلكتروني في الدور الذي تقوم به التقنية في كشف الدليل الإلكتروني، وهذه العلاقة تقتضي الاهتمام من ناحيتين، الأولى ضرورة الاهتمام بتقنية البرامج التي تتعامل مع الدليل الالكتروني من ناحية اكتسابه أو التحفظ عليه، وتحليله، وتقديمه، والثانية هي أن هذه البرامج في حد ذاتها يجب أن تكون مقبولة من قبل المحكمة، وهذا ما يستدعي الإشارة في محضر الاستدلال والتحقيق إلى التقنية المستخدمة في الحصول على هذا الدليل.

[1] فتحي محمد أنور عزت، المرجع نفسه ، ص648.

فإن إطلاق صفة الكتروني تعني أن يكون هناك توافق بين الدليل المرصود وبين البيئة التي يعيش فيها، فلا وجود للدليل الإلكتروني خارج بيئته التقنية أو الإلكترونية[1].

3: الدليل الإلكتروني يصعب التخلص منه:

وتعد هذه الخاصية أو الميزة من أهم خصائص الدليل الالكتروني ويتمتع بها عن باقي الأدلة التقليدية، بحيث يمكن التخلص بكل سهولة من الأوراق، والأشرطة المسجلة إذ كانت تحمل اعتراف شخص بارتكابه للجريمة، وذلك بتمزيقها وحرقها، كما أنه يمكن التخلص من بصمات الأصابع بمسحها من موضعها ، كما أن هناك في بعض الدول يتم فيها التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة ، هذا فيما يخص الأدلة التقليدية، أما بالنسبة للأدلة الإلكترونية فإن الحال غير ذلك، حيث أنه يمكن استرجاعها بعد محوها، وإصلاحها بعد تلافها، وإظهارها بعد إخفاءها، مما يؤدي إلى صعوبة التخلص منها ،لان هناك العديد من البرامج الحاسوبية تتمثل وظيفتها في استعادة البيانات التي تم حذفها، مثل Recovre lost data سواء تم هذا الإلغاء بالأمر أو بإعادة تهيئة أو تشكيل للقرص الصلب باستخدام الأمر، سواء كانت هذه البيانات صور أو رسومات أو كتابات أو غيرها ، كل ذلك يشكل صعوبة إخفاء الجاني لجريمته أو التخفي عن أعين الأمن و العدالة، بشرط العلم بوقوع الجريمة من رجال البحث والتحقيق الجنائي.

كما يعتبر نشاط الجاني لمحو الدليل دليلا أيضا، فنسخة من هذا الفعل أي محاولته إخفاء الدليل يتم تسجيلها في الكمبيوتر، ويمكن استخلاصها كدليل إدانة ضده[2].

بمعنى أن الإلغاء أو الحذف للدليل الالكتروني هو في الحقيقة واقعة إخفاء له ما دام أن القاعدة المشار إليها ثابتة.

فهذه الخاصية في الحقيقة تعد حافزا لمواصلة البحث في الجريمة الالكترونية، وبالتالي تعد دافعا لاتخاذ الحيطة والحذر.

---

[1] فتحي محمد أنور عزت المرجع السابق، ص 650.

[2] عائشة بن قارة مصطفى المرجع السابق، ص 62 ،63.

إن خاصية صعوبة التخلص من الدليل الالكتروني تقابلها مسألة أخرى هي أن هذا الدليل نتيجة لمرونته وضعفه ، فإنه يسهل إتلافه أو فقدانه أو كما يطلق عليه Spoliation of Evidence» و بالتالي التخلص منه بغير الحذف أو الإلغاء، ومسألة إتلاف الدليل الإلكتروني، هي في الواقع ليست حقيقة، إنما تعني أن هناك قصور في القدرات التكنولوجية لدى مؤسسات العدالة، مما يجب العمل على التطوير المستمر لنظم العدالة وتطوير قدرات القائمين على مهامها وأعمالها[1].

4: الدليل الإلكتروني متنوع ومتطور:

على الرغم من أن الدليل الالكتروني في أساسه متحد التكوين في مجال الحوسبة والرقمية، إلا أنه يتخذ أشكالا مختلفة، فمصطلح الدليل الالكتروني يشتمل كافة أشكال وأنواع البيانات الإلكترونية الممكن تداولها رقميا، بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية مما يحقق وجود رابطة بينها وبين الجاني.

أما فيما يخص التنوع المتعلق بالدليل الإلكتروني، فإنه يظهر علنا في هيئات مختلفة الأشكال كأن يكون بيانات غير مقروءة، كما هو الشأن في حالة المراقبة عبر الشركات والملقمات أو الخوادم وقد يكون الدليل الالكتروني مفهوما للأشخاص كما لو كان وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام، كما يمكن أن يكون صورة ثابتة أو متحركة أو معدة بنظام التسجيل السمعي المرئي، أو أن تكون مخزنة في نظام البريد الالكتروني، فهذه الخاصية تستوجب مواكبة التطور في عالم تكنولوجيا المعلومات[2]

5: الدليل الإلكتروني قابل للنسخ :

يمكن استخراج نسخ من الأدلة الجنائية الالكترونية مطابقة لأصل، ولها نفس القيمة العلمية وهذه الخاصية لا تتوافر في باقي الأدلة الجنائية التقليدية، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق النسخ طبق الأصل من الدليل، وهذا

[1] فتحي محمد أنور عزت، المرجع السابق، ص655، 656.

[2] فتحي محمد أنور عزت، المرجع السابق، ص651، 652.

ما نص عليه القانون البلجيكي 28 نوفمبر 2000 بإضافة المادة 39 التي سمحت بضبط الأدلة الإلكترونية مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية. كما أن الدليل الالكتروني يمتاز بالسعة التخزينية العالية ، فآلة الفيديو الرقمية يمكنها تخزين مئات الصور، ودسك صغير يمكنه تخزين مكتبة صغيرة إضافة أن له خاصية رصد معلومات عن الجاني ويحللها في ذات الوقت بحيث يمكنه أن يسجل تحركات الفرد و تسجيل عاداته وسلوكياته وبعض الأمور الشخصية لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي[1].

ومنه نقول إن هذه الخصائص السالف ذكرها اكتسبت الدليل الالكتروني طابعا متميزا جعلت منه الدليل الأفضل لإثبات الجرائم الالكترونية، لأنه من طبيعة الوسط الذي ارتكبت فيه، سواء كانت هذه الجرائم مرتكبة بواسطة نظام المعالجة الآلية أو كانت تشكل اعتداء أو مساسا على نظام المعالجة الآلية.

الفرع الثاني: المعاينة والتفتيش:

أولا: تعريف المعاينة: هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد آثارها بنفسه وتقتضي المعاينة إثبات حالة الأشخاص والأشياء[2]،وكل ما يعتبر في كشف الحقيقة، وبهذا المعنى تستلزم المعاينة للانتقال إلى محل الواقعة أو أي محل توجد به أشياء، أو آثار يرى المحقق أن لها صلة بالجريمة، كما أن المعاينة في الجريمة التقليدية تكون ذات أهمية متمثلة في تصور كيفية وقوع الجريمة وظروف ملا بستها وتوفير أدلة مادية لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة الالكترونية، وضبط الأشياء التي قد تفيد في إثباتها ونسبتها إلى مرتكبيها، لأن الجريمة التقليدية غالبا لها مسرح تجرى عليه الأحداث التي تخلف آثار مادية، على خلاف الجريمة الالكترونية يتضاءل دورها في الإفصاح عن الحقيقة

[1] عائشة بن قارة مصطفى، المرجع السابق، ص64.

[2] عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الالكترونية، دراسة مقارنة رسالة مكملة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط 2014 ص77.

المؤدية للأدلة المطلوبة، لأن الجريمة الالكترونية فلما تخلف أثار مادية، وأن كثير من الأشخاص يردون إلى مسرح الجريمة خلال فترة من زمان وقوع الجريمة أو حتى اكتشافها أو التحقيق فيها وهي طويلة نسبيا. الأمر الذي يجعل الجاني يغير أو يتلف أو يعبث بالآثار المادية للجريمة إن وجدت، وهذا ما يورث الشك في دلالة الأدلة المستقاة من المعاينة[1]. ومن الإجراءات الواجب إتباعها عند إجراء المعاينة ما يلي:

- تصوير جهاز الحاسوب وما قد يتصل به من أجهزة طرفيه ومحتوياته.
- عدم التسرع في نقل أي مادة معلوماتية للتيقن من عدم وجود أي مجالات مغناطيسية في العالم الخارجي
- حذف المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية.
- ربط الأقراص التي تحمل أدلة مع جهاز يمنع الكتابة عليها، مما يتيح لجهات التحقيق قراءة بياناتها من دون تغييرها.

1_ أهمية المعاينة: للمعاينة أهمية كبيرة في كشف غموض العديد من الجرائم التقليدية، إلا أن دورها في كشف غموض الجرائم الإلكترونية وضبط الأشياء التي قد تفيد في إثبات وقوعها، ونسبتها لمرتكبيها ليس بنفس الدرجة من الأهمية مقارنة بالجريمة التقليدية، وهذا يرجع إلى الأسباب الآتية:

- إن الجرائم الإلكترونية من النادر ما يتخلف عنها آثار مادية.
- تردد العديد من الأشخاص على مسرح الجريمة الإلكترونية، خلال الفترة الزمنية الطويلة بين ارتكابها و اكتشافها مما يؤدي إلى إمكانية حدوث إتلاف أو تغيير في الآثار المادية، مما يجعل الدليل المستمد من المعاينة محل للشك[2].
- إمكانية تلاعب الجاني في البيانات عن بعد، أو محوها عن طريق التدخل من خلال وحدة طرفية، لذا كان ينبغي تقرير جزاءات جنائية على كل من يجري تغيير أو تعديل

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت دار الكتب القانونية مصر، ص20ص21.

[2] عائشة بن قارة مصطفى، المرجع السابق، ص81.

في المعلومات المسجلة في الحاسوب قبل قيام سلطة التحقيق بإجراء المعاينة، وهذا ما نص عليه المشرع الجزائري في المادة 43 من قانون الإجراءات الجزائية الجزائري:" يحظر في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو نزع الأشياء منها قبل الإجراءات الأولية للتحقيق القضائي، و إلا عوقب بغرامة 200 إلى 1000 دج.

غير أن المشرع استثنى حالة ما إذا نزع الأشياء للسلامة والصحة العمومية أو تستلزمها معالجة المجني عليهم.

وإذا كان المقصود من طمس الآثار أو نزع الأشياء وهو القيام بعرقلة سير العدالة بهدف ما يقوم به لطمس الأدلة التي تدينه مثلا، فإن المشرع عاقب على هذا الفعل بالحبس من 3 أشهر إلى 3 سنوات وبغرامة من 1000 إلى 10.000 دج."

نجد أن المشرع الجزائري كان واضحا ومتشددا في هذه المادة فيما يخص القيام بأي تغيير على مسارح الجريمة والذي من شأنه عرقلة مسار العدالة وتصعيب كشف الحقيقة، وقد قرر عقوبات في هذا الشأن، بالإضافة إلى وضعه استثناء على هذا الأمر إذا كان تغيير من شأنه أن ينقص في القوة الثبوتية للدليل.

كما نص المشرع الفرنسي من خلال المادة 55_1 من قانون الإجراءات الجنائية الفرنسي، و هذا حرصا على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي و الملاحظ أن أحكام هذه النصوص و إن كانت تنصرف إلى أغلب الجرائم التقليدية، إلا أنه يمكن تطبيقها عند معاينة مكونات الحاسوب ذات الطابع المادي، على خلاف معاينة المكونات الغير مادية لأنها تتطلب إجراءات خاصة[1].

[1] عائشة بن قارة مصطفى، المرجع السابق، ص82، 83.

- تتخذ المعاينة في الجرائم الإلكترونية عدة أشكال، وهذا بحسب نوع الجريمة المرتكبة فمثلا في جرائم العدوان، على الملكية الفكرية، يتم إنزال نسخة من المصنف المعتدى عليه بطباعتها واستخراجها على هيئة ورقية أو صلبة.

وحديثا تستخدم تقنية الطباعة على خشب أو بلاستيك خاص، إضافة إلى وجود طرق تتوافق مع طبيعة النظام ألمعلوماتي كوسيلة تصوير شاشة الحاسوب، وهو ما يعرف بطريقة تجميد مخرجات الشاشة.(Frozen)

ثانيا: تعريف التفتيش:

هو إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر ، لذلك يعتبر من أهم الإجراءات لأنه غالبا ما يسمى عن أدلة مادية تؤدي إلى نسبة الجريمة للمتهم[1]، والمستهدف من التفتيش هو جهاز الحاسوب بمكوناته المادية (وحدات لكل منها وظيفة معينة متصلة ببعضها البعض في شكل نظام متكامل)، والمكونات المعنوية (الكيانات المنطقية)، فعندما يستهدف التفتيش الكيانات المادية لا يشكل عائق ، وإنها الإشكال يثور عندما ينصب على المكونات المعنوية (البرامج ، قواعد البيانات...) لأنه هنا يتطلب الكشف عن الرقم السري للمرور إلى الملفات أو الشفرات أو ترميز البيانات[2].

1_تفتيش مكونات الحاسوب المادية:

لا يوجد مانع قانوني من أن ينصب التفتيش على المكونات المادية للحاسوب وملحقاته، وذلك تبعا لطبيعة المكان الذي يتواجد فيه الحاسوب، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت خاصة كمسكن المتهم أو أحد ملحقاته كانت لها حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجور فيها تفتيش مسكنه، وحسب المادة رقم 45 ف 3 تنص على:" لا

[1] بوعناد فاطمة زهرة مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، سيدي بلعباس 2013، العدد01 ص68.

[2] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر، الجزائر 2011 ص من 131 إلى 133.

تطبق هذه لأحكام إذا تعلق الأمر بجرائم.... والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات " والمادة 47 ف 3 تنص على: "عندما يتعلق الأمر ب ... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ... فإنه يجوز إجراء التفتيش ... في كل محل سكني أو غير سكني كل ساعة من ساعات النهار أو الليل..." و المادة 64 ف 2 تنص على: " وتطبق فضلا عن ذلك أحكام المواد 44،47 من هذا القانون"[1]،بمعنى عدم تطبيق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بالجريمة الالكترونية حيث لا يشترط حضور الشخص المشبه به في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه، وأنه يحوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل ودون حاجة إلى رضائه عند القيام بهذا الإجراء[2].

2_خضوع مكونات الحاسوب المعنوية للتقديم:

عرف الفقه اختلاف حول مدى خضوع المكونات المعنوية للحاسوب لإجراء التفتيش ، وانقسم إلى اتجاهين، اتجاه يرى عدم جواز تفتيش المكونات المعنوية للحاسوب ، وقد عملت الدول التي تبنت هذا الاتجاه إلى حماية هذه الكيانات المنطقية عبر قانون الملكية الفكر بيه ، واتجاه آخر يرى إمكانية تفتيش المكونات المعنوية للحاسوب لأن كل ما يشغل حيزا ماديا في فراغ معين، هذا الحيز يمكن قياسه والتحكم فيه ،وبناءا عليه فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب، ويمكن قياسه بمقياس معين هو "البايت " و"الكيلوبايت " و"الميغابايت " وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسوب بعدد الحروف التي يمكن تخزينها فيها، غير أن النصوص القانونية التي تنص على أحكام التفتيش تم سنها قبل أن يعرف القانون الأشياء غير المادية، لذا فإن طبيعة البيانات والمعطيات

[1] المواد 45، 47، 64 من الأمر رقم 22/06 الصادر في 20 ديسمبر 2006، المعدل والمتمم لقانون الإجراءات الجزائية، ج ر العدد 84.

[2] سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص145.

المعالجة تتطلب قواعد خاصة تحكمها ، فالنصوص التقليدية الخاصة بالتفتيش لا يمكن إعمالها على النظم المعلوماتية ،لأن قياسها على الأشياء المادية سيكون منافيا للشرعية الإجرائية[1].

3_مدى خضوع شبكات الحاسوب للتفتيش عن بعد:

_اتصال حاسوب المتهم بحاسب موجود في مكان أخر داخل الدولة : لقد أجاز المشرع في المادة 05 من القانون رقم 09-04 إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، فيجوز تمديد التفتيش بعد إعلام السلطة القضائية المختصة مسبقا بذلك[2]، حيث تنص المادة 05 منه على: "...في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى و أن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك..."

_اتصال حاسب المتهم بحاسب موجود في مكان آخر خارج الدولة : ويكون بالدخول إلى منظومة معلوماتية أو جزء منها ،كذا المعطيات المخزنة فيها ولو عن بعد، وذلك في حالة ما إذا كانت المعطيات القائم البحث عنها يمكن الدخول إليها انطلاقا من منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة، ووفقا لمبدأ المعاملة بالمثل تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث ،أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، حيث تنص المادة 05 من القانون رقم 09 – 04على أنه:"... إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات

[1] سعيداني نعيم، نفس الرسالة، ص147.

[2] بوعناد فاطمة زهرة، المجلة السابقة الذكر ص69.

الأجنبية المختصة طبقا لاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل[1].

المطلب الثاني: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

انطلاقا من أساليب التحري الخاصة ومنها اعتراض المراسلات وتسجيل الأصوات والتقاط الصور الواردة في الفصل الرابع من الباب الثاني، ضمن المواد من65 مكرر 5 إلى 65 مكرر 10 من ق ع ج. هي استثناء على قاعدة التجريم الواردة بنصوص القانون العقوبات بموجب المواد من 303مكرر إلى 303 مكرر3 من ق ع ج، فلا بد من تحديد طبيعتها ونطاقها. من خلال تحديد مفهومها على النحو التالي:

الفرع الأول: تعريف اعتراض المراسلات:

لم ينص المشرع الجزائري ضمن قانون الإجراءات الجزائية على تعريف خاص محدد لعملية اعتراض المراسلات إلا انه اكتفى بتحديد سر العملية والإجراءات المعمول بها، وبالرجوع إلى المادة 65 مكرر 5 فقرة أولى من ق إ ج ج، تجد إن المشروع اعتبر إن اعتراض المراسلات تلك العملية التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية. ولتحديد نوع المراسلات محل الاعتراض الموصوفة بكونها تتم عن طريق وسائل الاتصال السلكية واللاسلكية بالمادة الإجرائية الواردة أعلاه، يتعين علينا الرجوع إلى القوانين الخاصة المنظمة لهذه الوسائل، فوضعت المادة 08 من القانون 2000-03 المحدد للقواعد العامة المتعلقة بالبريد و المواصلات السلكية، أهم التعاريف للمواصلات السلكية و اللاسلكية[2].

كما يدخل كذلك ضمن المراسلات محل اعتراض الاتصالات الالكترونية وقد ورد هذا المصطلح أو هذه التقنية في المادة 2 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها[3].

---

[1] المادة 05 من القانون رقم 04/09 القانون السابق الذكر.

[2] القانون رقم 2000-03 المؤرخ في 05 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية – عدد 48 المؤرخة في 06 أوت 2000.

[3] القانون رقم 09-04 المؤرخ في 5 أوت 2000 يتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، جريدة الرسمية – عدد47 مؤرخة في 16 أوت 2009.

التي نصت على انه: "المواصلات السلكية واللاسلكية: كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية "، كما نصت المادة 3 من نفس القانون على انه:".... وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها ...

يرى الأستاذ أحسن بوسقيعة: أن اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية يقصد به أساس التنصت التليفون[1].

كما عرفها البعض على أنها المراقبة السرية للمراسلات السلكية واللاسلكية في إطار البحث و التحري عن الجريمة و جمع الأدلة و المعلومات حول الأشخاص المشبه في ارتكابهم للجريمة[2]

باعتقادنا فإن المشروع الجزائري أحسن ما فعل عندما لم يعطي تعريف محدد لاعتراض المراسلات كما ورد في المادة 65 مكرر05 ق1 من ق إ ج.ج، وذلك لترك المجال مفتوح لاحتواء أي تطور تكنولوجي في مجال وسائل الاتصال على عكس بعض التشريعات التي ربطت هذه العملية بالتنصت على المكالمات التي تتم عبر التلفون.

وبمفهوم المخالفة للنص الإجرائي الوارد بالمادة 65مكرر5 الأنف ذكره ،فلا يدخل ضمن اعتراض المراسلات ما يسمى بوضع الخط التليفوني تحت المراقبة ،فبينما يكون الأول دون رضا المعنى ويكون الثاني برضا أو طلب من صاحب الشأن وهو يخضع لتقدير السلطة القضائية يهدف إثبات المجني عليه للجريمة الواقعة عليه خاصة في المجال جرائم القذف و السب بواسطة التليفون[3] .

[1] أحسن بوسقيعة : التحقيق القضائي ،الطبعة الثامنة ،الجزائر دار هومة،2009،ص113.

[2] آمنة أمحمدي بوزينة: أساليب، الكشف عن جرائم الصفقات العمومية في ظل قانون 06-01، ورقة بحث قدمت في الملتقى الوطني السادس الموسوم بالصفقات العمومية في حماية المال العام، جامعة المدنية ،20ماي 2013 .

[3] آمنة أمحمدي بوزينة :المرجع السابق، ص13.

-الجانب الفني والتقني الاعتراض المراسلات:

هناك طريقتين للتنصت على المكالمات التي يجريها الشخص عبر التليفون منها للتنصت المباشر عن طريق الدخول على الخط المراد مراقبة لاسلكي بواسطة سماعة تليفون يمكن وصلها بجهاز تسجيل، والقادم من مركز التوزيع الرئيسي ،إذ يتم ربط سلكي هذه السماعة إلى سلكي دائرة المشترك في مكان ما، وتعد هذه الطريقة من الطرق القديمة، أما أسلوب التنصت الغير مباشر يكون هذا النوع من التنصت لاسلكية، حيث انه يتم دون إن يكون هناك اتصال سلكي بالخط الهاتفي الموضوع تحت المراقبة[1]،وهناك العديد من الأجهزة التي يتم استخدامها للتنصت على الاتصالات الهاتفية، ومنها أجهزة تنصت دقيقة يطلق عليها اسم (Les micros clous) تسمح بالتنصت على المكالمات الخاصة التي تتم خلف حواجز أو حيطان دون الحاجة إلى تثبيتها في المبنى المراد التنصت على المحادثات التي تتم داخله ، وكذلك أجهزة تنصت أخرى جد دقيقة تسمى (Le micro directionnel) على درجة عالية الحساسية يمكنها التقاط المحادثات الخاصة على مسافات بعيدة, كما تستخدم أشعة الليزر (le laser) القادرة على التقاط الحديث الذي يتم في مكان خاص، وإرسالها من خلف الحيطان أو النوافذ الزجاجية[2].

وأما فيما يخص المحادثات التي تتم عبر الانترنت فيمكن التنصت عليها أيضا باستعمال الأجهزة التي تستعمل للتنصت على المكالمات الهاتفية , ويرجع ذلك إلى استخدام شبكات الحاسب الآلي خطوط التليفون عن طريق جهاز يعرف بالمودام[3] ،ويقوم هذا الجهاز بتحويل

---

[1] سليمان بن عبد الله، حق الإنسان في حرية مراسلاته واتصالاته الهاتفية الخاصة، رسالة ماجستير، غير منشورة، جامعة نايف للعلوم الأمنية، الرياض، كلية الدراسات العليا،2004-2005، ص227.

[2] صفية بشاتن: الحماية القانونية للحياة الخاصة، رسالة دكتوراه غير منشورة جامعة مولود معمري، تيزي وزو كلية الحقوق, 07 ماي 2012 ص 216 ص217.

[3] المودام بالفرنسية(modem) وهو اختصار لكلمتي (modulatordé de modulator)

محمد فتحي، تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة، الطبعة الأولى، القاهرة المصدر القومي للإصدارات القانونية ،2012، تهميش (1) ص485 .

الإشارات الرقمية من جهاز الحاسب الآلي إلى إشارات صوتية يمكن انتقالها عبر خط الهاتف ويقوم بتحويل الإشارات المرسلة عن طريق خط الهاتف إلى إشارات رقمية يفهمها جهاز الحاسب[1].

الفرع الثاني: تعريف تسجيل الأصوات:

ورد ذكر عبارة " تسجيل الأصوات " في نص المادة 56 مكرر 5 فقرة ثالثة من ق إ ج ج، ومصطلح الأصوات قصد به المشرع الجزائري من خلال نص الوارد أعلاه "الكلام المفوه به بصفة خاصة أو سرية ".

ويتمثل تسجيل الأصوات في وضع الترتيبات التقنية، من دون موافقة المعنيين، من أجل التقاط، تثبيت، بث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية، من طرف شخص أو عدة أشخاص يتواجدون في أما كان خاصة أو عمومية[2]، كما عرف تسجيل الأصوات على أنه : تسجيل الأحاديث التي يتم عبر الهواتف بعد وضعها تحت المراقبة , كما يتم أيضا عن طريق وضع ميكرفونات حساسة تستطيع التقاط أصوات وتسجيلها على أجهزة خاصة , وقد يتم أيضا عن طريق التقاط إشارات سلكية أو إذاعية[3].

وبالرجوع إلى النص الإجرائي السالف الذكر فالتسجيل الصوتي لا يقتصر فقط على التسجيل(enregistrement) الكلام المتفوه به فحسب، بل يشمل أيضا الالتقاط وتثبيت وبث الكلام.

فتسجيل الكلام أو الحديث فهو حفظه على الشريط المخصص لذلك أو أي وسيلة أخرى ثم الاستماع إليه بعد ذلك[4].

---

[1] محمد فتحي، المرجع السابق، ص485.

[2] أحسن بوسقيعة، التحقيق القضائي، المرجع السابق، ص113.

[3] آمنة أمحمدي بوزينة، المرجع السابق، ص12.

[4] محمد الشهاوي، الحماية الجنائية لحرمة الحياة الخاصة، الطبعة الأولى، القاهرة، دار النهضة، العربية 2005، ص176.

أما التثبيت و البث، فيقصد بالتثبيت (fixation) وضع الكلام المتفوه به على دعامة الكترونية أو مغناطيسية ،كما أن لفظ التثبيت يتعلق بالصورة أكثر من تعلقه بالصوت، أما البث فيقصد به النقل (transmission) من خلال النص الإجرائي المذكور المترجم إلى اللغة الفرنسية،أي نقل الحديث الذي تم الاستماع إليه أو تسجيله من المكان الذي تمت فيه إحدى الأفعال السابقة[1]. أما فيما يخص الطبيعة القانونية لعملية التسجيل الصوتي[2]، فقد اختلفت الآراء حول ذلك، فأعتبرها البعض أن لها علاقة كبيرة بعملية التفتيش حيث يهدفان كلاهما للكشف عن الحقيقة الجريمة المرتكبة و كما أن محل[3] مباشرة التسجيل الصوتي هو ذات المحل الذي ينصب عليه التفتيش[4]،لكن أوجه الاختلاف بينهما جوهريا، فالغرض من التفتيش[5]هو ضبط الأدلة المادية المتعلقة بالجريمة أما الأحاديث الصوتية ليس لها مكان مادي يمكن ضبطه.

ويعتقد البعض الأخر أن عملية تسجيل الأصوات تنشأ عن ضبط الرسائل التي تتضمن حديث كتابي وإن التسجيلات الصوتية تتضمن حديث شفوي إلا أن هناك فرق واضح بين عملية ضبط الرسائل وتسجيل الأصوات تكمن في كون ضبط الرسائل تعتبر أدلة مادية إلا أن

[1] عبد المالك بن ذياب، حق الخصوصية في التشريع العقابي، الجزائري، رسالة ماجستير، غير منشورة، جامعة الحاج لخضر باتنة كلية الحقوق ،2012-2013، ص138.

[2] نفس الشيء بالنسبة لعملية اعتراض المراسلات الذي سبق التطرق إليه.

[3] ويعتبر تسجيل الأصوات تفتيش كلما كان فيه مساس بحرمة السكن إذا وضع جهاز تسجيل بالمسكن، وقد يكون فيه اعتداء على حرمة الرسائل إذا سجلت محادثات شفوية، ويكون اعتداء على حرية الشخص إذا سجل حديث شخصي في مكان عام أو خاص. خلاف بيو، تطور حماية الحياة الخاصة للعامل، رسالة ماجستير، غير منشورة، جامعة قاصدي مرباح ورقلة كلية الحقوق، 9 مارس 2012، ص51.

[4] حمزة قريشي، الوسائل الحديثة للبحث والتحري، رسالة ماجستير، غير منشورة، جامعة قاصدي مرباح، ورقلة كلية الحقوق، 16 جوان 2012، ص50.

[5] لم تتضمن التشريعات تعريفا للتفتيش لذلك تعددت التعريفات التي صاغها الفقه وجميعها لا تخرج على انه إجراء من إجراءات التحري أو التحقيق التي تهدف إلى ضبط الجريمة موضوع التحقيق، وكل ما يفيد في كشف الحقيقة سامي حسني الحسني النظرية العامة للتفتيش رسالة دكتوراه غير منشورة جامعة القاهرة كلية الحقوق , 1971-1972 ص180.

التسجيلات الصوتية ليست بأدلة مادية ولا يقبل بالضبط بالمعنى القانوني[1]،فالطبيعة القانونية للتسجيلات الصوتية تكمن في أنها إجراء من نوع خاص فهي مستقلة عن عملية التفتيش وكذلك عن ضبط الرسائل.

-الجانب الفني والتقني في تسجيل الأصوات:

تزداد أجهزة التسجيل يوم بعد يوم كفاءة وقدرة وتفوقا كبيرا، سواء من ناحية كيفية النقاط الحديث وتسجيله، أو من ناحية صغر حجمها وسهولة استخدامها، وقد تعددت أنواع هذه الأجهزة، بحيث أصبح من الصعب تتبع تطورها والوقوف على أحدثها لذا سنتناول أهم هذه الوسائل أكثرها شيوعا في العمل.

ومن بينها أجهزة تعمل بالاتصال السلكي أو اللاسلكي ، وهي الأجهزة التي تعمل عن طريق إخفاء ميكروفون داخل المكان الذي يراد سماع المحادثات التي تدور به، وتوصيل هذا الميكروفون بواسطة أسلاك دقيقة بجهاز للاستماع خارج المبنى بواسطة أسلاك دقيقة ، وقد ظهرت عدة أنواع من الميكروفونات المستخدمة لهذا الغرض ومن بينهما كذلك أجهزة تسجيل صوتي تعمل من خارج المكان ، وتستعمل هذه الأخيرة في تسجيل المحادثات الجارية في الغرف والأماكن دون الحاجة إلى وضعها بداخلها[2] ومن أهم أنواعها : ميكروفونات التوجيه ، ميكروفونات التلامس ، ميكروفونات مسمارية[3] .

أما عن مدى تطابق الصوت المسجل مع صوت المشتبه فيه ومدى تطابق النبرات بينهما ، فيتم استعمال جهاز إعلام آلي متطور مزود ببرنامج لفك الأصوات ومضاهاتها، فلكل شخص

---

[1] ياسر الأمير فاروق، مراقبة الأحداث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية،2009، ص138.

[2] محمد أمين خرسة: مشروعية الصوت والصورة في الإثبات الجنائي، الطبعة الأولى، الأردن، دار الثقافة للنشر والتوزيع، 2001، ص 261.

[3] راجع في تعريف هذه الأنواع: محمد أمين خرسة، المرجع نفسه، ص124، ص125.

صوت خاص يختلف تمام عن أي شخص أخر ويمكن تمييزه والتعرف عليه من بين العديد من الأصوات بمجرد سماع صوته[1].

وكخلاصة القول أن عملية تسجيل الأصوات تتقابل في الجوهر مع عملية اعتراض المراسلات السلكية واللاسلكية، فكلاهما انتهاك للحق في الخصوصية وينحصر الاختلاف بينهما من ناحية الوسيلة المستخدمة[2].

وهذا ما يمكن قوله عن مفهوم التصنت على المكالمات الذي يشمل اعتراض المراسلات السلكية واللاسلكية، كما أشرنا إليه سابقا، فماذا عن مفهوم التقاط الصور كأسلوب من أساليب التحري الخاصة الواردة بالمادة 65مكرر5 من ق إج ج، وهذا ما ستتطرق إليه من خلال الفرع الموالي

الفرع الثالث: تعريف التقاط الصور:

عرف التقاط الصور بأنه "وضع أجهزة تصوير صغيرة الحجم وإخفاؤها في أمكنة خاصة لالتقاط صور تفيد في إجلاء، الحقيقية وتسجيلها"[3].

وبالرجوع إلى نص المادة 65مكرر5 المذكورة أعلاه نجد أن ذكر عبارة التقاط الصور ورد على الشكل الآتي:"...وضع ترتيبات تعقبية...التقاط صور شخص أو عدة أشخاص يتواجدون في مكان خاص ".

وبمفهوم نص المادة 65مكرر5 فقرة ثالثة، أنا الصور المعنية بهذا النص هي تلك الملتقطة بالمكان الخاص. وبمفهوم المخالفة للنص الإجرائي الوارد أعلاه لا تخضع لأي ضبط من الضوابط المنصوص عليها بالمراد 65مكرر5 إلى 65مكرر10 مسألة التقاط الصور في المكان العام ، فجهاز الأمن يعتمد على أسلوب المراقبة عن طريق استخدام أجهزة التصوير في الطريق العامة بالمدن لمراقبة حركة المارة والسيارات وأماكن التجمعات فضلا عن تصوير

---

[1] خالد بخوش: الدليل العلمي وأثره في الإثبات الجنائي، رسالة الماجستير جامعة العربي بن مهيدي أم البواقي كلية الحقوق ،2007-2008، ص 26.

[2] معتصم مشعع خميس: إثبات الجريمة بالأدلة العلمية، مجلة الشريعة والقانون، العدد السادس والخمسون، أكتوبر 2013.

[3] عبد المالك بن ذياب : المرجع السابق ص141 ، نقلا عن عبد القادر مصطفاوي، أساليب البحث و التحرير الخاصة ، مجلة المحكمة العليا قسم الوثائق العدد2، 2009 ص71 .

المسيرات و المظاهرات ومن حيث الظاهر تكون غاية المراقبة واضحة وهي حفظ النظام العام وحمايته[1] .

ـوسائل التقاط الصور: تفيد عبارة:" وضع الترتيبات التقنية " والوارد ذكرها في المادة 65مكرر5 فقرة ثانية على استخدام كل أنواع أجهزة التصوير ووسائل المراقبة المرئية المختلفة المرتبطة بالتطور التقني من وسائل الرؤية والمشاهدة التي تسهل عمليات الالتقاط، تثبيت بث وتسجيل الصور مثل: عدسات التلفزيونية والسينمائية، إذ أدى تطور الجريمة الملحوظ خلال أواخر القرن الماضي وبداية هذا القرن واستخدام المجرمين لأحدث الأساليب العلمية في ارتكاب الجرائم الدوائر التلفزيونية المغلقة التي تسمح بمراقبة مكان ما ومعرفة ما يدور داخله دون علم الحاضرين على شرائط سينمائية[2]، كما ظهرت آلات التصوير عن بعد والتي تلفي حاجز المسافة، وأجهزة التصوير بالأشعة الحمراء و التي تنتج اقتحام المجال الشخصي للأفراد ليلا بقدرتها على التقاط صور دقيقة لما يأتيه تحت جنح الظلام ،كما تعد أساس لأجهزة تسجيل الصورة ،فقد أحدث التطور التقني نقلة نوعية لهذه الأجهزة إذا جرى تصغير حجم هذه الآلات ،بحيث أصبح من السهل وضعها في المباني أو على جسم الشخص الذي يستعملها بطريقة تجعل اكتشافها صعبا[3].

ولابد من الإشارة هنا إلى إن تطور هذه الأجهزة مستمر لا تستطيع الوقوف عن الحد الذي وصل إليه التقدم التكنولوجي في مجال تصنيع أجهزة التصوير، حيث أصبحت صغيرة الحجم، يسهل تركيبها في أي مكان سهل الحمل والاستعمال.

ومن حيث مصداقة الأدوات المستعملة في تقنيات التصوير أو بمعنى أعم في اعتراض المراسلات وتسجيل الأصوات و التقاط الصور، فلاشك أن التقدم العلمي قد وصل مرحلة من

[1] محمد أمين خرسة، مشروعية الصوت والصورة، المرجع السابق، ص181.

[2] علي أحمد الزعبي، حق الخصوصية في القانون الجنائي الطبعة الأولى، لبنان، المؤسسة الحديث للكاتب، 2000، ص551.

[3] محمد أمين خرسة، المرجع السابق، ص447.

التطور تسمح بالقول بارتياح عن مدى مصداقية هذه الأدوات، إذا سلمت من يد العبث إذا أن السؤال الذي يطرح حول مصداقية هذه الأخيرة بل على الظروف التي أنجزت فيها[1].

المبحث الثاني: الآليات الإجرائية الحديثة:

في هذا المبحث سنتطرق إلى الإجراءات الحديثة لمكافحة الجريمة الإلكترونية، التسرب الإلكتروني وشروطه (المطلب الأول)، تحديد الموقع الجغرافي للتسرب (المطلب الثاني).

المطلب الأول: التسرب الإلكتروني:

في هذا المطلب سنتطرق إلى دراسة التسرب الإلكتروني وشروطه وكيفية تحديد الموقع الجغرافي للتسرب الإلكتروني.

الفرع الأول: تعريف التسرب الإلكتروني:

التسرب لغة مشتق من الفعل تسرب تسربا أي دخل وانتقل خفية وهي الولوج والدخول بطريقة أو بأخرى إلى مكان أو جماعة[2](سماحة، 1984)، ويعني تسرب تسربا أي دخل وانتقل خفية[3]، وكذلك لكلمة التسرب كلمة مرادفة لها هي: الاختراق وهي مستخدمة في الكثير من الكتب والمؤلفات القانونية وتعني: اختراق، يخترق، اختراقا.

كما عرف المشرع التسرب الإلكتروني على أنه: " تقنية إلكترونية من تقنيات الحديثة لتحري والتحقيق الخاصة، تسمح من خلالها لضباط الشرطة القضائية بالتوغل إلى منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أكثر كإنشاء عدة صفحات على مواقع التواصل الاجتماعي أكثر شيوعا واستخداما من طرف الجمهور كالفايسبوك وتوتير، بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، مع إمكانية إخفاء الهوية الحقيقية وفق ماقرره القانون تحت طائلة بطلان الإجراءات وذلك طبقا للمادتين 157و158 من قانون 66 الإجراءات الجزائية.

من خلال التعريف الذي أورده المشرع يتبين أن التسرب الإلكتروني هو نظام من أنظمة البحث والتحري الخاصة والحديثة التي تسمح لضباط الشرطة القضائية بموجب القوانين بإختراق

[1] حمزة قريشي، المرجع السابق، ص71.

[2] سهيل حسيب سماحة، معجم اللغة العربية، الطبعة الأولى، مكتبة سمير، 1984، ص120.

[3] المجند الأبجدي، دار المشرق للتوزيع، الطبعة الثامنة، لبنان، 1980، ص250.

المنظومة المعلوماتية أو أنظمة الاتصالات السلكية والتوغل فيها تحت مسؤولية ضابط الشرطة القضائية بعد إعلام وكيل الجمهورية الذي يأمر بإستمرار العملية أو إيقافها بهدف الكشف عن الجرائم المتعلقة بالتمييز وخطاب الكراهية وملاحقة مرتكبيها، وذلك مع إمكانية إخفاء الهوية الحقيقية من خلال إنشاء صفحات بأسماء مستعارة على مواقع التواصل الاجتماعي.

الفرع الثاني: شروط التسرب الإلكتروني:

باعتبار إجراء التسرب من الإجراءات الاستثنائية والخاصة للضبط القضائي لما ينطوي عليه من مساس بخصوصية الأفراد فإن المشرع الجزائري قد أحاطه بمجموعة من الشروط وهي:

1-ضرورة صدور إذن قضائي يجيز عملية التسرب.

2- احترام المدة القانونية المقررة للتسرب.

3- تسبيب عملية التسرب.

الشروط الموضوعية: وهو الشرط الخاص الذي نصت عليه المادة 26 من القانون 20-05، المتعلق بموضوع عملية التسرب أو محل التسرب وهو البحث عن المشتبه في ارتكابهم لجرائم التمييز وخطاب الكراهية.[1]

المطلب الثاني: تحديد الموقع الجغرافي:

أجاز القانون 20-05 للسلطات الضبط القضائي في مهمة ضبط الجرائم المتعلقة بالتمييز وخطاب الكراهية استعمال تقنية التحديد الجغرافي لتحديد الأشخاص المشتبه فيهم أو لرصد وسيلة

ارتكاب الجريمة وذلك ما نصت عليه المادة 27 بقولها " يمكن وكيل الجمهورية أو قاضي التحقيق بعد اخطار وكيل الجمهورية ان يأذن تحت رقابته لضباط الشرطة القضائية متى توفرت دواع ترجح ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون بتحديد الموقع الجغرافي للشخص المشتبه فيه أو المتهم أو وسيلة ارتكاب الجريمة أو أي شيء اخر له صلة بالجريمة..."

[1] قانون رقم 20-05 المؤرخ في 28 افريل 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها.

وعلى خلاف التسرب الالكتروني الذي يجد ضوابطه العامة في قانون الإجراءات الجزئية فان تحديد الموقع الجغرافي يعتبر اجراء جديد يدخل ضمن منظومة الإجراءات الخاصة بالحقيق في الجرائم التمييز وخطاب الكراهية، ونظرا لخطورة هذه الوسيلة فان اللجوء اليها لا يكون الا في حالة توفر دواعي ترجح ارتكاب الجريمة هذا بالإضافة الى شرط وجود الاذن القضائي.

الفصل الثاني

الفصل الثاني: الآليات القانونية المؤسساتية للجريمة الإلكترونية

إن موضوع الآليات القانونية المكافحة الجريمة المعلوماتية أصبح هاجسا يؤرق رجال القانون بصفة خاصة لذلك بات من المستعجل أن تتسع دائرة التعاون مع رجال العلم المتخصصين في التقنيات الرقمية ورجال القانون والمؤسسات الرسمية في الدولة وعلى المستوى الدولي أيضا بغية سن قوانين تكافح مرتكبي تلك الجرائم كما تبرز أهمية هاته الدراسة من الناحية النظرية في معرفة مدى كفاية النصوص القانونية الحالية لمنع الجريمة المعلوماتية وردع مرتكبيها ومدى الحاجة إلى خلق نصوص قانونية جديدة للحد من هذه الظاهرة.

في هذا الفصل سنتطرق إلى دراسة مكافحة الجريمة الإلكترونية بموجب القوانين العامة والخاصة (المبحث الأول) وإلى الآليات المساعدة لمكافحة الجريمة الالكترونية (المبحث الثاني).

المبحث الأول: مكافحة الجريمة الالكترونية بموجب القوانين العامة والخاصة

رغبة من المشرع الجزائري في التصدي لظاهرة الإجرام الالكتروني عمد منذ الألفية الثانية إلى تعديل العديد من القوانين الوطنية بما فيها التشريعات العقابية على رأسها قانون العقوبات لجعلها تتجاوب مع التطورات الإجرامية في مجال تكنولوجيا الإعلام والاتصال، وقام باستحداث قوانين أخرى خاصة الضمان الحماية الجنائية للمعاملات الإلكترونية.

في هذا الحديث سنتطرق إلى دور القوانين والهياكل الخاصة في مكافحة الجريمة الإلكترونية (المطلب 1) وصولا إلى دراسة القوانين العامة في مكافحة الجريمة الالكترونية (المطلب 2).

المطلب الأول: مكافحة الجريمة الإلكترونية بموجب القوانين والهياكل الخاصة.

في هذا المطلب سنحاول دراسة القوانين والهياكل الخاصة لمكافحة الجريمة الإلكترونية، بموجب القوانين الخاصة (الفرع 1)، وبموجب الهياكل الخاصة (الفرع 2).

الفرع الأول: مكافحة الجريمة الإلكترونية بموجب القوانين الخاصة:

أ-القانون الخاص بحماية حق المؤلف والحقوق المجاورة: يرى معظم الفقه أن "**الموقع الالكتروني مصنف متعدد الأغراض**" يتم استخدامه من الشركات التجارية كعلامة تجارية لتمييز منتجاتها المعروضة للتسوق أو الدعاية عن غيرها على شبكة الانترنت، أو كاسم تجاري أو شعار لجذب الجمهور، كما يمكن أن يستغل كمصنف أدبي أو فني من المؤلفين عند عرض أفلامهم

السينمائية أو لوحاتهم الزيتية أو العاب الفيديو...وغيره، وفي كل الحالات يختار صاحب الموقع العنوان الذي يريده في شكل علامة أو إسم تجاري أو مصنف بهدف تحديد هويته عبر الشبكة لكي يعرض ما يريد من سلعة أو خدمة عن إبرام العقد مع إحدى الشركات التي تقدم الخدمات على الشبكة ، وبمجرد تسجيل اسم الموقع يحظى بالحماية القانونية المقررة لحق الملكية الفكرية الذي يتضمنه ، أي يتحدد القانون الواجب التطبيق حسب الطبيعة القانونية للمواقع تعقد تسجيل كمصنف أدبي أو فني" لا يجوز أن يعتدي على أي جانب من جوانب الحياة الخاصة للأفراد[1].

ب- قانون البريد و الاتصالات اللاسلكية : باستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد و الاتصالات، لاحظنا أن هناك تسارع في مواكبة التطور الذي شهدته التشريعات العالمية مسايرة للتطور التكنولوجي، لذلك بات من السهولة بمكان إجراء التحويلات المالية عن الطريق الإلكتروني، ذلك ما نصت عليه المادة 87 منه، كما نصت المادة 2/84 منه على استعمال حوالات دفع عادية أو الكترونية أو برقية، كما نص في المادة 105 منه على احترام المراسلات، بينما أتت المادة 127 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحاول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات[2].

ج- القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:

لقد جاء في القانون 09-04 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر، وهي كالتالي:

1.مراقبة الاتصالات الالكترونية: لقد نصت المادة 4 من القانون 09-04 على أربع حالات التي

[1] حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الاعتداء على الحق في الحياة الخاصة الكترونيا، الملتقى الوطني " آليات مكافحة الجرائم الالكترونية في التشريع الجزائري " الجزائر، 29 مارس17، ص121-122.

[2] فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، المؤتمر الدولي الرابع عشر "الجرائم الإلكترونية "، طرابلس، بتاريخ 24-25 مارس 2017، ص 118.

يجوز فيها لسلطات الأمن القيام بمراقبة المراسلات والاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحمية وهي:

- ❖ للوقاية من الأفعال التي تحمل وصف جرائم الإرهاب والتخريب وجرائم ضد امن الدولة.
- ❖ عندما تتوفر معلومات من احتمال وقوع اعتداء على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.
- ❖ لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.
- ❖ في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

2.إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية: وذلك ممن خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد 10، 11، 12 بالشكل التالي:

- ➢ الالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات والتحقيق.
- ➢ الالتزام بحفظ المعطيات المتعلقة بحركة السير وكل المعلومات التي من شأنها أن تساهم في الكشف عن الجرائم ومرتكبيها، وهذين الالتزامين موجهين كل مقدمي خدمات الاتصالات الالكترونية(fournisseurs de services) دون استثناء.
- ➢ الالتزام بالتدخل الفوري لسحب المحتويات التي تسمح لهم للاطلاع عليها بمجرد العلم بطريقة مباشرة أو غير مباشرة بمخالفتها للقانون، وتخزينها أو جعل الوصول إليها غير ممكن.
- ➢ الالتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع إخطار المشتركين لديهم بوجودها.

❖ إضافة إلى التدابير الوقائية السالفة الذكر تبنى المشرع القانون رقم 09-04 إجراءات جديدة يدعم بها تلك المنصوص عليها في قانون الإجراءات الجزائية الخاصة بمكافحة جرائم تكنولوجية الإعلام الآلي والاتصال تتلخص فيما يلي:

- ❖ السماح للسلطات الجزائرية المختصة اللجوء إلى التعاون المتبادل مع السلطات الأجنبية في مجال التحقيق وجمع الأدلة للكشف عن الجرائم المتصلة بتكنولوجية الإعلام والاتصال غير الوطنية ومرتكبيها ، وذلك عن طريق تبادل المعلومات أو اتخاذ تدابير احترازية في إطار الاتفاقيات الدولية ومبدأ المعاملة بالمثل[1].
- ❖ السماح للجهات القضائية المختصة وضباط الشرطة بالدخول لغرض التفتيش ولو عن بعد إلى منظومة معلوماتية أو جزء منها و المعطيات المعلوماتية المخزنة فيها واستنساخها، مع إمكانية تمديد التفتيش ليشمل المعطيات المخزنة في منظومة معلوماتية أخرى التي يمكن الدخول إليها بواسطة المنظومة الأصلية، بشرط إخطار السلطات المختصة مسبقا.
- ❖ إمكانية الاستعانة بالسلطات الأجنبية المختصة للحصول على المعطيات محل البحث المخزنة في منظومة معلوماتية موجودة خارج الإقليم الوطني، وذلك طبقا للاتفاقيات الدولية ومبدأ المعاملة بالمثل.
- ❖ توسيع دائرة اختصاص الهيئات القضائية الجزائية لتشمل النظر في الجرائم المتصلة بتكنولوجية الإعلام والاتصال المرتكبة من طرف الأجانب خارج الإقليم الوطني، عندما تكون مؤسسات الدولة الجزائرية والدفاع الوطني والمصالح الإستراتيجية للدولة الجزائرية مستهدفة.

د- قانون التأمينات: لقد تطرق هذا القانون 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

[1] براهيمي جمال، مكافحة الجريمة الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة معمري تيزي وزو، العدد 2، الصادرة في 2016/11/15 ص151-154.

المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة للبطاقة الالكترونية حسب المادة 93 مكرر 2 [1].

الفرع الثاني: مكافحة الجريمة الالكترونية بموجب الهياكل الخاصة:

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

نصت على إنشاء هذه الهيئة المادة 13 من القانون 04/09 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها" تنشا هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته. تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم " أما مهامها فقد أوردتها المادة 14 من نفس القانون.

- **مهام الهيئة: للهيئة دوران أساسيان هما:**

1. الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الإلكترونية، التلاعب بحسابات العملاء أو ببطاقات ائتمانهم، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية... إلخ.

2. مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بحسب نص المادة 14 من القانون 04/09 فهناك نوعان من المكافحة تقوم بهما هذه الهيئة:

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية المادة 14 فقرة ب من القانون 09/04 ، وبالنسبية للوكالة المركزية لمكافحة الإجرام المتعلق بتكنولوجيات الإعلام والاتصال بفرنسا، فان لها مهام أدرجها

[1] فضيلة عاقلي، المرجع السابق، ص132.

المرسوم رقم 405.2000 المؤرخ في 15 ماي 2000 المتضمن إنشاء هذه الهيئة تتمثل في[1]:

- تنشيط وتنسيق على المستوى الوطني عمليات المكافحة ضد الفاعلين والمشتركين في ارتكاب الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.
- التدخل من تلقاء نفسها بعد موافقة السلطات القضائية المسبقة (المادة 4 فقرة 2 من القانون04/09 في كل مرة تفرضها الظروف من أجل البحث الميداني في وقائع مرتبطة بتحقيق تقوم به).
- من أجل القيام بمهامها فلها تركيز تحليل، استقراء كل المعلومات المتعلقة بأفعال أو جرائم متصلة بتكنولوجيات الإعلام والاتصال، والاتصال بكل من مصالح الأمن والدرك الوطنيين، إدارات ومصالح الدولة (المديريات العامة)، وكذلك كل الادارات والمصالح العامة للدولة المعنية للقيام بمهامها.
- تقديم المساعدة المصالح الأمن والدرك الوطنين، ولجميع إدارات ومصالح الدولة المركزية (المديريات العامة المختلفة) فيما يخص الجرائم التي تدخل في اختصاص هذه الهيئة، إذا طلبت منها هذه المصالح ذلك، ودون أن يؤدي ذلك إلى رفع يد هذه المصالح.

3. تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل العمليات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم: في هذا الشأن تقوم الهيئة على المستوى الوطني بتنشيط وتنسيق الأعمال التحضيرية الضرورية ومن ثم تشاركها مع المنظمات(الهيئات) لمماثلة لها على مستوى الدول، بدون المساس بتطبيق الاتفاقيات الدولية ومبدأ المعاملة بالمثل كما أنها تدرس الروابط العملياتية مع الهيئات والمصالح المختصة مع

[1] لمعرفة مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المستقبلية، انظر www.legifrancegouv.fr/affichtexte.de

الدول الأخرى من أجل البحث عن جميع المعلومات المتعلقة بالجرائم المعلوماتية وكذلك التعرف على الفاعلين وأماكن تواجدهم [1].

ب . المعهد الوطني للأدلة الجنائية على الاجرام : يتكون من إحدى عشرة دائرة مختصة في مجالات مختلفة جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية ودائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات[2].

ج . الهيئات القضائية الجزائية المتخصصة: ان السلطة القضائية ستتعامل تأكيدا في قضايا الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ولا سيما بعد اللجوء الواسع والمتزايد إلى الشبكات الرقمية في حياة المواطنين، بينما يتطلب الأمر مظاهر تقنية وقانونية لمعالجة هذه القضايا، وعلى هذا فإن حتمية المعرفة ولو في حدها الأدنى لمعالجة فعالة في هذه المواد التي تجتاح المجال العقابي.

المطلب الثاني: مكافحة الجريمة الإلكترونية بموجب القوانين العامة:

في هذا المطلب سنتطرق إلى القوانين العامة التي تكافح الجرائم الإلكترونية والتصدي لها.

الفرع الأول: مكافحة الجريمة الالكترونية بموجب الدستور الجزائري والقانون المدني:

أ- **مكافحة الجريمة الإلكترونية بموجب الدستور الجزائري:** لقد كفل دستور الجزائر لسنة 1996 وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية الحقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان. وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق، ومن أهم المبادئ الدستورية العامة:

المادة 38: الحريات الأساسية وحقوق الإنسان والمواطن مضمونة.

---

[1] عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية مصر، 2007، ص232.233.

[2] فضيلة عاقلي، مرجع سابق، ص133.

المادة 44: حرية الابتكار الفكري والفني والعلمي مضمونة للمواطن حقوق المؤلف يحميها القانون لا يجوز حجز أي مطبوع أو تسجيل أو اية وسيلة أخرى من وسائل التبليغ والإعلام إلا بمقتضى أمر قضائي، الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون.

تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة.

إذ لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، كما أن القانون يحمي سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة. ان القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا أمر قضائي[1]

ب . مكافحة الجريمة الإلكترونية بموجب القانون المدني الجزائري : ترتيبا على الأهمية الدستورية الحرمة الحياة الخاصة فقد سارع المشرع ونص على أن لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وفق هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر في المادة 124 من التقنين المدني الجزائري " كل عمل أيا كان يرتكبه المرء يسبب ضرر للغير يلزم من كان سببا في حدوثه بالتعويض " وقد جاء هذا النص عاما وشاملا لأي اعتداء يقع على أي حق من الحقوق الملازمة للشخصية بما فيها الحق في الحياة الخاصة، وقد أورد هذا النص مبدا مهما هو حق من وقع إعتداء على حياته الشخصية في التعويض عما لحقه من ضرر، فالمسؤولية المدنية ترتب الحق في الحكم بالتعويض " فالفعل الضار هو أساس المسؤولية". وهو الركن الأساسي الذي يؤسس عليه الحق في رفع الدعوى القضائية عن الاعتداءات الالكترونية التي تمس بالحياة الخاصة على شبكة الأنترنت ، وهو عنصر متحول وصعب التحديد في الجرائم التي تمس الخصوصية على المواقع الالكترونية لما تشكله من صعوبات في الإثبات في تحديد هوية المعتدي، وفي هذه المسألة المشرع الجزائري حذا حذو المشرع الفرنسي الذي أقام المسؤولية عن الفعل الالكتروني الشخصي على أساس

[1] فضيلة عاقلي، مرجع سابق، ص 127.

الخطأ الواجب الاثبات فلا يكفي أن يحدث الضرر الذي يمس عناصر الحياة الخاصة بل يجب أن يكون ذلك الفعل الالكتروني قد وصل إلى درجة الخطأ يشكل اعتداء قابل للإثبات وان وقع على الشبكة [1].

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

أ- مكافحة الجريمة الالكترونية بموجي قانون العقوبات الجزائري: لقد تطرق المشرع الجزائري إلى تجريم الافعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجة القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 22-15 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر 7 [2].

قام المشرع الجزائري بموجب القانون رقم 04-15[3]باستحداث جملة من النصوص ة التي تجرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات ، وحدد كل فعل منها ما يقابله من الجزاء ، إذ قام المشرع الجزائري بسن جملة من القواعد القانونية الموضعية و التي حدد من خلالها كل الأفعال الماسة بنظام المعالجة الآلية للمعطيات و ما يقابلها من جزاء أو عقوبة [4]، والى جانب ذلك قام المشرع بسن قواعد جزائية جديدة تتعلق بالتحقيق تتماشى مع الطبيعة المميزة للجرائم الالكترونية وذلك من خلال تعديل قانون الاجراءات الجزائية بموجب قانون رقم 06-22 [5].

---

[1]حسين نوارة، مرجع سابق، ص 121، 122.

[2]فضيلة عاقلي، مرجع سابق، ص 127.

[3]قانون رقم 04 -15 مؤرخ في 10 نوفمبر 2004 يعدل ويتمم الأمر رقم 66 - 156، يتضمن قانون العقوبات، جريدة الرسمية، عدد 71، الصادرة بتاريخ 10 نوفمبر 2004، معدل ومتمم.

[4]قانون رقم 06-22 مؤرخ في 20 ديسمبر 2006 يعدل ويتمم الأمر رقم 66_155، يتضمن قانون الإجراءات الجزائية، جريدة رسمية، عدد 84، صادرة بتاريخ 24 ديسمبر 2006.

[5]براهيمي جمال، مرجع سابق، ص 124-125.

اذ نصت المادة 394 مكرر: " يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 إلى100000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات او يحاول ذلك "، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير المعطيات المنظومة وإذا ترتب عن الافعال المذكورة أعلاه تخريب نظام اشتعال المنظومة " تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج " ، وذلك مهما كانت قاعدة المعلوماتية أو طبيعتها لذلك يمكن أن تندرج ضمن هذه الاعتداءات تلك التي تمس ببعض صور الحياة الخاصة، ونصت المادة 394 مكرر2 على أنه: " يعاقب ... كل من يقوم عمدا وعن طريق الغش بما يأتي:

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

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

ونصت المادة 394 مكرر6 أنه بالإضافة إلى العقوبات الأصلية أي الحبس والغرامة وبالاحتفاظ بحقوق الغير الحسن النية يحكم بالعقوبات التكميلية التالية : "يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، العلاوة على إغلاق المحل أو المكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها " [1].

ب - مكافحة الجريمة الالكترونية بموجب قانون الإجراءات الجزائية الجزائرية: بالنسبة لمتابعة الجريمة الإلكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والشهادة و الخبرة [2].

[1] حسين نوارة، مرجع سابق ص118-119.

[2] فضيلة عاقلي مرجع سابق ص130.

نجد أن المشرع نص على تمديد لاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 قانون الإجراءات الجزائية ، ونص على التنفيش في المادة 45 الفقرة 7[1]،من نفس القانون المعدل حيث اعتبر أن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية الموضوعية، فالتفتيش وإن كان إجراء من إجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، و بالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذا على اعتراض المراسلات و تسجيل الاصوات والتقاط الصور من المادة 65 مكرر 5 [2].

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للإجرام الالكتروني لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية، إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية وقائية وتحفظية، والتي من شأنها أن تفادي وقوع الجريمة الالكترونية أو على الأقل الكشف عنها في وقت مبكر يسمح بتدارك مخاطرها، وهو ما استدركه المشرع بتضمين القانون رقم 06 – 22 المعدل لقانون الإجراءات الجزائية تدابير إجرائية مستحدثة تتعلق بالتحقيق في الجرائم الالكترونية تتمثل في مراقبة الاتصالات الالكترونية تسجيلها والتسرب .

يقصد باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تكون في شكل بيانات قابلة للإنتاج والتوزيع التخزين الاستقبال والعرض، التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية في إطار البحث والتحري عن الجريمة وجمع الأدلة عنها.

ولقد أشار المشرع الجزائري إلى ظروف وكيفية للجوء هذا الإجراء في المادة 65 مكرر 5 من قانون الإجراءات الجزائية على النحو: "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها، أو التحقيق الابتدائي في ... الجرائم الماسة بأنظمة المعالجة الالية للمعطيات ... يجوز لوكيل الجمهورية المختص أن يأذن:

– باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.

[1] مولود ديدان، قانون الإجراءات الجزائية، الأمر 11–02 دار بلقيس، الجزائر، ص33.

[2] فضيلة عاقلي المرجع نفسه ص130.

– وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط وتثبيت و بث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة اشخاص في أماكن خاصة او عموميه أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص".

بموجب هذه المادة فإن المشرع الجزائري يسمح لسلطات التحقيق والاستدلال إذا استدعت ضرورة التحري في الجريمة المتلبس بها ، أو التحقيق في الجريمة الالكترونية ، اللجوء إلى إجراء اعتراض المراسلات السلكية وتسجيل المحادثات والأصوات والتقاط الصور، والاستعانة بكل الترتيبات التقنية اللازمة لذلك من أجل الوصول إلى الكشف عن ملابسات الجريمة وإثباتها دون أن يتقيدوا بقواعد التفتيش والضبط المألوفة .ومع هذا فإن المشرع الجزائري لم يطلق حق اللجوء إلى هذا الإجراء، بل أحاطه بمجموعة من الضمانات القانونية التي تحد من تعسف سلطات الاستدلال والتحري وتصون الحقوق والحريات العامة والحياة الخاصة للأفراد[1].

المبحث الثاني: الآليات المساعدة على مكافحة الجريمة الإلكترونية

نظرا لارتفاع الجرائم الإلكترونية وتضاعف أعدادها وأنواعها، وتطور أساليبها، وانطوائها على مخاطر جمة تلحق بالأفراد والمؤسسات خسائر كبيرة، باعتبارها تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة(البيانات والمعلومات والبرامج بكافة أنواعها)وتطال المعطيات المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات، فهي تطال الحق في المعلومات والحقوق المالية، وحقوق الملكية الفكرية، والحق المعنوي كما أنها تمس الحقوق والحريات الشخصية، وتهدد الأمن القومي والسيادة الوطنية، وتشييع فقدان الثقة بالتقنية، وتهدد إبداع وابتكار العقل البشري[2].

فعلى الرغم من تخصيص آليات إجرائية ومؤسساتية عملياتية من أجل مكافحة الجريمة الالكترونية، إلا أن دائرة آليات المكافحة لن تكتمل من دون الآليات المساعدة التي تمثل في

[1] براهيمي جمال، مرجع سابق من 437، 139 –140

[2] محمد احمد السويحلي، تكاثف الجهود العربية لمكافحة الجريمة الالكترونية، مجلة الدراسات المالية المصرفية، السنة الثالثة والعشرون، العدد الأول، الأردن، مارس 2015.

كثير من الأحيان عامل تعزيز لوسائل المكافحة، أولا الجمعيات وما تؤديه من دور في عملية التوعية (المطلب الأول)، ثانيا معالجة الإدمان على الانترنت (المطلب الثاني).

المطلب الأول: الجمعيات:

إن للجمعيات دورا فاعلا في توعية أفراد المجتمع من المخاطر التي قد تسببها الوسائط الالكترونية الحديثة، وبالأخص على الأطفال، إذ يجب إتباع الإجراءات والتدابير اللازمة لضمان سلامتهم ووضع قيود لقبول دخولهم إلى المواقع الإلكترونية، وبالذات مواقع التواصل الاجتماعي، من الواجب على كل الفاعلين في المجتمع الإكثار من البرامج التوعوية وبث المعرفة وتثقيف الشباب لتحصينه ضد هذه الآفة وإقامة نشاطات جمعوية بديلة تمتص قدراته وطاقته وتوجيهها إلى منحى يقدم الأمة[1]، مستعينين في ذلك بتلك الوسائط حتى لا نتركها مصدرا لتخريب عقول الشباب فقط. فالشبكات الاجتماعية على سبيل المثال تعتبر من أهم الوسائل الاتصالية الحديثة، والتي بإمكان الجمعيات الاهتمام باستخدامها لأنها تشكل البديل عن وسائل الإعلام التقليدية، والتي لا يمكن للجمعيات الشبابية الجديدة الوصول إليها[2].

ولمعرفة المزيد بخصوص دور الجمعيات كآلية مساعدة على مكافحة الجريمة الإلكترونية.

سنتطرق لبعض النماذج عن جمعيات مكافحة الجريمة الالكترونية (الفرع1)، ثم لدورها في مكافحة الجريمة الكترونية والحد منها (الفرع 2).

الفرع الأول: نماذج عن جمعيات مكافحة الجريمة الالكترونية:

إن الحقبة التي نحياها هي بكل تأكيد حقبة الإنترنت والتكنولوجيات الحديثة، والتي تفرض على القائمين على أمر المجتمع وأصحاب القرار فيه استيعاب ذلك[3]،والعمل على التأقلم مع الوضع لإيجاد وسائل كفيلة لمحاربة الجرائم الإلكترونية التي قد تنتج عن ذلك، فالمجتمع ككل ينبغي

[1] دنيا عبد العزيز فهمي، الحماية الجنائية من إساءة استخدام مواقع التواصل الاجتماعي " دراسة مقارنة "، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 2018 ص112.

[2] أمال عزري، جمال بن زروق، استخدام جمعيات المجتمع المدني في الجزائر للشبكات الاجتماعية الالكترونية (دراسة ميدانية على جمعيات المجتمع المدني في ولاية سكيكدة). مجلة أفاق للعلوم، جامعة الجلفة ، الجزائر ، العدد السابع ، مارس 2017، ص235.

[3] عبد الفتاح حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، القاهرة، مصر، 2007 ص 218 المرجع نفسه ص 206.

أن يتحمل مسؤولية علاج المجرمين وتأهيلهم وتقديم الوسائل التي تؤدي إلى خفض الجريمة، فالمجتمع عند انحراف فرد منه وارتكابه الجريمة يكون قد خسر فردا إيجابيا[1]،لذا فإن تشجيع ودعم تأسيس جمعيات الوقاية من الإجرام والانحراف، ورعاية المبتلين، و تأهيل وإعادة إدماج المفرج عنهم وإصلاح المحكوم عليهم بعقوبات موقوفة التنفيذ، وحماية الأحداث، وتحصين أفراد المجتمع من الآفات الاجتماعية سيساهم في الوقاية من الإجرام والانحراف[2]وتعد جمعيات مكافحة الجرائم الالكترونية عينة من تلك الجمعيات التي تسعى إلى خفض نسبة ارتكاب الجرائم الالكترونية، والتي لم تبقى فئة من فئات المجتمع إلا وطالتها.

وعلى الرغم من أن الجزائر بها ما يقارب مائة وتسعة آلاف جمعية أي 108940 جمعية في مختلف المجالات[3]. إلا أننا لم نجد أي جمعية تنشط في مجال محاربة الجرائم الالكترونية، بخلاف الدول العربية الأخرى، كتونس ومصر والأردن التي بها جمعيات تعنى بهذا النوع من الجرائم، ففي تونس مثلا هناك الجمعية التونسية لمقاومة الجريمة الإلكترونية والجمعية التونسية للإنترنت[4]،وفي الأردن هناك الجمعية الأردنية المتخصصة في الجرائم الالكترونية والحد منها، والتي تم توقيع نظامها الأساسي عام 2006 ومركز عملها عمان ولها مجموعة من الأهداف يلاحظ عليها أنها جميعها تهدف إلى إنتاج التوعية ونشر الأفكار للحد من جرائم الحاسوب

[1] محمد شنة، جرائم العنف الأسري وآليات مكافحتها في التشريع الجزائري، أطروحة مقدمة لنيل درجة دكتوراه العلوم في الحقوق، تخصص علم الإجرام وعلم العقاب، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة 01 2017 – 2018 ص 171.

[2] عبد العزيز ديلمي، دورة الشرطة المجتمعية في الوقاية من الجريمة والانحراف دراسة نظرية لبناء نموذج للشرطة الجوارية في الجزائر، أطروحة مقدمة لنيل شهادة الدكتوراه في علوم اجتماع الجريمة والانحراف، قسم علم الاجتماع، كلية العلوم الإنسانية والاجتماعية، جامعة الجزائر 02،2012 ،2013.

[3] المصدر: الموقع الرسمي لوزارة الداخلية والجماعات المحلية
http://www.interieur.gov.dz/images/pdf/listeassossaciationar.pdf

[4] محمد محمد الألفي، الجرائم المضرة بأمن الدولة عبر الإنترنت، التجسس والإرهاب الإلكتروني، جامعة القاهرة، ص32.

والانترنت[1]، وفي مصر بعد انعقاد المؤتمر التأسيسي الأول لجمعيات قانون الانترنت بالقاهرة في شهر سبتمبر سنة2004، وكذا المؤتمر الدولي الأول لقانون الإنترنت بمدينة الغردقة في شهر أوت سنة 2005 ، بدأ الاهتمام بمكافحة الجريمة الإلكترونية، وتأسست على إثر ذلك الجمعية المصرية لمكافحة الجرائم المعلوماتية والإنترنت سنة 2005 و المشهرة تحت رقم (2176) لسنة 2005 بتاريخ 2005/08/05[2]وفي نفس السنة وبمناسبة نفس المؤتمر تم تأسيس الجمعية العربية لقانون الانترنت[3]،وهناك أيضا الجمعية الدولية لمكافحة الجريمة الالكترونية بفرنسا association international de lutte contre la cybercriminalité (A.I.L.C.C)

والتي هي عبارة عن منظمة دولية غير حكومية وغير هادفة للربح منشاة طبقا للقانون الفرنسي رقم 1901 حيث تم إيداع نظامها الأساسي بالجريدة الرسمية الفرنسية بتاريخ 18 مارس 2006، والجمعية معنية بمكافحة الجريمة الالكترونية بكافة صورها وأشكالها وتقليص حجم ارتكاب الجرائم المعلوماتية عبر شبكة الإنترنت.

الفرع الثاني: دور جمعيات مكافحة الجريمة الالكترونية في الحد منها.

إن السياسة الزجرية لا تكفي لوحدها لصد الجرائم الالكترونية ، لذا قامت عدة دول في السنوات الأخيرة بوضع سياسة وقائية أطلق عليها تسمية الثقة الرقمية[4]، وقامت بسن قوانين بمحفزات معينة لتشجيع تأسيس جمعيات يتعلق نشاطها بالإنترنت والحاسوب، هدفها نشر ثقافة

---

[1] محمد نافع فالح رشدان، حجية الدليل الإلكتروني كوسيلة من وسائل الإثبات في المسائل الجزائية" دراسة مقارنة بين القانونين الكويتي والأردني" قدمت هذه الرسالة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون العام، كلية الحقوق جامعة الشرق الأوسط الأردن تشرين الثاني 2015 ص72.

[2] معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ململة لنيل شهادة الماجستير في العلوم القانونية، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة العقيد لخضر، باتنة 2011 – 2012 ص97.

[3] المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، المؤتمر الدولي الأول القانون الانترنت (cyber Law) " نحو علاقات قانونية وإدارية واقتصادية وسياسية واجتماعية جديدة" 21، 2005/08/25, الغردقة – جمهورية مصر العربية.

[4] خالد عثماني، مكافحة الجريمة الالكترونية في ضوء التشريع المغربي، مجلة العلوم الجنائية، مطبعة الأمنية، العدد الأول، الرباط، 2014 ص 48.

الإنترنت والاستخدام الواعي للحاسوب، وإشراك القطاع الخاص في مكافحة جرائم الانترنت لأنها ضرورية لمساعدة السلطات العامة من خلال تحسين الحماية الذاتية كخط دفاع أول لهذا القطاع[1]، لأن البيئة الاجتماعية تأثير قوي على بعض الأشخاص ، فهم يتلقون فيها العديد من القيم والعادات ويأخذون منها نظرة على الحياة والمجتمع [2]كما أن مشاركة القطاع المدني والعمل الأهلي التطوعي في التصدي لهذه المشكلات التي تواجه المجتمع أصبحت عاملا حاسما لضمان النجاح في التصدي لهذه المشكلات من خلال تنمية الوعي المجتمعي وإيجاد ثقافة عامة على صعيد المجتمع بكامله تفض السلبيات وتعمل على تنمية الايجابيات[3]، وهنا يظهر بشكل جلي الدور الذي تلعبه جمعيات مكافحة الجرائم الإلكترونية في تسليط الضوء على السلبيات والأخطار التي قد تتسبب فيها الوسائل الإلكترونية الحديثة وبالذات الانترنت, ففي سبيل ذلك فإن الجمعيات تقوم بعدة أشياء منها على سبيل المثال:

1_ قيامها بعقد برتوكولات تعاون مع المؤسسات التعليمية من أجل تثقيف وتدريب الطلبة وخريجي الكليات في مختلف التخصصات، وكذا السادة القضاة وأعضاء النيابة العامة والسادة المحامين و العاملين في القطاعات القانونية في المؤسسات و تأهيل و إكساب المتدربين المهارات القانونية والعلمية والعملية والفنية الخاصة بارتباط المعلوماتية والاتصالات بتخصصاتهم، و تبين الإشكاليات القانونية التي قد يتلقونها في حقل المعاملات الالكترونية[4].

---

[1] بومامي العباس، الجريمة الإلكترونية بين التحصين التقني والتحصين الجنائي مذكرة مكملة لنيل شهادة الماجستير في علوم الإعلام والاتصال، قسم علوم الإعلام والاتصال، كلية علوم الإعلام والاتصال، جامعة الجزائر: 2005-2006 ص167.

[2] محمد الأزهر، مبادئ في علم الإجرام، الطبعة التاسعة، مطبعة دار النشر المغربية، الدار البيضاء، المغرب، 2015ص228.

[3] عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت (الجرائم الإلكترونية دراسة مقارنة في النظام القانوني لمكافحة جرائم المعلوماتية والانترنت معا لإشارة إلى جهود مكافحتها محليا وعربيا ودوليا) الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007. ص94.

[4] قامت الجمعية الأوربية للمعلومات بتعزيز التواصل والحوار بين الأطراف المعنية والعمل على تأهيل وتعليم العاملين في أجهزة العدالة الجنائية والمتعاملين معها بصفة خاصة والمجتمع بصفة عامة، عبد الصبور عبد القوي علي، الجريمة الإلكترونية والجهود الدولية للحد منها، محلة الدراسات المالية والمصرفية، السنة الثالثة والعشرون، العدد الأول، الأردن، مارس 2015 ص10.

2_ تتعاون الجمعيات فيما بينها لتخطي الصعوبات التي تواجه عملية مكافحة الجرائم الالكترونية ومع ذلك المبادرة التي تبنتها الجمعية الدولية لمكافحة الجرائم الإلكترونية بفرنسا والجمعية المصرية لمكافحة جرائم الانترنت في محاولة لسن قوانين رادعة تحمي رواد شبكة الإنترنت من التجاوزات غير اللائقة التي تحدث على الشبكة ، بداية من الإرهاب الإلكتروني ومرورا بالسطو على الحقوق الفكرية ، وانتهاء بتجريم تجارة الرقيق الأبيض على الشبكة العنكبوتية وماهية التنظيم القانوني للعالم الافتراضي بأقسامه من المعاملات القانونية الرقمية وعقود التجارة الإلكترونية وحماية الملكية الفكرية عبر الانترنت والتعريف بأنماط وأشكال الجرائم عبر الانترنت وماهية الدليل الرقمي وحجيته في الإثبات وعرض أحدث التقنيات الفنية العالمية للتعامل مع مثل هذه النظم[1].

3) إعداد الدراسات والبحوث حول العلاقة الرقمية بالقاعدة الموضوعية والإجرائية في القانون الجنائي والحث على تطويره ، وتشجيع البحث العلمي للوقاية من الجرائم الإلكترونية[2].

4) تنظيم ورشات عمل وملتقيات في مختلف المواضيع التي تمسها الجرائم الالكترونية لإيجاد حلول تتناسب مع خطورة هذه الجرائم، والاستفادة من خيرة ذوي الاختصاص.

المطلب الثاني: معالجة الإدمان على الإنترنت:

في هذا المطلب سنقوم بدراسة مفهوم الإدمان على الإنترنت وأسبابه وآثاره النفسية، وأيضا مجالاته وكيفية معالجته والوقاية منه.

الفرع الأول: مفهوم الإدمان على الانترنت.

اختلف العلماء في استخدام مفهوم الإدمان على الانترنت،اعترض البعض على أن الشخص يعتبر مدمنا إذا استخدم الانترنت بشكل زائد عن الحد فالشبكة ليست عادة، إنما هي ميزة للحياة الحديثة لا يمكن الاستغناء عنها، واعتبروا أن الانترنت عبارة عن بيئة ولا يمكن الإدمان على البيئة، غير أن الدراسات والبحوث الأخيرة، والتي قامت بها مراكز متخصصة، أكدت أن

[1] عبد العال الديربي، محمد صاد إسماعيل، الجرائم الإلكترونية دراسة قانونية فضائية مقارنة ع أحداث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة 2012 ص 120.

[2] عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية –دراسة مقارنة–، قدمت هذه الرسالة استكمالا للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، الأردن، 2014، ص 103–104.

الإدمان على الإنترنت أصبح واقعا وحمى مرضية، عكف الأطباء النفسانيون البحث عنها وعن مخاوف الاستعمال المفرط والمبالغ للشبكة وأصبحت تسميات تطلق على من يبالغ استعمالها مثل: الإدمان على الإنترنت، الاستخدام الباثولوجي للإنترنت، أو الاستخدام القسري للإنترنت، وحسب استطلاع أجري عام2005نظمته جامعة ستانفورد حددت من خلاله معدل قضاء الوقت في استخدام الإنترنت بشكل عام3ساعات و نصف ساعة يوميا (Pieree, v, 2006 p2) .

عرفه العالمانPerson and Hall ، من جامعة لورا الأمريكية فسلوك الإدمان على الانترنت هو: "عملية تصحيحية وتعويضية لنقص الثقة بالنفس في مجالات الحياة المختلفة".

عرفه (D.Tory, 2000) إن إدمان الانترنت حالة من الاستخدام المرضي وغير التوافقي للإنترنت يؤدي إلى اضطرابات في السلوك ، ويستدل عليها بعدة ظواهر منها ، زيادة عدد الساعات أمام الكمبيوتر بشكل مطرد تتجاوز الفترات التي حددها الفرد لنفسه في البداية".

الفرع الثاني: أسباب الإدمان على الانترنت:

- توفر غرف الدردشة وسيلة للتفريغ الانفعالي وتفريغ شحنات الغضب والكبت والعدوانية، لذلك تصبح تلك الغرف الملاذ الأمن والمنقذ الأكبر، لما يعتري النفس من مكبوتات اللاشعور وبكل ثقة، مما يؤدي إلى توهم الحميمية والألفة.

يحاول الفرد من خلال الإنترنت التخلص من حالات القلق النفسي وضغوطات الحياة اليومية[1].

- الافتقاد للسند العاطفي عند المراهقين يجعلهم يلهثون وراء الإشباع الوهمي واللذة المؤقتة من خلال الدردشة مع الغرباء. إطلاق الرغبات الدفينة والتعبير عنها عبر غرف الدردشة التي توفر للشباب فرصة ذهبية للتخلص من القيود المجتمعية الصارمة.
- انتشار مقاهي الانترنت وتوفير السيولة المالية للمراهقين.
- التأثر بثقافات أخرى خاصة في عصر التطور الهائل في الاتصالات.
- التأثير جماعة الأقران والأصدقاء خاصة إن كانوا مدمنين على الانترنيت.

[1] محمد وليد المصري، الأسرة العربية وهوس الإنترنت، مجلة العربي، الكويت، العدد 575، أوت 2006، ص 173.

- المفهوم السلبي للتحضر و القابلية للاستهواء [1].

من خلال دراسة الدكتورة **يونغ yang** حول الإدمان على الانترنت والهدف منه، حيث مست هذه الدراسة 396 متصل بالإنترنت تتوفر فيهم محاكات الإدمان، توصلت إلى إيجاد3 أفواج من الأشخاص المدمنين:

1-فوج يهدف إلى الحصول على علاقات اجتماعية، وهم أشخاص يعيشون في مناطق معزولة جغرافيا ومهمشون اجتماعيا.

2-فوج الباحثين عن الاتصالات الجنسية الخيالية حيث تصبح المواقع الإباحية وسيلة للحصول على الإشباع بدون خطر.

3-فوج المستعملين الذين يخترعون شخصية خيالية عنهم عبر انترنت ويصبح بإمكانهم أن يفحصوا مظاهر شخصيتهم التي لم تظهر في الواقع[2].

الفرع الثالث: مجالات الإدمان على الإنترنت:

قام الباحث السيكولوجي Green Field سنة 1998، العضو في APA بدراسة من أكبر الدراسات في موضوع" مواقع الإدمان على الإنترنت"، شملت الدراسة 18000 مستخدما للإنترنت يدخلون على موقع BBC الذي تبنى هذه الدراسة، وجد هذا الباحث أن 5,7% من العينة يعانون من هوس الانترنت، هؤلاء المدمنين يفضلون مواقع توفر القمار، الدردشة الإباحة، التسوق، البريد الالكتروني.

وفي الدراسة التي قدمتها كمبرلي يونغ حول الإدمان على الانترنت، وجدت أن هناك ثلاث جوانب مهيمنة على المدمن تتمثل في:

- **فكرة المجتمع:** تجمع الأصدقاء على الخط أو الشبكة.
- **التخيلات:** التخيلات الجنسية أو اعتماد شخصيات جديدة
- **السلطة:** أو القدرة على التحكم للوصول الفوري إلى المعلومات وإلى الأشخاص.

[1] محمد بيومي خليل، انحراف الشباب في عصر العولمة، ج2 (ب ط)، دار قباء للطباعة والنشر، القاهرة، 2002، ص166-168.

[2] كمبرلي يونغ، ترجمة هاني أحمد ثلجي، الإدمان على الإنترنت، (ب ط)، دار الأفكار الدولية، الرياض، ب سنة، ص 104-106.

أما على الصعيد العربي، فتجمع تقريبا معظم الدراسات العربية التي بحثت في هذا الموضوع أن الهدف الرئيسي لعدد كبير من مستخدمي الانترنت هو الترفيه والتسلية وعلى رأسهم المراهقين، عن أكثر المواقع التي يدمنون عليها هي:

- **حجرات الحوارات الحية أو غرف الدردشة IRC:** يفضل المراهق التعرف على أفراد جدد خاصة من الجنس الآخر، ويقضي وقتا طويلا في الحديث معهم عن مشكلاته الشخصية وعن أسرته، ويكون الحوار في أكثر الأحيان حسب الدكتور فضيل دليو من جامعة منتوري–قسنطينة– يدور حول العلاقات الجنسية وتعاطي المخدرات والتشجيع على الإدمان عليها وكيفية اقتنائها.
- **المواقع الإباحية:** التي تعرض الصور الفاضحة فيقع المراهقون في هاوية الدخول إليها بدعوى الفضول ودافع للاستطلاع، ثم يقع في مصيدة الإدمان عليها، حيث تشير الإحصائيات أن 63%من المراهقين يرتادون صفحات وصور إباحية دون علم أوليائهم بطبيعة ما يتصفحون ، مما يؤثر على سلوكياتهم وتصرفاتهم[1].
- **الألعاب الإلكترونية:** تعتبر الألعاب الالكترونية عبر الانترنت أكثر جاذبية وشعبية في وسط الأطفال والمراهقين، نظرا للتطور الهائل الذي تشهده هذه الألعاب، والتي توفر للمشارك منافسة وتحد حقيقي عبر الشاشة، حيث تعطي له لذة في القتل والعنف والشعور بالانتصار والإثارة، باقتناء الأسلحة والمتفجرات وركوب الدبابات وصعود الجبال واختراق الثكنات والتكتيك للاختفاء والهروب.
- **نوادي النقاش أو المنتديات – Forum :** يقوم كل ناد بتبني قضية معينة أو هواية، ويتم عمل مقالات وحوارات بين المشتركين مع حرية التغيير والتنفيس الانفعالي والرغبة في تواصل وتقاسم الاهتمامات و الميولات والرغبات، و تنظيم اتجاهات مشتركة و تبريرها و تدعيمها حيث يتقمص المشترك شخصية معينة دون قدرة الآخر عن الكشف عنها

[1] رشيد فيلالي:"95,% يرتادون مواقع إباحية "، جريدة الشروق اليومي، الجزائر (1636)، 15–03، 2006، ص12.

➢ **قهر الانترنت:** مثل القمار على الانترنت أو التسوق على الانترنت[1].

الفرع الرابع: آثار الإدمان على الانترنت الصحية والاجتماعية:

بقدر ما توفر شبكة الانترنت الكثير من الخدمات للفرد وتفسح له الكثير من المجالات للغوص فيها، بقدر ما يؤدي الجلوس لساعات طويلة أمام شاشة الكمبيوتر ومن ثمة الإدمان على الشبكة التي لها آثار صحية، وأسرية ونفسية علمية وأكاديمية نذكر منها ما يلي:

❖ **الصحية:** ضعف الجهاز المناعي، مما يجعل الفرد عرضة للكثير من الأمراض، فالجلوس الطويل أمام شاشة الكمبيوتر يؤدي إلى آلام في الظهر والعمود الفقري، كذلك احتمال الإصابة بما يعرف بتناذر" النفق الرسغي"، حيث يصيب الأشخاص الذين يجلسون لساعات لطويلة أما شاشة الكمبيوتر، ويستخدمون أصابعهم للضغط على عضلات الإبهام والمسؤول عن الحس. كما أن طول مدة الجلوس أمام شاشة الكمبيوتر، يؤدي لركود في الدورة الدموية مما يسبب حدوث جلطات ودماغية وقلبية وضعف في أداء الأجهزة الحيوية بالجسم[2].

❖ **المشكلات الأسرية والاجتماعية:** لقد أصبحت الإنترنت رعب حقيقيا للأسر العربية، وخصوصا ما يعرف بغرف الدردشة، والتي يكون زوارها من فئة المراهقين، والذين هم أكثر تعرضا للإدمان الإنترناتي.

ولقد أكد بتنان (Putnon,1995) أن الانتشار الواسع لاستخدام الإنترنت صوحب بانخفاض كبير في الاندماج المدني والمشاركة الاجتماعية في الولايات المتحدة الأمريكية.

كما أن الذين يتعاملون بصورة متكررة مع الانترنت ربما يفقدون القدرة على التفاعل التلقائي.

❖ **النفسية:** فيما يخص الناحية النفسية، فقد وجد أن الإدمان على الانترنت له تأثيرات على الجملة العصبية، إذ يؤدي إلى عدم الاتزان الانفعالي، مما يؤدي إلى ضعف ردود الأفعال، وقد تحدث توترات عصبية بالإفراز المفرط والمتزايد لهرمون الكورتيزول(هرمون الإجهاد والتعب)، وهرمون الأدرينالين والنور أدرينالين، فيولد ذلك سرعة الغضب

[1] بشرى الأرنوط، إدمان الإنترنت وعلاقته بكل بعد من أبعاد والاضطرابات النفسية لدى المراهقين، رسالة دكتوراه غير منشورة، جامعة الزقازيق، مصر، 2005، ص 9.

[2] محمد وليد المصري، المرجع السابق، ص172.

والعدوانية، وظهور اضطرابات نفسية وعقلية، لدرجة أن بعض العلماء أطلق عليه اسم "الهوس النفسي"[1]كما يؤدي إدمان الإنترنت إلى ما يسمى " الإصابة بالتعب المتكرر"، وتعرف الإصابة بالتعب المتكرر بأنها الإصابة التي تلحق بالرسغ، والأيدي والرقبة، عندما يتم الضغط على المجموعة العضلية من خلال الحركات السريعة.

فالأفراد الذين يستخدمون لوحة المفاتيح الملحقة بجهاز الكمبيوتر، والذين يقومون بالضرب على المفاتيح بمعدل قد يصل إلى (31200) ضربة في الساعة يعدون حوالي13 بالمائة من إجمالي بنسبة المصابين بالتعب المتكرر[2].

الفرع الخامس: الوقاية والعلاج:

نشر الوعي إزاء استخدام الانترنت مسؤولية مشتركة تقع على عاتق الجميع كالآباء والمعلمين والقائمين في مجال الصحة النفسية وأصحاب مقاهي الانترنت حيث ينصح الأطباء المستخدمين للإنترنت بتنظيم ساعات العمل أو الترفيه في الإنترنيت، كأن تكون ساعتان فقط يوميا حتى لا ننسحب من حياتنا الطبيعية والاجتماعية وتقع فريسة لهذا الإدمان عن طريق:

- ✓ متابعة استخدام الأبناء للإنترنت من حيث الفترة والمدة والمضمون مع ضبط الوقت واستخدام بعض برامج الحماية لمنع دخولهم إلى مواقع التي تشكل تربة خصبة للإدمان.
- ✓ إرشادهم إلى المواقع الناجحة والهادفة والتربوية.
- ✓ ضرورة إلزام مقاهي الانترنت بالالتزام في عرض خدماتهم وفقا للدين والخلق بإدراج برامج تمنع المراهقين من الدخول في المواقع الحساسة، وصنع جدول زمني لا استخدام الانترنت لا يزيد عن 3 ساعات للمستخدم اليوم (ضبط أوقاتها).

أما عن علاج الإدمان على الإنترنت، لقد بدأت بالظهور عيادات نفسية لعلاج إدمان الانترنت حيث أنشئت أول عيادة نفسية عام 1996 في مستشفى **ماكلين** بجامعة **هارفرد** وبدأت تلك العيادات تقدم خدماتها الإرشادية والعلاجية.

---

[1] محمد وليد المصري، المرجع نفسه، ص172.

[2] شريف درويش اللبان، تكنولوجيا الاتصال، المخاطر و التأثيرات الاجتماعية، ط1، دار المصرية اللبنانية، القاهرة، 2002، ص 25-27.

إن مجمل الاستراتيجيات العلاجية يجب أن تنطلق من الإرشادات والصائح التي تخفف من وطأة هذه المشكلة وتساعد المدمنين على الوصول إلى شاطئ الأمان أهمها:

أ- أسلوب الضبط الذاتي:

- تعويد المدمن على أسلوب كبح جماع نفسه.
- ممارسة الرياضية أو التواصل مع الأهل والأصدقاء بدل تصفح الإنترنت.
- تحديد وقت الدخول إلى الشبكة وبساعة واحدة كضبط خارجي.
- الرقابة الأسرية التي تحدد ساعات استخدام الانترنت ومجالاتها.

ب- علاج متلازمة النفق الرسغي: عادة تعالج بإعطاء المريض فيتامينB، نصح المريض بإضافة المكملات الغذائية، تجنب تناول الأغذية الغنية بالحديد، عدم الإفراط في تناول الأطعمة التي تحتوي على فيتامين E(إتباع حمية لعلاج تناذر النفق الرسغي)[1].

ج- العلاج التبصري: يرتكز على اعتراف الشخص بأنه مدمن، وهذه خطوة مهمة في العلاج وبالتالي عليه أن يتحمل جزء من مسؤوليته في العلاج.

د- العلاج الأسري: غرس في نفوس الأبناء أهمية الانترنت في الاستكشاف والبحث العلمي الذي يفيد الذات والمجتمع، التعرف على مشاكل الأبناء، زيادة مساحة الحوار في إطار الاحترام المتبادل حتى لا يسعى هذا المراهق نحو البحث عن آذان صاغية عبر الانترنت والتي يجهل محتواها وأهدافها. أما **(يونغ)** فتقترح طرق عديد لعلاج الإدمان على الانترنت، حيث أنشأت موقعا خاصا لعلاج الإدمان على الانترنت، يتلقى ويستقبل الموقع زواره 24/ 24ساعة وبدون انقطاع، وأهم ما أضافته**(يونغ)** في خطتها العلاجية:

- ❖ إعداد بطاقات من أجل التذكير بأهم المشاكل الناجمة عن استخدامه للإنترنت وكلما اندمج في الاستخدام يخرج هذه البطاقات.
- ❖ إعادة توزيع الوقت والانضمام إلى مجموعات التأييد كعلاج جماعي يساعد في تعزيزه وتحفيزه نحو الإقلاع عن استخدام انترنت [2].

[1] محمد وليد المصري، المرجع السابق، ص 174.

[2] كمبرلي يونغ، مرجع سابق، ب سنة ، ص362،ص363.

الخاتمة

خاتمة

لقد أدى التطور الكبير والمتسارع للوسائل التكنولوجية الحديثة، والتحول إلى العالم الرقمي لخلق مجموعة من أخطر الجرائم التي يشهدها العالم، وهي الجرائم الالكترونية التي صارت تهدد فئات المجتمع دون استثناء، الأمر الذي دفع أغلب الدول إلى تخصيص مجموعة من القوانين والأليات القانونية للحد منها ومكافحتها.

وإزاء التطور العلمي الهائل، فإن المزايا التي جلبتها المعلوماتية قد جلبت إلى جانبها أيضا مخاطر عدة ناجمة عن إساءة استخدام شبكة الانترنت وتطويعها لصالح المجرم المعلوماتي لممارسة نشاطاته الإجرامية، حيث سهلت ظهور طائفة جديدة من الجرائم المستحدثة، بالإضافة إلى إمكانية ارتكاب الجرائم التقليدية، والتي تعجز النصوص العقابية في مواجهة أغلب صورها المستحدثة، فالقوانين الجنائية التقليدية_ الموضوعية والإجرائية_ باتت قاصرة عن مواجهة الجرائم المرتكبة عبر الإنترنت، فلابد أن تكملها استراتيجيات مختلفة على المستوى الفني والتقني والقضائي، وذلك لمراقبة الأمن في مجال تقنية المعلومات أو في مجال التدريب، أو حتى في مجال التعاون والتنسيق الدولي لمواجهة هذا النوع المعقد من الاجرام.

بالإضافة إلى الجانب التوعوي الذي يمكن أن تساهم فيه الجهات الأمنية المختصة والجامعات والمساجد والأسر لتوضيح الصورة عن مدى خطورة هذه الجريمة لدى مختلف الفئات، خاصة المتمدرسة منها لأننا في بلدنا على مشارف مرحلة ستلعب فيها الوسائل الإلكترونية الأداة الرئيسية في المنهج التعليمي والتكويني في مختلف المؤسسات على المستوى الوطني، هاته الوسائل التي ستكون المحرك الرئيسي في الإدارات الجزائرية التي تسعى لأن تكون في مصف الإدارات الالكترونية المتطورة، وهو سبب من الأسباب التي ستزيد من نسبة المدمنين على الانترنت والوسائل الالكترونية عامة. هذا النوع من الإدمان الذي لا يقتنع الكثيرون بأنه مرض من أمراض التكنولوجيا الحديثة، التي تستوجب الخضوع للعلاج، هذا النوع من العلاج الذي سيكون مستقبلا كنوع من أنواع العقاب تلجأ إليه الجهات القضائية في معاقبة الجرائم الالكترونية البسيطة، وبالأخص التي يكون مرتكبوها صغار السن.

لقد خلصت هذه الدراسة إلى جملة من النتائج والتوصيات والمتمثلة في:

أولا: النتائج

1 – أول ما تم استنتاجه هو عدم وجود تعريف جامع مانع للجريمة الالكترونية.

2– لم يضع المشرع الجزائري نصا قانونيا خاصا بالجرائم الإلكترونية رغم ما تسببه هذه الجرائم من اضرار على المجتمع والدولة معا. خاصة وأن الجزائر تتجه نحو رقمنة الإدارة الجزائرية بما يتماشى مع العصرنة الحاصلة في العالم.

3– الدليل الالكتروني له طبيعة خاصة تستدعي التعامل معها بحذر، خاصة حين القيام بعملية التفتيش والضبط، لأن المجرم الالكتروني لديه خبرة جيدة في اخفائها ما ينتج عنه من أدلة.

4– آليات المكافحة الحالية غير كافية لمجابهة الجريمة الإلكترونية، فلا يمكن لأي دولة مهما بلغ تطورها الإلكتروني ان تتصدى لهذه الجريمة العالمية بمفردها، فالمجرم الالكتروني قد يكون في دولة ما وينفذ جريمته الإلكترونية في دولة ثانية، وبالإمكان أن تتحقق نتيجتها في دولة ثالثة، أو حتى في عدة دول، مما يصعب عملية متابعته، خاصة في حالة عدم وجود اتفاقية بين الدولة التي يتواجد على أرضها.

5– شكلت الهيئة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها محور اهتمام العديد من السلطات، مما أدى إلى تعاقب السلطات على ترأسها، بداية من وزارة العدل سنة2015، ثم وزارة الدفاع الوطني سنة2019، لتوضع تحت سلطة رئيس الجمهورية سنة 2020.

6–الإدمان على الانترنت، والمخدرات الرقمية هما حقيقة موجودة رغم إنكارها من قبل الكثيرين، فانشغال الشباب بالساعات بالألعاب الإلكترونية، وسقوط بعضهم في مصيدة مصممي الألعاب الإلكترونية الخطيرة خير دليل على ذلك.

7–تعد مراكز معالجة الإدمان على الانترنت آلية استباقية مهمة للحد من الاستعمال المفرط للإنترنت والذي قد يوقع صاحبه في مخاطر الجرائم الإلكترونية سواء كضحية أو كمرتكب للجريمة الإلكترونية.

ثانيا: التوصيات

1- نناشد المشرع الجزائري بإصدار قانون خاص لمكافحة الجرائم الإلكترونية، وإرفاقه بالآليات الإجرائية والمؤسساتية الكفيلة التي تسهل تلك المكافحة.

2 – لابد من تفعيل آليات التعاون الدولي التي تتسم بسرعة التنفيذ حتى لا يترك للمجرم الالكتروني ملاذ آمن يلتجئ إليه، وتوسيع الاتفاقيات الدولية الثنائية والجماعية لمكافحة الجرائم الإلكترونية.

3 – يتعين على الدولة حجب المواقع المخالفة للقوانين والأخلاق.

4 – نظرا لكثرة الجرائم الإلكترونية وتنوعها، يستحسن إنشاء شرطة مختصة بهذه الجرائم، تكون مهمتها الوحيدة متابعة هذا النوع من الجرائم.

5 – تشجيع البحث العلمي في المجال الجنائي، وبالأخص ما يتعلق بالجريمة الإلكترونية والعمل بنتائجه في السياسة الجنائية.

قائمة المصادر

والمراجع

قائمة المراجع

القرآن الكريم

أولا: النصوص القانونية

1 – المادة 394 مكرر من الأمر 155/66 من قانون العقوبات المؤرخ في جوان 1966، المعدل والمتهم بالقانون 15/04 المؤرخ في 10 نوفمبر 2004، ج ر 71، بتاريخ 10 نوفمبر 2004 ص 11 12.

2 – المادة 01/40 من دستور 1996، ج ر رقم 76 المؤرخة في 8 ديسمبر 1996، المعدل والمتمم بالقانون رقم 16 – 01 المؤرخ في 6 مارس 2016، ج ر رقم 14 المؤرخة في 07 مارس 2016.

03 – الأمر 03 –05 المؤرخ في 19 جويلية 2003، المتعلق بحقوق المؤلف أو الحقوق المجاورة، وكذلك الأمر 03–07 المؤرخ في 19 جويلية 2003، المتعلق ببراءات الاختراع، ج ر رقم 44 المؤرخة في 23 جويلية 2003.

4– المواد 45، 47، 64، من الأمر رقم 22/06 الصادر في 20 ديسمبر 2006، المعدل والمتمم لقانون الإجراءات الجزائية، ج ر العدد 84.

5 – القانون رقم 2000 – 03 المؤرخ في 5 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، ج ر، عدد 48، المؤرخة في 06 أوت 2000.

6 – القانون رقم 09 – 04 المؤرخ في 5 أوت 2000 يتضمن القواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال ومكافحتها، ج ر، عدد 47، مؤرخة في 16 أوت 2009.

7 – قانون رقم 04 – 15 مؤرخ في 2004/11/10 يعدل ويتمم الأمر رقم 66 – 155، يتضمن قانون العقوبات، ج ر، عدد 71، صادرة 2006/12/24.

8- قانون رقم 06-22 مؤرخ في 20 /2006/12 يعدل ويتمم الأمر رقم 66-155، يتضمن قانون الإجراءات الجزائية، ج ر، عدد 48، صادرة بتاريخ 2006/12/24.

9-قانون رقم 20-05 مؤرخ في 28 أبريل سنة 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها.

ثانيا: الكتب

1- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، الاردن ،2008 ص 46.

2 – محمد أمين أحمد الشوابكة، جرائم الحاسوب والإنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان الاردن، 12 – 13 /5 / 2008.

3 – د. سليم عبد الله الجبوري، الحماية القانونية لمعلومات شبكة الإنترنت، الطبعة الاولى، منشورات الحلبي الحقوقية، بيروت لبنان. 2011 ص 292.

5 –د. هدى حامد قشقوش، جرائم الحاسب الآلي، دار النهضة العربية، القاهرة، 1992 ص 8.

6 – بن قارة عائشة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي، دار الجامعة الجيدة، مصر 2010، ص46، 49.

7 – أحمد خليقة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، القاهرة، الطبعة الثانية 2006 ص 87.

8 – أحسن بوسقيعة، التحقيق القضائي، الطبعة الثامنة، الجزائر، دار هومة، 2009، ص 113.

9 – عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر 2007، ص232 – 233.

10 – محمد فتحي، تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة، الطبعة الأولى، القاهرة، المصدر القومي للإصدارات القومية، 2012، تهميش (1) ص 485

ثالثا: الرسائل العلمية

1 – شنتير خضرة، الآليات القانونية لمكافحة الجريمة الإلكترونية (دراسة مقارنة)، أطروحة مقدمة لنيل شهادة الدكتوراه، جامعة احمد دراية، أدرار، كلية الحقوق والعلوم السياسية، سنة 2020 /2021.

2 – نايري عائشة، الجريمة الالكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، جامعة أحمد دراية، ادرار، كلية الحقوق والعلوم السياسية، سنة 2017/2016.

3 – شهرزاد حداد، الدليل الالكتروني في مجال الاثبات الجنائي، مذكر مكملة لنيل شهادة الماستر، جامعة العربي بن مهيدي، أم البواقي، كلية الحقوق والعلوم السياسية، سنة 2017/2016.

4 – بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائري (دراسة مقارنة)، مذكر مكملة لنيل شهادة الماستر، جامعة محمد خيضر، بسكرة، كلية الحقوق والعلوم السياسية، سنة 2016/2015.

5 – صغير يوسف الجريمة المرتكبة عبر الانترنت، مذكرة تخرج لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو2013/03/06 ص42.

6 – محمد شنة، جرائم العنف الأسري وآليات مكافحتها في التشريح الجزائري، أطروحة مقدمة لنيل درجة دكتوراه العلوم في الحقوق، تخصص علم الإجرام وعلم العقاب قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة2017،2018/01 ص 171.

رابعا: المقالات والمجلات

1 – حسين نوارة، آليات تنظيم المشرع الجزائري لجريمة الإعتداد على الحرق في الحياة الخاصة الكترونيا، الملتقى الوطني " آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، الجزائر، 29 مارس 2017، ص 121 – 122.

2 – حمودة سليمة، الإدمان على الأنترنيت، اضطراب العصر، مجلة العلوم الإنسانية والاجتماعية، العدد 21، ديسمبر (2015) جامعة قاصدي مرباح ورقلة (الجزائر).

3 – مجلة العلوم السياسية والقانون، مجلة علمية دولية محكمة تصدر فصليا عن المركز الديمقراطي العربي برلين – ألمانيا – باحثة دكتوراة سورية ديش، أنواع الجرائم الالكترونية وإجراءات مكافحتها، جامعة سيدي بلعباس (الجزائر)، العدد الأول جانفي2017.

4 – بوعناد فاطمة الزهراء، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول /2013، جامعة الجيلالي الياس، سيدي بلعباس، كلية الحقوق والعلوم السياسية.

5 – د. بوضياف إسمهان، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 11، سبتمبر 2018.

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

7–د. بن عودة نبيل، أ. نوار محمد، الصلاحيات الحديثة للضبطية القضائية للكشف وملاحقة مرتكبي الجرائم المتعلقة بالتمييز وخطاب الكراهية،" التسرب الإلكتروني نموذجا"، مجلة الأكاديمية للبحوث في العلوم الاجتماعية، المجلد 01/العدد 02(2020) ص319–334.

8-د. درعي العربي، خصوصية إجراءات الضبط القضائي في جرائم التمييز وخطاب الكراهية وفق القانون 20-05، مجلة حقوق الإنسان والحريات العامة (م.ح.إ.ح.ع) المجلد 6 العدد 2 سنة 2021 صمن 211-232.

الفـــــهـــرس

الملخص

الملخص:

لقد عرفت البشرية مرحلة من التطور التكنولوجي خاصة المعلوماتي، والذي كثر معه استعمال الوسائل الإلكترونية، التي تعتبر أشد خطورة لأنها تشكل تهديدا كبيرا على أمن الدولة والمجتمعات والأفراد معا، الأمر الذي جعلها من مواضيع البحث العلمي القانوني، تثير عدة إشكاليات تستوجب الوقوف عندها.

وما دراستنا هذه إلا نموذج عن الدراسات السابقة، حيث تضمنت هذه المذكرة مفهوما للجريمة الإلكترونية وبيان دوافع ارتكابها، وخصائصها وأنواعها، وضمت أيضا مجموعة من الآليات القانونية التي سيكون لها دور كبير في مكافحة هذه الجرائم الإلكترونية، من بينها آليات قانونية وإجرائية وآليات قانونية مؤسساتية لمكافحة الجريمة الإلكترونية، بالإضافة إلى آليات مساعدة على مكافحة الجريمة الإلكترونية، كالجمعيات ومراكز معالجة الإدمان على الإنترنت.

كلمات مفتاحية: جريمة إلكترونية، أدلة إلكترونية، آليات مكافحة.

Abstract :

The humanity has witnessed a phase of technological development, especially in the field of information, which in creased the use of electronic means, This latter Play an effective role in making Our life easier, but in the Othre Sid, It leaded to the appeorance of the cybercrim , which Is Considered as a dangereuse one, since It threatened enormously the state Security, society and citizens.

Consequently, it becomes one of the legal scientific topic researches That should be studied. Our study Is a sample of the pevions studies, since This report includes thre concept, of the cybercrime, the catalysts for comintting it, its features and its types also, It conlaines a set of legal mechanisms, that will contribute to fight these cyber crimes.

Legal, procedural and institutional mechanisms to combat the cyberimes.Inaddition to the helping mechanisms to fight against the cyber crimes suchas, associations and internet addiction recovery centers.

Key words: Electronic Crime, Electronic Evidence, Control Mechanisms.