جـــــامعة غـــــرداية

كليـــــة الحقوق والعلـــوم السياسيـــة

قسم الحـــــقوق

جريمة القرصنة الإلكترونية في التشريع الجزائري

مذكرة مقدمة ضمن متطلبات نيل شهادة ماستر اكاديمي حقوق

تخصص قانون جنائي وعلوم جنائية

إعـداد الطـالبتين:

- دحو نجاة
- أولاد علي فاطمة

إشـــراف الأستـــاذ:

* اولاد النـوي مـــراد

لجنة المناقشة

الاسم واللقب	الرتبة	الجامعة	الصفة
بن فردية محمد	أستاذ محاضر "أ"	غرداية	رئيسا
أولاد النوي مراد	أستاذ محاضر "أ"	غرداية	مشرفا
هوام نسيم	أستاذ مساعد محاضر "أ"	غرداية	مناقشا

السنة الجامعية 2021 -2022

إهـــداء

الحمد لله وكفى والصلاة على الحبيب المصفى وأهله ومن وفى أما بعد:

الحمد لله الذي وفقنا لتثمين هذه الخطوة في مسيرتنا بمذكرتنا هذه

ثمرة الجهد والنجاح

أهدي نجاحي إلى من أوصانا الله بهما برا واحسانا الراحلين من الدنيا والباقين في قلبي بحر الحب والحنان والدي رحمه الله الذي كان سندي في حياتي ، والدتي جنتي ملاكي الطاهر رحمهما الله وغفر لهما

إلى العائلة الكريمة التي ساندتني ولا تزال تساندني

إلى من تحملت معي عناء هذه المذكرة فاطمة

إلى زملائي زميلاتي

إلى كل من كان لهم أثر على حياتي وإلى كل من أحبهم قلبي ونسيهم قلمي

إلى الذين مضوا والذين سيأتون من بعدنا

نجـــاة

إهـــــداء

الحمد لله الذي وفقنا لهذا ولم نكن لنصل إليه لولا فضل الله علينا أما بعد

أهدي هذا العمل المتواضع إلى أمي فاطنة رحمها الله التي كانت تسهر وتتمنى دائما لي النجاح

إلى أبي العزيز حميدة أطال الله في عمره

إلى أخواتي دون استثناء

إلى رفيقتي في هذه المهمة دحو نجاة

إلى رئيسي في العمل وكل الزملاء

فاطمة

شكر وعرفان

قال الله تعالى " فاذكروني اذكركم وأشكروا لي ولا تكفروني"

قال صلى الله عليه وسلم" من لم يشكر الناس لم يشكر الله"

الحمد لله على نعمه وصلاته وسلامه على خاتم الأنبياء فبعد شكرنا لله عز وجل خيرا المتوكل عليه لا يسعنا في هذا المقام إلا توجيه أسمى عبارات الشكر والتقدير إلى أستاذنا المشرف الأستاذ أولاد النوي مراد الذي أمدنا بيد العون لإنجاز هذا العمل وجعله يرى النور باعثا فينا روح المسؤولية وحب العمل، والذي لم يتوانى للحظة في مساعدتنا وفي إسداء النصح لنا ولم يصعب أو يعقد علينا تنفيذ عملنا وعلى ما أمدنا به من نصح ورأي سديد فنتقدم لك بعميق الإمتنان وخالص التقدير داعين الله عز وجل أن يديمك في خدمة العلم وينتفع بك طلاب العلم، فحياك الله أستاذنا الفاضل

ونتقدم بالشكر والعرفان إلى كل أساتذة تخصص القانون الجنائي والعلوم الجنائية: رابحي قويدر، الأخضري فتيحة، الحاج ابراهيم عبد الرحمان، بن حمودة مختار، فروحات سعيد، لغلام عزوز الذين لم يبخلوا علينا بالنصح والإرشاد، راجين من المولى عز وجل أن يجعل ما غنمناه منهم صدقة جارية تضاف إلى ميزان حسناتهم

ولا ننسى أن نشكر الطاقم الإداري بكلية الحقوق

وفي الأخير نتمنى أن تكون هذه المذكرة في المستوى المطلوب

ليس علينا أن نصيب الحقيقة ولكن علينا أن نحاول، إن أصبنا فذلك ما نبتغيه وإلا فلنا أجر المجتهد

نجاة- فاطمة

الملخص

تهدف هذه الدراسة إلى التعرف على جريمة القرصنة الإلكترونية و التي تعتبر من أخطر أنواع الجرائم الإلكترونية لما لها من آثار سلبية على النظام المعلوماتي من حيث الإعتداء على المعلومات بالحذف أو التغيير أو الإتلاف، وفي هذه الدراسة قمنا بدراسة الإطار المفاهيمي لهذه الجريمة والجوانب الموضوعية والإجرائية التي اتبعها المشرع الجزائري للحد من هذه الجريمة ومكافحتها و أبرز المشاكل القانونية التي تحيط بجريمة القرصنة الإلكترونية.

الكلمات المفتاحية: الجرائم الإلكترونية – القرصنة الإلكترونية – النظام المعلوماتي – المكافحة.

Abstract

This study aims to identify the crime of cyber hacking which is considered one of the most dangerous types of cyber crimes because of its negative effects on the information system in terms of attacking information by deleting, changing or destroying. In this study, we have studied the conceptual framework of this crime and the substantive and procedural aspects that the Algerian legislator followed to reduce and combat this crime and the most prominent legal problems surrounding the crime of cyber hacking .

Key words : cyber crimes - cyber hacking - the information system – combat.

مـــقدمـــة

بما أن الوسائل العلمية التقنية لم تخترع الجريمة بل كانت ضحية لها حيث أن هذه الوسائل قد استعملت بشكل سيء ومضر وقام المجرمين بتوظيف هذه الوسائل بما يخدم نشاطاتهم الاجرامية وكنتيجة لهذه النشاطات ظهرت الجرائم المعلوماتية، حيث تعدت الجريمة بعدها الواقعي إلى الافتراضي، وعرفت انتشارا رهيبا، محطمة بذلك كل القيم والمفاهيم بسبب التطور السريع لثورة الاتصالات وتكنولوجيا المعلومات وقد زادت أهمية تلك المعلومات في هذا العصر الذي أطلق عليه عصر المعلومات، كونها أصبحت بمثابة المادة الخام التي يقوم عليها التطور الحادث في شتى مجالات الحياة المختلفة، حتى أطلق عليها بالبترول الرمادي، بحيث يمكن القول بأن من يمتلك الكم الهائل من المعلومات، بلا شك يمتلك حضارة يتفوق بها عن من هو أقل منه في امتلاكها، كما أنها تعد أساس عمل النظام المعلوماتي، ولهذا السبب أصبحت محلا للاعتداء عليها بحذفها أو تغييرها أو إتلافها وهو ما يطلق عليها بجريمة القرصنة الإلكترونية وهي موضوع دراستنا والتي تعد من أهم الجرائم الاكترونية، حيث أصبح بإمكان القرصان المعلوماتي اليوم كسب مليارات الدولارات دون التحرك من مكانه ودون الحاجة إلى عدد كبير من الأفراد أو المعدات، فيكفي وجود حاسب إلكتروني موصول بشبكة الأنترنت للحصول على أي معلومة على شبكة الأنترنت و هذا هو عصر المعلوماتية أو ما يصطلح على تسميته بالعصر الرقمي.

ونتيجة لكثرة وقوع هذه الجرائم قد شهد المجال القانوني تدخلا في تنظيم تلك الظاهرة المعلوماتية وتجريمها من خلال الاتجاهات التشريعية والقضائية والفقهية الحديثة فنجد أن أغلب الدول بادرت في إصدار الدولية وإصدار قوانين خاصة بهذا النوع من الجرائم من أجل تحديد المسؤول عن هذه الجرائم ومعاقبته وتقديم الحماية القانونية للمتضررين، والمشرع الجزائري بدوره استحدث نظم قانونية جديدة لمواجهة التحديات التكنولوجية المعاصرة نظرا لعدم مواكبة هذه الأفعال للتشريعات التقليدية وذلك بتعديل قانون العقوبات الجزائري وقانون الإجراءات الجزائرية،

وحتى استحداث قوانين جديدة وذلك لتحقيق التوازن بين الحماية الجنائية لحرمة الحياة الخاصة التي يكفلها الدستور، حيث خلف الفراغ القانوني أثره على نمو الاجرام المعلوماتي سواء كانت هذه الانشطة الاجرامية المتصلة بتكنولوجيات المعلومات وسيلة أم محل لهذه السلوكيات، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة على المستويين الدولي والوطني.

لموضوع جريمة القرصنة الإلكترونية أهمية بالغة كانت دافعا لاختياره وتناوله بالبحث والدراسة، بتوضيح مختلف المفاهيم المبهمة المحيطة بالموضوع وذلك للخطورة التي تتميز بها هذه الجريمة المستحدثة كونها سهلة الارتكاب نتيجة الاستخدام السلبي للتقنية المعلوماتية.

ومن أسباب إختيارنا لدراسة هذا الموضوع ومن بين أسباب اختيارنا لدراسة هذا الموضوع هو التطور الهائل والتقدم في الأنظمة المعلوماتية الذي ساهم بشكل مباشر في تطور الجرائم المعلوماتية بصفة عامة و جريمة القرصنة الإلكترونية التي تعتبر احدى صور تلك الجرائم، وكذلك ندرة الدراسات التي تناولت جريمة القرصنة الالكترونية.

تهدف هذه الدراسة إلى تسليط الضوء على جريمة القرصنة الالكترونية اذ ان اغلب الدراسات تطرقت الى الجرائم الالكترونية بصفة عامة، و دراسة وتحليل القوانين التي سنها المشرع الجزائري لمكافحة والحد من هذه الجرائم و تحديد المسؤولية الجنائية عند ارتكاب جريمة القرصنة وبالتأكيد تزويد المكتبة الجامعية بمذكرة تعالج الظاهرة .

ومن بين الدراسات السابقة لموضوع القرصنة الإلكترونية قمنا بالاستعانة بدراسة الباحثين عبابسة فاروق و عبوب خديجة التي كان موضوعها القرصنة الإلكترونية وأثرها على المستخدم وهي مذكرة لنيل شهادة الماستر في الإعلام والإتصال، حيث تناول الباحثان فيها الإطار المفاهيمي للقرصنة الإلكترونية من حيث دراسة المصلحات المحيطة بالجريمة إلى واقع القرصنة الإلكترونية في الجزائر وأهم مظاهرها.

الدراسة الثانية كانت للباحث فايز محمد راجح غلاب وهي أطروحة دكتوراه في القانون الجنائي والعلوم الجنائية تحت عنوان الجرائم المعلوماتية في القانون الجزائري واليمني، حيث تطرق فيها الباحث لدراسة أهم أنواع الجرائم المعلوماتية والتي كان من بينها جريمة القرصنة الإلكترونية وذلك بدراسة أركانها ومظاهرها والعقوبة الموقعة على مرتكبيها وإجراءات البحث عن الأدلة فيها.

من بين الصعوبات التي واجهتنا في دراستنا لموضوع جريمة القرصنة الإلكترونية هي موضوع البحث وذلك لأن أغلب الدراسات تناولت دراسة الجرائم المعلوماتية عامة ولم تسلط الضوء على دراسة كل صور من هذه الجرائم بشكل مفصل، مع أننا لا ننكر أن هناك العديد من المقالات والمداخلات التي قامت بدراسة صور الجريمة المعلوماتية بتفصيل كل صورة على حدى ولكنها جاءت بشكل سطحي ومختصر.

من خلال ما سبق يمكن رح الإشكالية التالية: كيف تصدى المشرع الجزائري لجريمة القرصنة الإلكترونية وفيها تكمن أبرز المشاكل القانونية التي تحيط بجريمة القرصنة الإلكترونية، وتندرج عن هذه الإشكالية تساؤلات فرعية وهي كالتالي:

- ماهي جريمة القرصنة الالكترونية من بين الجرائم المعلوماتية؟
- ماهي مميزات جريمة القرصنة عن غيرها من الجرائم؟
- ماهي عقوبة جريمة القرصنة الالكترونية وما هي اجراءات مكافحة الجريمة؟
- ماهي إجراءات الحصول على الأدلة في هذه الجريمة؟
- فيما تتمثل الجهود الأمنية لمحاربة هذه الجريمة؟

للإجابة على هذه الإشكالية اعتمدنا في دراستنا لهذا البحث المنهج الوصفي وذلك في تحديد المفاهيم المتعلقة بجريمة القرصنة الالكترونية ووصف الجانب الإجرائي منها، واعتمدنا كذلك على المنهج التحليلي وذلك في تحليل المواد القانونية واستخلاص معانيها.

قد قمنا بتقسيم موضوع دراستنا إلى فصلين حيث تناولنا في الفصل الأول: الإطار المفاهيمي لجريمة القرصنة الإلكترونية وذلك بإبراز مفهومها ومظاهرها وأسباب وقوعها والخصائص التي تتميز بها ، أما الفصل الثاني خصصناه لدراسة مكافحة جريمة القرصنة والذي يتمحور حول الجوانب الموضوعية والإجرائية لهذه الجريمة، وختمنا بحثنا بتوضيح أهم النتائج الي توصلنا لها من خلال دراستنا لهذا الموضوع وقمنا بتقديم إقتراحات التي خلصنا لها بعد هذه الدراسة.

الفصل الأول

دراسة الجرائم المعلوماتية بصفة عامة تثير العيد من التساؤلات المفاهيمية والإجرائية وفي هذه الدراسة سنقوم بالتطرق إلى صورة من صور هذه الجرائم وهي جريمة القرصنة الإلكترونية وذلك بدراسة طبيعتها وما تتمتع به من خصوصية وما يميزها عن غيرها من الجرائم وطريقة مكافحتها والحد منها، وقد قمنا بتقسيم هذه الدراسة إلى فصلين حيث خصصنا الفصل الأول إلى دراسة الإطار المفاهيمي لجريمة القرصنة الإلكترونية حيث خصصنا المبحث الأول لدراسة مفهوم جريمة القرصنة، أما المبحث الثاني فخصصناه لدراسة أنواع جريمة القرصنة الإلكترونية وخصائصها، أما الفصل الثاني فتطرقنا فيه إلى مكافحة جريمة القرصنة الإلكترونية في التشريع الجزائري وقسمناه هو بدوره إلى مبحثين خصصنا المبحث الأول لدراسة الجوانب الموضوعية لجريمة القرصنة في التشريع الجزائري، أما المبحث الثاني فدرسنا فيه الجوانب الإجرائية لجريمة القرصنة الإلكترونية.

المبحث الأول: مفهوم جريمة القرصنة الإلكترونية

قبل التطرق لدراسة جريمة القرصنة الإلكترونية يجب علينا دراسة الجريمة المعلوماتية وتحديد فيجب المقصود منها، حيث تعددت التعريفات التي تناولتها وكما قيل وبحق فإنها تستعصي على التعريف أو تقاوم التعريف il résiste de la définition ولعل أقرب التعريفات إلى موضوع بحثنا ذلك التعريف الذي ينظر إليها على أنها جريمة المعالجة الآلية للبيانات فيعرفها بأنها " أي عمل يضر بالأشخاص أو الأموال ويوجه ضد أو يستخدم التقنية المتقدمة لنظم المعلومات" أو بأنها " كل فعل او امتناع من شأنه الإعتداء على الأموال المادية أو المعنوية، ويكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[1].

وكتعريف أكاديمي يمكننا القول انها :" كل فعل اجرامي متعمد أيا كانت صلته بالمعلوماتية[2] ترتبت عنه خسارة تلحق بالضحية أو مكسب يحققه الجاني"[3] ، وفي تعريف آخر تعرف بأنها: " جريمة ذات طابع مادي، والتي تتمثل في كل سلوك غير قانوني من خلال استخدام الأجهزة الإلكترونية، ينتج منه حصول المجرم على فوائد مادية أو معنوية مع تحصيل

---

[1]– بكرى يوسف بكرى: التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الاسكندرية، ط1، 2011،ص ص 89-90.

[2]–المعلوماتية كلمة مكونة من مقطعين، المقطع الأول Information و المقطع الثاني Automatique ويرجع الفضل في اقتراح مصطلح المعلوماتية إلى الأستاذ Drefus حيث استخدمه عام 1962 لتمييز المعالجة الآلية للمعلومات وتبنته بعد ذلك الأكاديمية الفرنسية في أبريل 1966 ومنحته التعريف الآتي: علم المعالجة المنطقية للمعلومات التي تعتبر بمثابة دعامة للمعارف الإنسانية والاتصالات في المجالات الفنية والاقتصادية والاجتماعية وذلك باستخدام معدات آلية"، أنظر نهلا عبد القادر المومني: الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط1،2008، ص46.

[3]– عز الدين عز الدين: الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، ملتقى حول الجرائم المعلوماتية، قيادة الدرك الوطني، وزارة الدفاع الوطني، بسكرة في 16 نوفمبر 2015، ص3.

الضحية خسارة مقابلة وغالبا ما يكون هدف الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات الموجودة في الأجهزة ومن ثم ابتزاز الأشخاص باستخدام المعلومات،[1] و من التدقيق في التعريفات الواردة في بيان جريمة الحاسوب يتضح أن هناك صعوبة يواجهها الفقه في تعريف الجريمة المعلوماتية –لها أسبابها– فالظاهرة الإجرامية برمتها المتصلة بالحاسوب جديدة، والاجتهاد التشريعي والقضائي والفقهي مازال في بدايته[2]، وعلى هذا الأساس سنقوم بدراسة هذا المبحث بتقسيمه إلى مطلبين، سنتناول في المطلب الأول تعريف جريمة القرصنة الإلكترونية، أما المطلب الثاني فسنقوم فيه بدراسة أسباب ومظاهر هذه الجريمة.

المطلب الأول: تعريف جريمة القرصنة الالكترونية

سنقوم بتقسيم هذه الجزئية إلى فرعين، الأول منهما خصصناه إلى نشأة القرصنة الإلكترونية أما الفرع الثاني فدرسنا فيه التعريف القانوني لجريمة القرصنة الإلكترونية.

الفرع الأول: نشأة القرصنة الإلكترونية بدأت ظاهرة القرصنة والاختراق مع بداية ظهور الحاسبة الالكترونية وازدادت بشكل كبير مع استخدام تقنية الشبكات، حيث يشمل الاختراق الهجوم على شبكات الحاسوب من قبل مخترقي الأنظمة و المواقع الالكترونية ومنتهكي القوانين، غير أن القرصنة لا تمس الشبكة العنكبوتية فقط، بل تمتد إلى تقنيات أخرى

[1]– لطرش فيروز، بن عزوز حاتم: الجريمة الإلكترونية في الجزائر: من جريمة فردية إلى جريمة منظمة، مجلة آفاق للعلوم، جامعة زيان عاشور الجلفة، العدد01، مجلد 01، 2016، ص324.

[2]– علي حسن محمد الطوالبة: التفتيش الجنائي على نظم الحاسوب والأنترنت – دراسة مقارنة– أطروحة دكتوراه في القانون الجنائي، جامعة عمان العربية للدراسات العليا، كلية الدراسات القانونية العليا، 2003، ص ص 59–60.

كالاتصالات والبرمجيات ، ذلك أن عمليات القرصنة تطورت بسرعة فائقة، وأصبح من الشائع جدا العثور على مواقع بالانترنت خاصة لترويج البرامج المقرصنة مجانا أو بمقابل مادي رمزي.[1]

الفرع الثاني: التعريف القانوني لجريمة القرصنة الالكترونية:

عرفتها إتفاقية بودابست في المادة 4 منها تحت مصطلح التدخل في البيانات حيث جاء في نصها: "تعتمد كل دولة طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى لتجريم الأفعال التالية في قانونها الوطني، إذا ما ارتكبت عمدا، وبغير حق: إتلاف، محو، أو إفساد، أو تعديل، أو تدمير بيانات موجودة على كومبيوتر" وأضافت مصطلح التدخل غير المشروع في المنظومة وذلك في المادة 5 منها.

يمكن تعريف القرصنة الالكترونية على أنها: "عملية اختراق لأجهزة الحاسوب او المواقع تتم عبر شبكة الانترنت غالبا لأن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة أو حتى عبر شبكات داخلية يرتبط بها أكثر من جهاز حاسب ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في اختراق برامج الحاسوب وطرق إدارتها أي أنهم مبرمجون ذو مستوى عالي ستطيعون بواسطة برامج مساعدة اختراق حاسوب معين للتعرف على محتوياته ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة[2]

[1]– عبابسة فاروق، عبوب خديجة: القرصنة الإلكترونية وأثرها على المستخدم، مذكرة لنيل شهادة الماستر تخصص إعلام واتصال، جامعة عبد الحميد ابن باديس مستغانم،2016/2015، ص40.

[2]– نفسه، ص43.

وتشمل جريمة القرصنة الالكترونية جرائم الإدخال ، الإتلاف المحو، أو الطمس لبيانات أو برامج الحاسب الآلي، الإضرار ببيانات وبرنامج الحاسبات ويشمل المحو والإتلاف، التعطيل أو الطمس غير المشروع لبيانات وبرامج المعلومات، تخريب الحاسبات ويحتوي على: الإدخال، الإتلاف، المحو، الدخول غير المصرح به وهو: الدخول غير المشروع لنظام معلوماتي أو مجموعة نظم، الإعتراض غير المصرح به وهو: الذي يتم بدون وجه حق عن طريق استخدام وسائل فنية للإتصال،[1] وفي تعريف آخر تعرف بأنها: " الدخول أو إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات والمعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي"[2]

المطلب الثاني: مظاهر وأسباب جريمة القرصنة الإلكترونية

سنقوم بتقسيم هذه الدراسة إلى فرعين، حيث سنخصص الأول لدراسة مظاهر جريمة القرصنة الإلكترونية، أما الفرع الثاني فسندرس فيه أسباب هذه الجريمة.

[1]–خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، الاسكندرية، س2010، ص ص211–212.

[2]–جمال زين الدين العابدين أمين أحمد: جرائم إختراق النظم الإلكترونية بين التشريع المصري والمغربي، مجلة مستقبل العلوم الاجتماعية،جامعة عبد الملك السعدي، العدد الأول، أفريل 2020، المغرب، ص9.

الفرع الأول: مظاهر جريمة القرصنة الإلكترونية

وفي هذه الدراسة سنقوم بدراسة مظاهر القرصنة الإلكترونية بصفة عامة ومظاهرها بصفة خاصة في الجزائر، حيث تتمثل مظاهر جريمة القرصنة الإلكترونية في العديد من الأشكال التي نذكر منها:

قرصنة البرمجيات: ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى

قرصنة البيانات: والمعلومات ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة البطاقات الإئتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر

القنابل البريدية: وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملغومة[1].

أولا: مظاهر القرصنة عامة: هناك حوالي 80% من أعمال الجريمة الإلكترونية تنشأ في شكل من أشكال النشاط المنظم، مع سوق الجرائم الإلكترونية الأسود، على شكل عمل دورة البرمجيات الخبيثة، وفيروسات الكومبيوتر، وإدارة الروبوتات، وحصاد البيانات المالية، وبيع البيانات وقبض ثمن المعلومات المالية حيث لم يعد يحتاج مجرمو الجرائم الإلكترونية مهارات أو تقنيات معقدة، على الصعيد العالمي تظهر أفعال الجريمة الإلكترونية انتشارا واسعا عبر أعمال مدفوعة ماليا وأعمال ذات صلة بمحتوى الكومبيوتر، وكذلك العمل ضد السرية والسلامة والوصول إلى أنظمة الكومبيوتر، و تختلف تصورات المخاطر والتهديد النسبي بين الحكومات

[1]– ذياب موسى البداينة، مرجع سبق ذكره، ص23.

ومؤسسات القطاع الخاص، حاليا لا تمثل إحصاءات الجريمة المسجلة لدى الشرطة أساسا سليما لإجراء مقارنات عبر الوطنية على الرغم من أن هذه الإحصاءات غالبا ما تكون هامة لرسم السياسات على المستوى الوطني، يرى ثلثي الدول أن أنظمتها غير كافية لإحصاءات الشرطة في تسجيل الجريمة الإلكترونية، وترتب سجلات الشرطة للجريمة مع مستويات الدولة التنموية وقدرة الشرطة المتخصصة.[1]

ففي الولايات المتحدة مثلا تمت جريمة قرصنة أرقام بطاقات الدفع المغناطيسية بما يقارب 1.7 مليون بطاقة دفع مقرصنة، مما أدى إلى خسائر قدرت بـ 4.3 مليون دولار،[2] وقد ارتفعت الخسارة الناجمة عن الجرائم المعلوماتية مقارنة بالجرائم العادية إذ حسب تقرير المركز الوطني للبيانات (NCCCD) أنه في 21 جوان 1999 للباحث Pernard D Standlar أن إجمالي الخسائر الناجمة في الشهر بلغت حوالي 810000 دولار أي ما يساوي 800 بليون دولار سنويا، وتوصل مكتب التحقيقات الفيدرالي FBI إلى أن متوسط الخسارة التي تخلفها الجريمة المعلوماتية يبلغ حوالي 500000 دولار في حين لا تزيد الخسارة التي تخلفها جرائم السرقة العادية 3500 دولار[3].

[1]– ذياب موسى البداينة، المرجع السابق ذكره، ص9.

[2]– لطرش فيروز، بن عزوز حاتم، مرجع سبق ذكره، ص329.

[3] –Rose (philipe) la criminalité informatique à l'horizon 2005 – analyse prospective, l'harmattan, 1992.p 49.

ثانيا: مظاهر القرصنة في الجزائر

إن المتتبع لظاهرة القرصنة الإلكترونية في الجزائر يدرك التناقض الذي يميز هذه الظاهرة، ففي حين لا يزال تصنيفها في مؤخرة التقنية التكنولوجية، تبقى تحتل المراتب الأولى في مجال القرصنة الالكترونية، حيث تشير التقارير والمعطيات المنشورة من قبل الهيئات المختصة والصحافة الوطنية إلى أن الجزائر تأتي على رأس البلدان العربية في ميدان القرصنة، كما أنه اختراق البرامج المعلوماتية يهم القراصنة الجزائريين وذلك لنزع الشفرة لباقات القنوات التلفزيونية الرقمية مثلا، فعلى سبيل المثال فإن منتدى تبادل شفرات الدخول للباقات التلفزيونية المشفرة فإن الجزائريين يوجدون على رأس القائمة، ففي متوسط 40ألف متصل يوميا، 9آلاف منهم جزائريون ويستعملون القرصنة كلمات سرية عن طريق برامج معروفة في هذا الميدان والمتواجدة في السوق الوطنية.[1]

الفرع الثاني: أسباب جريمة القرصنة الاكترونية

تتشارك جريمة القرصنة الإلكترونية مع الجريمة المعلوماتية في أغلب الاسباب ببيعة الحال لأنها صورة من صورها ومن بين هذه الأسباب نذكر ما يلي:

البطالة: حيث ترتبط الجريمة المعلوماتية شأنها شأن الجرائم التقليدية بالبطالة والظروف الاقتصادية الصعبة وترتكز البطالة بنسبة كبيرة في فئة الشباب، الأمر الذي يدف بعضهم، نحو البحث عن طرق الكسب السهل و السريع للمال ولو بطرق غير مشروعة.

[1]–عبابسة فاروق، عبوب خديجة، مرجع سبق ذكره، ص27.

المنافسة: محاولات الشركات المنافسة الحصول على معلومات تقنية حديثة أو أسرار تكنولوجية أو عسكرية أو معلومات عن البنوك والمعاملات المالية مثل الأسهم والسندات المتعامل بها في البورصات العالمية وذلك بواسطة أشخاص مؤجرين لهذا الغرض.

الدوافع الشخصية: حيث أن الدافع لارتكاب جرائم الكومبيوتر يغلب عليه الرغبة في قهر النام أكثر من شهوة الحصول على الربح، ويميل مرتكبوا جرائم نظم المعلومات إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مركبو هذه الجرائم لديهم شغف الآلة يحاولون إيجاد الوسيلة إلى تحطيمها بل والتفوق عليها، فقد أثبتت إحدى الدراسات أن القراصنة يتملكهم جميعا شعور البحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الكومبيوتر إلى تعويضهم عن الإحساس بالدونية.[1]

وقد جاء في دراسة الأستاذ ذياب موسى البداينة أن الجرائم الإلكترونية تقسم إلى ثلاث أقسام وهي المستوى الفردي، المستوى المجتمعي والمستوى الكوني ونحن سنذكر من بين هذه الأسباب ما له علاقة الوثيقة بجريمة القرصنة الإلكترونية وذلك كما يلي[2]:

أولا: على المستوى الفردي

الفرصة (opportunity): لقد وفرت التقنيات الحديثة والأنترنت فرصا غير مسبوقة لانتشار الجريمة الإلكترونية، حيث أن الفرصة تنتج الجريمة، وتلعب البيئة و ترتيباتها دورا كبيرا في

[1]– رابحي لخضر، بن بعلاش خاليدة: معالجة الجرائم المعلوماتية في ظل التعاون الدولي والاستجابة الدولية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، جامعة محمد خيضر بسكرة، ص 4.

[2]– ذياب موسى البداينة، مرجع سبق ذكره، ص10.

إنتاج الجريمة والخروج على القواعد الاجتماعية، فوقت الانحراف عن قواعد الامتثال ليلا ونهارا وفي أي مكان وعدم وجود رقابة كلها عوامل تزيد من فرصة ارتكاب الجريمة الالكترونية، وقد تشكل المعلومات هدفا سهل المنال ويحقق المنفعة السريعة، فهي فرصة مربحة وقليلة المخاطر واحتمالية الكشف عن الفاعل فيها ضئيلة.

ضبط الذات المنخفض: تنطلق هذه الدراسة من النظرية العامة في السلوك الطائش، وتؤكد أن احتمالية انخراط الأفراد في فعل اجرامي تحدث بسبب وجود الفرصة مع توفر سمة شخصية من سمات الضبط الذاتي المنخفض، فقد يتعرض الأفراد لنماذج التعلم الاجرامي والأقران قد يكونون أكثر ميلا للانخراط في الجريمة الإلكترونية.

ثانيا: على المستوى المجتمعي

البحث عن الثراء: يسعى الإنسان إلى المتعة ويتجنب الألم، ويسعى الناس إلى الوسائل غير المقبولة اجتماعيا لتحقيق أهداف مقبولة اجتماعيا، فالرغبة في الثراء يواجهها صعوبات بالغة في تحقيقه بالرق المقبولة اجتماعيا وقانونيا، ولذا يلجأ بعض الناس إلى الجرائم الالكترونية حيث المستهدف مجتمع أكبر وسهولة التنفيذ وسرعة المردود وقلة الخطورة.

ضعف إنفاذ القانون وتطبيقه في الجريمة الالكترونية: هناك الكثير من الدول التي لم تور تشريعاتها وأجهزة العدالة فيها لكي تتمكن من مجاراة التقدم في الجرائم الالكترونية وأساليبها، وهذا لا يتوقف عند التشريعات وإنما يشمل الشرطة والتحقيق والقضاء، وكيفية التعامل مع الأدلة

الرقمية على المستوى الوطني، كما هو الحال على المستوى الدولي، مما يشعل الجريمة الإلكترونية غياب التشريعات الجزائية والجنائية وضعف الممارسات العدلية والشرطية والقضائية في المحاكمة والتحقيق في الجرائم الالكترونية.[1]

ثالثا: على المستوى الكوني

التحول للمجتمع الرقمي: من اهم سمات عصر المعلومات تداولها بين جميع الأفراد بطريقة رقمية مثل البريد الالكتروني، الجوال..إلخ ففي الفضاء الافتراضي تكونت التفاعلات وحلت محل التفاعل وجها لوجه وتكونت السلوكيات الافتراضية والمجتمع المحلي الافتراضي.

العولمة: إن هور الفضاء الالكتروني يخلق ظواهر جديدة متميزة عن وجود أنظمة الكومبيوتر التي وفرت الفرص المباشرة للجريمة ضمن الفضاء الالكتروني، وذلك من خلال السلوك المادي للأفراد بين الواقع والفضاء الالكتروني، فعلى سبيل المثال قد يرتكبون جرائم في الفضاء الالكتروني لا يرتكبونها في الواقع المادي بسبب مكانتهم وموقعهم، بالإضافة إلى ذلك مرونة الهوية وعدم ظهورها وضعف عوامل الردع تحفز السلوك الإجرامي في العالم الافتراضي.[2]

[1]– ذياب موسى البداينة، المرجع السابق ذكره، ص15.

[2]– نفسه، ص16.

المبحث الثاني: أنواع جريمة القرصنة الإلكترونية وخصائصها

في هذا المبحث سنقوم بدراسة أنواع جريمة القرصنة الإلكترونية والتي خصصنا لها المطلب الأول من المبحث أما المطلب الثاني فسندرس فيه خصائص جريمة القرصنة الإلكترونية وما يميها عن غيرها من الجرائم التقليدية.

المطلب الأول: أنواع جريمة القرصنة الإلكترونية

تتنوع جرائم القرصنة الإلكترونية بتنوع مرتكبيها وقبل دراسة هذه الأنواع سنقوم بالتطرق إلى أنواع القراصنة في الفرع الأول، أما الفرع الثاني فسندرس فيه أنواع جريمة القرصنة الإلكترونية.

الفرع الأول: أنواع القراصنة

تتنوع جرائم القرصنة الإلكترونية بتنوع مرتكبيها وقبل دراسة هذه الأنواع سنقوم بالتطرق إلى أنواع القراصنة بشكل مختصر، حيث ينقسم الجناة في الجرائم المعلوماتية بصفة عامة إلى05 فئات وهي فئة صغار مجرمي المعلوماتية ويقصد بهم الشباب البالغ المفتون بالمعلوماتية وأنظمتها و يجب عدم التقليل من خطورتهم لأن هذه الفئة قد تتعدى مرحلة الهواية وتنتقل إلى مرحلة الاحتراف لهذه الجرائم[1]، الفئة الثانية وهي فئة القراصنة وهم مبرمجون من أصحاب الخبرة يهدفون إلى الدخول إلى الأنظمة المعلوماتية غير المسموح لهم بالدخول إليها

[1]–للتدليل على خطورة أفعال هذه الفئة نذكر على سبيل المثال تلاميذ مدرسة الثانوية في ولاية منهاتن الذين استخدموا عام 1980 طرفيات غرف الدرس للدخول إلى شبكة اتصالات ودمروا ملفات زبائن الشركة في هذه العملية.

وكسر الحواجز الأمنية المحيطة بهذه الأنظمة وتضم هذه الفئة نوعين من القراصنة وهم الهاكرز والكراكرز، الفئة الثالثة هم الموظفون العاملون في مجال الأنظمة المعلوماتية(الحاقدين)، أما الفئة الرابعة فهم مجرمو المعلوماتية أصحاب الآراء المتطرفة (الجماعات الإرهابية أو المتطرفة هدفها فرض معتقداتهم أو تحقيق رغباتهم باللجوء إلى النشاط الإجرامي)[1] أما الفئة الأخيرة فهم مجرمو المعلوماتية في إطار الجريمة المنظمة (تبييض الأموال، تجارة الأعضاء البشرية)،[2] وفي دراستنا سنقوم بدراسة الفئة الثانية التي تضم الهاكرز والكراكرز.

الهواة (الهاكرز): المخترقون الهواة المتميزون ويسمون بتسمية الهاكر haker أو haking ويقصد به مخترق شبكات الحاسب، وهم عادة من الشباب الفضوليين الذين يسعون إلى التسلية ولا يشكلون خطورة على الصناعات وأنظمة المعلومات.

ويعود الفضل في الكشف عن هذا المصلح إلى كاتب الخيال العلمي الأمريكي "وليام جيبسون" في مؤلفه the new- romancer الذي صدر سنة 1984 والذي ذكر فيه المجرم

[1]– ومن بين هذه الجرائم نذكر الهجوم الواقع على بريطانيا العام الماضي حيث في يوم 2017/05/12، عانت المستشفيات البريطانية من هجمات إلكترونية واسعة النطاق بدافع الابتزاز المالي أو دفع فدية مالية وهو ما تم تسميته بهجوم الفدية باستعمال فيروس "الفدية(WannaCry) " وقد استهدف أجهزة كومبيوتر وقاعدة بيانات 81 مستشفى و600 عيادة طبية في مختلف المناطق البريطانية وأدى الهجوم، حسب تحقيق أجرته السلطات البريطانية، إلى تعطيل قاعدة بيانات المرضى والغاء قرابة 20 الف موعد طبي من ضمنها مواعيد عاجلة تخص مرضى مصابين بأمراض خطيرة،حيث أفضى إلى شلل شبه تام في معظم المراكز الصحية و المستشفيات في البلاد، ما دفع الحكومة إلى التدخل من خلال المركز الوطني لأمن الإنترنت للتعاون مع القطاع الصحي من أجل حماية أمن سجلات المرضى و عودة الخدمة الصحية في البلاد، مقال منشور على موقع https://www.skynewsarabia.com بتاريخ 2018/04/11 على الساعة: 05:44، تاريخ الاطلاع: 2022/04/20.

[2]–نهلا عبد القادر المومني، مرجع سبق ذكره، ص76.

التقني، في حين أن هذا المصطلح كان يطلق قبل ذلك على الأشخاص الذين يملكون قدرات عالية المستوى في البرمجة، والذين يتميزون بقدرات إبداعية في معهد ماسشوستس للتكنولوجيا، وكذلك المبرمجين المبدعين في جامعة ستانفورد وجامعة berkeley.

المحترفون (الكراكرز): هو نوع آخر من مرتكبي جرائم المعلوماتية يطلق عليهم تسمية المحترفين أو المخترقين تتروح أعمارهم ما بين 25 و 45 سنة ويقصد بهم فئة المخترقين ذوي النوايا الإجرامية في الإتلاف أو التخريب، باستخدام الفيروسات أو القنابل المنطقية، وهم يتميزون بأنهم من أصحاب التخصصات العالية، ولهم الهيمنة الكاملة على تقنيات الحاسب وشبكات المعلوماتية، وهم يمثلون التهديدات المباشرة للأنشطة والمصالح عبر شبكة الأنترنت. [1]

الفرع الثاني: أنواع جريمة القرصنة الإلكترونية

عند الحديث عن أنواع جرائم القرصنة الإلكترونية يجب أن نعلم بأن هذه الطائفة من الجرائم تستلزم معرفة فنية عالية في مجال البرمجة، وقد تقع على البرامج التطبيقية أو على برامج التشغيل وسنقوم بدراسة هذه الأنواع كما يلي:

أولا: الإدخال: (input): ويقصد بفعل الإدخال(input) إضافة معلومات جديدة على الدعامة سواء كانت خالية من المعلومات أم كان يوجد بها معطيات وإدخال بيانات غير معتمدة في نظام الحاسب أو تحريف البيانات المعتمدة المراد إدخالها وهي تعد من أكثر أساليب ارتكاب الاحتيال المعلوماتي أمنا، وأكثر أشكاله وقوعا، حيث يشكل ما يقع باستخدامه أكثر من نصف

[1]– رابحي لخضر، بن بعلاش خاليدة، مرجع سبق ذكره ص ص4-5.

إجمالي حالات الاحتيال المعلوماتي.[1] كما يمكن أن يتم فعل الإدخال في كل حالة يتم فيها إدخال برنامج غريب فيروس أيا كان النوع من الفيروسات[2]، حصان طراودة[3] ، قنبلة معلوماتية، أو نوع من الديدان.

ثانيا المحو: (erasure): يقصد بالمحو أو الإزالة اقتطاع خصائص مسجلة على دعامة ممغنطة عن طريق محوها أو طمسها، وكذلك عن طريق تحويل خصائص مزالة في منطقة محفوظة من الذاكرة.[4]

ثالثا التعديل: (alteration): يقصد بتعديل المعطيات الموجودة داخل نظام المعالجة الآلية للبيانات أو استبدالها بمعطيات أخرى، كما يقصد به قيام الغير ممن لا يملك الحق في إحداث تعديل في المعلومات بتعديلها.[5]

---

[1]– هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، ط1، مكتبة الآلات الحديثة، أسيوط، 1992،ص59.

[2]– يقصد بالفيروس Virus بصفة عامة برنامج يحتوي على مجموعة من الاوامر الخاصة بكيفية انتشاره داخل الملفات وتكرار نفسه والآثار التخريبية الخاصة به، والتي قد تكون حذف البيانات، إبطاء الحركة، استغلال الذاكرة العشوائية بحيث لا يمكن تشغيل أي برنامج. أنظر:هلالي عبد اللاه أحمد: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية،ط1، القاهرة، 2006، ص47.

[3]– برنامج له قدرة كبيرة على الاختفاء بالبرنامج الأصلي، وعند تشغيل البرنامج يبدأ نشاه التدميري الذي يؤدي إلى تعديل ومحو بعض البيانات وقد يصل به الحد إلى تدمير النام كله، أحمد خليفة الملط: الجرائم المعلوماتية، دار الفكر الجامعي، ط3، سنة 2006،، ص543.

[4]– محمد خليفة: الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية،2007، ص157.

[5]– عمر أبو بكر بن يونس: الجرائم الناشئة عن استخدام الانترنت، كلية الحقوق، جامعة القاهرة، دار المنار، القاهرة، 1994،ص363.

و يختلف فعل التعديل عن فعل الإدخال في كون التعديل يتضمن التغيير في البيانات المخزنة في النظام، أما الإدخال فقد يتم بإدخال بيانات إلى نظام خال من البيانات، وقد يتم إدخال بيانات إلى البيانات الموجودة في النظام، كما يختلف فعل التعديل عن فعل الإزالة كون الأول –التعديل– يتضمن تغييرا في البيانات الموجودة أصلا في النظام أما الثاني– الإزالة– فيتضمن إزالة ومحو البيانات الموجودة، وتعديل المعطيات المخزنة في نظام المعالجة الآلية قد يشمل تعديل المعطيات فقط وقد يشمل تعديل البرامج،[1] والهدف الرئيسي من تعديل البرامج يتمثل في اختلاس النقود وتكثر هذه الجرائم في مجال الحسابات[2]، ومن أمثلة ذلك قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zzwick وحصل على إثر ذلك على مئات الدولارات كل شهر وكان من الممكن أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وآخر عميل له ليكتشف عدم وجود ما يدعىZzwick[3]

وإضافة لما سبق نجد نوع آخر وهو التلاعب في بيانات نظم معالجة البيانات: تتمثل الجريمة هنا في أفعال الإدخال أو المحو والتعديل ولا يشترط اجتماعهما وإنما يكتفي بتوافر إحداهما، فالجريمة في هذه الحالة تقع على المعطيات أو البيانات المعالجة آليا دون المعلومة

[1]–فايز محمد راجح غلاب: الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه في الحقوق فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر،2010/2009، ص215.

[2]–أحمد خليفة الملط، مرجع سبق ذكره، ص173.

[3]– Duleroy ®et rocco (A.M), l'informatique nouvelle, avril 1976, les escrocs a l'informatique, le nouvel Economsiste , les octobre,1979 ,n202.

ذاتها، لكن القاسم المشترك بين هذه الأفعال جميعا هو انطواؤها على تلاعب في المعطيات التي يتضمنها نظام معالجة البيانات بإدخال معطيات جديدة أو غير صحيحة أو محو أو تعديلات أخرى قائمة،[1] وهناك أيضا التلاعب في البرنامج حيث يأخذ عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية[2] أو عن طريق قيام أحد المبرمجين زرع برنامج فرعي غير مسموح به في البرنامج الأصلي يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نام معلوماتي، ويصعب اكتشاف هذا البرنامج لصغره ودقته.

المطلب الثاني: خصائص جريمة القرصنة الالكترونية وما يميزها عن غيرها من الجرائم

في هذا المطلب سنقوم بتقسيم الدراسة إلى فرعين سنتناول في الأول خصائص جريمة القرصنة الإلكترونية، أما الفرع الثاني فسنتناول فيه المميزات التي تميز جريمة القرصنة الإلكترونية عن غيرها من الجرائم الأخرى.

[1]–جمال زين الدين العابدين أمين أحمد، مرجع سبق ذكره، ص20.

[2]– هي عبارة عن برنامج أو جزء منه ينفذ في لحظة محددة أو كل فترة زمنية منتظمة ويتم وضعه في شبكة معلوماتية بغرض تسهيل تنفيذ عمل غير مشروع، أحمد خليفة الملط، المرجع السابق ذكره، ص545.

الفرع الاول: خصائص جريمة القرصنة الإلكترونية

جريمة القرصنة الالكترونية صورة من صورة الجرائم المعلوماتية وبهذا نجدها تحمل نفس الخصائص التي تتميز بها الجرائم المعلوماتية والتي سنقوم بدراستها كمايلي:

أولا: الجرائم الإلكترونية والتي من بينها جريمة القرصنة تعد من أبرز الجرائم الجديدة والمستحدثة التي يكن أن تشكل أخطارا جسيمة في ظل العولمة، فلا غرابة أن تعتبر الجرائم المعلوماتية من الجرائم المستحدثة، بحيث أن التقدم التكنولوجي الذي تحقق خلال السنوات القليلة الماضية جعل العالم بمثابة قرية صغيرة، بحيث نجد أن هذا التقدم بقدراته وإمكانياته قد تجاوز وفاق أجهزة الدولة الرقابية، وأكثر من ذلك فقد أضعف من قدرات أجهزة الدولة في تطبيق قوانينها، التي أصبحت لا تواكب هذا التطور، وبالتالي هذا الضعف والعجز أصبح يهدد أمن الدولة وأمن مواطنيها.[1]

ثانيا: جريمة القرصنة عابرة للحدود: ذلك أن قدرة تقنية المعلومات على إختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم انعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى استخدام هذه التقنيات في خرقهم للقانون، وهو ما يعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل وبين المعلومات

[1]– رابحي لخضر، بن بعلاش خاليدة، مرجع سبق ذكره، ص03.

محلا لاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد آخر، وهو بهذا السلوك قد يضر شخصا آخر موجود فيبلد ثالث.[1]

ثالثا: صعبة الاكتشاف: ذلك لأن معظمها تتم في الخفاء ولا يلاحظها المجني عليه ولا يدري حتى بوقوعها، حتى أنها لا تترك أثرا في مسرح الجريمة وإن وجد فمن الصعب إثباته، فليس هناك شيء ملموس أو مادي فهي عبارة عن مجموعة من البيانات والمعطيات يتم التلاعب بها في عالم غير مرئي ونقل المعلومات عبر نبضات إلكترونية، وما يزيد من صعوبات إثبات هذا النوع من الجرائم هي عدم إبلاغ الضحية أو المجني عليه.[2]

رابعا: محل الجريمة المعلوماتية ينصب على الأنظمة المعلوماتية سواء ما يقع عليها، أو ما يقع باستخدام أدواتها المعلوماتية المادية من أجهزة، وشرائط وكابلات ودعامات ممغنطة، كلها وسائل تتميز في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد.[3]

خامسا: جريمة وسيلتها ونطاق أهدافها الشبكة العنكبوتية(الأنترنت)[4]: إن حوسبة معظم القطاعات والمؤسسات(الاقتصادية، المالية، العسكرية والأمنية) منذ النصف الثاني من القرن

---

[1]–نائلة عادل محمد فريد قورة: جرائم الحاسب الآلي الاقتصادية، المنشورات الحلبي الحقوقية،ط1، س ط2005،ص52.

[2]– مزيود سليم: الجريمة المعلوماتية وواقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، جامعة المدية، العدد الأول، أفريل2014، ص120.

[3]– رابحي لخضر، بن بعلاش خاليدة، مرجع سبق ذكره، ص3.

[4]-network- interconnecting : عبارة عن شبكة تتألف من العديد من الحاسبات الآلية المرتبطة ببعضها البعض إما عن طريق خطوط التلفون أو عن طريق الأقمار الصناعية، تعتبر شبكة الاتصالات الدولية والتي ربطت بين الملايين من أجهزة الحاسب الآلي على مستوى العالم، حتى أصبحت كافة التعاملات سواء كانت معلومات أو أموال تتم من خلالها من أهم التطورات التكنولوجية في تاريخ البشرية، وهي تعتبر أضخم شبكة كومبيوتر على مستوى العالم، هي ثمرة الاندماج بين=

الماضي بالإضافة إلى استعمال هذه البنى للاتصالات الحديثة وأنظمة المعلومات المتطورة والمرتبطة بالأنترنت، والتي أصبحت تغطي النطاق المعلوماتي والخدماتي، حيث أصبح الفضاء السيبيري مكان خصب لانتشار الجرائم المعلوماتية، إذ تستعمل للعثور على الأهداف المطلوبة وذلك بغية تخريبها أو قرصنتها أو اختلاسها أو سرقة المعلومات منها(الاقتصادية، العسكرية، الفكرية أو الشخصية).[1]

سادسا: الجريمة المعلوماتية من الجرائم الناعمة التي لا تتطلب استخدام أدوات العنف كما في غيرها من جرائم الإرهاب والسرقة والسطو المسلح، فمثلا نقل البيانات من حساب إلى حساب آخر أو السطو الالكتروني على أرصدة بنك ما لا يتطلب المواجهة المباشرة مع موظفي وحراس البنك وإنما التواجد أمام الكمبيوتر واستخدام الذكاء البالغ من المخترق،[2] حتى أنه يقال أنه لا

=تكنولوجيا الحاسب وتكنولوجيا الاتصالات لأن شبكة الأنترنت استطاعت أن تصل المراكز بالفروع بالرغم مما بينها من مسافات، وقد بدأت جذور الشبكة عام 1969 حينما أنشأت شبكة ARPA NET التي أنشأتها وكالة مشاريع الأبحاث المتقدمة (Advanced Research Projects Agency-ARPA) التابعة لوزارة الدفاع الأمريكي (بنتاجون) وكان الهدف الأساسي منها هو تأمين تبادل المعلومات العسكرية بالغة السرية والحيوية بالنسبة للأمن القومي الأمريكي ومع بداية حقبة السبعينات وبانضمام وكالة الفضاء الأمريكية NASA والمؤسسة القومية للعلوم ومراكز البحث العلمي، أخذت الشبكة الطابع المدني وأصبح التمويل الخاص بها يتم عن طريق جهات حكومية، بانضمام أعداد هائلة من الشبكات الخاصة بالشركات والمؤسسات، أخذت الشبكة الطابع التجاري بعد أن كانت مقتصرة على الجوانب الأكاديمية والعسكرية فقط، أنظر طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي–النظام القانوني للحماية المعلوماتية–دار الجامعة الجديدة للنشر، الاسكندرية،ب ط، 2009،ص 109.

[1]- مع ظهور شبكات التواصل الإجتماعي سنة 2007 والتي عرفت تزايدا كبيرا في استعمالها وفي أقل من عشر سنوات من ظهورها، تم إحصاء أكثر من مليار مستخدم مختلف لها، منذ أكتوبر 2012 هنالك أكثر من مليار مستخدم للFacebook وبالتالي استغلال هذا العدد الكبير للحصول على المعلومات الشخصية للضحايا واستغلالها في السرقة المالية أو الفكرية أو القرصنة أو انتحال الشخصية أو الابتزاز، لطرش فيروز، بن عزوز حاتم، مرجع سبق ذكره، ص325.

[2]– رابحي لخضر، بن بعلاش خاليدة ، مرجع سبق ذكره، ص3.

يوجد شعور حقيقي بعدم الأمان في مواجهة الجريمة المعلوماتية كالذي يوجد بصورة دائمة في مواجهة غيرها من الجرائم.[1]

سابعا: سرعة التنفيذ لا يتطلب تنفيذ الجريمة الإلكترونية الوقت الكثير بضغطة واحدة على لوحة المفاتيح يمكن أن تنتقل ملايين الدولارات من مكان إلى آخر، وهذا لا يعني أنها لا تتطلب الإعداد قبل التنفيذ أو استخدام معدات وبرامج معينة[2].

ثامنا: التخصص التقني لارتكابها وكذلك لمكافحتها: يتطلب تنفيذ هذه الجريمة خبرة في مجال الإعلام الآلي وهذه الخبرة تتفاوت بين مرتكبي هذا النوع من الجرائم فكلما كان الهدف أكبر وأكثر حساسية(بسبب برامج الدفاع الإلكترونية القوية التي تضعها المؤسسات والشركات والحكومات) كلما تطلب ذلك خبرة فنية أكبر لذا فهذا النوع ينفذه عادة متخصصون في الإعلام الآلي (الهاكرز)، بالإضافة إلى أن اكتشاف ومكافحة هذه الجرائم يتطلب خبرة فنية عالية، وذلك للحد من أثرها وإيقاف مختلف الاختلافات والتعامل معها، ولذلك يتم توظيف خبراء وفنيين و متخصصين في مجال المعلوماتية والإعلام الآلي وذلك للتعاطي مع هذا النوع من الجرائم.[3]

مما تقدم يتضح لنا أ خصائص الجرائم المعلوماتية هي: سهولة ارتكابها وصعوبة اكتشافها من قبل رقابة الجهات الأمنية فهي جريمة مستترة يصعب عادة اكتشافها، بالإضافة إلى صعوبة تقدير حجم الأضرار وسهولة إتلاف الأدلة من قبل الجناة، وأنها جريمة عابرة للحدود لا تعترف

[1]– نائلة عادل محمد فريد قورة، مرجع سبق ذكره، ص50.

[2]– ذياب موسى البداينة، مرجع سبق ذكره، ص19.

[3]– لطرش فيروز، بن عزوز حاتم، مرجع سبق ذكره، ص ص 325–326.

بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني المجني عليه[1].

الفرع الثاني: مميزات جريمة القرصنة الإلكترونية عن غيرها من الجرائم

هناك العديد من المميزات التي تميز جريمة القرصنة أو جرائم المعلوماتية بصفة عامة عن غيرها من الجرائم وفيما يلي سنقوم بدراسة هذه المميزات.

أولا: من حيث المجرم المعلوماتي (الجاني)[2]: لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تميزها عن غيرها من الجرائم التقليدية فحسب، وإنما كان له أثره أيضا على تمييز المجرم المعلوماتي عن غيره وقد اختلف الباحثون في تحديد هذه السمات[3] ومن بين هذه المميزات نذكر مايلي:

أ-يتمتع بالذكاء والمهارة: حيث أن ارتكاب الجريمة المعلوماتية يتطلب مقدرة عقلية وذهنية عميقة وغير عادية، وعموما فإن تميز المجرم المعلوماتي في الغالب بالذكاء والخبرة الواسعة مقارنة بنظيره المجرم العادي، يمكنه من التخطيط لجريمته قبل أن يقدم على ارتكابها محاولا بذل الجهد في ألا يكتشف أمره متوسلا بأساليب وتدابير الحماية الفنية التي من شأنها إعاقة

[1]-حنان ريحان مبارك المضحكي، مرجع سبق ذكره، ص39، أنظر أيضا عبد الله عبد الكريم عبد الله: جرائم المعلوماتية والأنترنت، منشورات الحلبي الحقوقية، لبنان، ط1، 2007، ص ص 31-32.

[2]-الجاني هنا هو المجرم المعلوماتي وهو الشخص الذي لديه مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسب الآلي الإلكتروني والقادر على استخدام هذا التكتيك لاختراق الكود السري لتغيير المعلومات أو لتقليد البرامج عن طريق استخدام الحاسوب، مصطفى محمد موسى: التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة للطباعة والنشر و التوزيع، ط1، 2008، ص 134.

[3]- نائلة عادل محمد فريد قورة، مرجع سبق ذكره، ص54.

مهمة أجهزة الاستدلال والتحقيق في الوصول إلى الدليل، كما في استخدام كلمات المرور، وترميز البيانات وتشفيرها[1] للحيلولة دون الاطلاع على محتواها أو ضبطها،[2] ولكن التقدم التقني أسفر عن ابتكار برامج لمكافحة التشفير[3].

ب–شخص عائد للإجرام: يمتاز بكونه مجرم عائد إلى الإجرام، انطلاقا من رغبته في محاولة سد الثغرات التي أدت إلى التعرف عليه وتقديمه إلى المحاكمة في المرة السابقة.[4]

ج–انسان إجتماعي: هو لايضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل إنه انسان يستطيع التوافق والتصالح مع مجتمعه، حيث أن ذكاءه يساعده على عملية التكيف، والذكاء في نظر الكثير يمثل القدرة على التكيف، ولا يقصد من وراء ذلك التقليل من شأن المجرم المعلوماتي، بل إن خطورته الإجرامية تزداد بزيادة تكيفه مع المجتمع ومع توافر الشخصية الإجرامية لديه.[5]

---

[1]– هناك عدد من البرامج التشفيرية مثل البرنامج المعروف باسم البريد بالغ السرية، وبرنامج سري جدا، وهو من أكثر برامج تشفير البريد شيوعا في و.م.أ وأوروبا ، انظر علي حسن محمد الطوالبة، مرجع سبق، ص 143

[2]– عبد الباقي الصغير: القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، سنة 1992، ص115.

[3]–ابتكار جهاز يقال له Key Logger System يسمح بتسجيل ضربات الجهاز على لوحة المفاتيح بعد استعمال الجهاز وبالتالي تسمح بمعرفة كلمة السر، وبرنامج Magic Lantern ولتشغيله يلزم ارسال رسالة بشكل اعلان مثلا "اضغط هنا لتكسب" وعند الضغط تفتح الرسالة ويزرع البرنامج في جهاز المتهم دون أن يدري. أنظر: شيماء عبد الغني محمد عطاالله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ب ط، 2007، ص252.

[4]– رابحي لخضر، بن بعلاش خاليدة، مرجع سبق ذكره، ص 05.

[5]– نفسه،ص6.

د-مجرم متخصص ومحترف: فقد ثبت في العديد من القضايا أن عددا من المجرمين لا يرتكبون سوى الجرائم المعلوماتية دون سواها، كما أن المجرم المعلوماتي مجرم محترف بحيث أنه لا يمكن للشخص العادي إلا في حالات قليلة أن يرتكب مثل هذه الجرائم، فالأمر يقتضي من الدقة والتخصص في هذا المجال ما يلزم للتغلب على العقبات التي أوجدها المتخصصون لحماية أنظمة الكمبيوتر، كما يحدث على سبيل المثال في البنوك.[1]

هـ-الباعث الدافع[2] إلى الجريمة: في الجرائم المعلوماتية يكون الباعث في أغلب الأحيان الحصول على الأموال، أو التسلية أو التحدي كالرغبة في إثبات الذات، وقد يكون الدافع لارتكاب الجريمة المعلوماتية الرغبة بإلحاق الضرر بأحد ما كسرقة صورة شخصية من جهاز حاسب آلي شخصي وابتزاز صاحبها.[3]

ثانيا: من حيث طبيعة الجريمة:

تتميز الجريمة المعلوماتية بصفة عامة عن الجريمة التقليدية من عدة جوانب، سواء كان هذا التمييز في السمات العامة لها أو في الباعث على تنفيذها أو طريقة التنفيذ ذاته، كما تتميز بطابعها الدولي في أغلب الأحيان حيث تتخطى آثار هذه الجريمة حدود الدولة الواحدة، وجريمة

[1]- رابحي لخضر، بن بعلاش خاليدة، المرجع السابق ذكره ، ص6.

[2]- هو العامل المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والإنتقام، نهلا عبد القادر المومني، : مرجع سبق ذكره، ص89.

[3]- حنان ريحان مبارك المضحكي، مرجع سبق ذكره،ص 43.

القرصنة الإلكترونية تتميز بنفس مميزات الجريمة المعلوماتية كونها صورة من صورها وفي ما يلي سنقوم بدراسة بعض مميزات الجريمة المعلوماتية التي تميزها عن الجرائم الأخرى.

حيث تتميز هذه الجرائم التي هي من الجرائم المستحدثة بأنها سهلة الارتكاب نتيجة الاستخدام السلبي للتقنية المعلوماتية بما توفره من تسهيلات، وأن آثارها ليست محصورة في النطاق الإقليمي لدولة بعينها، فضلا على أن مرتكبيها يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية، ليس هذا فحسب بل إنها تستهدف محلا من طبيعة خاصة ونعني بذلك المعلومات التي يحتوي عليها نظام المعالجة الآلية وشبكات الاتصال العالمية بصورة آلية، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمان الأجهزة المعنية بمكافحة الجريمة وبالذات فيما يخص إثبات هذه الجرائم وآلية مباشرة الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمهم للعدالة،[1]

ثالثا: من حيث الأدلة: لم تتعرض قوانين الإجراءات الجنائية لتعريف الدلائل، وإنما اكتفت بالنص على تطلب الدلائل القوية والمتوافقة مع الاتهام، إلا أن الفقه تصدى لتحديد مفهومها حيث عرفها بأنها " مجموعة الوقائع الظاهرة والملموسة التي يستنتج منها أن شخصا معينا هو مرتكب الجريمة"[2]، وعرفها المشرع الفرنسي بأنها: " أمارات معينة تستند إلى العقل وتبدأ من ظروف أو وقائع يستنتج منها الفعل توحي للوهلة الأولى بان جريمة ما وقعت وأن شخصا معينا

[1]– حابت أمال: الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16–17 نوفمبر 2015، جامعة محمد خيضر بسكرة، ص2.

[2]– عائشة بن قارة مصطفى: حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، ب ط، 2010 ، ص 102

هو مرتكبها"[1]، و تختلف الأدلة في الجرائم المعلوماتية عن الأدلة في غيرها من الجرائم من حيث المادة، وذلك لأن الأولى تكون أشياء ذات طبيعة مادية وهي الحاسوب ومكوناته او معنوية وهي البيانات والمعلومات[2]، ففي جريمة القتل مثلا نجد أداة الجريمة وفي جرائم المخدرات نجد المخدر نفسه، بينما في الجرائم المعلوماتية يمكن أن تكون نسخة من المعلومات الكائنة في جهاز الكومبيوتر أو على دعامة مادية،[3] فقد تعودت الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين على التعامل مع الجريمة بصورها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثر مادية في مسرح الجريمة من بصمات او آثار أقدام أو بقع دم أو محررات مزورة....إلخ، وتتميز الجرائم الالكترونية عن الجرائم التقليدية في أن المشكلات الإجرائية التي تواجه جهات البحث عند تعاملها مع هذا النوع من الجرائم تبدأ من طبيعة البيئة الافتراضية التقنية التي ترتكب فيها، فهي لا تخلف أي آثار مادية محسوسة، كما أن هذه الجريمة تتم في الخفاء، فكثيرا ما يعمد المجرم المعلوماتي إلى إخفاء نشاطه الجرمي مما يعقد أمر كشفها وتحديد مرتكبها، لهذا يحتاج هذا النوع من الجرائم

---

[1]– بكرى يوسف بكرى، مرجع سبق ذكره، ص92.

[2]–ورد في تعريف منظمة التعاون الاقتصادي والتنمية عام 1992 والخاصة بأنظمة الحاسوب وشبكات المعلومات بأن البيانات مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلا محددا يجعلها قابلة للتبادل والتفسير أو المعالجة بواسطة الأفراد أو بوسائل إلكترونية، أما المعلومات فهمي المعنى المستقى من هذه البيانات ومن بين تعاريف سابقة يتضح أنه لا فرق بين البيانات والمعلومات بحيث انه يجب أن يخضعا للحماية القانونية فالبيانات عبارة عن معلومات وأرقام يتم تغذية الحاسب بها ومن ثم الحصول على مخرجات من الجهاز. أنظر: عادل عبد الله خميس المعمري: التفتيش في الجرائم المعلوماتية، بحث منشور على موقع المنهل https://platform.almanhal.com، ب ت. تاريخ الاطلاع: 2022/04/20

[3]– شيماء عبد الغني محمد عطاالله، مرجع سبق ذكره، ص357.

لإجراءات خاصة في البحث والتحري،[1] وسيلة تنفيذ الجريمة تتميز في أغلب الحالات بالطابع التقني، مما يجعل أدلة الإدانة فيها غير كافية ويرجع ذلك إلى عدم وجود أي أثر كتابي، إذ يتم نقل المعلومات بالنبضات الإلكترونية بالإضافة إلى إمكانية الجاني تدمير دليل الإدانة في أقل من ثانية.[2]

رابعا: من حيث المجني عليه: ومن مميزات الجريمة الإلكترونية ما يتعلق بالمجني حيث يكون دوره مثيرا للريبة، فهو قد يشارك بطريق مباشر أو غير مباشر في ارتكاب الفعل وذلك بسبب وجوده في روف تجعل من قابليته التعرض للجريمة مرتفع بشكل كبير ومرد ذلك إلى القصور الذي يكتنف أنظمة الحاسبات الآلية والذي يساعد في ارتكاب الفعل الإجرامي،[3] ونجد كذلك أن رد فعل المجني عليه في الجرائم الإلكترونية سلبي حيث نجد من النادر ما يقوم المجني عليه بالإبلاغ عنها وذلك لعدة أسباب تتعلق بسمعة المؤسسة التي يمثلها ومخافة زعزعة الثقة فيها.[4]

[1]– حابت أمال، مرجع سبق ذكره، ص04.

[2]– هشام محمد فريد رستم، مرجع سبق ذكره، ص41.

[3] – Rose (philipe), op,cit,p53.

[4]– هشام محمد فريد رستم، المرجع السابق ذكره، ص 41.

خاتمة الفصل:

في الأخير بعد دراستنا لهذا الفصل المخصص للمفاهيم المتعلقة بجريمة القرصنة الإلكترونية حيث تطرقنا إلى إبراز أهم المفاهيم المتعلقة بجريمة القرصنة والتي تتميز بعدة خصائص تميزها عن غيرها من الجرائم الإلكترونية والجرائم الأخرى ومن خلال دراستنا نخلص إلى أن جريمة القرصنة الالكترونية تعد من الجرائم الخطيرة والسريعة التطور والمتزايدة بشكل كبير وفي الفصل الموالي سنقوم بدراسة مكافحة جريمة القرصنة الإلكترونية في التشريع الجزائري.

الفصل الثاني

بعد دراسة فصل الإطار المفاهيمي لجريمة القرصنة الالكترونية اتضح لنا من الفصل السابق أنها ترتكب كغيرها من الجرائم الالكترونية باستخدام التقنية المعلوماتية مما يعني أنها ترتكب في فضاء افتراضي مفرغ سواء ارتكبت عبر شبكة الإنترنت أم في داخل نطاق ذات المؤسسة التي يتم الاعتداء عليها، أو ارتكاب الجريمة من خلالها، وقبل دراستنا لهذا الفصل نشير إلى أن جريمة القرصنة الإلكترونية صورة من صور الجرائم المعلوماتية وفي دراستنا سنقوم بتعميم الدراسة والتخصيص عند الحاجة إلى ذلك وبداية نشير إلى أن المشرع الجزائري لم يستعمل مصطلح الجرائم المعلوماتية بل استعمل مصطلحا آخر هو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وينصرف هذا المصطلح وفقا لدلالة الكلمة إلى المعلومات والنظام الذي يحتوي عليها بما في ذلك شبكات المعلومات، ليخرج من نطاق التجريم تلك الجرائم التي يكون النظام المعلوماتي وسيلة لارتكابها، وحصرها فقط في صور الأفعال التي تشكل إعتداء على النظام المعلوماتي، أي الجرائم التي يكون النظام المعلوماتي محلا لها، ثم في مرحلة لاحقة اختار المشرع الجزائري للتعبير عن الجريمة المعلوماتية مصلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب القانون رقم 04/09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والإتصال ومكافحتها، وقد تبنى المشرع الجزائري في هذا القانون تعريفا موسعا للجرائم الإلكترونية واعتبرها أنها تشمل بالإضافة إلى الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام الاتصالات الإلكترونية، و بذلك لم يعد مفهوم الجريمة المعلوماتية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للإعتداء بل توسع نطاقها لتشمل تلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها[1]، وعليه سنقوم بتقسيم هذا الفصل إلى مبحثين سنخصص المبحث الأول لدراسة الجوانب الموضوعية لجريمة القرصنة الإلكترونية، أما المبحث الثاني سنخصصه لدراسة الجوانب الإجرائية لهذه الجريمة.

[1]- حابت أمال، مرجع سبق ذكره، ص03.

المبحث الأول: الجوانب الموضوعية لجريمة القرصنة الإلكترونية في التشريع الجزائري

في هذا المبحث سنتطرق إلى دراسة الجوانب الموضوعية لجريمة القرصنة الإلكترونية وذلك بتقديم بدراسة الأركان الثلاثة لقيام هذه الجريمة في المطلب الأول، أما المطلب الثاني فخصصناه إلى دراسة العقوبات المقررة لجريمة القرصنة في التشريع الجزائري.

المطلب الأول: أركان جريمة القرصنة الإلكترونية

يقصد بأركان الجريمة عناصرها الأساسية التي يتطلبها القانون لقيام الجريمة وهي أركان خاصة وهي التي ينص عليها المشرع بصدد كل جريمة على حدى وأركان عامة وهي واجب توافرها أي كان نوع الجريمة أو طبيعتها[1]، و من المعروف أن الجريمة في صورها العادية تتكون من ثلاثة أركان ركن شرعي وركن معنوي وركن مادي وجريمة القرصنة الالكترونية بدورها تتكون من هذه الأركان حالها حال جميع الجرائم التي تدخل في نطاق الجريمة المعلوماتية، في هذه الدراسة سنقوم بتقسيم هذا المطلب إلى ثلاثة فروع، الفرع الأول منه سنخصصه لدراسة الركن الشرعي في جريمة القرصنة الإلكترونية، والفرع الثاني سندرس فيه الركن المادي لهذه الجريمة، أما الفرع الثالث فسندرس فيه الركن المعنوي لجريمة القرصنة الإلكترونية.

[1]– عبد الله سليمان: شرح قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، الجزائر، ط6، س ط2005، ص65.

الفرع الأول: الركن الشرعي في جريمة القرصنة الإلكترونية

بقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضح العقوبة المترتبة عليه، لا جريمة ولا عقوبة ولا تدابير أمن إلا بنص قانوني[1] فلا يعتبر الفعل الإجرامي مجرما إلا إذا وجد نص قانوني يقضي بذلك و الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان هذه الأفعال تختلف حسب نشاطات الإنسان وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه[2]، وفيما يخص الجرائم المعلوماتية فقد عملت أغلب التشريعات على تنظيم قوانين ومعاهدات تحمي هذه الحقوق الشخصية للأشخاص وفي نفس الوقت تكافح الجريمة المعلوماتية سواء على المستوى الدولي أو المحلي وعلى المستوى الدولي، نجد من بين أهم المعاهدات التي تصدت لمكافحة الجرائم المعلوماتية الإتفاقية الدولية حول الجرائم المعلوماتية المنعقدة ببودابست 2001/11/23[3]، جهود منظمة التعاون الاقتصادي والتنمية[4]، وغيرها من القوانين والمعاهدات

---

[1]- المادة 1 من الأمر رقم 66-156 مؤرخ في 8 جوان 1966 المتضمن قانون العقوبات معدل ومتمم لاسيما بالقانون رقم 14-04 المؤرخ في 2014/02/04.

[2]- أحسن بوسقيعة: الوجيز في القانون الجزائي العام، دار هومه، الجزائر، ط 10، 2011، ص27.

[3]- هي أولى المعاهدات الدولية التي تكافح الجرائم الإلكترونية، تمت تحت إشراف المجلس الأوروبي، ووقع عليها 30دولة تتكون من 48 مادة منظمة للجرائم المعلوماتية وكيفية التصدي لها، للاطلاع على النص الكامل للاتفاقية، يرجى مراجعة الموقع الخاص بالمجلس الأوروبي، منقول عن عائشة بن قارة مصطفى، مرجع سبق ذكره ، ص 153.

[4]- تضم هذه المنظمة في عضويتها 34 دولة وضعت المنظمة توصيات إرشادية بخصوص أمن المعلومات ومن مجمل أعمال المنظمة حول الجرائم الإلكترونية الاتفاق على ضرورة أن يغطي قانون العقوبات في كل دولة الأفعال الآتية: التلاعب في البيانات المعالجة آليا بما في ذلك محوها،التجسس المعلوماتي، التخريب المعلوماتي،قرصنة البرامج الدخول غير المشروع للبيانات،أنظر في ذلك: خلف فاروق: الآليات القانونية لمكافحة الجريمة المعلوماتية،الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، جامعة محمد خيضر بسكرة،ص06.

التي اهتمت بهذه الظاهرة، أما على المستوى الوطني فنجد أن المشرع الجزائري قد تصدى للجرائم المعلوماتية من الناحية الموضوعية والإجرائية أما الموضوعية فتتمثل في قانون العقوبات الجزائري، الذي تضمن في تعديله تحديد الجرائم المعلوماتية وذلك في القسم السابع مكرر منه تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات[1] الذي يعتبر وسيلة ردعية للكف عن ارتكاب الجرائم بصفة عامة و من الناحية الإجرائية نجد قانون الإجراءات الجزائية الجزائري[2]، الذي تطرق إلى اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وذلك في المواد من المواد 65 مكرر 05 –65 مكرر 10 بالإضافة إلى العديد من التعديلات الأخرى التي تخص الجرائم المعلوماتية، قانون رقم 09–04[3] الذي جاء بالعديد من الوسائل لمحاولة مكافحة الجرائم المعلوماتية ومن بينها تفتيش المنظومة المعلوماتية، قانون رقم 2000/03[4]،الذي تضمن الأحكام الجزائية المترتبة على مخالفة النظام القانوني، وأخيرا نذكر المرسوم الرئاسي رقم

[1]– "يعرف الأستاذ J-P Buffelan نظام المعالجة الآلية للمعطيات بأنه مجموع العمليات المنجزة بواسطة وسائل الإعلام الآلي المرتبطة بتجميع، تسجيل، إعداد، حفظ وتخريب معلومات اسمية و أيضا كل العمليات من طبيعة واحدة مرتبطة باستغلال الملفات أو قاعدة المعطيات وخاصة ربط أو تقريب أو فحص أو نشر معلومات اسمية"، أنظر: بدري فيصل:= =مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه، جامعة الجزائر01– بن يوسف بن خدة–كلية الحقوق،2018/2017، ص155.

[2]–أمر رقم 66–155 مؤرخ في 08 يونيو1966، المتضمن لقانون الاجراءات الجزائية، معدل ومتمم لاسيما بالأمر رقم 15–02 المؤرخ في 23 يوليو 2015

[3]– قانون رقم 09–04 المؤرخ في 14 05 اوت 2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية،ع 47، 2009.

[4]–قانون رقم 2000–03 مؤرخ في 2000/08/05 يحدد القواعد العامة المتعلقة بالبريد وبالموصلات السلكية واللاسلكية، الجريدة الرسمية الجزائرية، ع 48، 2000.ص23.

15-261 المحدد لتشكيل وتنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام الإتصال ومكافحتها.[1]

والهدف من كل هذه الجهود على المستوى الدولي أو الوطني هو حصر مصدر التجريم والعقاب حتى لا يقع المشرع تحت طائلة جرائم جديدة ذات أضرار بليغة من دون نصوص قانونية تجرمها.

الفرع الثاني: الركن المادي في جريمة القرصنة الإلكترونية:

يتكون الركن المادي في الجرائم التقليدية من السلوك الاجرامي والنتيجة الضارة والعلاقة السببية، و الركن المادي للجريمة الإلكترونية يتكون من السلوك الإجرامي والنتيجة والعلاقة السببية علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة كالتبليغ عن الجريمة قبل تحقق نتيجتها مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل،[2] و ما يميز الجرائم الإلكترونية بشكل عام، هو وجود حاسب آلي وشبكة معلوماتية، حيث لا يمكننا تصور وجود جريمة الكترونية من دون الحاسب الآلي وشبكة الأنترنت، التي يعتبر استخدامها كشروع كأصل عام ولكن الخلاف يثور من حيث استخدام هذه الوسائل الحديثة لغايات غير مشروعة، ولذلك تعد الوسيلة الإلكترونية من أهم مقومات السلوك الإجرامي في الجرائم الإلكترونية[3] ، ويقوم السلوك الإجرامي في جريمة

[1]- مرسوم رئاسي رقم 15-256 مؤرخ في 2015/10/08 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية، ع53، 2015،ص16.

[2]- أحسن بوسقيعة، مرجع سبق ذكره، ص28.

[3]- الحسيناوي علي جبار، جرائم الحاسوب والأنترنت، د.ط، دار الباروزي للنشر والتوزيع، عمان ، ص30

القرصنة الالكترونية بمجرد الدخول والبقاء غير المشروع في نظام المعالجة الآلية المنصوص عليه في قانون العقوبات الجزائري وتنطوي تحت هذا النوع ثلاث أفعال فعل الدخول والبقاء وعرقلة أو التعطيل أما النوع متمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات وتندرج تحت هذا النوع كذلك ثلاث أفعال وهي فعل الإدخال والمحو والتعديل ، أما الصورة الثانية متمثلة في الاعتداء على منتجات الإعلام الآلي وتحتوي هذه الصورة على فعل التزوير المعلوماتي[1]، وفي رأي آخر يتحقق الركن المادي لجريمة القرصنة الإلكترونية بحذف أو تغير معطيات المنظومة بعد الدخول أو البقاء غير المشروعين وتخريب نظام اشتغال المنظومة بعد الدخول أو البقاء غير المشروعين[2]، ويعد مساسا بالأنظمة المعلوماتية إحدى النشاطات غير المشروعة والمتمثلة في الصور التالية: التعطيل أو الإفساد أو المحو أو التعديل أو الإدخال والتي لا يشترط اجتماع هذه الصور، بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوفر الركن المادي.[3]

الفرع الثالث: الركن المعنوي في جريمة القرصنة الإلكترونية

يكتسي تحديد الركن المعنوي بالغ الأهمية في الجريمة المرتكبة عبر الأنترنت، كما هو الحال بالنسبة للجريمة المرتكبة في العالم المادي، حيث بموجبه يمكن تحديد مناط مسائلة الجاني وذلك بتحديد القصد الجنائي لديه، الذي بدونه لا يمكن أن يعاقب الشخص المرتكب

[1]– قانون العقوبات، الأمر رقم 09-01 المؤرخ في 25 فبراير 2009، د ط، ص120.

[2]– نائلة عادل محمد فريد قورة : مرجع سبق ذكره، ص223.

[3]– هيام حاجب: الجريمة المعلوماتية، مذكرة لنيل إجازة المدرسة العليا للقضاء، المدرسة العليا للقضاء، الجزائر،2008،ص48.

للفعل، يتلاقى القصد الجنائي بصورتيه العام والخاص في الجرائم المرتكبة عبر الأنترنت مع مثيله في الجرائم التقليدية في عدة نقاط، منها العلم والإرادة، فالمجرم يجب أن يكون عالم بأن الفعل الذي يقوم به يعتبر فعل غير مشروع، وذلك بإرادة صريحة من أجل إحداث الضرر للمجني عليه.[1] و تتعدد الجرائم المرتكبة عبر الأنترنت ونحن في هذه الدراسة سنقوم بالتطرق إلى الركن المعنوي في الجرائم التي تدخل في نطاق جرائم القرصنة الإلكترونية كما يلي:

1.**جريمة الإعتداءات على سير نظام المعالجة الآلية للمعطيات:** هي جريمة عمدية لأن أفعال العرقلة والتعطيل من الأفعال العمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام الذي يعتبر ظرف مشددا لجريمة الدخول والبقاء غير مشروع داخل النظام ، وعليه فالقصد الجنائي المفترض ينتج من طبيعة الأفعال المجرمة.[2]

2.**الإعتداءات العمدية على المعطيات:** هي جريمة عمدية يتخذ فيها القصد الجنائي بعنصريه العلم والإرادة ، فيجب أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل ،كما يجب أن يعلم الجاني بان نشاطه الإجرامي يترتب عليه التلاعب في المعطيات ، ويعلم أيضا أنه ليس له الحق في القيام بذلك و أنه يعتدي على صاحب الحق في السيطرة على تلك المعطيات بدون موافقته، ويشترط لتوافر الركن المعنوي بالإضافة إلى القصد الجنائي العام نية الغش لكن هذا لا يعني ضرورة توافر قصد الإضرار بالغير بل تتوافر الجريمة ويتحقق ركناها بمجرد فعل

[1]– صغير يوسف: الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون(تخصص القانون الدولي للأعمال)، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، س 2013، ص ص 70-71.

[2]– عائشة بن قارة مرجع سبق ذكره، ص125.

الإدخال أو المحو أو التعديل مع العلم بذلك واتجاه الإرادة إليه ، وإن كان الضرر قد يتحقق في الواقع نتيجة للنشاط الإجرامي إلا أنه ليس عنصرا في الجريمة.[1]

والركن المعنوي في هذا النوع من الجرائم محقق لأنه من المفترض أن أفعال العرقلة والتعطيل لا تكون إلا عمدية وهذا ما يميزه عن الاعتداء غير العمدي لسير النظام وعليه فالقصد الجنائي مفترض يستنتج من طبيعة الأفعال المجرمة.[2]

المطلب الثاني: العقوبات المقررة لجريمة القرصنة الإلكترونية في التشريع الجزائري

نصت المادة 13 من اتفاقية بودابست على ضرورة التزام الدول على اتخاد تدابير تشريعية وتدابير اخرى للتأكد من أن الجرائم المنصوص عليها معاقب عليها بعقوبات فعالة ومتناسبة ورادعة بما في ذلك تقييد الحرية وشملت المادة وجوب مساءلة و توقيع عقوبات أو تدابير جنائية والتي تكون ضمنها العقوبات المالية على الأشخاص الاعتبارية وهو ما تبناه المشرع الجزائري في قانون العقوبات.

الفرع الأول: العقوبات الأصلية لجريمة القرصنة الإلكترونية

من خلال دراستنا للمواد المتعلقة بالجرائم الماسة بالأنظمة المعلوماتية لاحظنا أن عقوبة جرائم القرصنة الإلكترونية من العقوبات المشددة لأن العقوبة فيها تكون مضاعفة عن العقوبة الأصلية و هذا ما سنقوم بدراسته بشكل مفصل في هذه الجزئية.

[1]– عائشة بن قارة ، المرجع السابق ذكره، ص ص 125–126.

[2]– علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة، الاسكندرية، 1999،ص136.

أولا: عقوبة الشخص الطبيعي: يعاقب بالحبس من ثلاثة أشهر إلى سنة واحدة وبغرامة من 50.000دج إلى 100.000دج كل من يدخل أو يبقى غن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، تضاعف العقوبة اذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة.

وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من50.000دج إلى 150.000دج.[1]

المادة تتضمن صور جريمة القرصنة الإلكترونية في الصورة المشددة لهذه الجريمة لأنها تتضمن مضاعفة العقوبة وذلك عند حذف أو تغيير لمعطيات المنظمة.

يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000دج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها.[2]

في هذه المادة تتجسد جريمة القرصنة الإلكترونية في جرم إزالة أو تعديل المعطيات التي يتضمنها نام المعالجة الآلية.

ثانيا: عقوبة الشخص المعنوي: مبدأ مساءلة الشخص المعنوي وارد في المادة 12 من اتفاقية بودابست، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا

[1]– المادة 394مكرر، ق ع ج.

[2]– 394 مكرر1، نفسه.

أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها، كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه.[1]

و قد نص المشرع الجزائري في المادة 51 مكرر من قانون العقوبات الجزائري على مساءلة الشخص المعنوي وذلك وفق شروط:

- أن ترتكب إحدى الجرائم المنصوص عليها قانونا
- أن تكون بواسطة أحد أعضاء أو ممثلي الشخص المعنوي
- أن ترتكب الجريمة لحساب الشخص المعنوي[2]

كما نص المشرع في المادة 18 مكرر من نفس القانون على أن العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي:

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

و يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي[3]

ثالثا: عقوبة الاشتراك: خصص قانون العقوبات الجزائري لجريمة الاشتراك في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي من بين شروطها الاتفاق الجنائي مادة معينة والتي جاء

---

[1]- عطاء الله قشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009.ص25.

[2]- ختير مسعود: الحماية الجنائية لبرامج الكومبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر، ط2010، ص ص 100-101.

[3]- 394 مكرر 4، ق ع ج.

في نصها مايلي: "كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها"،[1] يستخلص من نص المادة الشروط الواجب توفرها في الجريمة لتتم المعاقبة عليها وهي كما يلي:

- وجوب وقوع الجريمة ضمن مجموعة أو اتفاق،
- الغرض من تكوين المجموعة أو الاتفاق القيام بإحدى الجرائم المنصوص عليها في قسم الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،
- تجسيد التحضير لهذا النوع من الجرائم بفعل أو عدة أفعال مادية.

فالمشرع الجزائري يعاقب على الإشتراك في الاتفاق الجنائي بعقوبة الجريمة التي تم التحضير لها، فإذا تعددت الجرائم التي يتم التحضير لها تكون عقوبة الجريمة هي الأشد.[2]

وفي رأي آخر يرى بأن الإتفاق في حد ذاته جريمة وأن العزم الجماعي الإجرامي في الإتفاق الجنائي يظهر بمظهر مادي خارجي، لأن كل عضو يعلن عزمه إلى سائر الأعضاء فتتحد إرادتهم على ارتكاب الجريمة، ومن ناحية ثانية فإن الإتفاق الجنائي ظاهرة خطيرة لأنه يقوم على إلتقاء الإرادات الإجرامية للقيام بعمل إجرامي تجعل المصالح المحروسة بنصوص القانون مهددة بالخطر، وهذا التهديد هو الأمر الذي يدعو إلى تجريم الإتفاق، كما أن لا محل للقول

[1]– المادة 394مكرر 5، نفسه

[2]– أمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2006، ص131.

بأن الإتفاق الجنائي سيجعل المجرمين يقدمون على ارتكاب جريمتهم، لأن المشرع بتجريمه للاتفاق الجنائي يكون قد وقع العقاب لأول بادرة منهم في اتفاقهم.[1]

رابعا: عقوبة الشروع : الشروع في الشيء هو البدء في القيام به، والشروع في الجريمة ينصرف إلى البدء في تنفيذها.[2]

جاء في نص المادة 30 من ق ع ج ما يلي: " كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية إذا لم تتوقف أو لم يخب أثرها إلا نتيجة لروف مستقلة عن إرادة مرتكبها حتى لو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"

نصت المادة 11 من الاتفاقية بودابست على الزامية المعاقبة على الشروع في الجرائم الماسة بالأنظمة المعلوماتية و هو تبناه المشرع الجزائري في بالمادة 394 مكرر 7من قانون العقوبات: "يعاقب على الشروع في ارتكاب جنح المنصوص عليها في هذا القسم بالعقوبة المقررة للجنحة ذاتها". وهو النص الصريح الذي اشترط في نص المادة 31 من ق ع ج.

يبدو من خلال هذا النص رغبة المشرع في توسيع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ جعل الشروع في إحدى الجرائم الماسة بالأنظمة المعلوماتية معاقب بنفس عقوبة الجريمة التامة، ومن خلال استقراء نص المادة نستنتج أن الجنحة الواردة

---

[1]– فايز محمد راجح غلاب: الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه في الحقوق فرع القانون الجنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر،2010/2009، ص145.

[2]– علي حسن الشرفي: شرح الأحكام العامة للتشريع العقابي اليمني وفقا لمشروع القانون الشرعي للجرائم والعقوبات، دار المنار، القاهرة، 1993، ص254.

بنص المادة 394 مكرر5 من قانون العقوبات مشمولة بهذا النص، أي أن المشرع الجزائري بهذا المنطق يكون قد تبنى فكرة الشروع في الاتفاق الجنائي،[1] في الجريمة المعلوماتية قد يقوم الجاني بنشاطه المتمثل في الدخول إلى نظام معلوماتي إلا أن النشاط لا يكتمل بسبب تدخل شخص آخر أوقف ذلك النشاط، وقد يستكمل الجاني نشاطه إلا أن النتيجة لا تتحقق لسبب كان يجهله، ومثال ذلك في الجريمة المعلوماتية من يقوم باستخدام برنامج للدخول إلى النظام والتلاعب بالبينات، ويستطيع تحقيق الدخول لكنه لا يستطيع تحقيق الجريمة الأخرى لخلل في البرنامج، وبالتالي تتحقق جريمة الدخول، وجريمة الشروع في التلاعب بالمعطيات وفي هذه الحالة تسمى الجريمة بالجريمة الخائبة.[2]

الفرع الثاني العقوبات التكميلية

جاء في نص المادة394 مكرر 06 من ق ع ج " مع الإحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها" وفي ما يلي نفصل ما جاء في نص المادة:

[1]– عطاء الله قشار، المرجع السابق ذكره، ص35.

[2]– فايز محمد راجح غلاب، المرجع السابق ذكره، ص150.

المصادرة: هي الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة، أو مايعادل قيمتها عن الاقتضاء[1] وفي الجرائم المعلوماتية بصفة عامة تعني مصادرة الأجهزة والبرامج والوسائل المستخدمة لارتكاب الجرائم الماسة بالنظام وذلك ببيعها، أو حجزها مع مراعاة حقوق الغير حسن النية، وهذا القيد نابع من طبيعة العقوبة كونها شخصية يجب أن لا تطال الغير حسن النية، والغير هو كل أجنبي عن الجريمة تماما، ومبررات عدم عقوبة حسن النية لأنه لم يكن يعلم بأن تلك الأجهزة سوف تستخدم في ارتكاب الجريمة، فلم يتوافر بحقه القصد الجنائي العمدي أو حتى الخطأ، ولا تقتصر حقوق الغير حسن النية على حق الملكية فحسب، بل إن الحقوق الأخرى مثل حق الانتفاع والرهن يسري عليها ما يسري على حقوق الملكية، ولا تشملها عقوبة المصادرة بحق حسن النية.[2]

إغلاق المواقع :إغلاق مواقع الإنترنت أو المواقع الإلكترونية بصفة عامة، والتي كانت وسيلة لارتكاب هذه الجرائم أو ساهمت في ارتكابها.

إغلاق المحل(المقهى الإلكتروني) :يكون في الحالة التي يكون صاحب المحل مشاركا في الجريمة وذلك إذا تمت الجريمة وهو عالم بها ولم يتصدى لها بالإخبار عنها، أو بمنع مرتكبيها من ارتياد محله لارتكاب مثل هذه الجرائم.[3]

وفي المادة 18 مكرر من قانون العقوبات الجزائري نصت على العقوبات التكميلية للشخص المعنوي كما يلي:

---

[1]– المادة 15 من ق ع ج.

[2]– محمد خليفة: مرجع سبق ذكره، ص121.

[3]– ختير مسعود، المرجع السابق ذكره، ص ص 102–103.

- حل الشخص المعنوي،
- غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس (5) سنوات،
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس (5) سنوات،
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز خمس (5) سنوات،
- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها،
- نشر وتعليق حكم الإدانة،
- الوضع تحت الحراسة القضائية لمدة لا تتجاوز خمس (5) سنوات، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته.

المبحث الثاني: الجوانب الإجرائية لجريمة القرصنة الإلكترونية في القانون الجزائري

استقر الفكر القانوني على ضرورة إيجاد نصوص خاصة للمكافحة والحد من الجرائم الالكترونية والمشرع الجزائري بدوره استحدث نصوص قانونية تجريمية لقمع هذه الجرائم وذلك بالتعديلات الواردة على قانون العقوبات الجزائري وقانون الإجراءات الجزائية وسن القوانين المناسبة للحد من هذه الظاهرة في هذا المبحث سنقوم بدراسة المكافحة الإجرائية في القانون الجزائري في المطلب الأول، أما المطلب الثاني فنخصصه لدراسة إجراءات جمع أدلة الإثبات في جريمة القرصنة.

المطلب الأول: المكافحة الإجرائية في القانون الجزائري

سنقوم بدراسة المكافحة الإجرائية لجريمة القرصنة الإلكترونية في القانون الجزائري من خلال تقسيم هذا المطلب إلى فرعين، سنتناول في الفرع الأول المكافحة الإجرائية في قانون الإجراءات الجزائية الجزائري وفي القانون رقم 04/09، أما الفرع الثاني فسندرس فيه الأجهزة المختصة في متابعة جريمة القرصنة الإلكترونية.

الفرع الأول: المكافحة الإجرائية في قانون الإجراءات الجزائية الجزائري وفي القانون رقم04/09

أولا: المكافحة الإجرائية في قانون الإجراءات الجزائية الجزائري

سارع المشرع الجزائري بتعديل قانون الاجراءات الجزائية تماشيا مع التطور الذي لحق بالجريمة محاولة منه تطويقها والقضاء عليها أو على الأقل الحد من انتشارها، وذلك في إطار المكافحة الإجرائية لهذا النوع من الإجرام، حيث وضع قواعد وأحكام خاصة لسلطة التحري والمتابعة الغرض منها هو مواجهتها، وقد وردت في ق إ ج حسب آخر تعديل منه.

1- جواز تمديد الاختصاص المحلي والنوعي الدولي للمحاكم الجزائرية: حيث نصت المادة 32 من ق إ ج في فقرتها الأخيرة على جواز تمديد الاختصاص المحلي للمحكمة ليشمل اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

كما أنشئت الأقطاب القضائية الجزائية المتخصصة بموجب ق إ ج المعدل ومن بين الجرائم التي تختص بها نجد الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وذلك في المواد 37، 40 و 329 من نفس القانون.[1]

2- توسيع مجال اختصاص النيابة العامة: بموجب المادة 37 من ق إ ج، تم توسيع مجال اختصاص النيابة العامة ليشمل نطاقات أخرى لم يكن مرخص لها بها من قبل، حيث نصت هذه المادة على تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والارهاب والجرائم المتعلقة بالصرف، كذلك سحب نظام الملائمة من النيابة العامة في مجال متابعة بعض الجرائم، إذ يلتم وكيل الجمهورية بتحريك الدعوى العمومية بقوة القانون، بحيث لا يتمتع بشأنها بسلطة الملائمة بين تحريك الدعوى العمومية وعدم تحريكها مثلما فعل في الجرائم المنصوص عليها في المواد 144 مكرر و 144 مكرر1 و 144 مكرر2 من ق ع.[2]

ثانيا: المكافحة الإجرائية في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها (04/09)

تكمن أهمية هذا القانون في كونه يجمع بين القواعد الإجرائية المكملة لقانون الإجراءات الجزائية ويبين القواعد الوقائية التي تسمح بالرصد المبكر للاعتداءات المحتملة والتدخل السريع

[1]- أمحمدي بوزينة أمنة: إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، الملتقى الوطني بعنوان آليات مكافحة الجرائم المعلوماتية في التشريع الجزائري، جامعة الجزائر العاصمة، 2017/03/29، ص67.

[2]- نفسه، ص68.

لتحديد مصدرها والتعرف على مرتكبيها، وقد جرم الأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عامة، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الانترنت وعلى كل تقنية تهر مستقبلا، وقد حدد القانون الحالات التي يسمح فيها اللجوء إلى المراقبة الالكترونية كالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة أو في حالة توفر معلومات عن احتمال اعتداء منظومة معلوماتية، وقد تعرض الفصل الأول من القانون إلى أهدافه وتحديد مفهوم التقنية، أما الفصل الثاني فقد تعرض إلى أحكام خاصة بمراقبة الاتصالات الالكترونية، والفصل الثالث تعرض إلى القواعد الإجرائية الخاصة بالتفتيش في مجال الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، والفصل الرابع تعرض إلى تحديد الالتزامات التي تقع على المتعاملين في الاتصالات الإلكترونية، ثم الفصل الخامس نص على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحتها والفصل السادس فقد نص على التعاون والمساعدة القضائية الدولية بخصوص مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال خاصة منها المساعدة وتبادل المعلومات.[1]

الفرع الثاني: الأجهزة المختصة في متابعة جريمة القرصنة الإلكترونية

أولا: على مستوى جهاز الشرطة: في سنة 2007 استحدثت المديرية العامة للأمن الوطني بمخابر الشرطة العلمية الكائن مقرها بالجزائر العاصمة ووهران وقسنطينة، أقسام مختصة في تتبع الأدلة الرقمية من خلال استغلال أجهزة إلكترونية قصد استخراج وتتبع ما من شأنه أن يفيد في التحقيق ويساعد العدالة في تقرير الأحكام في القضايا التي تكون من هذا النوع و لتدعيم المصالح الولائية للشرطة القضائية، خلقت المديرية العامة للأمن سنة 2010 ما يقارب

[1]– خلف فاروق، مرجع سبق ذكره، ص13.

23 خلية لمكافحة الجرائم الإلكترونية موزعة على النحو التالي: 08 خلايا على مستوى ولايات الشرق، ونفس الأمر على مستوى وليات الوسط، 06 خلايا على مستوى ولايات الغرب و خلية واحدة على مستوى الجنوب، لتقوم بعدها المديرية العامة للأمن الوطني بتعميم الخلايا على جميع مصالح أمن ولايات الوطن، للإشارة يتم انتقاء عناصر خلايا مكافحة الجرائم الإلكترونية على أساس الشهادات الجامعية والمؤهلات التي يحملونها[1]

ثانيا: على مستوى الدرك الوطني: يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع لقيادة الدرك الوطني قسم الإعلام و الإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية[2].

ثالثا: الأعوان المؤهلين لدى المصالح العمومية أو الخاصة[3]: يمكن خلال إجراءات التحقيق وجمع الأدلة تسخير الأعوان المؤهلين للمساعدة في سير الإجراءات ونجد من بين الأعوان مايلي:

أ- **الموظفون في قطاع المواصلات السلكية واللاسلكية:** يمكن لوكيل الجمهورية ولقاضي التحقيق ولضابط الشرطة القضائية الذي أذن له من وكيل الجمهورية أو أنيب إليه من طرف قاضي التحقيق أن يسخر كل عون مؤهل في هيئة عمومية أو لدى الخواص في قاع المواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية لعملية اعتراض المراسلات التي تتم

[1]- حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، جامعة محمد خيضر بسكرة،ص08.

[2]-إدريس قرفي: تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية بين اتفاقية بودابست والتشريع الجزائري، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، جامعة محمد خيضر بسكرة ، ص ص 10-11.

[3]- حابت أمال، مرجع سبق ذكره، ص09.

بوسائل الاتصالات السلكية واللاسلكية، وكذا وضع الترتيبات اللازمة لإلتقاط الصور والصوت، بعد تثبيت أجهزة خاصة بذلك في أماكن عمومية أو خاصة دون إذن مالك المحلات، كل ذلك في صدد جرائم التلبس أو جرائم معينة من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

ب-مقدمي الخدمات[1] بالأخص خدمات الأنترنت: تنص المادة 10 من قانون 09-04 على " في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه تحت تصرف السلطات المذكورة، ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق"، هذه المادة تضع على عاتق مقدمي الخدمات واجب مساعدة السلطة القضائية في تحقيقاتها بإمدادها بمعلومات خاصة بمحتوى الاتصالات.

ج- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

تم بموجب المرسوم الرئاسي رقم 15-261 إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته السابق الذكر، حيث تمارس الهيئة المهام

[1]- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام اتصالات، أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها، طارق ابراهيم الدسوقي عطية، مرجع سبق ذكره، ص 47.

المنصوص عليها في المادة 14 من القانون رقم 09-04 تحت رقابة السلطة القضائية ومن مهامها مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والإتصال بما في ذلك تجميع المعلومات وإنجاز الخبرة القضائية.[1]

المطلب الثاني: إجراءات جمع أدلة الإثبات في جريمة القرصنة

يعتبر التحقيق من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لما له من أهمية في التثبت من حقيقة وقوعها وإقامة الإسناد المادي على مرتكبيها بأدلة الإثبات على اختلاف أنواعها من أجل استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه، وهناك تشابه بين التحقيق في الجرائم المعلوماتية وبين التحقيق في الجرائم التقليدية، فهي جميعا تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والخبرة والاستجواب والشهود وجمع الأدلة، إلا أن التحقيق في الجرائم المعلوماتية له خصوصية خاصة، لأنه في بيئة رقمية[2]، سنقوم بتقسيم هذه الدراسة إلى دراسة ثلاثة فرع سندرس فيها إجراءات جمع الأدلة في جريمة القرصنة الإلكترونية وهي الفرع الأول سنتناول فيه كيفية حفظ المعلومات، و الفرع الثاني سندرس فيه التسرب واجراءاته أما الفرع الثاني فسندرس فيه اعتراض المراسلات الإلكترونية.

[1]- حابت أمال، المرجع السابق، ص11.

[2]– خلف فاروق: ، مرجع سبق ذكره، ص2.

الفرع الأول: حفظ المعطيات

إن هذا الإجراء يعد للجزائر سلطة قانونية جديدة، فهو أداة تحقيق مستحدثة ويقصد به توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزتها وتحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية[1]، ويتضح أن التحفظ العاجل هو إجراء أولي تمهيدي الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها، و بالإضافة إلى الأجهزة المختصة بجمع الأدلة في الجرائم المعلوماتية السالفة الذكر التي وجدنا من بينها مقدمي الخدمات الوارد ذكرهم في القانون رقم 09-04 السالف الذكر وهم:

1-أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منومة معلوماتية و/أو نظام الاتصالات.

2-و أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو مستعمليها.[2]

حيث من واجبهم مساعدة السلطة القضائية في التحقيق وقد نص المشرع على أن يتم حفظ هذه الاتصالات ومحتواها عند طلب السلطة المختصة حيث جاء في نص المادة 11 من القانون 09-04 على إلزام مقدمو الخدمة بحفظ:

[1]- خالد ممدوح ابراهيم، مرجع سبق ذكره، ص197.

[2]- المادة 02 قانون 09-04، مرجع سبق ذكره.

أ- المعطيات التي تسمح بالتعرف على مستعملي الخدمة

ب-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال

ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال

د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها

هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

وقد حددت مدة حفظ المعطيات بسنة واحدة ابتداء من تاريخ التسجيل وهو ماورد ذكره في نص نفس المادة المذكورة أعلاه.

الفرع الثاني: التسرب

يعرف التسرب على أنه": تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط الشرطة القضائية أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب، بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على أنه فاعل أو شريك)[1] ، وفي تعريف آخر هو : قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جناية

[1]- عبد الرحمان خلفي: محاضرات في قانون الإجراءات الجزائية، دار الهدى، بجاية،2010، ص75.

أو جنحة بإيهامهم أنه فاعل معهم أو شريك[1]، وفي تعريف آخر نجده يعني " التسلل والتوغل داخل مكان أو هدف أو تنظيم يصعب الدخول إليه أو ما يسمى بالمكان المغلق لكشف نوايا الجماعات الإجرامية"[2] وقد ورد تعريف التسرب في المادة 65 مكرر 12 من ق إ ج في الفقرة الأولى منها كما يلي: " يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك لهم أو خاف".

والجرائم الإلكترونية والتي من بينها جريمة القرصنة الالكترونية ورد ذكرها في المادة 65 مكرر 05 من ق إ ج حددت الجرائم المستحدثة التي يجوز فيها اللجوء إلى هذا الإجراء، ويمكن تجسيد عملية التسرب في الجرائم الالكترونية كاشتراك ضابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال، أو كلام يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويحاول الاستفادة حول كيفية اقتحام الهاكر لموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم[3] ، ويعتبر التسرب آلية جديدة في البحث والتحري عن الجرائم البالغة الخطورة على أمن الضبطية القضائية، بحيث تتطلب جرأة وكفاءة ودقة في العمل يجب التحضير لها وتنظيمها بدقة تامة، تستهدف أوساطا معينة

[1]– بوعناد فاطمة زهرة: مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، سنة 2013، ص70.

[2]–شويرف يوسف: التسرب كأسلوب للتحري والتحقيق والإثبات، مجلة المستقبل، مدرسة الشرطة (طيبي العربي) سيدي بلعباس، 2007، ص03.

[3]– خالد ممدوح ابراهيم، مرجع سبق ذكره، ص191.

مدروسة بشكل متقن، حيث يتم الوقوف أمام أدق التفاصيل والخصوصيات قبل مباشرة التسرب، لأن هاته العملية تتطلب المشاركة المباشرة في نشاط الجماعة الإجرامية، فيدخل ضابط الشرطة القضائية أو العون المكلف في اتصال مع الأشخاص المشتبه فيهم، ويربط معهم علاقات محدودة من أجل المحافظة على السر المهني إلى غاية تحقيق الهدف النهائي من العملية، ويتم اللجوء لمثل هذا النوع من التدابير في مرحلة التحقيق عندما تقتضي الضرورة ذلك، وبعد عدم نجاعة الأساليب العادية وحتى الغير عادية في الحقيقة مما يستوجب معه اللجوء لهذا الأسلوب من التحقيق لكشف حقيقة الجريمة ومرتكبيها.[1]

وقد قيد المشرع إجراء التسرب بمجموعة من القيود والتي نذكر من بينها:

- تحرير تقرير من طرف ضباط الشرطة القضائية: قبل مباشرة العملية إلى وكيل الجمهورية كمبدأ عام على أعمال الشرطة القضائية مع ذكر الأسباب فيه.[2]
- الإذن: وكيل الجمهورية هو المخول قانونا حسب نص المادة 35 مكرر 11 من ق إ ج بمنح الإذن بعد الاطلاع على التقرير ومدى ضرورة التحقيق للقيام بعملية التسرب والذي يتقيد بمجموعة من الشروط ورد ذكرها في نص المادة 65 مكرر 15 من ق إ ج والتي تتضمن (الكتابة، السبب، هوية ضابط الشرطة القضائية، المدة الزمنية 4 أشهر قابلة للتمديد).

[1]– عبد الرحمان خلفي، مرجع سبق ذكره، ص 74.

[2]– فوزي عمارة: إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، العدد 33، جامعة منتوري قسنطينة، جوان 2010،ص248.

- السرية التامة لعملية التسرب:وهو ما رود ذكره في نص المادة65 مكرر16 من ق إ ج.
- استعمال هوية مستعارة: وهو ما رود ذكره في نص المادة65 مكرر12 من ق إ ج.

الفرع الثالث: اعتراض المراسلات الإلكترونية

يحق للفرد التمسك بأسراره الشخصية وعدم انتهاكها سواء كان ذلك في مسكنه أو مراسلاته أو معلومة مخزنة في جهاز الحاسب الآلي الخاص به أو نظامه المعلوماتي، ولهذا فله الحق بالتمتع بحماية القانون لهذا الحق، وهو حق محمي من طرف أغلب القوانين و الدساتير المعاصرة[1]، وهو والمشرع الجزائري بدوره كفل حرمة حياة المواطن في الفقرة الثانية من المادة 46 والفقرة الثالثة من المادة 47 من الدستور الجزائري[2].

1-مفهوم المراسلات: عرف المشرع الجزائري المراسلة في القانون رقم 2000-03 المؤرخ في 2000/08/05 المتضمن تحديد القواعد العامة المتعلقة بالبريد والمواصلات السلكية

[1]- نصت المادة 12 من الإعلان العالمي لحقوق الإنسان الصادر عن الجمعية العامة للأمم المتحدة في 1948/12/10 على أنه: (لا يجوز تعرض أحد لتدخل تعسفي في حياته الخاصة....أو مراسلاته.....ولكل شخص الحق في الحماية القانونية ضد هذا التدخل) وبهذه الصياغة تقريبا وردت كذلك المادة 17 من الإتفاقية الدولية بشأن الحقوق المدنية والسياسية الصادرة عام 1976، وعلى المستوى الدولي الإقليمي تحظر المادة 3 من الإتفاقية الأوروبية لحقوق الإنسان وحرياته الاساسية إلا في أحوال استثنائية حددتها كل صور التعرض للحق في المراسلة سواء بالرقابة أو غيرها، أما على مستوى الأقطار العربية والإسلامية فقد نصت المادة (18/ب) من إعلان القاهرة لحقوق الإنسان في الإسلام في عام 1990، ان للإنسان الحق في الاستقلال بشؤون حياته الخاصة في مسكنه وأسرته وماله واتصالاته، ولا يجوز التجسس أو الرقابة عليه أو الإساءة إلى شخصه، ويجب حمايته من كل تدخل تعسفي)، أنظر علي حسن محمد الطوالبة، مرجع سبق ذكره ص142.

[2]- المادة 46 :"لا يجوز انتهاك حُرمة حياة المواطن الخاصّة، وحُرمة شرفه، ويحميهما القانون.سرّيّة المراسلات والاتّصالات الخاصّة بكلّ أشكالها مضمونة.لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم.حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه.

واللاسلكية، وذلك في الفقرة 6 من المادة 09 التي ورد فيها أن المراسلة هي: " اتصال مجسد في شكل كتابي يتم عبر مختلف الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، لا تعتبر الكتب والمجلات والجرائد اليومية كمادة مراسلات".

وبالرجوع إلى نص المادة 02 الفقرة (و) من القانون رقم 09-04 نجد أن تعريف الاتصالات الإلكترونية هي: "أي تراسل أو ارسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية"

نلاحظ أن المشرع الجزائري لم يتطرق إلى تعريف إعتراض المراسلات في قانون الإجراءات الجزائية ولم يعرف حتى بالإجراء بل اكتفى بوضع تنظيم لهذا العملية وهو ما ورد في نصوص المواد 65 مكرر05 إلى غاية 65 مكرر 10 من نفس القانون ونفهم من ذلك أن المشرع ترك تعريفها للفقه وعند البحث وجدنا أن عملية اعتراض المراسلات يقصد بها:"اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض"، وقد ورد في اجتماع لجنة الخبراء للبرلمان الأوروبي بستراسبورغ المؤرخ في 2006/02/06 حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية تعريفا لإجراء اعتراض المراسلات بأنها: " عملية مراقبة سرية المراسلات السلكية واللاسليكة، وذلك في إطار البحث

والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجريمة"[1]،

وفيما يخص اعتراض المراسلات الالكترونية أكد المجلس الأوروبي في التوصية رقم R.(95)13 على أنه يتعين مراجعة القوانين في مجال الإجراءات الجنائية لسماح باعتراض الرسائل الإلكترونية وتجميع للبيانات المتعلقة بتداول المعلومات في حالة التحقيقات المتعلقة بجريمة من الجرائم الخطيرة الماسة بسرية أو سلامة الاتصالات أو أنظمة الكومبيوتر.[2]

و القانون الفرنسي الصادر في 1991/07/10 يجيز اعتراض الاتصالات البعدية بما فيها من شبكات تبادل المعلومات، وفي الولايات المتحدة الأمريكية يجوز اعتراض الاتصالات الإلكترونية بما فيها شبكات الحاسبة بشرط الحصول على إذن تفتيش صادر من القاضي المختص بناء على طلب من أعضاء النيابة ممن حددهم القانون الأمريكي بالموافقة على طلب تسجيل المحادثات الإلكترونية الذي يقدمه أحد رجال الضبط القضائي وقد حدد القانون الأمريكي الجرائم التي يجوز فيها استصدار إذن بتسجيل الاتصالات ومن أهمها الجرائم المعاقب عليها بالإعدام أو بالحبس لمدة تزيد عن سنة واحد.[3]

[1]– لوجاني نور الدين: أساليب البحث والتحري وإجراءاتها، يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية، يوم 2007/12/12، الجزائر، ص08. .

[2]– شيماء عبد الغني محمد عطاالله، مرجع سبق ذكره، ص268.

[3]–نفسه، ص252.

2-القيود الواردة على اعتراض المراسلات الالكترونية: نص قانون الإجراءات الجزائية على اعتراض هذه المراسلات اذا اقتضت ضرورات التحقيق في الجرائم المعلوماتية للبحث عن الدليل وقد أحاط هذا الإجراء بمجموعة من الشروط وهي كالتالي:

- ترخيص السلطة القضائية ومراقبتها لعملية تنفيذ الضبط: حيث لا يمكن لضابط الشرطة القضائية القيام بإجراء اعتراض المراسلات دون الحصول على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق وهو ضمانة لازمة لمشروعية القيام بهذا الإجراء[1]، وتتم العملية تحت رقابة السلطة القضائية التي أذنت بالإجراء;[2]
- تحديد طبيعة الإتصالات المراد ضبطها ومدة الإعتراض: حيث يتم التعرف على الاتصالات المطلوب التقاطها، والمدة المحددة للقيام بهذا الإجراء هي أربعة أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق.[3]
- الإذن وهو شرط أساسي وضروري لمباشرة عمليات اعتراض المراسلات وتسجيل الأصوات، إذ يجب أن يضمن جمع المعلومات والعناصر المكونة للجريمة والتي تسمح لوكل الجمهورية أو لقاضي التحقيق بالتعرف على الاتصالات المطلوب التقاطها وكذلك طبيعة الجريمة التي تبرر اللجوء إلى هذه التدابير ويشترط لصحة الإذن أن يكون مكتوبا وهذا كمبدأ عام على أعمال الضبطية القضائية حسب المادة19من قانون

[1]-المادة 65 مكرر 5 من ق إ ج، مرجع سبق ذكره.

[2]- المادة 65 مكرر 9، نفسه.

[3]- المادة 65 مكرر 7، نفسه.

الإجراءات الجزائية و تحديد المدة الزمنية وهي أربعة أشعر قابلة للتجديد حسب مقتضيات التحري و التحقيق.[1]

- وضع الترتيبات التقنية: بعد الحصول على رخصة الإذن يستطيع رجال الضبطية القضائية مباشرة وضع الوسائل والترتيبات التقنية، دوم موافقة الأشخاص المعنيين وهذا للمحافظة على السرية.[2]
- تحرير محضر عم العملية: نص قانون الإجراءات الجزائية وفي المادة :**18**منه، على وجوب التدوين وتحرير تقارير عن كل عملية وهذا كمبدأ عام لأعمال الضبطية القضائية[3]، كما جاءت في المادة :**65**مكرر **09**من قانون الإجراءات الجزائية لتعزز ما

جاء في المادة: 18 من نفس القانون فيما يتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور وعليه يجب على ضابط الشرطة القضائية أن يقوم بتحرير محضر عن كل عملية يذكر فيها جميع تفاصيل العملية من بدايتها أي من وضع الترتيبات اللازمة لمباشرة العملية حتى نهايتها، كما يجب ذكر في المحضر تاريخ وساعة بداية العملية وتاريخ الانتهاء منها. أما نتائج التحريات التي تتعلق بمضمون المراسلات المسجلة أو الصور الملتقطة فعلى ضابط الشرطة القضائية المأذون له أو المناب بهاته العملية أن ينسخ أو يصف المحتوى

[1]– فوزي عمارة: مرجع سبق ذكره، ص ص 241–242.

[2]– عبد الله أوهابية: شرح قانون الإجراءات الجزائية الجزائري، دار هومة،ط2، الجزائر،2011،ص280.

[3]– فوزي عمارة، مرجع السابق ذكره، ص243.

الضروري واللازم لإظهار الحقيقة في محضر ليودع بالملف، أما إذا كانت المكالمات باللغات الأجنبية، فإنه يتم الاستعانة بمترجم لترجمة محتوى المكالمات ونسخها[1].

[1]– عبد الله أوهابية، مرجع سبق ذكره، ص280.

خاتمة الفصل:

وختاما ومن دراستنا لهذا الفصل نخلص إلى أن المشرع الجزائري قد قام بالإجراءات المناسبة للتصدي ومكافحة جريمة القرصنة الإلكترونية و الجرائم المعلوماتية عامة وذلك بتعديل القوانين واستحداث قوانين جديدة لتجريم كل صور الإعتداء على أنظمة المعالجة الآلية للمعطيات، وقد خص هذا النوع من الجرائم بإجراءات خاصة في كيفية الحصول أو تجميع الأدلة التي تدين القراصنة وتسخير مختلف الأجهزة الأمنية لمحاربة هذه الجريمة.

الخاتمة

في الأخير نخلص إلى القول بأن الجزائر واجهت مشاكل جرائم القرصنة الالكترونية و الجرائم المعلوماتية عامة بتعديل مجموعة من القوانين وسن قوانين جديدة تعالج المشاكل الإجرائية لهذه الجرائم ولا شك بأن التعديل القانوني تدارك الفراغ التشريعي كونه جسد مختلف أحكام الاتفاقية الدولية للإجرام المعلوماتي وتشديد العقوبة عند ارتكاب احدى الجرائم المنصوص عليها في الاتفاقية ، لأن الحماية من هذه الجرائم ليس الغرض منه حماية الحواسيب أو الأجهزة الالكترونية إنما حماية للمصالح العامة والخاصة التي تهم المجتمع والمرتبطة بالأجهزة الإلكترونية، ومن أهم النتائج التي خلصنا إليها بعد هذه الدراسة هي:

– تتسم الجريمة المعلوماتية بصعوبة اكتشافها، وذلك راجع لعدم ترك لأي أثر خارجي مرئي بالعين المجردة.

– جريمة عابرة للحدود يصعب تقفي أثرها مسببة لأضرار كبيرة وخسائر مادية وأمنية للدول والمؤسسات والأفراد.

– الطبيعة الخاصة بجريمة القرصنة الإلكترونية دعت المشرع إلى تعديل القوانين بما يتماشى مع مواجهة هذا النوع من الجرائم.

– تكتم المجني عليهم عن جريمة القرصنة وعدم التبليغ وتقديم شكاوي عن حالات القرصنة خوفا من المشاكل التي قد يواجهونها، مما يمثل عائق أمام محاربة الجريمة.

– نقص الوعي بسلبية الاستخدام السيئ للإنترنت مما يجعل بعض مرتكبي هذه الجرائم ينظرون إلى افعالهم كاختراق المواقع وتدميرها عمل بطولي يستحق الإشادة عليه.

من خلال هذه النتائج نقوم بطرح التوصيات التالية:

– تسخير كل الوسائل والجهات المختصة لمواجهة هذه الجريمة على المستوى الوقائي قبل حدوثها أو المستوى الإجرائي بعد حدوثها.

–وضع ضوابط لمقاهي الأنترنت وحصر المترددين عليها وتصميم قاعدة بيانات لهم حتى تسهل متابعتهم.

– الاستعانة بوسائل الإعلام وجميع مواقع التواصل الإجتماعي لتوضيح أهمية الإبلاغ عن الجرائم المعلوماتية وما يمكن أن ينتج من مخاطر عن الإحجام على ذلك.

– القيام بتنظيم ملتقيات وندوات علمية في الجامعات والمؤسسات التعليمية الشبابية حضوريا أو على المنصات الافتراضية وذلك للتوعية بأخطار هذه الجرائم.

أخيرا نرجو أن نكون قد وفقنا في دراسة هذا الموضوع من مختلف النواحي و لا نشك في نقص هذه الدراسة أو ما قد يعتريها من خطأ أو تجاوز وعزائنا في ذلك أننا لم ندخر جهدا ولا وقتا في محاولة إخراج هذه الدراسة في أتم وأحسن ما يكون، ولم يبقى لنا إلا أن نحمد الله على نعمته في مدنا بالصبر والقدرة على إخراج هذا العمل في صورته هذه فإن كنا قد وفقنا فمن الله وحده وإن كنا قد جانبنا الصواب فمن أنفسنا والشيطان.

–تم بعون الله–

المراجع

أولا: المصـــــادر

1/ القـــوانيـــن

- أمر رقم 66-156 مؤرخ في 8 جوان 1966 المتضمن قانون العقوبات معدل ومتمم لاسيما بالقانون رقم 14-04 المؤرخ في 2014/02/04.
- أمر رقم 66-155 مؤرخ في 08 يونيو1966، المتضمن لقانون الاجراءات الجزائية، معدل ومتمم لاسيما بالأمر رقم 15-02 المؤرخ في 23 يوليو 2015
- قانون رقم 09-04 المؤرخ في 14 05 اوت 2009 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المرتبطة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية،ع 47، 2009.
- قانون رقم 2000-03 مؤرخ في 2000/08/05 يحدد القواعد العامة المتعلقة بالبريد وبالموصلات السلكية واللاسلكية، الجريدة الرسمية الجزائرية، ع 48، 2000.
- مرسوم رئاسي رقم 15-256 مؤرخ في 2015/10/08 المحدد لتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية الجزائرية، ع53، 2015.

ثانيا: الكتب باللغة العربية

1/ الكتب العامة:

1.أحسن بوسقيعة: الوجيز في القانون الجزائي العام، دار هومه، الجزائر، ط 10، 2011

عبد الله أهايبية: شرح قانون الإجراءات الجزائية الجزائري (التحري والتحقيق)، دار هومه، ب ط، 2008.

2.عبد الله سليمان: شرح قانون العقوبات الجزائري القسم العام، ديوان المطبوعات الجامعية، الجزائر، ط6، س ط2005

3.علي حسن الشرفي: شرح الأحكام العامة للتشريع العقابي اليمني وفقا لمشروع القانون الشرعي للجرائم والعقوبات، دار المنار، القاهرة، 1993

4.مولود ديدان: قانون العقوبات، قانون رقم 09-01 المؤرخ في 25 فبراير 2009، د ط.

2/ الكتب المتخصصة:

1.أحمد خليفة الملط: الجرائم المعلوماتية، دار الفكر الجامعي، ط3، سنة 2006.

2.أمال قارة: الحماية الجزائية للمعلوماتية في التشريع الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2006.

3.بكرى يوسف بكرى: التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الاسكندرية، ط1، 2011.

4.الحسيناوي علي جبار، جرائم الحاسوب والأنترنت، د.ط، دار الباروزي للنشر والتوزيع، عمان.

5.حنان ريحان مبارك المضحكي: الجرائم المعلوماتية- دراسة مقارنة-منشورات الحلبي الحقوقية، لبنان، ط1، 2014.

6.خالد ممدوح إبراهيم: فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الاسكندرية، ط1، سنة 2009.

7.ختير مسعود: الحماية الجنائية لبرامج الكومبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر، ط2010.

8.شيماء عبد الغني محمد عطاالله: الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ب ط، 2007.

9.طارق ابراهيم الدسوقي عطية: الأمن المعلوماتي-النظام القانوني للحماية المعلوماتية- دار الجامعة الجديدة للنشر، الاسكندرية، ب ط، 2009.

10.عائشة بن قارة مصطفى: حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، ب ط، 2010.

11.عبد الباقي الصغير: القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، دار النهضة العربية، القاهرة، سنة 1992.

12.عبد اللاه أحمد هلالي: تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربية،ط1، القاهرة، 2006.

13.علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة، الاسكندرية، 1999.

14.علي عدنان الفيل: إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، ب ط، 2011.

15.مصطفى محمد موسى: التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة للطباعة والنشر و التوزيع، ط1، 2008.

16.نائلة عادل محمد فريد قورة: جرائم الحاسب الآلي الاقتصادية، المنشورات الحلبي الحقوقية،ط1، س ط2005.

17.نهلا عبد القادر المومني، : الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ط1،2008.

18.هشام محمد فريد رستم: قانون العقوبات ومخاطر تقنية المعلومات، ط1، مكتبة الآلات الحديثة، أسيوط، 1992.

ثالثا: الأطروحات والرسائل

1/أطروحات الدكتوراه:

1.بدري فيصل: مكافحة الجريمة المعلوماتية في القانون الدولي والداخلي، أطروحة دكتوراه، جامعة الجزائر 01- بن يوسف بن خدة-كلية الحقوق،2018/2017.

2.علي حسن محمد الطوالبة: التفتيش الجنائي على نظم الحاسوب والأنترنت- دراسة مقارنة- أطروحة دكتوراه، جامعة عمان العربية للدراسات العليا، كلية الدراسات القانونية العليا، 2003.

3.عمر أبو بكر بن يونس: الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، دار المنار، القاهرة، 1994.

4.فايز محمد راجح جغلاب: الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة دكتوراه، جامعة الجزائر1، كلية الحقوق، 2009-2010.

2/رسائل الماجستير والماستر:

1.صغير يوسف: الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون(تخصص القانون الدولي للأعمال)، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، س 2013.

2.عبابسة فاروق، عبوب خديجة: القرصنة الإلكترونية وأثرها على المستخدم، مذكرة لنيل شهادة الماستر تخصص إعلام واتصال، جامعة عبد الحميد ابن باديس مستغانم،2016/2015.

3.محمد خليفة: الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، رسالة ماجستير، دار الجامعة الجديدة، الإسكندرية،2007.

4.نعيم سعيداني: آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج لخضر –باتنة– كلية الحقوق والعلوم السياسية،2012–2013.

رابعا: المقالات

1.بوعناد فاطمة زهرة: مكافحة الجريمة الالكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، سنة 2013.

2.جمال زين الدين العابدين أمين أحمد: جرائم إختراق النظم الإلكترونية بين التشريع المصري والمغربي، مجلة مستقبل العلوم الاجتماعية، العدد الأول، أفريل 2020، المغرب.

3.شويرف يوسف: التسرب كأسلوب للتحري والتحقيق والإثبات، مجلة المستقبل، مدرسة الشرطة (طيبي العربي) سيدي بلعباس، 2007.

4.فوزي عمارة: إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، العدد 33، جامعة منتوري قسنطينة، جوان 2010.

5.لطرش فيروز، بن عزوز حاتم، مقال بعنوان: الجريمة الإلكترونية في الجزائر: من جريمة فردية إلى جريمة منظمة، مجلة آفاق للعلوم، جامعة زيان عاشور الجلفة، العدد01، 2016.

6.مزيود سليم: الجريمة المعلوماتية وواقعها في الجزائر وآليات مكافحتها، المجلة الجزائرية للاقتصاد والمالية، جامعة المدية، العدد الأول، أفريل2014.

خامسا: الملتقيات و المؤتمرات

1.إدريس قرفي: تفتيش البيانات المعلوماتية المخزنة كآلية إجرائية بين اتفاقية بودابست والتشريع الجزائري، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، جامعة محمد خيضر بسكرة.

2.أمحمدي بوزينة أمنة: إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)، الملتقى الوطني بعنوان آليات مكافحة الجرائم المعلوماتية في التشريع الجزائري، الجزائر العاصمة، 2017/03/29.

3.جراف سامية، مداخلة بعنوان: سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-17 نوفمبر 2015، جامعة محمد خيضر بسكرة.

4.حابت أمال: الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-17 نوفمبر 2015، جامعة محمد خيضر بسكرة.

5.حملاوي عبد الرحمان، دور المديرية العامة للأمن الوطني في مكافحة الجرائم الإلكترونية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، جامعة محمد خيضر بسكرة.

6.خلف فاروق: الآليات القانونية لمكافحة الجريمة المعلوماتية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، جامعة محمد خيضر بسكرة.

7.ذياب موسى البداينة: الجرائم الإلكترونية: المفهوم والأسباب، ورقة علمية مقدمة في الملتقى العلمي بعنوان الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية 2-2014/9/4، كلية العلوم الاستراتيجية، عمان، المملكة الأردنية الهاشمية.

8.رابحي لخضر، بن بعلاش خاليدة، مداخلة تحت عنوان: معالجة الجرائم المعلوماتية في ظل التعاون الدولي والاستجابة الوطنية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، جامعة محمد خيضر بسكرة.

9.عز الدين عز الدين: الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها، ملتقى حول الجرائم المعلوماتية، قيادة الدرك الوطني، وزارة الدفاع الوطني، بسكرة في 16 نوفمبر 2015.

10.عطاء الله قشار، مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009.

11.لوجاني نور الدين: أساليب البحث والتحري وإجراءاتها، يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية، يوم 2007/12/12، الجزائر.

سادسا:المواقع الإلكترونية

مقال منشور على موقع https://www.skynewsarabia.com بتاريخ 2018/04/11 على الساعة: 05:44، تاريخ الاطلاع: 2022/04/20.

عادل عبد الله خميس المعمري: التفتيش في الجرائم المعلوماتية، بحث منشور على موقع المنهل https://platform.almanhal.com، ب ت. تاريخ الاطلاع: 2022/04/20.

سادسا: المراجع الأجنبية

Rose (philipe) la criminalité informatique à l'horizon 2005 – analyse prospective, l'harmattan, 1992.

Duleroy ®et rocco (A.M), l'informatique nouvelle, avril 1976, les escrocs a l'informatique, le nouvel Economsiste , les octobre,1979 ,n202.

الفهرس

الفهرس