

جامعة عبد الحميد بن باديس مستغانم

المرجع:

كلية الحقوق و العلوم السياسية

قسم : القانون العام

مذكرة نهاية الدراسة لنيل شهادة الماستر

جريمة القرصنة في التشريع الجزائري

ميدان الحقوق و العلوم السياسية

التخصص: القانون الجنائي و العلوم الحنائية

تحت إشراف الأستاذة:

- بوكر رشيدة

الشعبة: الحقوق

من إعداد الطالبة :

- راحراح شهرزاد

أعضاء لجنة المناقشة

رئيسا	بوزيد خالد	الأستاذ
مشرفا مقرا	بوكر رشيدة	الأستاذة
مناقشا	بلباي إكرام	الأستاذة

السنة الجامعية: 2022/2021

نوقشت يوم: 2022/06/21

الإهداء

الحمد لله و كفى و الصلاة على الحبيب المصطفى و
أهله و من وفى اما بعد:

الحمد لله الذي وفقني لتتمين هذه الخطوة في مسيرتي
الدراسية بمذكرتي هذه ثمرة الجهد و النجاح بفضلته تعالى
،مهداة إلى من يفرحان لفرحي و يقدران اجتهادي و تعبى
إلى سندي بعد الله تعالى الوالدين الكريمين حفظهما الله
و ادامهما نورا لدربي ،

الى كل العائلة الكريمة التي ساندتني و لا تزال إلى
جدتي الغالية اطال الله في عمرها و إلى إخوتي حفظهم
الله

و الى كل من التقيتهم يوما في أبواب الجامعة و اروقتها
،الى كل من ساندني و لو بكلمة طيبة ،الى كل من كان
لهم اثر على حياتي

الشكر و العرفان

الحمد لله تمت بحمده الصالحات، واصلي وأسلم على
أفضل خلق الله ورسولنا وحبیبنا وشفیعنا محمدا صلی الله
عليه وسلم.

أتقدم بجزيل الشكر وعظيم الامتنان الى الأستاذة
" بوكر رشيدة "

التي تكرمت علي بإشرافها على هذه المذكرة، ولم تدخر
جهدا لتقديم النصح والتوجيه لإنجاز هذا العمل.
كما أتوجه لأعضاء اللجنة المناقشة كل باسمه لتفضلهم
بمناقشة هذا العمل، وعلى جهودهم المبذول وتقديمهم
التوجيهات القيمة.

كما أتوجه بالعرفان والامتنان الى الاساتذة الكرام لما قدموه
من جهد

مقدمة

تتوالى العصور والازمان على البشرية ويتوالى معها التطور والازدهار وزيادة المعرفة بما يحيط بالانسان ومدى قدرته على الاستفادة مما هو متوفر في بيئته .

وبعد الثورة الصناعية الكبرى في القرن التاسع عشر كان لا بد من تتويج هذه المرحلة باكتشافات تخدم الانسانية جمعاء ، وتحقق ذلك فعلاً بأختراع الحاسوب الآلي الذي ولج الى كل الميادين الصناعية والتجارية والطبية والعلمية وحتى العسكرية بل وتعدى الامر ذلك بكثير لدرجة اصبح من المستحيل الاستغناء عن الحواسيب في أي مكان حتى في المنازل .

للحصول على استشارة مجانية تفضل الى رقم مكافحة الابتزاز ومع اختراع الحاسوب كان هناك اختراع آخر لا يقل شأنأً واهمية عنه الا وهو وسائل الاتصالات وكان هذان الاختراعاان يتطوران يتقدمان بخطى ثابتة نحو الافضل كلاً على حده ، لحين اندماجها في خط واحد مع استخدام تقنية الشبكات السلكية واللاسلكية.

وبعد ان تحول العمل اليدوي الى الحاسوب الذي يرتبط عادة بحواسيب اخرى عبر شبكات صغيرة او كبيرة ، اصبحت المعلومات في خطر دائم لأن اختراق أي جهاز يعني امكانية الدخول الى الاجهزة الاخرى التي ترتبط عبر شبكة واحدة ، هذا الامر جعل العالم يفتح على نوع جديد من الجرائم والتي تعرف بسرقة المعلومات او كما يصطلح عليها بـ ((القرصنة الالكترونية)) التي اصبحت تشكل جناية لا تقل خطورة وتأثيراً عن باقي انواع الجرائم .

وللقرصنة الالكترونية عدة اشكال منها ما يهدف الى سرقة بيانات من حاسوب معين ومنها ما يهدف الى التخريب فقط كمسح البيانات على سبيل المثال ، وهذه الاهداف تعتمد على طبيعة المخترق فاذا كان هاوياً فأن اعماله لا تجاوز التجربة ومحاولة التعلم اكثر او حتى مجرد الاطلاع وهذا النوع يكون خطيراً جداً لأنه قد يتسبب بحذف انظمة كاملة دون ان يعلم كما انه يترك اثراً محسوساً على النظام الذي اخترقه ، اما اذا كان محترفاً فأن الامر يختلف كثيراً لأنه

يدرك جيداً ما يفعله ويكون له هدف محدد فعلى سبيل المثال يستطيع وعبر ثغرة معينة الدخول الى ارقام الحسابات المصرفية في بنك ما ويستطيع عبر عدة اجراءات تحويل مبالغ مالية الى رصيده الشخصي او الى اي زبون اخر لذلك المصرف دون ان يشعر الاخوين بذلك . او العبث في الانظمة الالكترونية التي تستخدم في المطارات مما يسبب ارباكاً كبيراً في حركة الطيران .

ومن خلال ظهور فكرة الدولة تولت بنفسها سلطة تحرم الأفعال و العقاب عليها، حيث أصدرت تشريعات منها ما هو موضوعي " قانون العقوبات"، الذي يجرم الأفعال ويحدد العقوبات عليها، ومنها ما هو إجرائي "قانون الإجراءات الجزائية " الذي يحدد الإجراءات الواجب إتباعها أمام الهيئات القضائية وكذا الضبطية القضائية، دون أن ننسى أن الشريعة الإسلامية المناسبة لكل زمان ومكان، قد حددت كليات خمس لاستتقيم الحياة إلا بها، وهي حفظ الدين، حفظ النفس، حفظ العقل، حفظ النسل، حفظ المال، وبينت أن مسألة المحرم تكون استناداً لمبدأ حرية الاختيار، قال تعالى : " إن الذين كذبوا بآياتنا واستكبروا عنها لا تفتح لهم أبواب السماء ولا يدخلون الجنة حتى يلج الجمل في سم الخياط وكذلك نجزي المجرمين ."¹

غير أنه بتطور الإنسان في شتى الميادين، خصوصاً في مجال التقنية، إذ ظهر الحاسب الآلي وشبكة الأنترنت، وغزت هذه الوسيطتين جميع المجالات نظراً لما تتسم به من الدقة والسرعة ، وأصبحت في متناول الجميع، كل ذلك أدى إلى بروز طائفة جديدة من الجرائم، ونوع جديد من المجرمين، وهو الإنعكاس السلبي لهذه الثورة العلمية، حيث تطورت الجريمة بدورها وأصبحت تمس المعلومات وهو ما يسمى بالجريمة الإلكترونية، فهذه التقنية تسمح بنقل المعلومة صوتاً وصورة عبر الأنترنت، وفي أي مكان من العالم، مما يسمح للبعض استغلال هذه الشبكة في ارتكاب جرائمهم، وهذا يعتبر خطر يهدد المجتمع والعالم ككل، وهذا ما يعطي أهمية كبيرة للموضوع تستدعي دراسة هذه الظاهرة المستجدة باعتبارها كانت غير معروفة في

1- سورة الأعراف، الآية 40.

القانون الجنائي، لذا كان اهتمامي بالبحث في موضوع الجريمة الإلكترونية، بغية شرح وتحليل المفاهيم القانونية المتعلقة بها.

أهمية الدراسة

ان أهمية دراسة في الموضوع هو إثراء المكتبة وسد النقص في المراجع المتخصصة في هذا المجال، ومحاولة دراسة الظاهرة وتحليلها وبيان كيفية مكافحتها، غير أنه قد واجهتني بعض الصعوبات في إنجاز البحث، كون أن الموضوع له علاقة بالجانب التقني والفني، وهذا ما يستدعي التخصص للإلمام أكثر بالموضوع.

طرح الإشكالية التالية

والإشكال الذي يطرح في هذا الصدد هو:

هل التدابير والإجراءات المتاحة لمراقبة الأنظمة المعلوماتية من القرصنة الإلكترونية

وما هي الآليات التي تتم محاربتها وطرق مكافحتها في الجريمة القرصنة

للإجابة عن هذه الإشكالية الجوهرية ، لابد بالبحث في بعض التساؤلات التي تتفرع

عنها والتي من بينها، ما الإطار المفاهيمي للجريمة الإلكترونية مقارنة بالجريمة التقليدية؟

ما إجراءات البحث والتحري عن الجريمة الإلكترونية؟

وما طبيعة الدليل المناسب لإثباتها؟ وماهي الصعوبات التي تحول دون مكافحتها؟

اسباب اختيار الموضوع

ومن الأسباب الشخصية التي دفعتني للكتابة في هذا الموضوع، هو أنه مجرد إسمها

يكتسي جانب من الغموض خصوصا في إطار مكافحتها، فتجعل العقل يفكر في شكل مسرح

الجريمة، وطريقة التفتيش وغيرها من الإجراءات، وهذا ما أعطاني دافع للبحث وحب التعرف

عليها باعتبارها متعلقة بالعالم الافتراضي، أما الأسباب الموضوعية تتمثل في كون أن الجريمة الإلكترونية موضوع حديث يمس الواقع المعاش، كما أن الجريمة الإلكترونية تمس كل القطاعات، إذ أن الدولة تسعى إلى إنشاء إدارة إلكترونية، حكومة إلكترونية، وهذا ما يساعد على انتشار هذا النوع من الجرائم، وللإجابة على الإشكالية المطروحة، اعتمدت في ذلك على

المنهج المتبع

ومن هنا نجد اننا المناهج الملائمة وطبيعة الموضوع، منها المنهج التحليلي و الإستقرائي وذلك باستقراء وجمع المادة العلمية من مختلف المراجع، ثم المنهج التحليلي الوصفي إذ قمت بوصف الظاهرة وبيان المفاهيم القانونية الخاصة بها، وتحليل المفاهيم وشرحها بالتفصيل، ثم المنهج المقارن من خلال مقارنة الجريمة الإلكترونية بالجرعة التقليدية،

التقسيمات الدراسية

ومن خلال متابعتنا في هذه الدراسة نجد ان التقسيمات الخطة متبعة منهجية ثنائية الفصول، حيث خصصت الفصل الأول إلى ماهية الجريمة القرصنة الإلكترونية، بالتطرق إلى مفهومها من خلال تعريفها والدوافع المؤدية لارتكابها وكذا خصائصها و أنواعها، أما الفصل الثاني عالجت فيه الاليات القانونية لمكافحة الجريمة القرصنة الإلكترونية

الفصل الأول

ماهية الجريمة القرصنة الإلكترونية

تمهيد :

عندما يتبادر الى اسماعنا كلمة قرصنة فأنا نتخيل عصابات سرقة السفن البحرية والسطو عليها ونهب ما فيها واسر طاقمها ، وهو ذاته ما يفعله قرصان الانظمة الالكترونية بالضبط لكن بوسائل حديثة ودون ان يعرض نفسه للخطر .

فالقرصنة الالكترونية او المعلوماتية هي عملية اختراق لأجهزة الحاسوب تتم عبر شبكة الانترنت غالباً لأن اغلب حواسيب العالم مرتبطة عبر هذه الشبكة او حتى عبر شبكات داخلية يرتبط فيها اكثر من جهاز حاسوب ، ويقوم بهذه العملية شخص او عدة اشخاص متمكنين في برامج الحاسوب وطرق ادارتها أي انهم مبرمجون ذوو مستوى عال يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين التعرف على محتوياته ومن خلالها يتم اختراق باقي الاجهزة المرتبطة معها في نفس الشبكة .

وهو ما يعرف بالجريمة الإلكترونية، ونظرا لحدثة هذه الجريمة، فقد اختلف الفقهاء في وضع تعريف موحد لها، كما اتسمت بمجموعة من الخصائص، وعرفت نوع جديد من المجرمين لهم عدة دوافع لارتكاب هذه الجريمة، وسأحاول التطرق في هذا الفصل إلى مفهوم الجريمة الإلكترونية في المبحث الأول، و بيان خصائص و أنواع الجريمة الإلكترونية في القانون الجزائري من خلال المبحث الثاني.

المبحث الأول: مفهوم الجريمة القرصنة الإلكترونية

ومن هنا نجد ان المفهوم القرصنة واسع وله متغيرات حسب من يصنفها على الطريقة النظام الذي يتعرض لها ومن هذه التحليل نركز على مختلف التعريفات سأحاول التعرض إلى التعاريف المختلفة للجريمة الإلكترونية وكذا الأركان التي تتركز عليها وبيان الدوافع المؤدية لارتكابها، نظرا لطبيعتها الخاصة باعتبارها تقع في العالم الافتراضي، على خلاف الجريمة التقليدية التي تقع في الواقع الملموس، وذلك من خلال المطلبين المواليين:

المطلب الأول: تعريف الجريمة القرصنة الإلكترونية وأركانها

القرصنة الإلكترونية أو المعلوماتية هي عملية اختراق لأجهزة الحاسوب تتم عبر شبكة الإنترنت غالباً؛ لأن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة، أو حتى عبر شبكات داخلية يرتبط فيها أكثر من جهاز حاسوب، ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في برامج الحاسوب وطرق إدارتها؛ أي: إنهم مبرمجون ذوو مستوى عال يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين والتعرف على محتوياته، ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة.

فإن جرائم الأنترنت تتحقق بنقل المعلومات والبيانات بين أجهزة الحاسب الألي عبر خطوط الهاتف أو الشبكات الفضائية إلا أن الواقع التقني أدى إلى اندماج الميدانين (الحوسبة والاتصالات) وظهور مصطلح ¹cybercrime . و

قد انقسم الفقهاء إلى اتجاهين، منهم من ينظر إلى الجريمة الإلكترونية بمفهوم ضيق، ومنهم من ينظر إليها بمفهوم واسع، كما أن للجريمة الإلكترونية أركان لا تقوم الجريمة إلا بتوافرها، وهذا ما سأتناوله في الفرعين المواليين.

1- مفتاح بويكر الممطرودي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان، المنعقد في 2012/ 02/23 ، ص 13.

الفرع الأول: تعريف الجريمة القرصنة الإلكترونية

هناك عدة مصطلحات يمكن ان تستخدم للتعبير عن الظاهرة الجرمية الناشئة في بيئة الحواسيب الالكترونية والشبكات كسوء الاستخدام ، الاحتيال ، الجريمة المعلوماتية ، جرائم القرصنة ، الاختراق وجرائم الانترنت .

واختيار المصطلح يتعين بارتباط البعدين التقني والقانوني ، فاذا عدنا للحقيقة الاولى المتصلة بنشأة وتطور تقنية المعلومات نجدها تشمل فرعين جرى بحكم التطور تقاربهما واندماجهما هما الحوسبة والاتصالات ، فتقوم الحوسبة على استخدام التقنية لأدارة وتنظيم ومعالجة البيانات في اطار تنفيذ مهام محددة تتصل بعلمي الحساب والمنطق ، اما الاتصال فقام على وسائل تقنية لنقل المعلومات بجميع دلالاتها الدارجة .

يتبين لنا من ذلك ان من الصعوبة ايجاد مصطلح شامل يعبر عن كل الحالة الجرمية المرتكبة التي يقوم بها المخترقون ، فاذا وصفنا جريمة معينة بأنها جريمة اتصالات فليس بالضرورة ان تكون مرتبطة بالحاسوب او الانترنت وانما مقتصرة على سرقة خطوط هاتفية مثلاً ، واذا وصفنا حالة اخرى بأنها جريمة حاسوب فليس بالضرورة ان يكون لها علاقة بأجهزة الاتصال وانما قد تكون زرع برنامج فايروس في حاسوب ما .

لذا يجب ان يكون المصطلح المستخدم لوصف جرائم المعلوماتية شاملاً لمعنى الجريمة بكل تفاصيلها وتفرعاتها .

لقد اختلف الراء الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية، ويعود ذلك للاختلاف حول تحدي نطاق هذه الجريمة، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق، والبعض الآخر ينظر إليها بمفهوم موسع، وسأحاول التعرض لهذه التعاريف من خلال البندين المواليين.

اولا: الإتجاه المضيق من تعريف الجريمة الإلكترونية.

يعرف أنصار هذا الإتجاه الجريمة الإلكترونية بأنها، "كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لإرتكابه من ناحية، لملاحقته و تحقيقه من ناحية أخرى".¹ حسب هذا التعريف يجب أن تتوفر معرفة كبيرة بتقنيات الحاسوب ليس فقط لارتكاب الجريمة، بل كذلك لملاحقتها، والتحقيق فيها. وهذا التعريف يضيق بدرجة كبيرة من الجريمة الإلكترونية، بمعنى يجب أن يتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة، والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم. وهناك من يعرفها على أنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في اقتراه الحاسوب باعتباره أداة رئيسية". كما يرى الأستاذ tredmann أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات.²

ويرى الاستاذ rosenblatt بأن الجريمة الإلكترونية هي "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه".³

حسب هذا التعريف فإن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التجريم. ويرى الأستاذ باركار أن الجريمة الإلكترونية هي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل.⁴

1- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و العقاب، جامعة باتنة، 2012/2011، ص 13، نقلا عن قورة تاتلة، جرائم الحاسب الاقتصادية، القاهرة، 2004، ص 21.

2- حمزة بن عقون، الرسالة السابقة الذكر، ص14، نقلا عن أحمد هلاي عبد اللاد، ص 13.

3- حمزة بن عقون، نفس الرسالة، ص 14، نقلا عن يونس عرب، دليل أمن المعلومات والخصوصية، ص 213.

4- محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن، 2004، ط1، ص

ثانياً: الإتجاه الموسع من تعريف الجريمة الإلكترونية .

على عكس الإتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلاً، وذلك باستخدام شبكات الأنترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الإجتماعية، بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الإستهداف الحربي، أو الإقتصادي، أو الإضرار بسمعتها أو العكس، ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها، أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب .¹

وفي تقرير الجرائم المتعلقة بالحاسوب، أقر المجلس الأوروبي بقيام المخالفة (الجريمة في كل حالة يتم فيها تغيير معطيات، أو بيانات، أو برامج، أو محوها، أو كتابتها، أو أي تدخل آخر في مجال إنجاز البيانات، أو معالجتها، وتبعاً لذلك تسببت في ضرر إقتصادي، أو فقد حيازة ملكية شخص أو بقصد الحصول على كسب إقتصادي غير مشروع له، أو لشخص آخر.²

ودائماً حسب أنصار هذا الإتجاه يرى البعض أن الجريمة الإلكترونية هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاماً حاسوبياً، أو شبكة حاسوبية، للوصول إلى البيانات، والبرامج بغية نسخها، أو تغييرها، أو حذفها، أو تزويرها، أو تخريبها، أو جعلها غير صالحة، أو حيازتها، أو توزيعها بصورة غير مشروعة.³ أما البعض من الفقهاء يعرفوها بأنها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسوب الآلي

1- سميرة بسطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث ، ص 04/01
http://br2016/11/30_20h30.culture/net.alukah.www/

2- مليكة عطوي، المحلة السابقة الذكر، ص 09، نقلاً عن الطاهر روايتية، المسائلة، مقال، العدد 01، 1991، ص 15.

3- كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب، 21/23/ تشرين الأول، (2000)، بدون صفحة.

الرقمي و شبكة الأنترنت) بطريقة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف.¹

ومن خلال هذه التعاريف يتضح لنا صعوبة قبول هذا التوجه، لأن جهاز الحاسوب الآلي قد لا يعدو أن يكون محلا تقليديا في بعض الجرائم، كسرقة الحاسب الآلي نفسه، أو الأقراص الممغنطة، أو الإسطوانات الممغنطة على سبيل المثال. ومن ثم لا يمكن إعطاء وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسب الآلي أو أي من مكوناته كانوا محلا للجريمة، كما أنه قد ترتكب الجريمة ويستعمل الحاسب الآلي، ولا نكون أمام جريمة إلكترونية، كمن يقوم بالإتصال بواسطة حاسب آلي بشركائه في ارتكاب جريمة السطو على بنك.

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وعرفها بموجب أحكام المادة 02 من القانون رقم 09-04² على أنهما: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للإتصالات الإلكترونية." "

من خلال هذا التعريف نستنتج أن المشرع الجزائري تبني معيار دور النظام المعلوماتي التحديد معالم الجريمة، فسمي الجرائم الموجهة ضد النظام المعلوماتي بجرائم المساس بأنظمة المعالجة الآلية للمعطيات، كما بينها في قانون العقوبات³ من المادة 394 مكرر إلى 394

1- صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013/03/06، ص 09، تقلال كلوش علي، جرائم الحاسوب وأساليب مواجهتها بمجلة صادرة عن مديريةية الأمن الوطني، العدد 84، 2007، ص 51

2- القانون رقم 09-04، الصادر في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، ج العدد 47

3- القانون رقم، 04-15، الصادر في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66/156، الصادر في 08 جوان 1966، المتضمن قانون العقوبات، ج رالعدد 71.

مكرر 07، وترك المجال واسع لإي جريمة أخرى ترتكب عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية.

وحسب المشرع الجزائري فإنه قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الإتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الإتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية¹. ومن أمثلة الجريمة الإلكترونية المرتكبة في الجزائر، تسرب أسئلة البكالوريا لسنة 2016، قيام القرصان الجزائري حمزة بن دلاج بقرصنة حسابات بنكية عالمية الذي ألقى عليه القبض من طرف الشرطة الفيدرالية الأمريكية².

الفرع الثاني: أركان الجريمة القرصنة الإلكترونية

إن للجريمة الإلكترونية أركان ثلاثة وتتمثل في الركن الشرعي وهو الصفة غير المشروعة للفعل، وتتمثل قاعدة التجريم و العقاب فيها من خلال ما ورد النص عليه في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها.

أما الركن المادي يتمثل في ماديات الجريمة التي تبرز به إلى العالم الخارجي ، وأخيرا الركن المعنوي وهو الإرادة التي يقترن بها الفعل سواء في صورة القصد أو الخطأ.

كما أن للجريمة الإلكترونية كغيرها من الجرائم أطراف تتمثل في الجاني (المجرم الإلكتروني) وهذا المعنى يكون الجاني شخصا طبيعيا ذا أهلية وقدرة على تحمل العقوبة أو شخص معنوي ، أما المجني عليه يكون في الغالب الأعم شخص معنوي، كالبنوك والشركات

1- اسوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإحرام، جامعة ابوبكر بلقايد، تلمسان، 2010-2011 ، ص من 14 إلى 16.

2- جازية سليمان، موقع العربي الجديد ، تاريخ الدخول 09/02/2017 ، الساعة (20^h30)

<https://www.alaraby.co.uk/medianews>

وغيرها من المنظمات والهيئات التي تعتمد في إنجاز أعمالها على الحاسب الآلي ، علما أن للجريمة الإلكترونية محلا يتمثل في المعلومات، الأجهزة، الأشخاص أو الجهات.¹

المطلب الثاني: دوافع ارتكاب الجريمة القرصنة الإلكترونية

من منها نستنتج يتضح لنا، أن الجريمة القرصنة التقليدية والمجرم التقليدي يختلفان تماما عن الجريمة الإلكترونية والمجرم الإلكتروني، لذا من الطبيعي أن نجد نفس الإختلاف في الأسباب والعوامل التي تدفع إلى ارتكاب الفعل غير المشروع، فالدافع الباعث)، الغرض، الغاية، مفاهيم الكل منها دلالاته في القانون الجنائي، تتصل بما يعرف بالقصد الخاص في الجريمة، وهي مسألة تثير جدلا فقهيًا وقضائيا واسعا، ذلك أن القاعدة القضائية تقرر أن الباعث ليس عنصرا من عناصر القصد الجرمي، وأن الباعث لا أثر له في وجود القصد الجنائي، وإذا كان الإستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب، فإما من حيث الدلالة تتمايز، فالدافع هو العامل المحرك للإرادة والذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والإنتقام، وهو إذن قوة نفسية تدفع الإرادة إلى ارتكاب الجريمة ابتغاء تحقيق غاية معينة، وهو يختلف من جريمة إلى أخرى. أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي، ويتمثل بتحقيق النتيجة التي اصرف إليها القصد الجنائي أو الإعتداء على الحق الذي يحميه قانون العقوبات. وأما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الإنتقام، أو سلب مال المجني عليه في جريمة القتل.

وبالنسبة للجريمة الإلكترونية، فنمة دوافع عديدة تحرك الجناة لارتكاب أفعال الإعتداء المختلفة المنطوية تحت هذا المفهوم² ، وأهم هذه الدوافع سيتم بيا لها من خلال الفرعين الآتيين.

1- عبد الله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية، دراسة مقارنة، رسالة مكملة للحصول على درجة

الماجستير في القانون العام، جامعة الشرق الأوسط، 2014، ص من 26 إلى 36

2- حمزة بن عقون، رسالة الماجستير السابقة الذكر، ص 46 - 47.

الفرع الأول: الدوافع الشخصية لارتكاب الجريمة القرصنة الإلكترونية

تصنف هذه الدوافع إلى دوافع مادية وأخرى ذهنية، وذلك بمدى تأثير العنصر المادي لتحقيق الربح في ارتكاب الجريمة الإلكترونية، أو تأثير العنصر الذهني المعنوي على المحرم الإلكتروني ودفعه لارتكاب جريمته، هذا ما سيتم بيانه من خلال البندين المواليين.

أولاً: الدوافع المادية.

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الإلكترونية، وذلك لأن الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الإلكتروني إلى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية، ويستغل الفرص ويسعى إلى الإحتراف حتى يحقق أعلى المكاسب وبأقل جهد دون أن يترك أثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح إلى التلاعب بأنظمة المعالجة الآلية للبنوك والمؤسسات المالية إن كان أحد موظفيها، أو اختراق نظم المعالجة الآلية لها من خلال اكتشافه لثغراتها الأمنية، فيعمل على استغلالها و برمجتها لتحويل مبالغ مالية لحساب، أو لحساب شركائه، أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة. كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج أو المعلومات المتحصل عليها بطريق الإختلاس من جهاز الحاسوب، وقد أشارت في هذا الإطار مجلة "securite informatique" وهي مجلة متخصصة في الأمن المعلوماتي، أن 43% من حالات الغش المعلن عنها قد تمت من أجل اختلاس أموال، و23% من أجل سرقة معلومات، و19% أفعال إتلاف، و15% الإستعمال غير المشروع للحاسوب لأجل تحقيق منافع شخصية. وفي حقيقة الأمر أن في حال نجاح المجرم الإلكتروني في ارتكاب جريمته فإن ذلك يحقق له أرباح كبيرة في وقت قصير، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المحرم نتيجة اقترافه هذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول جرائم الكمبيوتر، أين أجريت هذه الدراسة بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية، وبنوك ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجريمة الإلكترونية، حيث تبين أن

85% من المشاركين في الدراسة تعرضوا لاختراقات بالنسبة للأنظمة المعلوماتية، وأن 64% لحقت بهم خسائر مادية جراء هذه الإعتداءات.¹

ثانيا : الدوافع الذهنية لارتكاب الجريمة الإلكترونية.

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

الفرع الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية

قد يتأثر المحرم الإلكتروني ببعض المواقف قد تكون دافعة له على اقتناف الإجرام الإلكتروني ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن إبراز أهم الدوافع من خلال البندين التاليين.

أولاً: دافع الإنتقام وإلحاق الضرر برب العمل.

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترقيّة، فهذه الأمور تجعله يقدم على ارتكاب جريمته³، كما يعتبر هذا الدافع من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، ذلك أنه غالباً ما يصدر عن شخص يملك

1- سعيد ابني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2012-2013، مر(6-1)، نقلا عن ملا عبدالقادر المومني، الجرائم المعلوماتية، ط02، 2010، ص 90، ونقلا عن صاح محمود الحمود ونشأت مفضي الحالي، جرائم الأنترنت، دار المنار للنشر والتوزيع، 2005، ص 31.

2- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص 61-62.

3- صغير يوسف، رسالة الماجستير السابقة الذكر، ص 42

معلومات كبيرة عن المؤسسة أو الشركة التي يعمل بها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدى المحرم الإلكتروني الرغبة في الإنتقام من رب العمل، ومثال ذلك أن الإنتقام دفع بمحاسب إلى التلاعب بالبرامج المعلوماتية بحيث جعل هذه البرامج تعمل على إخفاء كل البيانات الحسابية الخاصة بديون الشركة التي يعمل فيها بعد رحيله بستة أشهر، وقد تحقق هذا الأمر في التاريخ المحدد من طرفه.

ثانيا: دافع التعاون والتواطؤ.

هذا النوع يتكرر كثيرا في الجرائم الإلكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الأنظمة المعلوماتية، أين يقوم بالجانب الفني من المشروع الإجرامي، وآخر من المحيط أو خارج المؤسسة المجني عليها يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الأنظمة وتبادل المعلومات بصفة منتظمة حول أنشطتهم.¹

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

1- سعيد اني تعيم، رسالة الماجستير السابقة الذكر، ص62

2- سعيد التي تعيم، نفس الرسالة، ص 62.

المبحث الثاني: خصائص وأنواع الجريمة الإلكترونية في القانون الجزائري.

بعد التطرق لمفهوم الجريمة الإلكترونية، وبيان الدوافع المؤدية لارتكابها من طرف المحرم الإلكتروني، أحاول من خلال هذا المبحث بيان خصائص هذه الجريمة وذلك بالتطرق للسمات الخاصة بالجريمة الإلكترونية والسمات الخاصة بالمجرم الإلكتروني وتتنوع هذه الجريمة في التشريع الجزائري بحسب ما إذا ارتكبت باستخدام النظام المعلوماتي، أو كانت موجهة ضده، وهذا ما يتم بيانه في المطالبين الآتيين.

المطلب الأول: خصائص الجريمة القرصنة الإلكترونية.

لما كانت الجريمة القرصنة الإلكترونية هي نتاج التطور العلمي والتكنولوجي إن عمليات القرصنة تتطور وبسرعة فائقة باستخدام تقنيات حديثة ومعقدة؛ مما جعل النظرة إليها تتغير كلياً عما كانت عليه في المراحل السابقة، وسأحاول سرد أهم حالات القرصنة التي حدثت ، وبالتالي فهي تختلف عن الجريمة التقليدية التي ترتكب في الواقع المادي الملموس، لذا نجد لها مجموعة من الخصائص، أو السمات تجعلها منفردة عن غيرها من الجرائم، سواء من حيث الجريمة ذاتها، أو من حيث مرتكب الجريمة، وهذا ما يتم بيانه من خلال الفرعين المواليين.

الفرع الأول: السمات الخاصة بالجريمة الإلكترونية.

نظرا للطبيعة المميزة للجريمة الإلكترونية باعتبارها تمس المعلومات هذا ما جعلها تتميز عن نظيرتها التقليدية مجموعة من الخصائص أو السمات، إذ أن التعرف أكثر على خصائص هذه الجريمة يساعد في إيجاد الحلول لمكافحتها، وتتلخص هذه السمات فيما يلي:

- خفاء الجريمة وسرعة التطور في ارتكابها، حيث تتسم بأنها خفية ومستترة في أغلبها لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على شبكة الإتصالات، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته بدقة، مثلا عند إرسال الفيروسات المدمرة وسرقة الأموال

والبيانات الخاصة أو إتلافها، والتجسس وسرقة المكالمات وغيرها من الجرائم¹ . وقد تتم في ثانية أو جزء من الثانية في بعض الجرائم.

- ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية، وأجهزة ومعدات و تجهيزات الحاسب الآلي، بمعنى تتم بواسطة المكونات المادية للحاسوب (hardware)، ومكوناته البرمجيات (software).

- يقوم بها محرم ذو طبيعة خاصة وإمكانات خاصة (علمية معلوماتية)، يستخدم في ارتكاب جريمته الموارد المعرفية و الأساليب الإحترافية.

- صعوبة الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على الدليل المتوفر². ولعل صعوبة كشف الدليل تزداد بصورة خاصة متي ارتكبت هذه الجريمة في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة في هؤلاء يسهل عليهم اقتراف جر ائهم دون أن يتركوا آثار تدل عليهم.³

- الجريمة الإلكترونية تستلزم طرقا خاصة مستحدثة للإثبات، قوامها التعليم و التدريب المتخصص المستمر لعلوم الحاسب الآلي، لذا فإنها تقتضي وجود رجل شرطة إلكتروني، ومحقق إلكتروني، وقاضي إلكتروني، فضلا عن الخبير الإلكتروني حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم، وعليه فإن الإستعانة بالخبراء تصبح حتمية لكشف و تحليل و تفسير الدليل الجنائي، الذي يثبت البراءة أو الإدانة.

- هذه الجريمة لا يحدها مكان، فهي عالمية، إذ يمكن عن طريق الحاسب الآلي - أو حتى هاتف نقال - لشخص في الصين مثلا أن يرتكب جريمة تزوير أو سرقة معلومات أو نقود ضد شخص طبيعي أو معنوي في الو.م. أ، أو العكس.

1- صغير يوسف، رسالة الماجستير السابقة الذكر، ص 14 - 15.

2- عبدالناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإتيات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة مقارنة)، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، الرياض، 2007، ص 10.

3- موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا، طرابلس، 2009/10/29/28، ص 03

- تدني نسبة الإبلاغ عن الجريمة من طرف المجني عليه خاصة في حالة شركات ومؤسسات ، لتجنب الإساءة للسمعة و الرغبة في عدم زعزعة ثقة العملاء، ففي إحدى الوقائع تعرض أحد البنوك، وهو بنك "marchant bank city" في بريطانيا لسرقة ثمانية مليون جنية إسترليني من إحدى أرصده إلى رقم في سويسرا، وتم ضبط الفاعل متلبسا بسحب المبلغ المسروق وبدلا من محاكمته، قام البنك بدفع مليون جنية له ، بشرط التزام الفاعل بعدم الإعلام عن جريمته، و إعلام البنك عن الألية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي .

- غالبا ما تكون الخسائر الناجمة عنها فادحة للمجني عليه.¹

- ذاتية الجريمة الإلكترونية تبرز بوضوح في أسلوب ارتكابها وطريقتها، فإن كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر، و تقليد المفاتيح كما هو الحال في جريمة السرقة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية - الأنترنت مع وجود محرم يوظف خيبراته وقدراته على التعامل مع الشبكة، للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير لتغيير أو التغيير بالقاصرين، كل ذلك دون الحاجة السفك الدماء.

- الجريمة الإلكترونية تتم عادة يتعاون أكثر من شخص على ارتكابها إضرارا بالمجني عليه، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والأنترنت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها، لتغطية عملية التلاعب وتحويل المكاسب² .

1- عبد الناصر محمد محمود فرغلي، محماد عبياد سعيد المسماري، المرجع السابق الذكر، ص 10-11
2- سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر بسكرة، 2013 - 2014، ص18

الفرع الثاني: السمات الخاصة بالمجرم الإلكتروني.

- المعرفة والمهارة والذكاء:

بمعنى التعرف على كافة الظروف التي تحيط بالجريمة وتنفيذها وإمكانية حها، واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على كافة الظروف المحيطة بهم، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم. كما أن المحرم الإلكتروني يستطيع أن يكون تصورا كاملا لجريمته، بالإضافة إلى أنه يتمتع بقدر لا يستهان به من المهارة في مجال تقنية الحاسوب والانترنت، فتنفيذ جريمة يتطلب قدرا من المهارة لدى الجاني التي قد يكتسبها عن طريق الخبرة في مجال تكنولوجيا المعلومات. الجريمة الإلكترونية هي جريمة الأذكاء بالمقارنة بالجريمة التقليدية التي يكون فيها الميل إلى العنف، فالمحرم الإلكتروني يسعى إلى معرفة طرق جديدة ومبتكرة لا يعرفها أحد سواه، من أجل اختراق الحواجز الأمنية في البيئة الإلكترونية، ثم نيل مبتغاه.¹

- المجرم الإلكتروني يبرر ارتكاب جريمته:

إذ يوجد شعور لدى كل مرتكب فعل إجرامي أن ما يقوم به لا يدخل في قائمة الجرائم، خاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبوا هذه الجرائم بين الإضرار بالأشخاص الذي يعدونه غاية في الأخلاقية، وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم، ويبدو أن الإستخدام المتزايد للأنظمة المعلوماتية قد أنشأ مناخا نفسيا ملائما لتصور استبعاد فكرة الخير والشر قد ساعد على عدم وجود احتكاك مباشر بالأشخاص، هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع، ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل .

1- سمية مزغيش، رسالة الماجستير السابقة الذكر، ص 20.

- المحرم الإلكتروني يتصف بالخوف من كشف جريمته:

وبالرغم من أن هذه الحشية تصاحب المحرم على اختلاف أنماطه، إلا أنها تميز المجرم الإلكتروني بصفة خاصة، لما يترتب على كشف أمره من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان، كما أن طبيعة الأنظمة المعلوماتية نفسها تساعد الجاني على الحفاظ على سرية أفعاله، ذلك أن كثير ما يعرض المحرم إلى اكتشاف أمره، هو أن يطرأ أثناء تنفيذ جريمته عوامل غير متوقعة، في حين أن أهم الأسباب التي تساعد على نجاح الجريمة الإلكترونية في الحواسيب إنما تؤدي عملها غالباً بطريقة آلية، بحيث لا تتغير المراحل المختلفة التي تمر بها، أي من العمليات التي يقوم بها من مرة إلى أخرى.

- الحرمة الإلكترونية يميل إلى التقليد:

حيث يبلغ هذا الأخير أقصاه حينما يوجد الفرد وسط جماعة، إذ يكون عندئذ أسهل و أسرع انسياقا لتأثير الغير عليه، ويظهر ذلك من خلال محاولة الفرد تقليد غيره بالمهارات الفنية، مما يؤدي به الأمر إلى ارتكاب الجريمة، وذلك لعدم الإستواء في شخصية الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يوصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط المحيط، وينتهي به الأمر إلى التقليد وارتكاب الجريمة¹.

- القيام بالتخطيط والتنظيم:

ففي عالم الشبكات الإلكترونية، كما هو الحال في العالم الحقيقي، يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة حيث ترتكب أغلب الجرائم من مجموعة متكونة من عدة أشخاص يحدد لكل شخص دور معين، ويتم العمل بينهم وفقاً للتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متضمنا فيها متخصص في الحاسب الآلي يقوم بالجانب الفني من المشروع الإجرامي و شخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب ولتحويل المكاسب إليه.

1- سمية مزغيش، رسالة الماجستير السابقة الذكر، ص 20-21

- التكيف الإجتماعي:

فالمجرم الإلكتروني يقوم بواجباته ويمارس حقوقه الإجتماعية والسياسية دون أي عائق في حياته اليومية¹، إذ تعتبر هذه الخاصية إمتداد السمة التخطيط و التنظيم، حيث أن التكيف الإجتماعي ينشأ بين مجموعة لها صفات مشتركة، فمثلا جماعة صغار نوابغ المعلوماتية لا شك أن يتكيفون في أفكارهم فيما بينهم، وتنشأ بالتالي بينهم روابط تساعد على ارتكاب جرائمهم، وتتعدى تلك الروابط النطاق المحلي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم و منهجهم في استثمار تلك المعرفة والتقدم العلمي، وإقامة المؤتمرات الدولية بين هذه المجموعات خير دليل على تلك الصلات والروابط الدولية بينها، بالإضافة إلى أن المحرم الإلكتروني هو عادة إنسان إجتماعي²، بطبعه حيث يحي وسط المجتمع، ويمارس عمله في الحال المعلوماتي أو غيره من المجالات، وبناء عليه فإن كثير من الجرائم ترتكب بدافع الكبرياء (موظف طرد من عمله)، أو بدافع النصب أو الحسد أو اللهو وإظهار قدراته .³

- التطور في السلوك الإجرامي:

حيث يساهم وجود المجرم الإلكتروني في جماعة إجرامية إلى سرعة اكتسابه المهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة، إلى أعلى معدلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة. وبناء على ما تقدم يمكن تقسيم المجرم الإلكتروني إلى عدة طوائف مختلفة :

المخترقون أو المتطفلون: يتحد في هذا الإطار نوعين من المجرمين.

1- مليكة عطوي، المرجع السابق الذكر، ص 12.

2- سمية مزغيش، رسالة الماجستير السابقة الذكر، ص 22

3- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجاليسية، الإسكندرية، 2004، ص62

- الهاكرز :

وهو الشخص الذي يقوم بإنشاء أو تعديل البرمجيات و العتاد الحاسوبي، ويقصد بسم الشباب البالغ المقترن بالمعلوماتية والحاسبات الآلية، وقد يطلق على بعضهم صغار نوابغ المعلوماتية، وأغلبهم طلبة لهم معرفة في مجال التقنية المعلوماتية. إن الباعث الأساسي لدى الهاكرز هو الإستمتاع باللعب والمزاح باستخدام هذه التقنية لإثبات قدراتهم، باكتشاف مواطن الضعف في الأنظمة المعلوماتية دون إلحاق ضرر بها، لديهم الرغبة في المغامرة والتحري و الإكتشاف¹ ، والهاكرز أنواع، الهاكر ذو القبعة البيضاء (الهاكرز الأخلاقي)، ويطلق عليه الهاكر المصلح، ثم يوجد الهاكر ذو القبعة السوداء وهو الهاكر المفسد، وأخير هناك الهاكر ذو القبعة الرمادية ويسمى بالمترنح بين الإصلاح والعبث²، وما يهمننا هنا هو الهاكر ذو القبعة السوداء وذو القبعة الرمادية، أما الهاكر الأبيض فهو أخلاقي ولا يرتكب جرائم.

- الكراكرز :

وهو المقتحم، وتعرف هذه الطائفة بالمحرمين البالغين أو المخربين المهنيين وأعمارهم تتراوح بين 25-45 عاما، ومن أبرز سمات هذه الطائفة أهم ذوي مكانة في المجتمع، و أنهم غالبا من المتخصصين في مجال التقنية الإلكترونية، أي أنهم يتمتعون بمهارات فنية في مجال الأنظمة الإلكترونية، تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية للمعلومات.³ مجرموا الحاسب الآلي المحترفون: هذا النوع من المجرمين يعرف كيف يصل إلى أهدافه، باستخدام ما لديه من علم يطورونه باستمرار، وهدفهم المصاريف وسحب الأموال من الأرصد و نيتهم إحداث التخريب⁴، تتميز هذه الطائفة بسعة الحيرة والإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها، لذا فإن هذه الطائفة تعد الأخطر من

1- سمية مزغيش، رسالة الماجستير السابقة الذكر، ص 23.

2- مخترق، ويكيبيديا الموسوعة الحرة، التاريخ 2017/04/27 23:00h. <https://ar.wikiped.org/wiki>.

3- سمية مزغيش، رسالة الماجستير السابقة الذكر، ص 22-23.

4- مليكة عطوي، المرجع السابق الذكر، ص 13.

بين محرمي التقنية، حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم وللجماعات التي كلفتهم وسخرخم لارتكاب جرائم الكمبيوتر، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي. إن الأفعال الصادرة عن هذه الفئة تعكس ميولا إجرامية خطيرة، تنبئ عن رغبتها في إحداث التخريب، وهم أكثر خطورة من الصنف الأول.

الحاقدون:

هذه الطائفة يحرك أنشطتهم الرغبة في الإنتقام من صاحب العمل، أو لتصرف المنشأة المعنية معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين بالنظام محل الجريمة، و إلى غرياء عن النظام تتوفر لديهم أسباب الإنتقام من المنشأة المستهدفة في نشاطهم، إن أعضاء هذه الطائفة لا تتسم بالمعرفة التقنية الإحترافية، ومع ذلك يسعى الواحد منهم إلى الإلمام بالمعرفة المتعلقة بالفعل المخصوص الذي ينوي ارتكابه، ويستخدمون تقنيات الفيروسات والبرامج وتعطيل النظام أو الموقع المستهدف إن كان من مواقع الأنترنت، كما أحم من أعمار مختلفة، ولا تتوافر عناصر التفاعل بين أعضاء هذه الطائفة، وهم الطائفة الأسهل من حيث كشف أنشطتهم لتوفر ظروف و عوامل تساعد على ذلك.¹

صغار السن :

يسمون بصغار نوابغ المعلوماتية، وهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية، ومن بينهم فئة لم تنزل دون سن الأهلية مولعين بالحوسبة والاتصال، وقد تعددت أوصافهم في الدراسات الاستطلاعية، وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بالمتعلمين، الدال حسب تعبير الأستاذ " طوم فورلستر على الصغار المتحمسين للحاسوب بالشعور بالبهجة دافعهم التحدي لكسر الرموز السرية التركيبات الحاسوب، ويسميهم البعض

1- سمية مزغيش، رسالة الماجستير السابقة الذكر، ص 23- 24

كذلك مجانيين (معدلات ومعدلات عكسية)، بالإستناد إلى كثرة استخدامهم لتقنية المعدل و المعدل العكسي "الموديم"، الذي يعتمد على الإتصال الهاتفي الاختراق شبكة النظم، ويشير محرموا الحوسية من هذه الطائفة جدلا واسعا، ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، ظهرت مؤلفات ودراسات تخرج هذه الفئة من دائرة الإجرام إلى دائرة العبث و أحيانا البطولة من هذه المؤلفات على سبيل المثال، كتاب "خارج نطاق الدائرة الداخلية كيف تعملها؟"، لمؤلفه الأمريكي لبيب لاندريد، وكتاب " الدليل الجديد للمتعلمين"، لمؤلفه هوجوكوزن، وكتاب " المتعلمين أبطال ثورة الحاسوب"، لمؤلفه ستيفن ليفي .¹

مجرمون ذوي دوافع سياسية:

وهم أشخاص لهم ميول ودوافع سياسية معينة، تدفعهم الإختراق نظم الحاسب الآلي غير المصرح بالدخول إليها، والتي تحتوي على معلومات وبيانات غاية في السرية تتعلق بالدفاع والأمن، ويمثل المساس بها مخاطر كارثية .²

- الحرمة الإلكترونية مجرم يعود للإجرام، فهو يوظف مهاراته في كيفية عمل الحاسوب، وكيفية تخزين البيانات والمعلومات، والتحكم في أنظمة الشبكات من خلال الدخول غير المصرح به مرات ومرات، فهو قد لا يحقق جريمة الإختراق بهدف الإيذاء، وإنما نتيجة شعوره بقدرته ومهارته في الإختراق.

فالإجرام الإلكتروني هو إجرام الذكاء دونما الحاجة إلى استخدام القوة والعنف، وهذا الذكاء هو مفتاح الحرمة الإلكتروني، لإكتشاف الثغرات واختراق البرامج المحصنة. ويمكن إجمال القواسم المشتركة بين هؤلاء المجرمين في عدة صفات وهي: - عادة ما تتراوح أعمارهم ما بين 18 و 45 عاما- المهارة والإلمام الكامل والقدرة الهائلة في مجال نظم المعلوماتية - الثقة

1- سمية مزغيش، نفس الرسالة، ص 24-25

2- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، المرجع السابق الذكر، ص 09

الزائدة بالنفس - الإلمام التام بمسرح الجريمة، وبما يجنبه فجائية المواقف التي قد تؤدي إلى إفشال مخططه واقتضاح أمره.¹

المطلب الثاني: أنواع الجرائم القرصنة الإلكترونية في القانون الجزائري

تعتبر الجريمة القرصنة الإلكترونية في القانون الجزائري تصنف الجرعة التقليدية بحسب خطورتها إلى جنائية وهي أخطر الجرائم، وجنحة وهي متوسطة الخطورة، ثم مخالفة وهي أقل خطورة، وتصنف بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية². على خلاف هذه الجريمة، فإن الجريمة الإلكترونية عرفت اختلاف حول تقسيماتها، وذلك بسبب الاختلاف في تسميتها، حيث استند كل اتجاه على معيار معين، فالبعض يصنفها حسب الأسلوب المتبع في الجريمة، والبعض الآخر يستند إلى دوافع ارتكابها، وآخرون يؤسسون تقسيمهم على تعدد محل الإعتداء وتعدد الحق المعتدي عليه.³ أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الإلكترونية إلى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والاتصال، أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات، وهذا ما سيتم بيانه في الفرعين المواليين.

1- محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، الجزء الأول، بدون.

2- أحسن بوسقيعة، الوجيز في القانون الجزائري العام الديوان الوطني للأشغال التربوية، 2002، ط 01، ص 24

3- رضاع فتيحة، رسالة الماجستير السابقة الذكر، ص 69

الفرع الأول: الجريمة القرصنة الإلكترونية المرتكبة باستخدام النظام المعلوماتي

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، وهي أنواع منها الجريمة الواقعة على الأشخاص، الجريمة الواقعة على النظم المعلوماتية الأخرى، الجريمة الواقعة على الأسرار¹، وسأوضح كل نوع منها في البنود الآتية.

أولاً: الجريمة الإلكترونية الواقعة على الأشخاص الطبيعية.

تنقسم هذه الجرائم بدورها إلى جرائم واقعة على حقوق الملكية الفكرية، وجرائم واقعة على حرمة الحياة الخاصة.

1- الجريمة الإلكترونية الواقعة على حقوق الملكية الفكرية .

يكون النظام المعلوماتي وسيلة للإعتداء على حقوق الملكية الفكرية، ومثاله السطو على بنك المعلومات وتخزين واستخدام هذه المعلومات دون إذن صاحبها، لأن استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، ويندرج ضمن الحقوق الفكرية كذلك براءات الإختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع. وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الأمر رقم 0305 الصادر في 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 الصادر في 2003 المتعلق ببراءات الإختراع.²

2- الجريمة الإلكترونية الواقعة على حرمة الحياة الخاصة.

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الإعتداء على هذه الحرمة. ولما كان الحاسب الآلي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين أكبر قدر ممكن من المعلومات، وهذا ما جعل للحاسب الآلي دور في تسهيل

1- سوبر سفيان، رسالة الماجستير السابقة الذكر، ص 33

2- سوبر سفيان، رسالة الماجستير السابقة الذكر، ص 34-35

الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة، ومثاله أن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني ولكن يقوم المكلف بحفظها بإطلاع الغير عليها دون إذن صاحبها، أو أن يقوم شخص باختراق معلومات هي بمثابة أسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص آخر.

ثانياً: الجريمة الإلكترونية الواقعة على النظم المعلوماتية الأخرى.

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام أداة إلكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى، بالإضافة إلى إساءة استخدام البطاقة الائتمانية.

بالنسبة للحالة الأولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هنا الإستيلاء على المعلومات المخزنة لدى النظام المعلوماتي بعدة طرق باستخدام آلة الطباعة ، أو استخدام شاشة النظام، أو الإطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت، أما الحالة الثانية تكون في حالة اساءة استخدام العميل البطاقة الائتمانية، وذلك عن طريق عدم احترام العميل المصدر إليه البطاقة الائتمانية شروط العقد المبرم بينه وبين البنك، كاستعماله بطاقة إئتمانية إنتهت مدة صلاحيتها أو تم إلغاؤها، أما الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة إئتمانية للحصول على السلع والخدمات.¹

ثالثاً: الجريمة الإلكترونية الواقعة على الأسرار.

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة. ويتخذ هذا النوع من الجرائم صورتين،

1- سوير سفیان، رسالة الماجستير السابقة الذكر، ص 35-36-37.

الأولى تتعلق بالجرائم الواقعة على أسرار الدولة¹، حيث أتاح الأنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على الأسرار العسكرية والإقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات²، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمله الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الإمتناع عن القيام بعمل.³

وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنايات ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر من قانون العقوبات، بالإضافة إلى المادة 394 مكرر 03 التي تنص على: " تضاعف العقوبات المنصوص عليها في هذا القسم اذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون إخلال بتطبيق عقوبات أشد." ⁴

الفرع الثاني: الجريمة الإلكترونية الواقعة على النظام المعلوماتي

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 0415 الصادر في 10 نوفمبر 2004، المتضمن قانون العقوبات بتجريم كل أنواع الإعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394 مكرر إلى 394 مكرر 07، وتأخذ صور الإعتداء صورتين وهما : الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش، وهذا ماسأتناوله في البنود الموالية.

1- سوير سفيان، نفس الرسالة، ص 38

2- صغير يوسف، رسالة الماجستير السابقة الذكر، ص 54

3- سوير سفيان، رسالة الماجستير السابقة الذكر، ص 38

4- الأمر رقم 04-15، القانون السابق الذكر .

أولاً: جرمي الدخول والبقاء غير المشروعان في منظومة معلوماتية.

تنص المادة 394 مكرر من قانون العقوبات السابق الذكر على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فإن العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام.¹

1- فعل الدخول غير المشروع:

لا تعني هنا الدخول بالمعنى المادي، أي الدخول إلى مكان معين كمنزل أو غيره، وإنما ينظر إليه كظاهرة معنوية تشابه تلك التي تعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات، وتقع هذه الجريمة من كل إنسان أياً كانت صفته سواء كان شخص يعمل في مجال المعلوماتية أو لا يعمل، وسواء كان يستطيع أن يستفيد من الدخول أم لا، فيكفي أن يكون الجاني ممن ليس له الحق في الدخول إلى النظام أو من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها، كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط، أي أن الجريمة تقوم بفعل الدخول إلى النظام مجرداً عن أي نتيجة أخرى، ولا يشترط لقيامها النقاط أو حصول الشخص على المعلومات الموجودة داخل النظام أو البعض منها، أن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام، ففعل الدخول يتسع ليشمل كل قنيات الدخول الإحتيالي في منظومة محمية كانت أو غير محمية، كما تشمل استعمال من لاحق له في ذلك المفتاح للدخول إلى المنظومة.

1- حمزة بن عقون، رسالة الماجستير السابقة الذكر، ص 182-183.

2- فعل البقاء غير المشروع:

يقصد بفعل البقاء التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول في النظام وقد يجتمعان، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول إلى النظام مشروعا، ومن أمثلة ذلك إذا تحقق الدخول إلى النظام بالصدفة أو عن طريق الخطأ، وهنا يجب على المتدخل أن يقتطع وجوده داخل النظام وينسحب، فإذا بقي رغم ذلك فإنه يعاقب على جريمة البقاء غير المشروع، ويكون البقاء جريمة في الحالة التي يطبع الشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الإطلاع فقط، ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية، والتي يستطيع الجاني فيها الحصول على الخدمة دون أن يدفع المقابل الواجب دفعه أو يحصل على مدة أطول من المدة التي دفع مقابلها، ففعل البقاء يشمل البقاء بعد الدخول الشرعي أكثر من الوقت المحدد، وذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب أو حصل عن بعد، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية.¹

ثانيا: جريمة المساس بمنظومة معلوماتية

نصت المادة 394 مكرر 01 من قانون العقوبات رقم 15/04 بمعاينة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش، هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي، و أفعال الإدخال و الإزالة و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل، كما أن هذا السلوك يجسد فعل التخريب

1- حمزة بن عقون، رسالة الماجستير السابقة الذكر، ص 183 - 184.

و إفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها.

ثالثا: أفعال إجرامية أخرى.

جرمت المادة 394 مكرر 02 من قانون العقوبات السابق الذكر الأعمال الآتية: تصميم أو بحث أو تجميع أو توفير أو نشر أو الانتحار في معطيات مخزنة أو معالجة أو مرسله عن طريق منظومة معلوماتية، يمكن أن ترتكب بما إحدى جرائم الغش المعلوماتي السابقة الذكر¹، ويقصد بتصميم العمليات هذا الفيروسات المعلوماتية، برامج القرصنة التي يمكن أن تستعمل في ارتكاب جرائم معلوماتية إما ضد الأنظمة المعلوماتية، أو المعطيات المعلوماتية في حد ذاتها²، كما جرم المشرع كذلك أفعال الحيازة أو إفشاء أو نشر أو استعمال المعطيات المتحصلة من إحدى جرائم الغش المعلوماتي لإي غرض³.

من خلال التعرض إلى ماهية الجريمة الإلكترونية، يتضح بأن هذا النمط من الجرائم طبيعة خاصة و متميزة، وهي جريمة ناعمة حال ارتكاجا، تجاوز حد الخشونة في نتائجها، إذ مجرد ملامسة الجاني لزر أو أكثر من لوحة المفاتيح، قد ترتكب أخطر الجرائم في بضعة ثواني، ودون التقاء بين الجاني والمجني عليه، وهذا ما يؤدي إلى صعوبة في مكافحتها، ويعاب على المشرع الجزائري أنه اهتم بالجريمة الإلكترونية بالنص على بعض الجرائم الإلكترونية وليس كلها وأهمل المجرم الإلكتروني، إذ لم يتعرض له في أي نص قانوني، بالإشارة إلى تعريفه أو سماته.

كما أن التطرق لماهية الجريمة الإلكترونية والتعرف عليها بعمق يفيدنا في إيجاد الحلول

لمواجهتها.

1- حمزة بن عقون، نفس الرسالة، ص 184

2- دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن. مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منشوري، قسنطينة، 2012-2013، بدون صفحة.

3- حمزة بن عقون، رسالة الماجستير السابقة الذكر، ص 184 - 185.

الفصل الثاني

الآليات القانونية لمكافحة الجريمة القرصنة الإلكترونية

تمهيد :

بعد التطرق إلى ماهية الجريمة الإلكترونية، من خلال تعريفها وأنواعها والدوافع المؤدية لارتكابها. أتعرض في هذا الفصل إلى بيان كيفية التصدي للجريمة الإلكترونية من طرف المشرع الجزائري، وذلك بتوفير الحماية الموضوعية والإجرائية للنظام المعلوماتي، من خلال مختلف التشريعات التقليدية أو المستحدثة التي تناولت الجريمة الإلكترونية، وهذا ما سيتم توضيحه في المبحثين الآتيين:

1-المبحث الأول: الحماية الموضوعية للنظام المعلوماتي من القرصنة

2-المبحث الثاني : الحماية الإجرائية للنظام المعلوماتي

المبحث الأول: الحماية الموضوعية للنظام المعلوماتي من القرصنة

بما أن المعلومة تمثل قيمة أو ثروة اقتصادية كبرى، استوجب ذلك توفير حماية جنائية خاصة بها، فالمعلومة أصبحت تقوم مالياً، وبالتالي تدخل في عتاد الأموال الإقتصادية، وقد تكون المعلومة شخصية وإفشائها يهدد الحياة الخاصة من جوانب متعددة. ونظراً للتطور السريع في التكنولوجيا وتقنيات المعلومات شبكة الأنترنت، أظهرت الدراسات الجنائية عدم كفاية النصوص التقليدية في تطبيقها على الجرائم المستحدثة في ظل التطور الهائل في أنظمة معالجة المعلومات ونقلها عبر الشبكات، وبانت الحاجة ضرورية لاستحداث قواعد قانونية جديدة لمواجهة هذه الجرائم المستحدثة.¹

المطلب الأول: الحماية في نصوص الملكية الفكرية من القرصنة الإلكترونية

يقصد بالحقوق الذهنية أو الفكرية، بأنها حقوق ملكية معنوية ترد على أشياء غير مادية وتقسّم إلى ثلاثة أنواع: - حق الملكية الصناعية، ويرد على ابتكارات جديدة تمكن صاحبها من احتكار استغلال ابتكاره قبل الكافة، وهي أنواع، حقوق تتعلق بابتكار جديد من حيث الشكل والمظهر الخارجي للمنتجات الرسوم أو التصميمات أو النماذج الصناعية، حقوق تتعلق بابتكار جديد من حيث الموضوع كالإختراعات، حقوق ترد على شارات مميزة تمكن صاحبها من احتكار استغلال علامة تستخدم لتمييز المنشآت كالإسم التجاري.

- حقوق الملكية التجارية وهي تتضمن ما للتاجر من حق على محله التجاري، باعتباره مال منقول .

- حقوق الملكية الأدبية والفنية، وتعني ما للمؤلف من حق على إنتاجه الذهني في الأدب والفنون والعلوم.²

1- رضاع فتيحة، رسالة الماجستير السابقة الذكر، ص 88.

2- محمد عبد الرحيم الناغي، الحماية الجنائية للرسوم والنماذج الصناعية (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2009، ص 12-13.

وقد اعتمد المشرع الجزائري من أجل حماية المصنفات الفكرية شروطا عامة، تتمثل في وجود المصنف أولا ثم عدم مخالفته للنظام العام ثانيا، وأخرى خاصة وهي وجود ابتكار جديد في المصنف أولا ثم القيام بإيداعه القانوني ثانيا¹ .

الفرع الأول: مدى خضوع معطيات الحاسب الآلي لنصوص الملكية الصناعية

ترمز حقوق الملكية الصناعية إلى المبتكرات الجديدة كالإختراعات، ومعنى الإختراع إيجاد شيء لم يكن موجودا من قبل، أو اكتشاف شيء كان موجودا ولكنه كان مجهولا وغير ملحوظا ثم أبرزه في المجال الصناعي، فالإختراع الذي لا يؤدي إلى تقدم ملموس في الفن الصناعي لا يستحق براءة عنه² ، ولما كانت البرامج تتضمن استخدامات جديدة لأفكار أو مبادئ علمية لتشغيل الحاسب الآلي، فهي من هذه الزاوية تصبح قابلة للبراءة³. وقد نص عليها الأمر رقم 07-03 الصادر في 2003، حيث نصت المادة الثالثة منه على الشروط الواجب توافرها حتى يحظى الإختراع بالحماية بقولها: "يمكن أن تحمي بواسطة براءة الإختراع ، الإختراعات الجديدة والناجمة عن نشاط اختراعي والقابلة للتطبيق الصناعي..."⁴. وعليه يمكن القول أنه حتى يحظى أي اختراع ما بالحماية ضمن نطاق براءات الإختراع، وجب توافر شرطي الإبتكار والجدة والقابلية للتطبيق الصناعي⁵.

وتجدر الإشارة إلى أنه يمكن الحصول على براءة الإختراع بخصوص برامج الإعلام

الآلي في حالتين:

- 1- بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، الجزائر، 2007، ط 01، ص 37.
- 2- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، 2000، ص 51.
- 3- بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، بمحلة الندوة للدراسات القانونية، سيدي بلعباس، 2013، العدد 01، ص 68.
- 4- الأمر رقم 07-03، الصادر في 19 يوليو 2003، المتعلق بجراءات الإختراع، ج رالعدد 44.
- 5- ختير مسعود، الحماية الجنائية لبرامج الكمبيوتر ، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر طبعة 2010، ص

- أن يكون البرنامج جزءا من ذاكرة الحاسوب نفسه ومثاله البرنامج المبني. - أن يكون البرنامج جزءا، أي أن طلب البراءة ينصب على وسيلة صناعية جديدة، يستخدم البرنامج في تحقيق إحدى مراحلها، فالحماية تبقى رهينة توفر الشرطان المذكوران، مما يصعب توفرها، فالمشرع الجزائري استبعد صراحة المعطيات من مجال الحماية بواسطة براءات الإختراع¹ طبقا للمادة 07 من الأمر رقم 03-07 التي تنص على: " لاتعد من قبيل الإختراعات في مفهوم هذا الأمر برامج الحاسوب"²

الفرع الثاني: خضوع معطيات الحاسب الآلي لنصوص الملكية الأدبية و الفنية .

تظهر الملكية الأدبية والفنية من خلال حق المؤلف، وهو حق استثنائي يمنحه القانون المؤلف أي مصنف للكشف عنه، كابتكار له أو استساخه أو توزيعه أو نشره على الجمهور، والإذن للغير باستعماله على وجه محدد³. وقد انقسم الفقه إلى اتجاهين، اتجاها يرى أن برامج الحاسب الآلي مصنفة ضمن قانون حق المؤلف وأنه لا حاجة لتعديل النصوص التقليدية في قانون حق المؤلف، باعتبار برامج الحاسب الآلي ما هي إلا طرق مختلفة للتعبير عن الأفكار الإنسانية وهو مثل سائر المصنفات، أما الإتحاد الأخر أقر لبرامج الحاسب الآلي الصفة المميزة عن سائر المصنفات الأخرى المحمية، بموجب قانون حماية حق المؤلف، وتبني هذا التوجه العديد من الدول التي عدلت قوانينها بما ينسجم والصفة المميزة لبرامج الحاسب الآلي، ومنهم الجزائر حيث جاء الأمر رقم 03-05 المتعلق بحق المؤلف والحقوق المجاورة باستخلاص ما يلي:

1- بوعناد فاطمة زهرة، المحلة السابقة الذكر، ص 66

2- الأمر رقم 03-07، القانون السابق الذكر .

3- غيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2003، ص 75

- أن المشرع وسع قائمة المؤلفات المحمية، حيث أدمج تطبيقات الإعلام الآلي¹ ضمن المصنفات الأصلية والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي- تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين، لاسيما المصنفات المعلوماتية²، حيث تنص المادة 05 من القانون رقم 03-05³ على أنه: " تعتبر أيضا مصنفات محمية الأعمال الآتية مجموعات من مصنفات التراث الثقافي التقليدي وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للإستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى... تكفل الحماية لمؤلف المصنفات المشتقة دون المساس بحقوق مؤلفي المصنفات الأصلية." والمادة رقم 04 من نفس القانون نصت على أنه: " تعتبر على الخصوص كمصنفات أدبية أو فنية محمية ما يلي: المصنفات الأدبية المكتوبة مثل... و برامج الحاسوب....". كما أن مدة الحماية تحدد ب 50 سنة بعد وفاة المبدع وفقا للمادة 58 فقرة الأولى من نفس القانون، ويعتبر كل اعتداء على الحق المالي أو الأدبي المؤلف برنامج فعلا من أفعال التقليد، حيث نص المشرع في المادة 151 من الأمر رقم 03-05، على قيام جنحة التقليد في حالة الكشف غير المشروع عن مصنف أو أداء في أو في حالة المساس بسلامة مصنف أو أداء فني، أو في حالة استنساخ مصنف أو أداء فني بأي أسلوب في شكل نسخ مقلدة أو في حالة استيراد نسخ مقلدة أو تصديرها أو بيع نسخ مزورة من مصنف أو أداء فني و أخيرا في حالة تأجير مصنف أو أداء فني أو عرضه للتداول.

وقد قرر المشرع جزاءات لجرائم التقليد، حيث ربط المشرع الجزائري حماية المصنف بتاريخ الإنتهاء من الإبتكار أو تاريخ النشر أو التوزيع لأول مرة، كما حول المشرع لصاحب المصنف المعتدى عليه القيام بإجراء تحفظي يتمثل في حجز التقليد، وبواسطته يتم حجز

1- جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر

والتوزيع، عمان الأردن، 2010، ط 01، ص 189

2- بوعناد فاطمة زهرة، المحلة السابقة الذكر، ص 66

3- الأمر رقم 03-05، الصادر في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر العدد 44.

الوثائق والنسخ الناتجة عن الإستتساخ غير المشروع أو التقليد. والعقوبات المقررة للاعتداء على حقوق الملكية الأدبية والفنية تشمل المواد من 156/153 إلى 159 من نفس القانون السابق الذكر، حيث قدرت العقوبة الأصلية بالحبس من ستة أشهر إلى ثلاث سنوات وغرامة من 500.000 دج إلى 1.000.000 دج سواء تمت عملية النشر داخل الجزائر أو خارجها، ومنح المشرع للقاضي سلطة تقرير عقوبات تكميلية تتمثل في مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الإستغلال غير الشرعي لمصنف أو أداء محمي، ومصادرة و إتلاف كل عتاد أنشأ خصيصا المباشرة النشاط غير المشروع، وكل النسخ المقلدة والمصادرة في هذه الحالة تكون وجوبية، كما للقاضي أن يضاعف العقوبة في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر¹.

المطلب الثاني: الحماية في قانون العقوبات.

إن القانون الجنائي التقليدي لا يتطور دائما بنفس السرعة التي تتطور بها التكنولوجيا الجديدة، لاسيما أن نصوصه وضعت في عصر لم يكن الأنترنت قد ظهر فيه ولم تظهر المشاكل القانونية الناتجة عن استخدامه²، لكن نجد أن المشرع الجزائري تدارك الفراغ القانوني في مجال الإجرام المعلوماتي ولو نسبيا، خصوصا بموجب القانون رقم 04-15 المتضمن تعديل قانون العقوبات، إذ بموجبه جرم بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات، وقد سبق ذكرها في المبحث الثاني من الفصل الأول، أما العقوبات سأطرق لها من خلال الفروع الموالية.

1- سوبر سفيان، رسالة الماجستير السابقة الذكر، ص 75-78-80

2- سمير سعدون مصطفى، وآخرون، الجريمة الإلكترونية عبر الأنترنت وسبل مواجهتها، بحث مقدم بتاريخ بدون سنة، بدون صفحة 20/09/2010.

الفرع الأول: العقوبات الأصلية

نص المشرع الجزائري في القانون رقم 15/04 على عقوبات أصلية لجريمتي الدخول والبقاء غير المشروعان للنظام المعلوماتي، وكذا جريمة المساس بمنظومة معلوماتية وفق الآتي:

- عقوبة الدخول أو البقاء غير المشروعان للنظام: في حالة الدخول غير المشروع من طرف الحرم الإلكتروني للنظام كله أو جزء منه أو متى كان مسموح له بالدخول إلى جزء معين من النظام وتجاوزه، ومتى كان الدخول أو التواجد داخل النظام مخالف لإرادة صاحب النظام، تكون العقوبة بالحبس من ثلاثة أشهر إلى سنة وغرامة من 50.000 دج إلى 100.000 دج طبقا للمادة 394 مكرر من قانون العقوبات رقم 15/04 .

أما في حالة الدخول أو البقاء ونتج عنه حذف أو تغيير لمعطيات المنظومة، أو انجر عن هذا الدخول أو البقاء تخريب لنظام اشتعال المنظومة، فإن العقوبة تضاعف إلى الحبس من ستة أشهر إلى سنتين وغرامة من 50.000 دج إلى 150.000 دج، وذلك وفقا للمادة 394 مكرر من قانون العقوبات السابق الذكر.

- عقوبة المساس بمنظومة معلوماتية: نص المشرع الجزائري في المادة 394 مكرر 01 من نفس القانون السابق الذكر على عقوبة الإعتداء العمدي على المعطيات الموجودة داخل النظام، وذلك بالحبس من 06 أشهر إلى 03 سنوات وغرامة من 500.000 دج إلى 2.000.000 دج، وذلك في حالة ارتكاب الجرائم الماسة بالأنظمة المعلوماتية، وفي حالة حيازة أو إنشاء أو نشر أو استعمال المعطيات المتحصل عليها من إحدى الجرائم الماسية بالأنظمة المعلوماتية تكون العقوبة الحبس من شهرين إلى 03 سنوات وغرامة من 1.000.000 دج إلى 5.000.000 دج.¹

1- أختير مسعود، المرجع السابق الذكر، ص 99-100

الفرع الثاني: العقوبات المقررة للشخص المعنوي

نص المشرع الجزائري في المادة 51 مكرر من القانون رقم 15/04 على مسألة 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، كما نصت المادة 394 مكرر 04 من نفس القانون على العقوبات الواجبة التطبيق على الشخص المعنوي في حالة ارتكابه لأي جريمة اعتداء على نظام المعالجة الآلية للمعطيات يغرمة تعادل خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي.¹

الفرع الثالث: عقوبة الإشتراك و الشروع في الجريمة.

عقوبة الإشتراك: نصت عليها المادة 394 مكرر 05 من القانون رقم 15/04 بقولها: " كل من شارك في مجموعة أو إتفاق 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."

عقوبة الشروع: نصت عليها المادة 394 مكرر 07 من نفس القانون بقولها: " يعاقب على الشروع في ارتكاب الجرح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنة ذاتها ."

الفرع الرابع: العقوبات التكميلية.

نصت المادة 394 مكرر 06 من نفس القانون على مجموعة من العقوبات التكميلية، يحكم بها إلى جانب العقوبات الأصلية وهي كالتالي:

المصادرة:

وتعني مصادرة الأجهزة والبرامج والوسائل المستخدمة لارتكاب الجرائم الماسة بالنظام وذلك ببيعها، أو حجزها مع مراعاة حقوق الغير حسن النية.

1- أختي مسعود، المرجع السابق الذكر، ص 100-101.

إغلاق المواقع:

إغلاق مواقع الأنترنت أو المواقع الإلكترونية بصفة عامة، والتي كانت وسيلة الارتكاب 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 كما ولم يتصدى لها بالإخبار عنها، أو يمنع مرتكبها من ارتياد محله لارتكاب مثل هذه الجرائم.¹

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

الفرع الخامس : الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

صدر القانون رقم 04-09 الصادر في 05 أوت 2009، ويتضمن 19 مادة موزعة على ستة فصول، وهو ثمرة عامين من التحضير والدراسة والتحليل والمقارنة مع أحدث القوانين ، وقامت بإعداده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المهنية، كما يتضمن القانون أحكام خاصة بالمراقبة الإلكترونية التي لا يجوز إجراؤها إلا بإذن من السلطة القضائية المختصة وفي حالات تم تحديدها وهي الأفعال الموصوفة بجرائم الإرهاب والتخريب، والجرائم الماسة بأمن الدولة أوحالة توفير معلومات عن اعتداء محتمل يهدد منظومة من المنظومات المعلوماتية لمؤسسات الدولة أو الدفاع الوطني أو النظام العام. وينص القانون على إنشاء هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيات الإعلام والاتصال ومكافحته، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم الإلكترونية ومساعدة مصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه

1- ختير مسعود، المرجع السابق الذكر، ص 102 - 103.

الجرائم، كما تتكفل اللجنة أيضا يتبادل المعلومات مع نظيراتها في الخارج، علما بأن القانون أكد على مبدأ التعاون الدولي من منطلق المعاملة بالمثل. يعتبر القانون رقم 09-04 ذو نطاق شامل في مجال مكافحة الجريمة الإلكترونية، حيث جاء تحريمه للأفعال المخالفة للقانون و التي ترتكب عبر وسائل الاتصال عامة، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الأنترنت وعلى كل تقنية تظهر مستقبلا.¹

1- رضاع فتية، رسالة الماجستير السابقة الذكر، ص 113 - 115.

المبحث الثاني: الحماية الإجرائية للنظام المعلوماتي

إن القاعدة الإجرائية ليست غاية في ذاتها، وإنما هي وسيلة لغاية تتمثل في حسن تطبيق القانون الجنائي الموضوعي، فبينما تجرى بالدعوى العمومية محاكمة القاضي للمتهم، فإنه بتطبيق القواعد الإجرائية التي خالفها الدعوى تجرى محاكمة القانون للقاضي، وبالتالي فإن الإجراءات الجنائية خطيرة لاتقل بحال القواعد المقررة في قانون العقوبات، لأنها تمس مباشرة بحريات المواطنين واستقرارهم¹، وعليه كان لابد من التطرق إلى الجوانب الإجرائية بخصوص الجريمة الإلكترونية، ومدى توافر الحماية الإجرائية للنظام المعلوماتي، وذلك من خلال المطالب الآتية.

المطلب الأول: التحقيق في الجريمة الإلكترونية.

يعرف التحقيق بأنه إجراء يتخذ بعد وقوع الجريمة، لما له من أهمية في التأكد من وقوع الجريمة، وإسنادها إلى مرتكبيها بأدلة الإثبات بأنواعها، وبالتالي تتحلّى الحقيقة التي تهدف إلى إدانة المتهم من عدمه، وتتم الدعوى الجنائية بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتتم عملية التحقيق بدورها بمرحلتين، مرحلة التحقيق الأولي (الضبطية القضائية) ومرحلة التحقيق الابتدائي (قاضي التحقيق)، وفي كل أنواع التحقيق يكون لضباط الشرطة القضائية والقضاة صلاحية ممارسة إجراءات البحث والتحري المحددة وفقا لقانون الإجراءات الجزائية، فإذا كان التحقيق يعتمد على نكاه المحقق وقوة ملاحظته، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى ذلك تطوير الأساليب، وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطورها² وهذا ما سيتم بيانه في الفروع الموالية.

1- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية

2009، ص 342-343

2- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص 102 - 103.

الفرع الأول: الأجهزة المكلفة بالبحث والتحري.

نظرا لخصوصية الجريمة الإلكترونية كان حتما توفير كوادر، وأجهزة متخصصة تعني بعملية البحث والتحري عن الجريمة الإلكترونية، وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني، بالنسبة لجهاز الشرطة فقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي على فروع تقنية من بينها خلية الإعلام الآلي، بالإضافة إلى فرق متخصصة مهمتها التحقيق في الجريمة الإلكترونية تعمل بالتنسيق مع هذه المخابر توجد على مستوى مراكز الأمن الولائي، أما على مستوى الدرك الوطني فإنه يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني، قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، بالإضافة إلى مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببنر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني¹.

الفرع الثاني: خصائص التحقيق والمحقق.

للتحقيق الإلكتروني مميزات خاصة عن التحقيق الجنائي التقليدي وكذا المحقق الإلكتروني ، المسايرة متطلبات الجريمة الإلكترونية بما فيها العالم الافتراضي الذي ترتكب فيه.

أولا: خصائص التحقيق الإلكتروني:**01- منهج أو أسلوب التحقيق الإبتدائي :****- وضع خطة عمل التحقيق:**

وذلك وفق المعلومات المتوفرة لدى المحقق، وتحديد الفريق الفني اللازم للقيام بمساعدته في أعمال التحقيق وذلك بوضع خطة مناسبة، ولا تبدأ إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة، ثم التخطيط الفني للتحقيق من أجل الوصول إلى أفضل الطرق للتعامل مع هذه الجريمة بالتفصيل

1- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص 106-107.

والوضوح، وبعدها عمل دراسة وافية وجادة لكافة إجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في فريق التحقيق، تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في إنجاز العمل، وهو ما يؤدي إلى ضمان مستوى جيد من الأداء، تحديد الإجراءات المسبقة التي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبراء أو نقص المعرفة، وبالتالي تساعد على إيجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أن الخطوات التي يقوم بها المحقق خلال جميع مراحل التحقيق تسير ضمن الضوابط التشريعية وتقلل من الأخطاء التي قد تضر بالقضية في مرحلة المحاكمة. ويجب أن تركز خطة العمل على مجموعة من البنود الأساسية، يتم الإرتكاز عليها أثناء تنفيذ الخطة وهي أن يتم تعيين الأشخاص الذين سيتم التحقيق معهم وتحديد النقاط التي يجب إيضاحها معهم وتقدير مدى الحاجة للإستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق، بالإضافة إلى مراعاة الظروف المحيطة بالواقعة، إذ أن هذه الظروف قد تشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل ومنها: مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة - مدى حساسية البيانات التي يحتمل سرقتها أو إتلافها - مدى الإختراق الأمني الذي تسبب فيه الجاني.

ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش، وذلك بتحديد نوع الأدلة التي يريد فريق التحقيق البحث عنها.¹

- تشكيل فريق التحقيق:

يجب أن يتشكل الفريق من فنيين وأخصائيين ذوي الخبرة في مجال الحاسوب والأنترنت ما يكفي لمكافحة هذا النشاط الإجرامي، وهذا لا يتحقق إلا بعد تلقيها التعليم والتدريب الكافيين في مجال المعلوماتية، والمعرفة باللغات الأجنبية²، ولهم مهارات في التحقيق الجنائي بشكل

1- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص110-111.

2- كوثر فرام، الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث غاية التدريب، المعهد العالي للقضاء،

عام والتحقيق الجنائي الإلكتروني بشكل خاص، ولهم الإستعانة بخبراء ليتمكنوا من فك التعقيدات التي تفرضها ملابسات كل جريمة، ويتكون الفريق من المحقق الرئيسي، ويكون ممن لهم خبرة في التحقيق الجنائي، خبراء الحاسوب وشبكات الأنترنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم، خبراء ضبط وتحرير الأدلة الرقمية العارفين بأمور تفتيش الحاسوب، خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية ، خبراء التصوير والبصمات والرسم التخطيطي.

02- إجراءات التحقيق:

- إجراءات سابقة على بدء التحقيق الإبتدائي:

- تحديد نوع نظام المعالجة الآلية للمعطيات، أي هل الحاسوب معزول أم متصل بشبكة معلومات- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة، مع كشف تفصيلي عن المسؤولين بها و دور كل واحد منهم - إذا وقعت الجريمة على شبكة، فإنه يجب حصر طرفيات الإتصال بنا أو منها، المعرفة الطريقة التي تمت بها عملية الإختراق من عدمه، وهل هناك حواسب آلية خارج هذه المشكلة ولها إمكانية الإتصال بما أم لا؟ - مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة الإلكترونية - مراعاة أن الجاني قد يتدخل من خلال الشبكة الإتلانف كل المعلومات المخزنة - يجب فصل التيار الكهربائي عن موقع المعاينة أو جمع الإستدلال لشل فاعلية الجاني في أن يقوم بطريقة ما يمحو آثار جريمته - فصل خطوط الهاتف حتى لا يسيء الحان استخدامها والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق - التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، لأنه من الخدع التي يستعملها الجاني عند الإختراق أن يتم ذلك بخط هاتفي مسروق الدخول إلى شبكة الهاتف والتلاعب فيها وتضليل أجهزة المراقبة والتخطيط)- إبعاد الموظفين عن أجهزة الحاسب الآلي بعد حصول المتهم على كلمة السر، وكذا الشفرات في حالة وجودها- تصوير

الأجهزة المستهدفة - التي وقعت بما أو عليها الجريمة - من الأمام والخلف لإثبات أنها كانت تعمل.¹

- إجراءات أثناء التحقيق الابتدائي :

- عمل نسخة احتياطية من الأقراص الصلبة أو الإسطوانة المرنة قبل استخدامها، والتأكد فنيا من دقة النسخ عن طريق الأمر - نزع غطاء الحاسب الآلي المستهدف، والتأكد من عدم وجود أقراص صلبة إضافية - أن يكون الهدف من نسخ محتوى الإسطوانة والأقراص تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات المسووحة، ويمكن استعادها من سلة المهملات، وكذا معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب - العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في اختلاس معلوماتي - العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها- حفظ المعدات والأجهزة التي تضبط بطريقة فنية سليمة.²

ثانيا: خصائص المحقق الإلكتروني:

تتمثل في الخصائص الفنية للمحقق الإلكتروني، وتأهيل وتدريب المحقق الإلكتروني.

الخصائص الفنية للمحقق الإلكتروني :

- معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والانترنت، لأن افتقار ضابط الشرطة القضائية إلى التأهيل الكافي في الميدان التقني قد يؤدي إلى إتلاف وتدمير الدليل - إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة وتخزينها في الأقراص المعدة لذلك، ومنع حذفها والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة لأي مؤثرات خارجية، كالقوة الكهرومغناطيسية حتى لا تتلف محتوياتها- معرفة آلية عمل تشكيلات الحاسوب والانترنت - معرفة المحقق بالأنظمة

1- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص من 111 إلى 113

2- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص 113-114.

المختلفة، لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة - معرفة معطيات الحاسوب المعرفة صيغ الملفات وما تحويه - معرفة وإدراك أساليب ارتكاب الجريمة الإلكترونية، وتقنيات الأمن المعلوماتي .

تأهيل وتدريب المحقق الإلكتروني:

لابد من وضع سياسة جنائية رشيدة، تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، ويمتد هذا التدريب إلى العاملين بأجهزة الضبطية القضائية، ويرى الفقه الجنائي أنه في حالة التدريب على التحقيق يتعين مراعاة شخص المتدرب، ومنهج الدورة التدريبية، وصفة وأسلوب التدريب، كما يجب أن يشمل منهج التدريب تدريس الأساليب الفنية المستخدمة في ارتكاب الجريمة، والمتعلقة بالكشف عنها وكيفية اتباعها ومعاينتها وفحصها فنيا¹. ومن العقوبات التي تعيق عمل الأجهزة حتى على فرض أنه تم إعدادها الإعداد المناسب، ضخامة حجم البيانات محل الفحص، ما يتعذر على المحقق الكفئ الوصول إلى الدليل المناسب.²

الفرع الثالث: الدليل المناسب لإثبات الجريمة الإلكترونية.

الدليل هو أثر يولد، أو حقيقة تتبع من الجريمة المرتكبة، فدليل التزوير يأتي من إثبات تغيير الحقيقة في المحرر مثلا، وبالنسبة للجريمة الإلكترونية فإنها تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها أو من خلالها، وهي تعرف بالدليل الرقمي المتواجد في أماكن افتراضية، ويعرف الدليل الرقمي بأنه الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل مجالات، أو نبضات مغناطسية أو كهربائية، يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجية خاصة، ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، أو أنه ذلك الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة. ويتميز الدليل الرقمي جملة من الخصائص: - أنه دليل علمي يحتاج إلى بيئته التقنية التي يتكون فيها، لكونه من طبيعة تقنية المعلومات - أنه من طبيعة تقنية إذ ما تنتج هذه الأخيرة هو

1- سعيداني تعيم، رسالة الماجستير السابقة الذكر، ص 116-117-119.

2- موسي مسعود أرحومة، المرجع السابق الذكر، ص 05

نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب، وبالتالي لا وجود للدليل الرقمي خارج بيئته الرقمية، ويتميز الدليل الرقمي بقابليته للنسخ مطابق الأصل مع نفس القيمة العلمية، وهذا ما لاتجده في الدليل المادي- أنه دليل متنوع ومتطور، حيث يشمل كافة البيانات الرقمية الممكن تداولها رقميا، وتطوره يظهر في حركة الإتصال عبر الأنترنت ومدى تطورها- أنه دليل صعب التخلص منه، إذ أنه كلما حدث اتصال بتكنولوجيا المعلومات بإدخال بيانات إلى هذا العالم، فإنه من الصعب التخلص منها، إذ تتوفر برمجيات ذات طبيعة رقمية، يمكن بمقتضاها استرداد كافة الملفات التي تم إلغاؤها أو إزالتها من الحاسوب - أنه ذو طبيعة رقمية ثنائية "0-1"، حيث تعتمد تكنولوجيا المعلوماتية الحديثة على تقنية الترميم، التي تعني ترجمة أو تحويل أي مستند إلى نظام ثنائي في تمثيل الأعداد يفهمه الحاسب الآلي، قوامه الرقمان "0 و 1" ، فالكتابة مثلا في العالم الرقمي ليس لها وجود مادي، وإنما هي مجموعة أرقام لها أصل واحد وهو الرقم الثنائي "0 و 1" . والدليل الرقمي نوعان، الدليل الرقمي الأصلي والدليل الرقمي المكرر، وهذا الأخير هو استنساخ رقمي لجميع المستمسكات البيانية التي يحتويها الدليل الرقمي الأصلي.¹

المطلب الثاني: إجراءات جمع الأدلة التقليدية.

إن التطور التقني الذي لحق نظم المعالجة الآلية، فضلا عن الطبيعة الخاصة للدليل الرقمي، أدى إلى تغيير المفاهيم السائدة حول إجراءات وطرق الحصول على الدليل، وهو ما أدى إلى ضرورة إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية²، لذا سابين مدى اعتماد هذه الإجراءات في مجال الجريمة الإلكترونية للحصول على الدليل الرقمي وفق الفرعين المواليين.

1- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص 119-120-121-123-124-125-126

2- سعيداني نعيم، نفس الرسالة، ص 221

الفرع الأول: الإجراءات المادية (المعاينة، التفتيش، الضبط)

أولاً: المعاينة:

هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليُشاهد آثارها بنفسه وتقتضى المعاينة إثبات حالة الأشخاص والأشياء¹ ، وكل ما يعتبر في كشف الحقيقة، وكذا المعنى تستلزم المعاينة الانتقال إلى محل الواقعة أو أي محل توجد به أشياء، أو آثار يرى المحقق أن لها صلة بالجريمة، كما أن المعاينة في الجريمة التقليدية تكون ذات أهمية متمثلة في تصور كيفية وقوع الجريمة وظروف ملابساتها وتوفير أدلة مادية، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة الإلكترونية، وضبط الأشياء التي قد تفيد في إثباتها ونسبتها إلى مرتكبيها، لأن الجريمة التقليدية غالباً لها مسرح تجرى عليه الأحداث التي تخلف آثار مادية، على خلاف الجريمة الإلكترونية يتضاءل دورها في الإفصاح عن الحقيقة المؤدية للأدلة المطلوبة، لأن الجريمة الإلكترونية قلما تخلف آثار مادية، وأن كثير من الأشخاص يردون إلى مسرح الجريمة خلال فترة من زمان وقوع الجريمة، وحتى اكتشافها أو التحقيق فيها وهي طويلة نسبياً، الأمر الذي يجعل الجاني يغير أو يتلف أو يعبث بالآثار المادية للجريمة إن وجدت، وهذا ما يورث الشك في دلالة الأدلة المستقاة من المعاينة² ، ومن الإجراءات الواجب اتباعها عند إجراء المعاينة ما يلي: تصوير جهاز الحاسوب وما قد يتصل به من أجهزة طرفيه ومحتوياته - عدم التسرع في نقل أي مادة معلوماتية للتيقن من عدم وجود أي مجالات مغنطيسية في العالم الخارجي حذف المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقية - ربط الأقراص التي تحمل أدلة مع جهاز يمنع الكتابة عليها، مما يتيح لجهات التحقيق قراءة بياناتها من دون تغييرها.

1- عبدالله دغش العجمي، المرجع السابق الذكر، ص 77.

2- عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2002 من 20-21.

ثانيا: التفتيش:

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

- تفتيش مكونات الحاسوب المادية:

لا يوجد مانع قانوني من أن ينصب التفتيش على المكونات المادية للحاسوب وملحقاته، وذلك تبعا لطبيعة المكان الذي يتواجد فيه الحاسوب، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت خاصة كمسكن المتهم أو أحد ملحقاته كانت لها حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه، وحسب المادة رقم 45 ف3 تنص على: "لا تطبق هذه الأحكام إذا تعلق الأمر بجرائم... والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات." و المادة 47 في 3 تنص على: "عندما يتعلق الأمر... الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات... فإنه يجوز إجراء التفتيش... في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل..."، والمادة 64 ف2 تنص على: "وتطبق فضلا عن ذلك أحكام المواد 44، 47 من هذا القانون."³، بمعنى عدم تطبيق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بالجريمة الإلكترونية، حيث لا يشترط حضور الشخص

1- بوعناد فاطمة زهرة، المحلة السابقة الذكر، ص 68.

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

3- المواد 45، 47، 64، من الأمر رقم 22/06، الصادر في 20 ديسمبر 2006، العدل والمتمم لقانون الإجراءات الجزائية، ج و العدد 84.

المشتبه في أنه ساهم في ارتكاب الجريمة عند تفتيش مسكنه، وأنه يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل ودون حاجة إلى رضائه عند القيام بهذا الإجراء.¹

- مدى خضوع مكونات الحاسوب المعنوية للتفتيش:

عرف الفقه اختلاف حول مدى خضوع المكونات المعنوية للحاسوب للإجراءات التفتيش، وانقسم إلى اتجاهين، إتجاه يرى عدم جواز تفتيش المكونات المعنوية للحاسوب، وقد عملت الدول التي تبنت هذا الإتجاه إلى حماية هذه الكيانات المنطقية عبر قانون الملكية الفكرية، واتجاه آخر يرى إمكانية تفتيش المكونات المعنوية للحاسوب لأن كل ما يشغل حيزا ماديا في فراغ معين، هذا الحيز يمكن قياسه والتحكم فيه، وبناءا عليه فإن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب، ويمكن قياسه مقياس معين هو " البايث" و" الكيلوبايت" و "الميغابايت"، وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسوب بعدد الحروف التي يمكن تخزينها فيها، غير أن النصوص القانونية التي تنص على أحكام التفتيش تم سنها قبل أن يعرف القانون الأشياء غير المادية، لذا فإن طبيعة البيانات و المعطيات المعالجة تتطلب قواعد خاصة تحكمها، فالنصوص التقليدية الخاصة بالتفتيش لا يمكن إعمالها على النظم المعلوماتية، لأن قياسها على الأشياء المادية سيكون منافيا للشرعية الإجرائية.²

- مدى خضوع شبكات الحاسوب للتفتيش عن بعد: نفرق هنا بين فرضين.

الفرض الأول: إتصال حاسوب المتهم بحاسب موجود في مكان آخر داخل الدولة:

لقد أجاز المشرع في المادة 05 من القانون رقم 04-09 إذا كانت هناك أسباب تدعو للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، فيجوز تمديد التفتيش بعد إعلام السلطة القضائية المختصة مسبقا بذلك³، حيث تنص المادة 05 منه على: "... في الحالة المنصوص عليها في الفقرة" أ "من هذه المادة إذا كانت هناك أسباب تدعو

1- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص145.

2- سعيداني نعيم، نفس الرسالة، ص 147

3- بوعناد فاطمة زهرة، المحلة السابقة الذكر، ص 69.

للإعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها إنطلاقاً من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقاً بذلك..."

الفرض الثاني: إتصال حاسب المتهم بحاسب موجود في مكان آخر خارج الدولة.

ويكون بالدخول إلى منظومة معلوماتية أو جزء منها، وكذا المعطيات المخزنة فيها ولو عن بعد، وذلك في حالة ما إذا كانت المعطيات القائم البحث عنها يمكن الدخول إليها انطلاقاً من منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة، ووفقاً لمبدأ المعاملة بالمثل، تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث، أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها،¹ حيث تنص المادة 05 من القانون رقم 09-04 على أنه: "... إذا تبين مسبقاً بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقاً من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقاً للاتفاقيات الدولية ذات الصلة ووفقاً لمبدأ المعاملة بالمثل .²

ثالثاً - ضبط الأشياء:

يختلف ضبط الأشياء في الجريمة الإلكترونية عن الضبط في الجريمة التقليدية من حيث المحل، ففي هذه الأخيرة يكون المحل أشياء مادية، أما في الجريمة الإلكترونية تكن الأشياء ذات طبيعة معنوية كالبيانات، المراسلات الإلكترونية، وتجدر الإشارة إلى أن ضبط الأشياء قد يرد على عناصر معلوماتية منفصلة مثل الإسطوانات الممغنطة، وهنا لا بثور أي إشكال عند القيام بالضبط، لكن الصعوبة تكون عندما يلزم ضبط النظام كله، أو الشبكة كلها

1- بن دعاس فيصل، إجراءات التحري في الجرائم المعلوماتية، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة، ص 33

2- المادة 05 من القانون رقم 04/09 ، القانون السابق الذكر.

لأنها تحتوي على عناصر لا يمكن فصلها. أما بالنسبة للمكونات المادية للحاسوب فيمكن ضبط الوحدات المعلوماتية الآتية:- وحدات الإدخال (لوحة المفاتيح، الفأرة، نظام القلم الضوئي)، وضبط وحدة الإخراج (الشاشة، الطابعة، الرسم والمصغرات الفيلمية)، وكل ما يتم ضبطه من بيانات إلكترونية يتعين تحريزها وتأمينها فنيا¹، تنص المادة 06 من القانون رقم 04-09 على أنه: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم، أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحرار وفقا للقواعد المقررة في قانون الإجراءات الجزائية ...²

الفرع الثاني: الإجراءات الشخصية (الشهادة، الخبرة)

أولا: الشهادة

في الجريمة الإلكترونية الشاهد هو الفني صاحب الخبرة والتخصص في التقنية وعلوم الحاسب الآلي، لديه معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التفتيش عن أدلة الجريمة داخله، ويطلق عليه اسم الشاهد الإلكتروني، تمييزا له عن المشاهد التقليدي³. نتيجة لقصور أحكام الشهادة في الحصول على الدليل الإلكتروني، يرى بعض الفقهاء ضرورة البحث عن وسيلة قانونية جديدة، ما لم تستطع فكرة الإلتزام بالشهادة أن تؤديه، وهذه الوسيلة هي الإلتزام بالإعلام في الجريمة الإلكترونية ، وذلك بضرورة وجود نص صريح في القانون يفرض تقديم أي معلومات ضرورية من أجل إعانة

1- بوعناد فاطمة زهرة، المحلة السابقة الذكر، ص 69

2- المادة (6) من القانون رقم 04-09 ، السابق الذكر

3- كوثر فرام، المرجع السابق الذكر، ص 93

سلطات التحقيق والإستدلال في الحصول على الدليل، وفرض مثل هذا الإلتزام قد بلعب دور وقائي في حفظ النظام المعلوماتي¹.

ثانياً: الخبرة:

تكون الحيرة في مجال المعلوماتية بتحري الحقيقة، عن طريق جمع معلومات من الأدلة الرقمية، وتحصيلها من خوادم المواقع، ومن الجهاز المعتدى عليه بعد التوصل إلى تحديده، ثم يقوم الخبير بعملية تحليل رقمي لها، لمعرفة كيفية إعدادها اليرمحي، ونسبتها إلى مسارها الذي أعدت فيه وتحديد عناصر حركتها، ثم التوصل إلى معرفة بروتوكول الإنترنت للحاسوب الذي صدرت منه الرسائل والنبضات الإلكترونية²، غير أنه قد تواجه سلطات الإستدلال والتحقيق بعض المشاكل الفنية والتقنية التي تستلزم خبير إلكتروني مختص، وهنا قد لا تتوفر مثل هذه النوعية من الخبرة في من يحملون جنسية الدولة، وهنا يثور التساؤل حول مدى إمكانية الإستعانة بخبير إلكتروني أجنبي؟³ فالبعض يرى أن الإستعانة بخبير أجنبي يشكل تحديد وخطر على سيادة الدولة وأمنها، والبعض يرى أنه ليس هناك مانع باللجوء إلى خبير إلكتروني أجنبي، وهو أمر تسمح به مقومات العالم الإفتراضي، باعتباره بيئة إتصالية رقمية عالمية.⁴

الفرع الثالث: إجراءات جمع الأدلة الحديثة.

تتمثل هذه الإجراءات في حفظ المعطيات والتسرب واعتراض المراسلات الإلكترونية.

أولاً: حفظ المعطيات.

ألزم المشرع الجزائري مقدي الخدمات بحفظ المعطيات، وذلك بتجميع المعطيات المعلوماتية وحفظها وحيازها في أرشيف، ووضعها في ترتيب معين، في حين اتخاذ إجراءات قانونية محتملة أخرى كالتفتيش وغيره، وقد حصر المشرع المعطيات المعلوماتية الواجب حفظها من طرف مزودي الخدمة، وهي المعطيات المتعلقة بحركة السير (معطيات المرور)، وهي

1- بوعناد فاطمة زهرة، المجلة السابقة الذكر، ص 70.

2- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص 171.

3- بوعناد فاطمة زهرة، المحلة السابقة الذكر، ص 70

4- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص 168.

كما عرفت المادة الثانية من قانون رقم 09-04 تلك المعطيات المتعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة، باعتبارها جزءا في حلقة الاتصالات توضح مصدر الإتصال، الوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الإتصال ونوع الخدمة، وقد حصر المشرع الجزائري معطيات المرور التي ألزم بحفظها في المادة 11 من القانون رقم 09-04 وتتضمن المعطيات التي تسمح بالتعرف على مستعملي الخدمة - المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال - الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها المعطيات التي تسمح بالتعرف على المرسل إليه، الإتصال وكذا عناوين المواقع المطلع عليها وما أن حفظ المعطيات إجراء وقتي، واحتراما للحق في الخصوصية، فإن المشرع الجزائري فرض على مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها بعد سنة من تاريخ التسجيل، إن مزودي الخدمات يعتبرون مصدرا لجهات التحقيق، للحصول على الدليل الرقمي من خلال المعطيات التي يكونون ملزمين بحفظها، وفي نفس الوقت ملزمين بوضعها تحت تصرف هذه الجهات إذا ما تم طلبها.¹

ثانيا: التسرب واعتراض المراسلات الإلكترونية.

1- التسرب:

استحدث المشرع الجزائري في مجال مكافحة جرائم المساس بأنظمة الحاسب الألي عدة إجراءات، وذلك بسبب عجز الأساليب التقليدية، ومن بينها إدراج المشرع لعملية التسرب بموجب القانون رقم 06-22، مؤرخ في سنة 2006، المتضمن قانون الإجراءات الجزائية، حيث خص الفصل الخامس منه تحت عنوان "في التسرب"، المواد من 65 مكرر 11 إلى المادة 65 مكرر 18، إذ تناول من خلالها مفهوم هذه العملية وشروط إجرائها، والحماية الجنائية للقائم بعملية التسرب.

1- سعيداني نعيم، رسالة الماجستير السابقة الذكر، ص من 139 إلى 141.

أ- تعريف التسرب:

قيام ضابط أو عون شرطة قضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك، وهذا ما نصت عليه المادة 65 مكرر 12 من قانون الإجراءات الجزائية، ومثاله في الجريمة الإلكترونية إشتراك 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 الإستفادة حول كيفية اقتحام الهاكرز الموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم.¹

ب- شروط صحة التسرب:

- صدور إذن من وكيل الجمهورية، أو قاضي التحقيق بعد إخطار وكيل الجمهورية .
- أن يكون الإذن مكتوبا ومسيا- يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة .
- يحدد مدة عملية التسرب التي لا يمكن أن تتجاوز 04 أشهر، غير أنه يمكن أن تحدد، حيث تنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية على : "... يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن... حسب الحالة مباشرة عملية التسرب."²

2- إعتراض المراسلات الإلكترونية:

يقصد بهذا الإجراء مراقبة الإتصالات الإلكترونية أثناء بثها، وليس الحصول على اتصالات إلكترونية مخزنة، وقد استحدثت المشرع الجزائري هذا الإجراء من خلال القانون رقم 04-09 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال، حيث حدد الحالات التي يجب فيها اللجوء إلى المراقبة الإلكترونية كالأفعال الموصوفة بجرائم الإرهاب أو

1- بوعناد فاطمة زهرة، المحلة السابقة الذكر، ص 69-70

2- بوعناد فاطمة زهرة، نفس المحلة، ص 70.

التخريب أو الجرائم الماسة بأمن الدولة أو في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام، أو مؤسسات الدولة أو في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة، أو لمقتضيات التحريات والتحقيقات القضائية، وهذا طبقاً للمادة 04 من القانون رقم 09-04 ، وبترتب على المراقبة السرية للإتصالات عموماً، ومن ضمنها الإتصالات الإلكترونية في الغالب تسجيل محتوى تلك الإتصالات وتخزينها على وسائط مادية قابلة للنقل، بغية استخدامها فيما بعد الإثبات الجريمة الواقعة، وتختلف نوعية التسجيل هنا بحسب ما إذا كانت المحادثة الإلكترونية المراقبة هي عبارة عن اتصال صوتي فقط، أو أنها اتصال صوتي مرئي، ففي الأول يكون التسجيل صوتي فقط، في حين أنه يكون في الثاني تسجيل صوتي مرئي، كما تجدر الإشارة إلى أن المراقبة السرية للإتصالات الإلكترونية، ومن ضمنها المحادثات الهاتفية، لا يمكن اعتبارها نوع من أنواع التفتيش، لأن المراقبة الإلكترونية ترد على البيانات الإلكترونية المتحركة للإتصالات الإلكترونية حال إجرائها، دون التي انتهت وخرنت، في حين التفتيش يرد فقط على البيانات الإلكترونية الساكنة أو المخزنة (الإتصالات الإلكترونية التي تمت وخرنت)، وتكون عملية المراقبة في جميع الحالات بإذن مكتوب من السلطة القضائية المختصة طبقاً للمادة 04 من القانون الرقم 0904 التي تنص على: " لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه، إلا بإذن مكتوب من السلطة القضائية المختصة..."¹

1- بوعناد فاطمه زهرة، المحلة السابقة الذكر، ص 72.

الفرع الرابع : صعوبات مكافحة الجريمة الإلكترونية.

يعترف المهتمون بشؤون تكنولوجيا المعلومات بصعوبة اكتشاف الجريمة الإلكترونية، وذلك للأسباب التالية:

- يمكن أن تنقضي عدة أشهر أو سنوات قبل اكتشاف الجريمة.
- صعوبة التوصل إلى الجاني، فكثيرا ما يقوم الجاني بالدخول إلى شبكة الأنترنت باستخدام إسم مستعار، وغالبا ما يقوم بالدخول للأنترنت عن طريق مقاهي الأنترنت، فيصعب معرفة الجاني وتحديد موقع اتصاله.
- تتعارض القوانين الجنائية من حيث المكان، إذ أن هناك مبادئ تحكم تطبيق القانون الجنائي منها مبدأ إقليمية القانون الجنائي، وتثور المشكلة في حالة ارتكاب الفعل الإجرامي في الخارج فأبي من القوانين سوف يخضع لها الجاني؟
- صعوبة تحديد المسؤول جنائيا عن الفعل الإجرامي، كأن يدخل المستخدم للشبكة على موقع فيجد به أفعال إباحية، فهل يسأل عن هذه الجريمة عامل الإتصال، أم مورد المنافذ، أم مورد المعلومات، أو غيرهم من العاملين في مجال الأنترنت.
- إفتراض العلم بقانون جميع الدول، ففي حالة ارتكاب الجريمة في بلد ما، وتحقق النتيجة في بلد آخر يجد الجاني نفسه يخضع لقانون هذه الدولة، وقد يكون هذا الفعل المرتكب مباح في بلده .
- صعوبة المطالبة بالتعويض المدني، حيث يرجع في ذلك لأحكام القانون الدولي الخاص. -
- جهل الناس بثقافة الأنترنت يجعلهم يقومون بأفعال لا يعرفون بأنها تشكل جريمة يعاقب عليها القانون.¹

1- جعفر حسن جاسم العطاوي، جرائم تكنولوجيا المعلومات (رؤية جديدة للحرية الحديثة)، دار البلدية، عمان الأردن، 2007، ط 01، ص من 220 إلى 223.

- عدم ظهور الدليل المادي للجريمة الإلكترونية أو آثار مادية ملموسة.
 - عجز الوسائل التقليدية عن ضبط آثار الجريمة الإلكترونية.¹
 - عولمة هذه الجريمة تؤدي إلى تشتت جهود التحري والتنسيق الدولي، لتعقب مثل هذه الجرائم، وهي بمثابة صورة صادقة من صور العولمة.²
 - صعوبة تقدير حجم الجريمة الإلكترونية، فالإحصائيات الجنائية لا تعبر عن الإحرام الحقيقي، إذ منها ما يصل إلى علم السلطات المختصة بصورة دائمة، ومنها ما لا يصل إلى علمها إلا نادراً، كالجرائم الماسة بالعرض، وهنا يظهر الفارق بين الحجم الحقيقي للجريمة الإلكترونية، وبين ما هو مسجل بالإحصائيات.³
- من خلال التطرق لمكافحة الجريمة الإلكترونية في التشريع الجزائري استنتج أنه لا بد من الوقاية من هذا النوع من الجرائم قبل انتشارها، واللجوء إلى مكافحتها، وذلك بتربية النشأ على الوازع الديني والأخلاق الفاضلة، اللذان هما بمثابة وافي للفرد يحول دون ارتكاب أي نوع من الجرائم، و يجعلان الفرد يعي مدى خطورة التعدي على حقوق الغير، علاوة على ذلك توعية الأفراد بأخطار وسلبيات الأنترنت، من خلال عقد ندوات ودراسات حول مخاطر الأنترنت في الجامعات والثانويات، وجميع الأنشطة من جمعيات وغيرها.

1- عبد الفتاح يومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2007، ص 105.

2- عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والانترنت الجرائم الإلكترونية)، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2007، ط 01، ص 33.

3- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، 2005، ط 01، ص 68.

خاتمة

ومن هنا نستخلص ان الجريمة القرصنة الإلكترونية من الجرائم في العصرنا في آخر المطاف، فإنني حاولت معالجة الموضوع من خلال فصلين أساسيين، حيث تعرضت للفصل الأول إلى ماهية الجريمة القرصنة الإلكترونية، وذلك بالتطرق إلى مفهومها المتضمن الإتجاه المضيق والموسع لها، وكذا الدوافع المؤدية لارتكابها، ثم بيان خصائصها التي جعلتها تنفرد عن نظيرتها التقليدية، سواء تعلقت هذه الخصائص بالجريمة ذاتها، أو بامحرم الإلكتروني، كما أن هذا النمط من الجرائم يتنوع بحسب ما هو واقع أو مستهدف النظام المعلوماتي، أو ما يرتكب باستخدام النظام المعلوماتي، هذه الطبيعة المتميزة للجريمة الإلكترونية جعلت المشرع الجزائري يدرك مدى خطورة هذه الجريمة على الفرد وعلى المجتمع على حد سواء، وكان لا بد من التصدي لها، خصوصا أن الجزائر تشهد استعمال موسع للتقنية المعلوماتية في جميع القطاعات، وهذا ما تعرضت له بالتفصيل من خلال الفصل الثاني، حيث تطرقت للحماية الموضوعية والإجرائية للنظام المعلوماتي في التشريع الجزائري، إذ أن المشرع الجزائري قام بتعديل قانون العقوبات رقم 15/04 ، وإصدار قانون رقم 04/09 ، لما يتناسب والظاهرة المستجدة . من خلال هذه الدراسة توصلت للنتائج التالية:

- إن عدم إجماع الفقهاء على تعريف موحد للجريمة الإلكترونية يعود أساسا إلى الإختلاف حول تحديد نطاق هذه الجريمة، خصوصا أن البعض وسع كثيرا من نطاقها واعتبر أن كل فعل غير مشروع يكون للحاسب الآلي دورا فيه جريمة إلكترونية، وقد تبني هذا الإتجاه المشرع الجزائري، حيث نص على ذلك في القانون رقم 04/09 ، و حدد نطاق الجريمة الإلكترونية بالجريمة التي تمس بالنظام المعلوماتي، أو أي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام للاتصالات، وهو توسيع لا يتفق وماهية الجريمة الإلكترونية، باعتبارها تستهدف بالدرجة الأولى الجانب البرمجي للنظم المعلوماتية.

- إن هذه الجريمة مع تعدد أنماطها وأحتراف مرتكبيها، سواء كانت جرائم واقعة على النظام المعلوماتي أو باستخدامه، فإن لها جوانب سلبية خطيرة تهدد أمن وسلامة الفرد و المجتمع،

وهي تتسم بالغموض، حيث يصعب إثباتها والتحقيق فيها، مما يضع مسؤولية كبيرة على ضباط الشرطة والقضاء .

- قام المشرع الجزائري بمكافحة الجريمة الإلكترونية على غرار باقي الدول بموجب تعديل قانون العقوبات رقم 15/04 ، حيث اعتبر الدخول غير المشروع للنظام المعلوماتي والبقاء فيه، والمساس بمنظومة معلوماتية وبعض الأفعال الأخرى أفعال إجرامية و سطر لها عقوبات، واستدرك النقص في المجال الإجرائي، بإصدار قانون رقم 04/09 ، إذ تضمن قواعد إجرائية وأخرى وقائية وهذه خطوة إيجابية إلا أنها غير كافية لمواجهة خطر الجريمة الإلكترونية.

- إن المشرع الجزائري تطرق للجريمة الواقعة على النظام المعلوماتي، وأغفل الجرائم الماسة منتوجات الحاسب الآلي، حيث لم ينص على جريمة التزوير المعلوماتي، وإنما أخضعها للنصوص التقليدية الخاصة بتزوير المحرر، ولم يوسع من مفهوم المحرر ليشمل المستند المعلوماتي .

- المشرع الجزائري لم يقد بتحديد الجريمة المرتكبة باستخدام النظام المعلوماتي، وترك المجال واسع ليدخل في نطاقها كل ما تفرزه التقنية الجديدة وتطوراتها.
من خلال هذه النتائج أتوصل إلى التوصيات الآتية:

- ضرورة إعادة النظر في المناهج المتبعة في كلية الحقوق، وذلك بتدريس مقاييس لها علاقة بالتقنية الجديدة، مثل إدراج الجريمة الإلكترونية في مقياس قانون العقوبات، الإدارة الإلكترونية في مقياس القانون الإداري، المحكمة الإلكترونية في مقياس قانون الإجراءات الجزائية.

- نرجو من المشرع الجزائري أن يتوقف عن استيراد القوانين من بلدان أجنبية، والإهتمام أكثر بالأدمغة الجزائرية، إذ يوجد عدة كفاءات جزائرية لا بد من الإعتماد على خيرقا في وضع التشريعات الوطنية.

- الاستفادة من التجارب الدولية في هذا المجال لكسب المهارات اللازمة لمكافحتها.
- ضرورة انضمام الجزائر في الاتفاقيات الدولية والعربية للتعاون على مكافحة الجريمة الإلكترونية.

قائمة المراجع

القرآن الكريم.

النصوص القانونية :

1. الأمر رقم 03-07، مؤرخ في 19 جمادى الأولى عام 1424، الموافق ل 19 يوليو 2003، المتعلق ببراءات الاختراع، ج ر العدد 44
2. الأمر رقم 03-05، مؤرخ في 19 جمادى الأولى عام 1424، الموافق ل 19 يوليو 2003، المتعلق بحقوق المؤلف والحقوق المجاورة، ج ر العدد 44
3. الأمر رقم 04-15، مؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156، الصادر في 08 جوان 1966، المتضمن قانون العقوبات، ج ر العدد 71.
4. الأمر رقم 06-22، مؤرخ في 20 ديسمبر 2006، المعدل والمتمم لقانون الإجراءات الجزائية، ج ر العدد 84، صادر في 2006.
5. الأمر رقم 09-04، مؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 47.

الكتب:

1. أحسن بوسقيعة، الوجيز في القانون الجزائري العام، الديوان الوطني للأشغال التربوية، 2002، ط 01، بدون بلد نشر.
2. بن زبطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، الجزائر، 2007، ط 01 .
3. جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات (رؤية جديدة للجريمة الحديثة)، دار البلدية، عمان الأردن، 2007، ط 01 .
4. جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2010، ط 01.

5. حنير مسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر، طبعة 2010 .
6. زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر ، الجزائر، 2011، بدون طبعة.
7. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي ، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009، بدون طبعة.
8. عبد الفتاح بيومي حجازي، الإثبات الجنائي في جرائم الكمبيوتر والأنترنترنت، دار الكتب القانونية، مصر، 2007، بدون طبعة.
9. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والأنترنترنت، دار الكتب القانونية، مصر، 2002، بدون طبعة.
10. عبدالله عبدالكريم عبدالله، جرائم المعلوماتية والأنترنترنت (الجرائم الإلكترونية)، دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، 2007، ط 01.
11. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، 2000، ط 02، بدون بلد نشره .
12. عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة، منشورات الحلبي الحقوقية بيروت، 2003، بدون طبعة.
13. محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنترنت (الجريمة المعلوماتية)، مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن، 2004، ط 01.
14. محمد عبد الرحيم الناغي، الحماية الجنائية للرسوم والنماذج الصناعية (دراسة مقارنة)، دار النهضة العربية، القاهرة، 2009، بدون طبعة.
15. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، بدون طبعة.

16. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الإقتصادية، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقية، بيروت، 2005، ط 01 .
- الرسائل العلمية:**
1. حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام و علم العقاب، جامعة الحاج لخضر، باتنة، 2011-2012 .
 2. رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2011-2012
 3. سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2012 - 2013 .
 4. سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2013-2014.
 5. سوبر سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، 2010-2011.
 6. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، تاريخ المناقشة 2013/03/06 .
 7. عبدالله دغش العجمي، المشكلات العملية والقانونية للجرائم الإلكترونية ، (دراسة مقارنة)، رسالة مكملة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.

8. دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منتوري قسنطينة، 2012-2013.

المقالات والمجلات:

1. عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية و أزمة الشرعية الجزائية، كلية القانون، جامعة الكوفة، 2008، العدد 07 .

2. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية (دراسة تطبيقية مقارنة)، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، 2007/11/14/12، الرياض.

3. فشار عطاء الله، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدم إلى الملتقى المغاربي حول القانون والمعلوماتية المنعقد بأكاديمية الدراسات العليا بليبيا في أكتوبر 2009.

4. كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، 2000/23/21 تشرين الأول 2000، حلب.

5. محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، وزارة الداخلية.

6. مفتاح بوبكر المطرودي، الجريمة الإلكترونية والتغلب على تحدياتها، ورقة مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا في الدول العربية بجمهورية السودان المنعقد في 2012/09/25/23 .

7. موسي مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، الذي تنظمه أكاديمية الدراسات العليا، طرابلس، خلال الفترة 2009/10/29/28 .

8. سميرة بيطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث،.

.culture/net.alukah.www/http/br

9. مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، مجلة علمية،
2012/06/01 .
10. بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، محلة الندوة
للدراسات القانونية، سيدي بلعباس، 2013، العدد 01 .
11. سمير سعدون مصطفى، محمود خضر سلمان، حسن كريم عبدالرحمن، الجريمة
الإلكترونية عبر الأنترنت وسبل مواجهتها، بحث مقدم بتاريخ 2011/05/04 .
12. بن دعاس فيصل، إجراءات التحري في الجرائم المعلوماتية، محاضرة في إطار التكوين
المحلي المستمر للقضاة، مجلس قضاء قسنطينة.
13. كوثر فرام، الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث نهاية
التدريب، المعهد العالي للقضاء، فترة التدريب، 2007-2009 .
14. جازية سليمان، موقع العربي الجديد، <https://www.alaraby.co.uk/media>
.news
15. المخترق، ويكيبيديا الموسوعة الحرة، <https://ar.wikipedia.org>.

الفهرس

01.....	مقدمة
06.....	الفصل الأول: ماهية الجريمة القرصنة الإلكترونية
07.....	المبحث الأول: مفهوم الجريمة القرصنة الإلكترونية
07.....	المطلب الأول: تعريف الجريمة القرصنة الإلكترونية وأركانها
08.....	الفرع الأول: تعريف الجريمة القرصنة الإلكترونية
12.....	الفرع الثاني: أركان الجريمة القرصنة الإلكترونية
13.....	المطلب الثاني: دوافع ارتكاب الجريمة القرصنة الإلكترونية
14.....	الفرع الأول: الدوافع الشخصية لارتكاب الجريمة القرصنة الإلكترونية
15.....	الفرع الثاني: الدوافع الموضوعية لارتكاب الجريمة الإلكترونية
17.....	المبحث الثاني: خصائص و أنواع الجريمة الإلكترونية في القانون الجزائري
17.....	المطلب الأول: خصائص الجريمة الإلكترونية
17.....	الفرع الأول: السمات الخاصة بالجريمة الإلكترونية
20.....	الفرع الثاني: السمات الخاصة بالمجرم الإلكتروني
26.....	المطلب الثاني: أنواع الجريمة القرصنة الإلكترونية في القانون الجزائري
27.....	الفرع الأول: الجريمة القرصنة الإلكترونية المرتكبة باستخدام النظام المعلوماتي

29.....	الفرع الثاني: الجريمة القرصنة الإلكترونية الواقعة على النظام المعلوماتي
34.....	الفصل الثاني: الآليات القانونية لمكافحة الجريمة القرصنة الإلكترونية
35.....	المبحث الأول: الحماية الموضوعية للنظام المعلوماتي من القرصنة.....
35.....	المطلب الأول: الحماية في نصوص الملكية الفكرية من القرصنة الإلكترونية
36.....	الفرع الأول: مدى خضوع معطيات الحاسب الآلي لنصوص الملكية الصناعية.....
37....	الفرع الثاني: مدى خضوع معطيات الحاسب الآلي لنصوص الملكية الأدبية والفنية....
39.....	المطلب الثاني: الحماية في قانون العقوبات
40.....	الفرع الأول: العقوبات الأصلية
41.....	الفرع الثاني: العقوبات المقررة للشخص المعنوي
41.....	الفرع الثالث: عقوبة الإشتراك والشروع في الجريمة.....
	الفرع الرابع الثالث: الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.....
41.....	41.....
	الفرع الخامس : الحماية في قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
42.....	42.....
44.....	المبحث الثاني : الحماية الإجرائية للنظام المعلوماتي.....
44.....	المطلب الأول: التحقيق في الجريمة الإلكترونية
45.....	الفرع الأول: الأجهزة المكلفة بالبحث والتحري

- 45..... الفرع الثاني: خصائص التحقيق والمحقق
- 49..... الفرع الثالث: الدليل المناسب لإثبات الجريمة الإلكترونية
- 50..... المطلب الثاني: إجراءات جمع الأدلة التقليدية
- 51..... الفرع الأول: الإجراءات المادية (المعاينة، التفتيش، ضبط)
- 55..... الفرع الثاني: الإجراءات الشخصية (الشهادة، الخيرة)
- 56..... الفرع الثالث: إجراءات جمع الأدلة الحديثة
- 60..... الفرع الرابع: صعوبات مكافحة الجريمة الإلكترونية
- 63..... خاتمة
- 66..... قائمة المراجع

ملخص مذكرة الماستر

ومن هنا نستخلص ان الجريمة القرصنة الإلكترونية من الجرائم في العصرنا في آخر المطاف، إلى ماهية الجريمة القرصنة الإلكترونية، وذلك بالتطرق إلى مفهومها المتضمن الإتجاه المضيق والموسع لها، وكذا الدوافع المؤدية لارتكابها، ثم بيان خصائصها التي جعلتها تنفرد عن نظيرتها التقليدية، سواء تعلقت هذه الخصائص بالجريمة ذاتها، أو بامحرم الإلكتروني، كما أن هذا النمط من الجرائم يتنوع بحسب ما هو واقع أو مستهدف النظام المعلوماتي، أو ما يرتكب باستخدام النظام المعلوماتي.
الكلمات المفتاحية:

- 1/ القرصنة الإلكترونية 2/ الجريمة الإلكترونية 3/ النظام المعلوماتي
4/ الوقاية من الجرائم

Abstract of The master thesis

From here, we conclude that the crime of electronic piracy is one of the crimes in our time in the end, to the nature of the crime of electronic piracy, by addressing its concept that includes the narrow and expanded direction of it, as well as the motives leading to its perpetration, and then explaining its characteristics that made it unique from its traditional counterpart, whether these characteristics are related to The crime itself, or the electronic forbidden, and this type of crime varies according to what is the reality or target of the information system, or what is committed using the information system.

keywords:

- 1 / Electronic piracy 2/ Cybercrime 3/ Information system
4/ Crime prevention