



الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد البشير الإبراهيمي - برج بوعريريج
الكلية: الحقوق والعلوم السياسية



مستخرج من محضر مكتب المجلس العلمي للكلية

المنعقد بتاريخ: 24 جانفي 2024

بناء على محضر اجتماع مكتب المجلس العلمي للكلية المنعقد بتاريخ: 24 جانفي 2024
وفي محور جدول الأعمال النقطة رقم 01: المصادقة على تقارير الخبرة الإيجابية
لتقييم مطبوعة بيداغوجية واعتمادها.

للدكتور: خضري محمد،

تحت عنوان: " مدخل للجرائم الالكترونية "، المقدمة لطلبة السنة الثانية ماستر تخصص
إعلام آلي و أنترنيت السنة الجامعية 2021/2022.

و المحكمة من طرف الخبراء الذين تم تعيينهم في المجلس العلمي للكلية المنعقد
بتاريخ: 28 فيفري 2022 والآتية أسماؤهم:

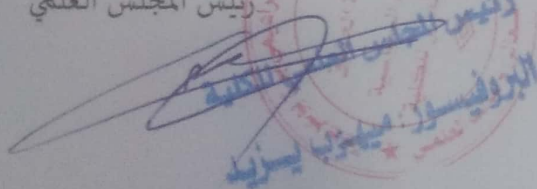
جامعة برج بوعريريج	رتبة أستاذ	الدكتور: فرشة كمال
جامعة برج بوعريريج	رتبة أستاذ	الدكتور: هدي العيد
جامعة المسيلة	رتبة أستاذ محاضر قسم أ	الدكتور: مقدم ياسين

تم اعتماد المطبوعة.

سلمت هذه الشهادة بطلب من المعني لاستعمالها في حدود ما يسمح به القانون

برج بوعريريج في: 24 جانفي 2024

رئيس المجلس العلمي


البروفيسور: محمد بن يزيدي

جامعة محمد البشير الابراهيمى - برج بوعريىج-

كلية الحقوق والعلوم السياسية

قسم الحقوق

مطبوعة مقدمة لطلبة السنة الثانية ماستر تخصص إعلام ألى وأنترنى

بعنوان:

مدخل للإجرام الالىكترونى

الدكتور خضرى محمد

2023-2022

مقدمة :

إن مصطلح الأنظمة المعالجة للمعطيات¹ مصطلح تم إدخاله في القانون الفرنسي سنة 1978 بموجب قانون الإعلام الآلي والحريات ؛ ثم تم إعادة ذكرها في قانون Godfrain حسب النائب الذي قدم المقترح²؛ والتي بقيت سارية إلى حد اليوم وتم اعتمادها من طرف المشرع الجزائري بموجب التعديل القانوني 15/04 المؤرخ في 10 نوفمبر 2004 والذي ورد تحت عنوان القسم السابع مكرر -3- بعنوان : المساس بأنظمة المعالجة الآلية للمعطيات من المواد 394 مكرر إلى المراد 394 مكرر 7 .

و قد ورد القسم السابع تحت عنوان الفصل الثالث بعنوان الجنايات والجنح ضد الأموال ؛ وهنا تبدأ بعض الإشكالات القانونية بالظهور حول طبيعة هذه الجرائم ولماذا ضمنها المشرع الجزائري تحت عنوان الجنايات والجنح ضد الأموال ؟ والمقصود بهذا النوع من الجرائم ؟ وهل يمكن اعتبارها بأنها جرائم من نوع جديد ؟

¹ système de traitement automatisé de données (ou STAD)

² La loi Godfrain du 5 janvier 1988, ou Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, est la première loi française réprimant les actes de criminalité informatique et de piratage

Voir : https://fr.wikipedia.org/wiki/Loi_Godfrain .

الفصل الأول:

ماهية الجريمة الالكترونية

المبحث الأول: تطور الجريمة الإلكترونية

المطلب الأول: تطور الجريمة الإلكترونية في التشريعات المقارنة:

لقد ظهرت جرائم الانترنت في حقل جرائم التقنية العالية في نهاية الثمانينيات، وكان ذلك من خلال العدوان الفيروس، وقد أطلق مصطلح جرائم الانترنت في مؤتمر المنعقد في أستراليا سنة 1998.

وتجدر الإشارة إلى أن الكثير من الباحثين يستخدمون مصطلحات غير دقيقة للتعبير عن جرائم الانترنت، إذ نجد بعض البعض يستخدم مصطلح الإجرام الالكتروني يستخدم مصطلح جرائم التكنولوجيا المتقدمة أو مصطلح "الغش الالكتروني" في حين أنه يجب استخدام المصطلح الدقيق مع طبيعة تلك الجرائم وهو "جرائم الانترنت".¹

ذلك لأن الإجرام الالكتروني وإن كان يقصد التعبير عن الجرائم الواقعة عن طريق جهاز الكمبيوتر إلا أن هذا لا يتغير من جهة أخرى أن الاعتداء على المعلومات يتحقق دائما باستخدام الكمبيوتر وخصوصا باستخدام الانترنت لذلك لأن الوسائل التقليدية هي دائما ما تكون أداة لارتكاب تلك الجريمة وبالتالي فالجريمة الالكترونية قد تكون أجمل من جرائم الانترنت وذلك الشأن بالنسبة للغش الالكتروني وكذا جرائم التكنولوجيا المتقدمة.²

مرت جرائم الانترنت بتطور تاريخي تبعا لتطور التقنية واستخدامها، ولهذا مرت بثلاث

مراحل وهي:

¹ نبيلة هبة هروال، الجوانب الإجرامية لجرائم الانترنت، في مرحلة جمع استدلالات، دراسة مقارنة، دار الفكر الجامعي 30

شارع سويتز - الإسكندرية، 2013، ص 31.

² المرجع السابق، ص 31.

– المرحلة الأولى: من شيوع استخدام الحواسيب من الستينات إلى السبعينات من القرن الماضي اقتضت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر؟ وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت جرائم شتى عابر أم ظاهرة إجرامية مستحدثة، ومع تزايد استخدام الحواسيب الشخصية في السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية، وبدأ البحث عنها بوصفها ظاهرة إجرامية لا مجرد سلوكيات مرفوضة.¹

– المرحلة الثانية: في الثمانينات حيث طغى على السطح مفهوم جديد لجرائم الكمبيوتر الانترنت وارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدميرية للملفات أو البرامج.

شاع اصطلاح "الهاكرز" المعبر عن مقتحمي النظم، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل محصورا في رغبة المحترفين تجاوز أمن المعلومات وإظهار تفوقهم التقني، ولكن هؤلاء المغامرون أصبحوا أداة إجرام، وظهور المجرم الإلكتروني المتفوق المدفوع بأغراض إجرامية خطيرة القدرة على ارتكاب أفعال تستهدف الاستيلاء على المال أو التجسس أو الاستيلاء على البيانات السرية والاقتصادية والاجتماعية والسياسية والعسكرية.²

– المرحلة الثالثة: شهدت التسعينات تناميا هائلا في حقل الجرائم الإلكترونية وتغيير في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الانترنت من تسهيل لعمليات دخول الأنظمة، واقتحام شبكة المعلومات ظهرت أنماط تقوم على فكرة تعطيل نظام تقني ومنعه من

¹ عبد الفتاح مراد، دور الكمبيوتر في مجال ارتكاب الجرائم الإلكترونية، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية، ص 43.

² عبد الفتاح مراد: المرجع السابق، ص 43.

القيام بعمله المعتاد وأكثر ما مورست ضد مواقع الانترنت التسويقية الهامة التي يتسبب انقطاعها عن القيمة في خسائر مالية بالملايين، ونشطت جرائم نشر الفيروسات عبر المواقع الإلكترونية لما تسهله من انتقالها إلى ملايين المستخدمين في ذات الوقت وظهرت الوسائل المنشورة على الانترنت أو المراسلة بالبريد الإلكتروني المنطوية على الأحقاد أو المساس بكرامة واعتبار الأشخاص أو المروجة لمواد غير قانونية أو غير المشروعة.¹

- نصت المادة 394 مكرر 02 على أن يعاقب بالحبس من شهرين إلى ثلاثة سنوات وبغرامة 1000.0000 إلى 5000.0000 دينار جزائري كل من يقوم عمداً أو عن طريق الغش بما يأتي:

1- تصميم أو بحث أو جمع أو توفير أو نشر أو الاتجار في معطيات المخزنة أو معالجة أو مرسله عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

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

- نصت المادة 394 مكرر 03 على أنه: "تضاعف العقوبة المنصوص عليها في هذا القسم، إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشبهه."

- نصت المادة 394 مكرر 04 على أنه: "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات بالحد الأقصى للغرامة المقررة للشخص الطبيعي".²

نفس المرجع، ص 1.43

مولود ديدان، قانون العقوبات، المرجع السابق، ص 212.

- نصت المادة 394 مكرر 05 على فعل إشراك في جريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم فإنه يعاقب بنفس العقوبة المقررة للجريمة في حد ذاتها وذلك بنصها: "كل من شارك في مجموعة أو في اتفاق بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم، يعاقب بالعقوبات المقررة للجريمة ذاتها:

نصت المادة 394 مكرر ولا على "مع الاحتفاظ بحقوق الغير حسن النية، بحكم مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا للجريمة من الجرائم المعاقبة عليها وفقا لهذا القسم، مع غلق المحل إذا كانت الجريمة قد ارتكبت بعلم مالكيها.¹

المطلب الثاني: تطور الجريمة الإلكترونية في التشريع الجزائري:

في بداية الألفينات شهدت الجزائر تطورا في حيز الجريمة الإلكترونية، إذ نجد أن المشرع الجزائري قد قام بسن نصوص قانونية لقمع الجريمة الإلكترونية وذلك بسبب التزايد اللامتناهي للاعتداءات على الأنظمة الإلكترونية في الجزائر من خلال تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة الإلكترونية من أشكال جديدة من الإجرام التي لم تستهدفها البشرية من قبل مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 المتمم للأمر رقم 66-156 المتضمن قانون العقوبات من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 مكرر ونصت هذه المواد على ما يلي:²

المرجع نفسه، ص 121.¹

² ماشوش مراد، مكافحة جرائم المعلوماتية في التشريع الجزائري، مذكرة لاستكمال متطلبات نيل شهادة ماستر أكاديمي في مسار الحقوق، تخصص قانون جنائي، سنة 2013-2014، ص 71.

نصت المادة 394 مكرر على جريمة الدخول والبقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات محاولة ذلك بنصها: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50,000 إلى 1000,00 دينار جزائري كل من يدخل أو يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات ويحاول ذلك.

- تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير معطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة بالحبس من ستة أشهر إلى سنتين والغرامة من 50,000 دينار جزائري إلى 150,000 دينار جزائري.

- نصت المادة 394 مكرر 1 على إدخال أو إزالة أو تعديل بطريقة الغش معطيات في نظام المعالجة الآلية بنصها: "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500,000 دينار جزائري إلى 2000,000 دينار جزائري كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية.

- نصت المادة 394 مكرر 07 على أنه يعاقب على الشروع في ارتكاب الجرح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنة ذاتها:¹

في عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون رقم 03-23 المؤرخ في 20 ديسمبر 2006 حيث مس ذلك التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وقد تم تسديد العقوبات المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريبية الواردة في هذا القسم من القانون 04-15 وربما يرجع بسبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث عن

(1) مولود ديدان، قانون العقوبات، قانون رقم 09-01 المؤرخ في 25 فبراير 2009، د ط، ص 120.

الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار والمستويات.¹

- المشرع الجزائري أكد نفس منوال المشرع الفرنسي الفرق نجد أن المشرع الجزائري لم يتطرق إلى جريمة استعمال المستندات الالكترونية المزورة بخلاف المشرع الفرنسي الذي نص على هذه الجريمة في المادة 06/462 المشار إليها سابقاً.²

المرجع السابق ، ص 120.¹

نفس المرجع، ص 120.²

المبحث الثاني: طبيعة الجريمة الالكترونية:

المطلب الاول: الطبيعة الخاصة للجرائم الالكترونية.

إن تحديد الطبيعة الخاصة للجريمة الالكترونية يقتضي تعريفها (أولاً)، وتحديد موضوعها (ثانياً)، وإبراز خصوصياتها المميزة (ثالثاً).

إذا كان هناك اختلاف حول تعريف الجريمة الالكترونية كظاهرة مستحدثة وأن موضوعها يختلف حسب نوعية الإعتداء موجه ضد أحد مكونات النظام الالكتروني أو وسيلة لتنفيذ جرائم معينة، وأخيراً كظاهرة إجرامية ذات طبيعة خاصة لها ذاتيتها، ولذلك فإننا سنتناول ذلك بالتفصيل هذه الفقرة على الشكل التالي:

- أولاً: تعريف الجريمة الالكترونية.
- ثانياً: موضوع الجريمة الالكترونية.
- ثالثاً: خصوصية الجريمة الالكترونية.

الفرع الاول: تعريف الجريمة الالكترونية.

- التعريف اللغوي:

الجريمة لغة كلمة مشتقة من الجرم وهو التعدي أو الذنب وجمع الكلمة إجرام وجروم وهو الجريمة وقد جرم يجرم واجترم وأجرم فهو مجرم جريم، وهي طبقاً للمفهوم الاجتماعي

كل سلوك إرادي غير مشروع يصدر عن شخص مسؤول جنائياً في غير حالات الإباحة عدواناً على مال أو مصلحة أو حق محمي بجزاء جنائي.¹

وعرفت الجريمة أيضاً: " على أنها على فعل غير مشروع صادر عن ارادة يقرر له القانون عقوبة أو تدبيراً احترازياً، وتعتمد الجرائم الناشئة عن الاستخدام غير²المشروع لشبكة الانترنت على المعلومة بشكل رئيسي."³

التعريف الفقهي:

هناك جانب من الفقه الفرنسي، يحاول وضع تعريف لظاهرة الغش الالكتروني حيث يرى الأستاذ "Massa" أن المقصود بها: "الإعتداءات القانونية التي ترتكب بواسطة الالكترونية بغرض تحقيق الربح". وفي الغالب ترتكب الجريمة الالكترونية ليس بغرض تحقيق الربح، وإنما بدافع الإنتقام والسخرية من المنافسين أو غير ذلك من الدوافع.

ويعرفها الأساتذة "Lestan & Vivant" بأنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب". ويؤكد الأستاذ "Devéze" أنه ليس المقصود مجرد إخفاء وصف قانوني، ولكن وضع مفهوم إجرامي، والذي سيكون من الممكن أن يطبق عليه أحد التعاريف المعمول بها في القانون المدني أو الجنائي أو المالي.³

بينما يعرف الفقيه الألماني تاديمان الجرائم الالكترونية بأنها "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب".

¹ هبة نبيلة هروال، جرائم الانترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص القانون، كلية الحقوق والعلوم السياسية، جامعة تلمسان، الجزائر، 2013/2014، ص 12

²- يوسف صغير، الجريمة المرتكبة عبر الانترنت، رسالة لنيل شهادة الماجستير، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، جامعة تيزي وزو، الجزائر، 2013، ص 7.

³- محمد علي العريان: "الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004. ص: 44.

ومن خلال هذه التعريفات يتضح أنها عمومية بحيث لا يمكن السيطرة عليها، بحيث كل تعريف ينظر إلى الجرائم الالكترونية من زاوية معينة تختلف عن أخرى.

لعل من هذه التعريفات الموسعة ما يقوله الفقيهان "Miche, Cerdo" من أن سوء استخدام الحاسب أو جريمة الحاسوب تشمل استخدامه كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد جريمة الحاسوب لتشمل الإعتداءات المادية، وسواء كان هذا الإعتداء على جهاز الحاسوب ذاته أو المعدات المتصلة به، وكذلك الإستخدم غير المشروع لبطاقات الإئتمان، وانتهاك ماكينات الحسابات الآلية، بما تتضمنه من شبكات تمويل الحسابات المالية بطريقة إلكترونية، وتزييف المكونات المادية والمعنوية للحاسب بل وسرقة جهاز الحاسب في حد ذاته أو مكون من مكوناته.¹

أما بالنسبة للفقهاء العربيين فهناك من يرى أن تعريف الجريمة المعلوماتية هي "كل فعل أو امتناع عمدي، ينشأ عن الإستخدم غير المشروع لتقنية المعلومات ويهدف إلى الإعتداء على الأموال والحقوق المعنوية".

هناك فريق آخر يرى أن الجريمة الالكترونية هي: "عمل أو امتناع يأتيه أضراراً بمكونات الحاسوب. وشبكات الإتصال الخاصة به، التي يحميها قانون العقوبات يفرض له عقاباً".²

¹ - أورده محمد علي العريان: المرجع السابق، ص: 45.

² - محمد علي العريان: المرجع السابق، ص: 46.

• التعريف التشريعي للجريمة الالكترونية

من المعلوم أن المشرع الجزائري والى وقت قريب أغفل تنظيم مجال الجريمة الالكترونية قانونا الا أنه ما فتئ أن تدارك ذلك الفارغ القانوني من خلال سن قواعد قانونية لمواجهة هذه الجريمة، وذلك ما تجلى في القانون رقم 04-15 المتضمن تعديل قانون العقوبات الذي نصت أحكامه في القسم السابع مكرر على المساس بأنظمة المعالجة الالية للمعطيات ثم تاله بالقانون رقم 04-09 الذي يتضمن القواعد¹ الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها.

ومما تجب الاشارة إليه، أن مصطلح نظام المعالجة الالية للمعطيات تعبير ذا طابع فني تقني يصعب على القانوني إدراك مغزاه ببساطة، فزال على أنه تعبير متطور² يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الالي.

ولذلك فالمشرع الجزائري على غرار الكثير من التشريعات لم يعرض نظام المعالجة الالية للمعطيات وأوكل بذلك المهمة لكل من الفقه والقضاء .

ولمزيد من التفصيل نتطرق الى تعريف ذلك من خلال القانونين 04-15 و 09-04 -
على التوالي:

أ- تعريف الجريمة الالكترونية حسب القانون 04-15:

بالرجوع الى قواعد القانون 04-15 من المادة 394 مكرر 1 ثم المادة 394 مكرر 2 نجد أنه حدد مفهوم المساس بأنظمة المعالجة الالية للمعطيات حيث حددها في المادة 394 مكرر بالاتي :

²محمد رحموني، خصائص الجريمة الالكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، 2018، ص 438

- الدخول وابقاء بالغش في كل جزء من منظومة للمعالجة الالية للمعطيات أو محاولة ذلك
 - حذف أو تغيير لمعطيات المنظومة إذا ترتب عن الدخول أو ابقاء غير المشروع بغرض تخريب نظام اشتغال المنظومة .أما المادة 394 مكرر 1 فقد أشارت الى ما يلي.:
 - تصحيح أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسله عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
 - حيازة أو إنشاء أو نشر أو استعمال ألي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم¹
- ب- تعريف الجريمة الالكترونية في حسب القانون 09-04:**

حددت المادة 02 منه الجريمة الالكترونية بقولها: " يقصد في مفهوم هذا القانون بما يأتي:

- الجرائم المتصلة بتكنولوجيات الاعلام والاتصال:
- جرائم المساس بأنظمة المعالجة الالية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية.

منظومة معلوماتية:

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

¹القانون رقم 04-15 المؤرخ في 10 نوفمبر يعدل ويتم الامر 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج.ر، ج.ج.د.ش، العدد 71 الصادر في 10 نوفمبر 2004.

معطيات معلوماتية:

أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها¹.

الفرع الثاني: موضوع الجريمة الالكترونية

يختلف موضوع الجريمة الالكترونية بحسب اختلاف الزاوية التي ينظر فيها إزاء الإعتداء الموجه ضد أحد مكونات النظام الالكتروني، فمن ناحية قد يكون هذا الأخير نفسه موضوع للجريمة الالكترونية، ومن ناحية قد يكون النظام الالكتروني هو وسيلة للجريمة الالكترونية وأداة تنفيذها.

أ. كون النظام الالكتروني موضوعا للجريمة الالكترونية.

في هذه الحالة إن جرائم المعلومات بمعناها الفني التي تتفق مع الجرائم التقليدية البحثية، فمن ناحية نجد أن مجل الجريمة الالكترونية في حالة وجود اعتداء على المكونات المادية للنظام الالكتروني (كالأجهزة والمعدات الالكترونية وغيرها) يتمثل في جرائم سرقة أو إتلاف هذه المكونات والمتمثل في الحاسبات أو شاشات أو شبكة الإتصال الخاصة أو حتى آلات الطبع المرفق بها.²

من ناحية أخرى، إذا كان الإعتداء موجه إلى مكونات غير مادية للنظام الالكتروني، (كالبيانات والبرامج) مثل جرائم الإعتداء على البيانات المخزنة في ذاكرة الحاسوب أو البيانات المنقولة عبر شبكات الإتصال المختلفة والتي تتمثل في جرائم السرقة أو التقليد أو

¹-القانون 04-09، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها، ج،ر، العدد 47، الصادرة في 16 أوت 2009.

²- محمد علي العريان: المرجع السابق، ص: 46.

الإتلاف أو محو وتعطيل هذه البيانات، أو كان الإعتداء ذاته موجه إلى برامج الحاسوب من خلال تزوير المستخرجات الإلكترونية وإفشاء محتوياتها وما اصطلح على تسميته "بسرقه ساعات عمل الحاسوب"¹.

ب . كون النظام الالكتروني هو أداة الجريمة الالكترونية ووسيلة تنفيذها.

ففي هذه الحالة، ليس هناك أدنى شك أننا بصدد جرائم تقليدية، يكون فيها النظام الالكتروني أو جهاز الحاسب الآلي هو أداة ارتكاب الجريمة الالكترونية ووسيلة تنفيذها، ومن هذه الناحية، نجد أن الجاني يمكن استخدام الحاسب الآلي لارتكاب جرائم السرقة أو النصب أو خيانة الأمانة أو تزوير المحررات الالكترونية، وذلك عن طريق التلاعب في الحاسوب وكذلك النظام الالكتروني بصفة عامة.²

الفرع الثالث: خصوصية الجريمة الالكترونية.

رغم أن البحث يدور حول نطاق تطبيق نصوص القانون الجنائي، إلا أنه وكما يبدو أننا بصدد ظاهرة إجرامية ذات طبيعة متميزة تتعلق غالباً بما يسمى بالقانون الجنائي الالكتروني.

ففي معظم حالات ارتكاب الجريمة الالكترونية نجد أن الجاني يتعمد التدخل في مجالات النظام الالكتروني المختلفة ومنها:

¹ - موقع: WWW.ARABLAW.ORG

² - محمد علي العريان: المرجع السابق، ص: 47.

أ . مجال المعالجة الإلكترونية للبيانات :

يتدخل الجاني من خلال ارتكاب الجريمة الالكترونية في مجال المعالجة الإلكترونية الآلية للبيانات سواء من حيث تجميعها أو تجهيزها حتى يمكن إدخالها إلى جهاز الحاسوب وذلك بغرض الحصول على معلومات.

ب . مجال المعالجة الإلكترونية للنصوص والكلمات الإلكترونية.

يتدخل الجاني في مجال المعالجة الإلكترونية للنصوص والكلمات وهي طريقة أتوماتيكية تمكن مستخدم الحاسوب من كتابة الوثائق المطلوبة بدقة متناهية بفضل الوسائل التقنية الموجودة تحت يده وبفضل إمكانيات الحاسوب، من تصحيح وتعديل ومحو وتخزين وطباعة واسترجاع وطباعة وهي إمكانيات لها علاقة وثيقة بارتكاب الجريمة، إذ ينبغي ألا ننسى من أننا نتعامل مع مفردات جديدة كالبيانات والبرامج.

وظاهرة الجريمة الالكترونية تهتم بصفة خاصة بالمجال المصرفي، وتفتح هذه الثورة الالكترونية مجالاً جديداً لخلق أدوات جديدة في المعاملات التجارية، فإذا كان التعامل والإثبات ينحصر في المستند الورقي، فإنه أصبحت الآن تسجيلات إلكترونية ومحركات إلكترونية أو سند شحن، وكذلك فإن المستخرجات لها قيمة في الإثبات، بجانب المستند الورقي. ويشهد الواقع العملي تقدم مذهل في عالم اليوم نحو الإعتماد على الوسائل الحديثة في الإثبات إذ كان ذلك لا يمنع من وجود وسائل الإثبات التقليدية بشرط أن ينظم المشرع الحديث هذه المسائل من خلال نصوص تشريعية¹ تعالج هذا الأمر، وبالمثل فإن الجريمة الالكترونية تتعلق بكل سلوك غير شرعي أو غير مسموح به نحو الولوج إلى المعالجة الآلية للبيانات أو نقلها، ومن ثمة فإن هذه المعالجة غير الشرعية تجعلنا في صدد القانون الجنائي

¹ - محمد علي العريان: المرجع السابق، ص: 48.

والتي تعتبر معظم نصوصه التقليدية عاجزة عن مواجهة هذا التطور التكنولوجي والالكتروني.

المطلب الثاني: الطبيعة القانونية للجريمة الالكترونية.

إذا كان السؤال ما هو الوضع القانوني للمعلومات؟ هل للمعلومات قيمة في ذاتها، أم لها قيمة ما تمثل في أنها مجموعة مستحدثة من القيم، ويرجع هذا التساؤل إلى ما إذا كانت المعلومات لها قيمة وتعتبر من ثمة من قبيل القيم القابلة للإستثناء. إذن يمكن الإعتداء عليها بأي طريقة كانت.¹

من أجل ذلك، فقد انقسم الفقه إلى اتجاهين:

الأول: يرى أن المعلومات لها طبيعة من نوع خاص.

الثاني: يرى أن المعلومات ما هي إلا مجموعة مستحدثة من القيم، ولنرى ذلك بشيء من التفصيل.

الفرع الأول: المعلومات لها طبيعة قانونية من نوع خاص.

يرى هذا الإتجاه التقليدي، أن المعلومات لها طبيعة من نوع خاص وذلك انطلاقاً من حقيقة مسلم بها هي أن وصف القيمة يضاف على الأشياء المادية وحدها بمعنى آخر أن الأشياء التي توصف بالقيم هي الأشياء التي تقبل الإستحواذ عليها، وبمفهوم المخالفة وباعتبار أن المعلومات لها طبيعة معنوية، فلا يمكن والحال كذلك اعتبارها من قبيل القيم القابلة للاستحواذ عليها إلا في ضوء حقوق الملكية الفكرية.

¹ - محمد علي العريان: المرجع السابق، ص: 49.

وأيا ما كان الأمر، فإن الأمر مستقر بصدد وجود خطأ عند الإستيلاء على المعلومات أو معلومات الغير ولذلك فقد حاول هذا الإتجاه أن يحمي هذه المعلومات بدعوى المنافسة غير المشروعة وذلك استنادا إلى حكم محكمة النقض الفرنسية: "إن الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استثنائي".¹ لذلك يذهب الأستاذ Debois بأن الملكية العلمية، ربما ستأتي يوما ويعترف بها لصاحب فكرة لم تحصل على حق براءة اختراع باعتبار أن الفكرة السابقة مستبعدة من مجال الملكية الذهنية.

الفرع الثاني: المعلومات مجموعة مستحدثة من القيم.

يرى هذا الإتجاه الحديث، أن المعلومات ما هي إلا مجموعة مستحدثة من القيم، ويرجع الفضل في ذلك إلى الأستاذين Catala & Vivaut ويذهب الأستاذ Catala² إلى قابلية المعلومات للإستحواذ كقيمة واستقلالاً عن دعايتها المادية.

على سند من القول أن المعلومات تقوم وفقا لسعر السوق متى كانت غير محظورة تجاريا وأنها تنتج بصرف النظر عن دعائها المادية عن عمل من قدمها وأنها ترتبط بمؤلفها عن طريق علاقة قانونية تتمثل في علاقة المالك بالشيء الذي يملكه وهي تخص مؤلفها بسبب علاقة التبني التي تجمع بينهما.

إن هذا الرأي يؤسس حجتين لإعطاء وصف القيمة على المعلومات:

¹ - محمد سامي الشوا: "ثورة المعلومات وانعكاساتها على قانون العقوبات". دار النهضة العربية، القاهرة. 1994، ص: 180.

² - Catala, la propriété de l'information, p : 97 et masse : la deliquance informatique aspects de droit pénal international in le criminel.

الأولى قيمة المعلومات الاقتصادية، والثانية وجود علاقة تبني تجمع بين مؤلفها. أما الأستاذ Vivaut فيؤسس ذلك على حجتين أيضاً، الأولى مستوحاة من بلا فيول روريبير وهي أن فكرة الشيء أو القيمة لها صورة معنوية، وأن نوع محل الحق يمكن أن ينتمي إلى قيمة معنوية ذات الطابع الإقتصادي، وأن تكون جديرة بحماية القانون، وأما الحجة الثانية فيقدم لنا الأستاذ فيفانتي نفسه حيث يرى إن كل الأشياء المملوكة ملكية معنوية والتي يعترف بها القانون وترتكز على الإقرار بأن للمعلومات قيمة، عندما تكون من قبيل البراءات أو الرسومات أو النماذج أو التحصيلات الضرورية أو حق المؤلف، والإنسان الذي يقدم ويكشف ويطلع الجماعة على شيء ما بصرف النظر عن الشكل أو الفكرة، فهو يقدم لهم معلومات بمعنى الواسع ولكنها خاصة به، ويجب أن تعامل هذه الأخيرة بوصفها قيمة تصبح محلاً لحق، فلا توجد ملكية معنوية بدون الإقرار بالقيمة الالكترونية، ولذلك فهو يرى أن القيمة الالكترونية ليست بالشيء المستحدث إذ أنها موجودة من قبل في مجموعة ما.

ويرى الدكتور محمد سامي الشوا، ويؤكد أن المعلومة وبالنظر إلى حقيقتها الذاتية واستقلالها، تعد قيمة في ذاتها، ولها بالتأكيد مظهر معنوي ولكنها تملك قيمة اقتصادية مؤكدة، وبحيث يمكن عند الاقتضاء أن ترفعها إلى مصاف القيمة القابلة لأن تحاز حياة غير مشروعة.

المطلب الثالث: خصائص الجريمة الالكترونية

الفرع الأول: أنها ترتكب من مجرم غير تقليدي

يختلف مجرم المعطيات كثيرا عن المجرم في الجرائم التقليدية، ذلك أن له سمات لا يوجد لها مثيل للغيره، كما أنه طوائف وأنماط خاصة به، كما أن العوامل التي تدفعه لارتكاب الجريمة مختلفة عند هأيا، فبالنسبة لسمات هذا المجرم فهو إنسان اجتماعي، أي أنهم توافق مع مجتمعه وغالبا ما تكون له مكانة معتبرة فيه ويحظ باحترام منه، كما أن هذا المجرم يمتلك المعرفة والمهارة والوسيلة الخاصة بهذه الجريمة، وهذا الاكتساب يتم عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة والاحتكاك بالآخرين، كما أنه هذا المجرم إنسان ذكي، إذ أنه يستغل ذكاءه هفيتها تنفيذ جريمته، ولا يستعين بالقوة الجسدية في ذلك إلا بالقدر اليسير جدا، ويفسر هذا أنهذا المجرم منذ وبالمستويات العلمية العالية غالبا.

وما يميز مجرم المعطيات أيضا هي الدوافع التي تدفعها لارتكاب الجريمة، فهيمتعددة ومختلفة فقد تكون السعي لتحقيق الربح أو قد تكون الرغبة في الانتقام من رب العمل وقد تكون الرغبة في هز النظام أو التفوق على وسائله التقنية وتعقيدها. وقدير تبطل الدافع بحب التعلم والاستكشاف، كما قدير تبطل السياسة والايديولوجيا الغير ذلكمنا البواعث.

كما يتميز مجرم المعطيات أيضا بفئاته وأنماطها المختلفة وهو ينقسم إلى نوعين رئيسيين:

الأول هم الهواة المولعون بالالكترونية، والثاني هم محترفو الجرائم الالكترونية وأساس التمييز بين النوعين هو الباعث والدافع لارتكاب الجريمة، بينما هو ساذج جدا بالنوع

الأول لا يتعدى الرغبة في الاستطلاع والاستكشاف، فهو خبيث بالنوع والثاني، والذي قد يكون مالياً أو سياسياً أو غيره.¹

الفرع الثاني: صعوبة اكتشاف اثبات الجرائم الالكترونية

من المفترض أننا اكتشفنا هذا الجرائم التي من غيرنا طرق الفحص والتدقيق وعن طريق الشكاوى التي تقدمها المجني عليهم، والوضع بخصوص جرائم المعطيات بالغال تعقيد في الأمرين معاً، فجهات التحقيق متصلة لابتلاك المعرفة أو الخبرة التي تملكها حياً للتحقيق في الجرائم التقليدية، لأننا الأمر يتطلب معرفة واسعة وإحاطة كاملة بهذا التكنولوجيا الحديثة، وتحديث هذا المعارف يومياً، هذا من جهة، ومن جهة أخرى الضحية في هذا الجرائم تمتنع في الغالب عن التبليغ عنها وقد يسعى إلى التعتيم عليها المحققين وتضليلهم محتلاً لا يكشفوا هذا الجرائم.

ويفترضنا إثبات هذا الجرائم الكثير من الصعوبات، فطبيعة هذا الجرائم غير مرئية في الغالب لأنها تتعلق بمعطيات في شبكات وذبذبات الكترونية، ويسهل على الجاني محو الأدلة المتعلقة بها وتدميرها في وقت وجيز، فضلاً عن العقبات التي تشكلها طبيعة هذه الجرائم العابرة للحدود.

لهذا الانعجاباً وجدنا أننا أكثر تلك الجرائم لمكتشفها إلا بمحض الصدفة وهناك من يشير إلى أن هذا الجرائم لم يكتشف منها إلا ما نسبته % 01 فقط وما تم الإبلاغ عنها إلى السلطات المختصة لم يتعد

¹ د. عبد الله حسين محمود: سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، ط 2، القاهرة 2002، ص

وانظر كذلك: محمد سامي الشوا: ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998،

وانظر: د. عمر محمد أبو بكر بن يونس: الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، 2004، ص 192
informatique sur l'internet. Journal of law é la criminalité :Dr. Mohammed boBuzubar
academic publication council KuwaitUniversity. No1 vol. 26 – march 2002 pp.41.4

15% من النسبة السابقة، وحتما طرحا ما القضاء منهذه

الجرائم فنادلة الإدانة فيها لمتكنا كافية إلا في حدود الخمس¹.

الفرع الثالث: الجرائم الإلكترونية للضحية دور مهم فيها

كالمجرم في جرائم المعطيات، فاللضحية أيضا ما يميزها في هذا الجرائم، ذلك أنها تلعب

دورا لا يستهان به في أغلبها، هذا الدور قد لا تلعبها الضحية بإرادتها، كما هو الحال عندما

تكون شخصيتها غير متجلية أمام الجاني، وذلك عندما لا يرب هذا الأخير أمامها إلا الحاسبات وما تحويه

أنظمتها من معطيات دون أن يدرك قيمتها وما قد تمثله في الواقع، وكذلك الأمر عندما

تلعب العلاقة بين الضحية والجاني دورها في حدوث الجريمة وذلك إذا كان الجاني يعمل

لحساب الضحية، لاسيما إذا كان عارفا بخبايا أنظمة الحاسبات والثغرات الأمنية فيها، أو

كان مؤتمنا علي ذلك، كأن يكون هو المسؤول عن المركز الإلكتروني فيستغل مركز الثقة

الذي يجوزه والألفة التي بينه وبين هذه الأنظمة²، وذلك كما حدث في

إحدا القضايا أن كان الجاني يعلم مستشار الدأ أحد البنوك الكبرى وكان يتم تعبئة مطلقا

من جانب هذا البنك كمنتهما للدخول في مفتاحي الكتر ونيين من أصل ثلاثة أساسية للتحكم

في التحويلات الإلكترونية للنقود من بنك لآخر، وتمكن بفضل قدراته في هذا المجال من

المفتاح الثالث، لينقل في الحال مبلغ عشرة (10) ملايين دولار للحساب

بنك فينتحبا سمه فيسويسرا وقد الق القبض عليه وهو صدر ضد حكم بالسجن لمدة ستة (6) سنوات .

وتقدم إحدا لإحصاءات الأرقام التالية % 25 : من أفعال الغش الإلكتروني يتركبها و % 18

يرتكبها المبرمجون، و % 17 يتركبها مستخدمون Informaticiens المحللون لهم أفكار

¹ د. سعيد عبد اللطيف حسن: اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت.. ط 1، دار النهضة العربية، القاهرة، 1999، ص 9.

وانظر: د: هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة. بأسويط، 1994، ص 35

²Philippe Rose. La criminalité informatique à l'horizon Analyse prospective. Le harmattan .491992 p

معلوماتية تتجاوز الدخول في النهاية الطرفية و % 16 يرتكبها الصرافون Opérateurs 12%
يرتكبها أشخاصاً جانباً المنشأة، و % 11 يرتكبها المشغلون عام CESE 1988
وفيدراسة أجراها مركز الدراسات الاجتماعية والاقتصادية بفرنسا تبيناً نحوالي % 65
من الجرائم محل الدراسة ارتكبها عاملون في المؤسسة المجنبي عليها .

الفرع الرابع : الجرائم الالكترونية ناعمة مغرية للمجرمين

إذا كانت بعض الجرائم التقليدية تحتها جنم تركبها القوة عضلية لتنفيذها فان جرائم
المعطيات لا تحتها جاليمثلتلك القوة العضلية وإنما تحتها جالقوة علمية وقد من الذكاء
ومهارة فيتوظيف ذلك، والجاني فيسبب تنفيذها لا يحتاج من الوقت لا ثواناً ودقائق
معدودات، ولا يحتاج من القوة العضلية غير تحريك الأنا لمنع ليو سائلاً لإدخال الوقود
يتسبب ذلك في حصول خسائر فادحة رغم أن جريمته قد لا تربى العين .

ونعومة هذه الجريمة وما تدرهمناً رباحاً حو مناشبا على الفضول عند البعض جعلها من الجرائم
المغرية والجاذبة للمجرمين .¹

الفرع الخامس : الجرائم الالكترونية جرائم معابرة للحدود

ليس هنا كفي العالم اليوم محدودات تقهائلاً أما منقلاً المعطيات تبين الحاسبات الآلية الموزعة
في مختلف دول العالم عبر شبكات المعلومات تقيم كنفية بضد قائق نقل كمها لمن
المعطيات تبين حاسوباً خرب بعد عنها آلاف الكيلومترات، كما يمكن أن تقع الجريمة من جان
فيدولة معينة علم جنبي عليه في دولة أخرى في وقت يسير جداً متكبدة أفدحاً الخسائر

¹ اسامة احمد المناعسة: جلال محمد الزعبي، صايل فاضل الهواوشة : جرائم الحاسب الآلي والإنترنت، دراسة تحليلية
مقارنة، دار وائل للنشر، عمان، الأردن، الطبعة الأولى، 2001 ص 107.

لا سيما مع تعاظم الدور الذي تقدمه شبكة الإنترنت، خاصة في مجال التجارة الإلكترونية وازدياد اعتماد البنوك عليها .

وتثير الطبيعة الدولية لهذه الجرائم العديد من المشاكل، كمشكلة السيادة والاختصاص القضائي وقبول الأدلة المتحصلة عليها في دولة ما أمام قضاء دولة أخرى¹ ، وتذكر في هذا وفيها قام مبرمجان إنجليز ببيع عملاد بنكب الكويت RN Thompson المجال القضائية بالتلاعب في معطيات برنامج الحاسب الآلي الخاص بالبنك، وذلك عن طريق الخس من أرصدة العملاء ثم لإيداع في حسابها الخاص، وبعد عودتها ل إنجلترا طلبنا البنك تحويل الحساب الخاص بالعدة حسابات بنكية في إنجلترا فقام البنك بذلك وكما لفا علبت همة الحصول على أموال الغير بطريقا لاحتيا ل و حكم عليه بعقوبة السجن، طعن في الحكم استنادا إلبعد ما خصصا لقضاء الإنجليز ل انفعليا لسحبوا لإيداع قدا في الكويت لافيا إنجلترا الكنم حكمة الاستئناف فضت عن هور دتبا أن النشاطا لإجراميل المتهم لم يكتملا لإبعد الطلب الذي تقدم بها المدير البنكب التحويل لوما أسفر عنهم حصوله على الأموال المحال لنشاطا لإجراميل بواسطة البنوكا لإنجليزية.

تما في الكويت لافيا إنجلترا الكنم حكمة الاستئناف فضت عن هور دتبا أن النشاط الإجراميل المتهم لم يكتملا لإبعد الطلب الذي تقدم بها المدير البنكب التحويل لوما أسفر عنهم حصوله على الأموال المحال لنشاطا لإجراميل بواسطة البنوكا لإنجليزية . ولهذا فمكافحة هذه الجرائم تتطلب تعاونا كثيفا بينا الدول وتوافقا كبيرا بين تشريعاتها .

¹ د. نائلة عادل محمد فريد قورة : جرائم الحاسب الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، 2003 ، ص 49.

المبحث الثاني: الأسس التي تقوم عليها الجريمة الالكترونية

المطلب الأول: أطراف الجريمة الالكترونية .

الفرع الأول: المجرم الالكتروني.

إن الشخص الذي يرتكب الفعل الإجرامي الالكتروني، ليس كالمجرم العادي الذي يرتكب جريمة القتل أو السرقة العادية، فهو مختلف تمام إذ يتميز بصفات خاصة (أولاً)، وأسباب مختلفة تدفعه إلى ارتكاب هذا النوع من الجرائم (ثانياً).

أولاً: صفات المجرم الالكتروني.

إذا كان المجرم الالكتروني يرتكب جرائمه وهو يمارس وظيفته في مجال الحاسوب، فلا بد وأن يكون إنساناً اجتماعياً ويقوم بواجباته ويمارس حقوقه الاجتماعية والسياسية دون وجود أي عائق في حياته العملية، وأيضاً لا بد أن يكون الشخص الذي ترتكب جريمته الالكتروني إنساناً محترفاً يتمتع بقدر كبير من الذكاء.

أ . المجرم الالكتروني هو إنسان ذكي:

يختلف الإجرام الالكتروني عن الإجرام العادي الذي يميل عادة إلى العنف مع ذلك إذا كانت الجرائم المقصود وقوعها في بيئة النظام الالكتروني تتفق أحياناً مع الإجرام التقليدي من حيث تتطلب العنف في سبيل ارتكابها، إلا أن الإجرام الالكتروني ينشأ من تقنيات التدبير الناعمة، وبمعنى آخر يكفي أن يقوم المجرم الالكتروني بالتلاعب في بيانات وبرامج الحاسوب لكي يحو هذه البيانات أن يعطل استخدام البرامج، وليس عليه سوى أن يلجأ إلى زرع الفيروسات في هذه البرامج أو باستخدام القنابل المنطقية أو الزمنية أو برامج

الدودة لكي يشل حركة النظام الالكتروني، ويجعله غير قادر على القيام بوظائفه الطبيعية.¹ قد يصل الأمر إلى حد احتراف الإجرام مما يشكل خطرا كبيرا على المجتمع سواء كان فردا أو جماعة منظمة أو غير ذلك.

ب . الشباب الحديثي العهد بالتكنولوجيا الالكترونية.

وهم الشباب الذين انبهروا بالثروة الالكترونية وانتشار الحواسيب، ولذلك كان أولئك الشباب يرتكبون الجرائم الالكترونية عن طريق استخدام الحواسيب الخاصة بهم أو بمدارهم. وهذه الطبقة من الشباب لديها قدر لا بأس به من الخبرة الالكترونية، ومن ثمة فهم يمارسون مواهبهم في استخدام الحاسوب بعرض اللهو أو هواية اللعب من أجل الوصول إلى نظم الالكترونية سواء الخاصة بالوزارات الخاصة أو الشركات العملاقة أو الشركات التجارية أو المؤسسات المصرفية والبرامج العسكرية...². وقد يتطور الأمر بالنسبة لهذه الفئة من الشباب خاصة إذا كان بينهم من لديه علم ومعرفة بعملية البرمجة.

ومع ذلك فهؤلاء الشباب تكون غايتها مجرد التسلية والملاحظة وليس لديهم النية في ارتكاب أفعال الجريمة الالكترونية، ومع ذلك خطر انزلاق هذه الفئة إلى احتراف الأفعال الغير مشروعة وارتكاب الجرائم الالكترونية هو احتمال قائم، وعندئذ يتحول من مجرد هاوي إلى محترف.

ج . الأشخاص المحترفون ارتكاب الجريمة الالكترونية.

هؤلاء الأشخاص الذين يحترفون ارتكاب الجريمة الالكترونية تتراوح أعمارهم ما بين 25 إلى 45 سنة. ومرحلة السنة الأولى تمثل الشباب الحديثي العهد بالالكترونية والحسابات أو الحواسيب الآلية، ولم يكن لديهم ميل لارتكاب الأفعال الغير المشروعة أي أنه مجرد

¹ - سنتطرق في المبحث الثاني لهذه الفيروسات بتفصيل.

² - محمد علي العريان: المرجع السابق، ص: 64.

هاوي، أما المرحلة الثانية فهي تمثل نضوج هؤلاء الشباب ويتزامن هذا النضوج مع تزايد انتشار الوسائل الالكترونية، وتكون ثورة قد وصلت مرحلة لا بأس بها من التقدم التكنولوجي. من ثم يتحول من مجرد هاوي إلى مجرم محترف في استخدام المعلومات واحتراف ارتكاب الأفعال غير المشروعة.

وغالبا ما يتم ارتكاب الجرائم الالكترونية في هذه المرحلة من هؤلاء الأشخاص وهم يعملون في نوادي ما أو في منشأة أو في إطار نظم معلوماتية أي أنهم مسؤولون عن الأنظمة الالكترونية، إذ يعرفون التقنيات اللازمة للتلاعب بالحواسب، ومن تم يقومون بتنفيذ أفعالهم غير المشروعة.

ثانيا: أسباب انتشار الإجرام الالكتروني.

إن أهم ما يتميز به الإجرام الملعوماتي عن الإجرام التقليدي هو وجود تقنية الالكترونية وثورة المعلومات التي تلقي بظلالها على نموذج الجريمة الالكترونية حتى أن أسباب انتشار الإجرام الالكتروني يتأثر بلاشك بهذه الثورة، وإذا كانت الأنماط المختلفة للمجرم الالكتروني تكشف عن انتشار هؤلاء المجرمين عند ارتكابهم الجريمة الالكترونية في غرض واحد هو مجرد الهواية واللهو نتيجة انبهارهم بثورة المعلومات، ثم من ناحية أخرى قد يكون الهدف هو تحقيق الثراء السريع أو إحدى الأسباب الشخصية.

أ: الانبهار بالتقنية الالكترونية.

مع ظهور التقنية الالكترونية وانتشارها في المجتمعات الحديثة سواء تعلق الأمر بالمعلومات أو الحواسب، فإن الأمر في النهاية يؤدي إلى انبهار المجرمين بهذه التقنية الحديثة، لذلك فإن هؤلاء ليسوا على جانب كبير من الخطورة، وإنما هم غالبا يفضلون تحقيق انتصارات تقنية ودون أن يتوفر لديهم أية نوايا سيئة، ونعطي مثلا على ذلك ما نشر في

مجلة Express الفرنسية في شتبر 1983 قصة بعنوان "ميلاد نزع¹" وتدور أحداث هذه القصة في أن عامل طلاء مباني قد توجه إلى أحد البنوك لإيداع شيك خاص به وتعاصر ذلك لحظة فصل الموزع الآلي للنقود حيث شاهد مستخدم صيانة الأجهزة الآلية، وهو يقوم باستخراج النقود من الآلة، عند الطلب عن طريق استخدام بطاقة خاصة، وقد أحدث هذا الإبتكار للآلة تصدعا في الحياة العادية لعامل الطلاء وقد حرص هذا الأخير على التدريب على تقنية الحاسوب لمدة عامين، ثم قام بالسطو على صانع الموزعات الآلية، وقد تمكن هذا العامل بفضل الآلة المسروقة من التوصل إلى أسلوب مطالعة السحب وألقي القبض عليه قبل أن يستفيد من نزعته المستحدثة.²

ب . الرغبة في تحقيق الثراء السريع.

قد تدفع الحاجة البعض إلى تحقيق الثراء السريع عن طريق إتاحة الإطلاع على معلومات معينة أساسية وذات أهمية خاصة لمن يطلبها، ولذلك تتعدد الأساليب اللازمة للوصول إلى هذا الهدف المنشود، ولذلك فإن هذا السبب يعد من أكثر الأسباب التي تدفع إلى انتشار الإجرام الإلكتروني، تبرز الحاجة إلى تحقيق الكسب السريع نتيجة وقوع البعض تحت ضغوط معينة (مشاكل مالية، الديون، إدمان المخدرات...) مثال ذلك استيلاء مبرمج يعمل لدى إحدى الشركات الألمانية³ على اثنين وعشرين شريطا تحتوي على معلومات بخصوص عملاء إنتاج الشركة، وقد هدد السارق ببيعها للشركة المنافسة ما لم تدفع له فدية بمقدار 200000 دولار، وقامت الشركة بتحليل الموقف فضلت الأداء مقابل استرداد الشرائط الممغنطة حيث أن قيمتها تفوق المبلغ المطلوب.

¹- محمد سامي الشوا: المرجع السابق، ص: 48.

²- المرجع نفسه، ص: 48.

³- محمد علي العريان: المرجع السابق، ص: 66.

ج . الأسباب الشخصية.

يتأثر الإنسان في بعض الأحيان ببعض المؤثرات الخارجية التي تحيط به، ونتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، مع توفر هذه المؤثرات، فإن الأمر يؤول في النهاية إلى ارتكابه للجريمة الالكترونية، هذا وتتعدد المؤثرات التي تدفع الإنسان إلى اقتراف مثل هذا السلوك سواء كان ذلك بدافع اللهو أو الحقد أو الإنتقام.

ومع انتشار الالكترونية، ووسائلها المختلفة، تبدأ الرغبة لدى الشباب نحو العبث بالأنظمة الالكترونية من أجل ممارسة هواية اللعب، أو تعود إلى وجود ميل زائد لدى البعض بأن الإعتقاد بأن كل شيء يرجع إليهم، إذن تلك تمثل آفة نفسية تصيبهم ويتفخرون بما قاموا به من جرائم، ليظهروا تفوقهم على الأنظمة الالكترونية، وقد يكون الدافع نحو ارتكاب الجريمة الالكترونية هو عامل الإنتقام، وذلك عندما يتم فصل العامل من عمله فإن ذلك من شأنه أن يهيء له المناخ لجريمته، كأن يدمر البرامج الالكترونية بالفيروسات عن طريق زرعها أو القنابل المنطقية التي تنشأ عنها أضراراً.

الفرع الثاني: ضحايا الإجرام الالكتروني.

يمكن القول أن ذبوع المعارف التكنولوجية نتيجة لثورة المعلومات ترتب عنه انتشار كبير للوسائل الالكترونية في جميع الأنشطة سواء منها الإقتصادية، الاجتماعية، العسكرية أو المؤسسات المالية والتجارية في الدولة.

ولما كانت الجرائم الالكترونية تنصب أساساً على المعلومات سواء عن طريق بيعها أو مقايضتها أو إتلافها، وتتمثل المعلومات العسكرية محل الإعتداء على أسرار الدولة والمشروعات العامة، وكل ما يمس الأمن القومي لهذه الدول، وتتمثل المعلومات المالية فيما يتعلق بالمراكز الإدارية والمالية والإستثمارات في المنشآت العامة، ويتبين رد فعل ضحايا

الإجرام الملغوي ما بين السكوت وعدم الكشف على أنهم وقعوا ضحية للأفعال غير المشروعة وذلك حفاظا على سمعتهم.

فالجرائم الالكترونية لا عنف فيها، ولا آثار اقتحام لسرقة الأموال، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب وليس لها أي أثر خارجي مرئي، بمعنى آخر فإن جرائم الالكترونية هي جرائم فنية تتطلب من المجرم مهارات لا تتوفر في الشخص العادي تتطلب تقنية معينة في مجال الحاسوب، إذن هي جريمة هادئة لا تتطلب العنف، ورغم ذلك فإن البعض يشبه هذه الجرائم بجرائم العنف، مثل ما ذهب إليه مكتب التحقيقات الفيدرالي بالولايات المتحدة FBI نظرا للتماثل دوافع المعتدين على نظم الحاسوب مع مرتكبي العنف.¹

فإذا تم اكتشاف الجريمة الالكترونية، فغالبا لا يكون إلا بمحض الصدفة نظرا لعدم وجود أثر كتابي لما يجري خلال تنفيذها من عمليات حيث يتم بالنبضات الإلكترونية نقل المعلومات، ولذلك يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية، إلى جانب إمكانية ارتكابها عبر الوطنية والدول والقارات وذلك باستخدام شبكات الإتصال ودون تحمل عناء الإنتقال وإلى جانب ذلك الرغبة في استقرار حركة المعاملات ومحاولة أسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب الآخرين.

فكل -هذه الأسباب- تدفع المجني عليه في الجرائم الالكترونية إلى الإحجام عن مساعدة السلطات المختصة في إثبات الجريمة والكشف عنها.

وحتى في حالة الإبلاغ، فإن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضرة وضياع ثقة المساهمين، حيث يكون المجني عليه عادة بنكا أو

¹ - Computer Hackers : Tomorrows Tarrarts Dynamics, News for and about members of the American society for in dustrialseturdy jam varylfebruary. 1990. p: 7.

أشار إليه محمد علي العريان في نفس المرجع، ص: 53.

مؤسسة مالية أو مشروع صناعي ضخم يهيمه المحافظة على ثقة عملائه وعدم اهتزاز سمعته أكثر من اهتمامه بالكشف عن الجريمة ومرتكبها، ولذلك يفضل المجني عليه تقديم ترضية سريعة لعملية وينهي الأمر داخليا حتى لا يفقده.¹

المطلب الثاني: أركان الجريمة الإلكترونية.

للجريمة الإلكترونية ثلاثة أركان تتمثل في الركن الشرعي والركن المادي وكذا الركن المعنوي، هذا ما سنعرضه في العناصر الآتية:

الفرع الأول: الركن الشرعي:

إن الجريمة هي نتيجة أفعال مادية صادرة عن إنسان هذه الأفعال تختلف حسب نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتجريم هذه الأفعال الضارة بموجب نص قانوني يحدد فيه الفعل الضار أو للمجرم والعقوبة المقررة لارتكابه.²

فالنص القانوني إذا هو مصدر التجريم وهو المعيار الفاصل بين ما هو مباح وما هو منهي عنه تحت طائلة الجزاء، وتبعاً لذلك فلا جريمة ولا عقوبة بدون نص شرعي، وهذا ما يعرف بمبدأ الشرعية³.

وقد خص المشرع الجزائري قسماً خاصاً للجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ضمن قانون العقوبات وهو القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات

¹ - أشار إليه جميل عبد الباقي الصغير: "القانون الجنائي والتكنولوجيا". الكتاب الأول: الجرائم الناشئة عن استخدام الحاسب الآلي. دار النهضة العربية سنة 1992. القاهرة، ص: 1 وما بعدها.

محمد علي العريان: المرجع السابق. ص: 54.

² تسرين محفوف، تاريخ النشر 19/01/2022 ، <https://www.ennaharoline.com> تاريخ الدخول 20-02-2023

ا بتوقيت 19:38

³ أحسن بوسقيعة، الوجيز في القانون الجزائري العام، دار هومه الجزائر ، ط10، 2011، ص 27.

والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، ويشتمل على ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر 07 تضمنت كل أنواع الاعتداءات.

على الأنظمة الإلكترونية، ولم يكتف المشرع الجزائري لذلك فرض حماية جنائية على الحياة الخاصة للأفراد من خلال القانون رقم 06-23¹ والذي مس المادة 303 وإقراره بالمادة 303 مكرر 3 وهذا تصدياً للاستخدام السيئ لوسائل التكنولوجيا الحديثة.²

الفرع الثاني : الركن المادي

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية علماً أنه يمكن تحقق الركن المادي دون تحقق النتيجة كالتبليغ عن الجريمة قبل تحقق نتائجها، مثلاً: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لامناص من معاقبة الفاعل³.

وباستقراء النصوص القانونية المنظمة لهذه الجريمة في قانون العقوبات الجزائري وبعض القوانين المقارنة نلاحظ أن المشرع الجزائري لم يشترط ضرورة أن تترتب نتيجة معينة بل اكتفى بتوفر السلوك المادي لقيام الجريمة الإلكترونية بغض النظر عن الضرر الذي تسبب فيه هذا السلوك للضحية، والدليل على ذلك أن القانون يعاقب على مجرد الدخول للمنظمة الإلكترونية دون أن يشترط حصول ضرر عن هذا الدخول، بل جعل تحقق النتيجة في الدخول والبقاء عن طريق الغش في المنظومة الإلكترونية كطرف مشدد وليس شرطاً للعقوبة⁴.

¹ أحسن بوسقيعة الوجيز في القانون الجزائري العام، دار هومه الجزائر ، 18، 2019، ص 65.

² غربي جميلة، المرجع السابق، ص 14.

³ القانون رقم 06-23 المؤرخ في 24 ديسمبر 2006 ، يعدل ويتمم الأمر رقم 66-156 الصادر في 08 جوان 1966، المتضمن قانون العقوبات ، ج. ر . العدد 84.

⁴ إيمان بغدادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مجلة أفاق للبحوث والدراسات المركز الجامعي، النيزي، الجزائر ، العدد 04، جوان 2019

والسلوك الإجرامي قد يكون:

إيجابيا بمباشرة الفعل من الجاني، وهو أغلب صور الجرائم الالكترونية كان الاتصال ويحصل على بيانات سرية ويقوم بنشرها. يقوم باختراق شبكة الاتصال ويحصل على بيانات سرية ويقوم بنشرها.

وقد يكون السلوك الإجرامي سلبيا، وهو الامتناع عن فعل كان من الواجب إتيانه:

مثل : امتناع موظف أمن عن حماية بيانات ومعلومات الشركة التي يعمل بها، وهونادر الحدوث، وفي الغالب يرتكب من قبل موظفين مختصين¹.

ويتخذ الركن المادي عدة صور حسب كل جريمة، ففي جريمة حيازة البيانات أو المعطيات يتحقق الركن المادي بمجرد قيام الجاني بحفظ البيانات وجعلها بحوزته، وفي حال إفشائها يتحقق الركن المادي لجريمة الإفشاء .²

وفي جريمة الغش الالكتروني الركن المادي فيها هو تغيير الحقيقة في التسجيلات الالكترونية والمحركات الالكترونية .³

الفرع الثالث: الركن المعنوي.

الركن المعنوي هو النصف الآخر للجريمة، ويمكن التعبير عنه بأنه الحالة النفسية للجاني وقت ارتكا بجريمة، حيث لا تقوم الجريمة قانونا بدونه، فلا بد من توفر الإرادة الأئمة لدى الجاني عند إقدامه على السلوك الإجرامي كما يجب أن تكون الأفعال إرادية وإلا انتفى الركن

¹بوضياف استمهان الجريمة الالكترونية والإجراءات التشريعية لمواجهتها ، مجلة الأستاذ الباحث للدراسات القانونية والسياسية جامعة محمد بوضياف المسيلة، العدد 11 سبتمبر 2018، ص 354

²د. حمود بن محسن الدعجاني، الجريمة الإلكترونية (دراسة فقهية تطبيقية)، مجلة الجامعة الإسلامية، ملحق العدد 183.558 ج16، ص558

³د. عمير عبد القادر ، المرجع السابق، ص 89.

المعنوي للجريمة، وأن تكون هذه الأفعال المتجهة نحو مخالفة القواعد القانونية، ليترتب على مخالفتها الجزاء الجنائي المناسب.¹

يتكون القصد الجنائي من عنصرين هما العلم والإرادة والذي يعد شرطاً ضرورياً لقيام المسؤولية الجزائية.²

العلم: هو إدراك الفاعل للأمر.

الإرادة: هي اتجاه السلوك الإجرامي لتحقيق النتيجة

ويتخذ القصد الجنائي صوراً متعددة فقد يكون القصد عاماً أو خاصاً ومباشراً أو غير مباشراً، فالقصد العام متوفر في جميع الجرائم العمدية وهو انصراف إرادة الجاني لتحقيق الفعل المجرم مع العلم بعناصر هذا الفعل المنهي عنه قانوناً كالاغتداء على الحق في الحياة في جريمة القتل العمدي مثلاً.³

أما القصد الخاص فهو الغاية التي يسعى إليه الجاني لتحقيقها من خلال ارتكاب الجريمة وهذا النوع من القصد يتطلبه القانون في بعض أنواع الجرائم إلى جانب القصد العام.⁴ مثلاً في جريمة القتل لا يكفي الجاني بالفعل فقط بل يتأكد من إزهاق روح المجني عليه.

أما فيما يتعلق بالجريمة الالكترونية فإنها تعد من الجرائم العمدية أي يكفي لقيامها توفر القصد الجنائي العام المتمثل في علم الجنائي بعناصر الجريمة واتجاه إرادته إلى إلحاق الضرر بالنفس أو المال أو البيانات المخزنة في الحاسوب،⁵ ولكن هذا لا يمنع من القول أن

¹ زبيحة بن زيدان المرجع السابق، ص 73.

² بوضياف اسمهان المرجع السابق، ص 354.

³ بوشعرة أمينة وموساوي سهام، المرجع السابق، ص 39.

⁴ د. عمير عبد القادر، نفس المرجع، ص 91.

هناك بعض الجرائم الالكترونية تتطلب توفر القصد الجنائي الخاص مثلا جرائم تشويه السمعة عبر الإنترنت.

ويرى الباحث أن القصد العام والخاص في جرائم الالكترونية هو أساسي لتحديد المسؤولية الجزائية ، والذي يحدد وجود قصد خاص في بعض الجرائم الالكترونية هو طبيعة الجريمة ونية الإضرار أو النية الخاصة للجاني والتي يمكن استشفاتها من مكونات كل جريمة على جدا وبشكل مستقل، وبالتالي فإن الجرائم الالكترونية وكجرائم مستحدثة هي كغيرها من الجرائم التقليدية يشترط وجود الركن المعنوي القيام الجريمة¹.

¹ د . بوضياف اسمهان المرجع السابق، ص 355.

المبحث الثالث: أنواع الجرائم الالكترونية

المطلب الاول: الجريمة الواقعة على الأشخاص

الفرع الأول: جرائم السب والقذف في صورتها الالكترونية

تعد جرائم السب والقذف من أكثر الجرائم انتشارا ، وهي جرائم المساس بشرف الغير وسمعتهم ويكوم عن طريق القذف والسب كتابيا ، أو عن طريق المطبوعات أو رسوم ، عبر البريد الإلكتروني ، صفحات الويب بعبارات تمس الشرف¹ ، ولقد اعتبر المشرع الجزائري صراحة أن من بين مكونات الركن المادي لإرتكاب هذه الجريمة أن تكون موجهة لشخص الرئيس لإعتبار هذا الأخير من رموز السادة الوطنية ، وهذا ما نصت عليه المادة 144 مكرر² يعاقب بغرامة من 100.000 دج إلى 500.000 دج ، كل من أساء إلى رئيس الجمهورية بعبارات تتضمن إهانة أو سبا أو قذفا سواء كان عن طريق الكتابة أو الرسم أو التصريح أو بأية الية لبث الصوت أو الصورة أو بأية وسيلة إلكترونية أو معلوماتية أو إعلامية".

الفرع الثاني: جرائم الإعتداء على حرمة الحياة الخاصة.

تعتبر جرائم الإعتداء على حرمة الحياة الخاصة من الجرائم القديمة ولكنها سرعان ما تطورت نظرا للتقدم التكنولوجي الذي لعب دورا في سرعة وسهولة انتشار الأخبار والصور الذي من شأنه أن يمثل تهديدا لخصوصية الأشخاص وسهولة الإعتداء على حرمة حياتهم

¹ خالد حسن أحمد لطفي : جرائم الأنترنت " بين القرصنة الإلكترونية وجرائم الإبتزاز الإلكتروني ، دار الفكر الجامعي ، ط1 ، مصر ، 2018 ، ص 31.

² المادة 144 من القانون 11-14 المؤرخ في 2/08/2011 معدل ومتمم الأمر 66-156 ، المتضمن قانون العقوبات ، ج ر ، عدد 44.

ومن هنا كانت الحاجة إلى وجود حماية قانونية صارمة في الحد من هذه الجرائم¹ ، وهذا ما نصت عليها المادة 303 مكرر² " يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات وبغرامة من 50.000 دج إلى 300.000 دج، كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص . بأية تقنية كانت وذلك :

1. بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه.
2. بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص ، بغير إذن صاحبها أو رضاه.

الفرع الثالث: الجرائم الماسة بالحرية العامة

1: الجرائم الإلكترونية الماسة بالآداب العامة.

تتلخص عموماً هذه الجرائم في تلك السلوكات الماسة بالأخلاق ولو أن التعرض لجرائم الأخلاق ليس بالأمر الهين، بالنظر إلى تباينها لقيماً اجتماعية من مجتمع لآخر، بل وحتى بين طبقات المجتمع نفسه فما يعد انحلالاً خلقياً في مجتمع ما قد يكون غير ذلك في مجتمع آخر، وجرائم الأخلاق هي تلك التي تتضمن العدوان على القيم الاجتماعية والأخلاقية المتعارف عليها في النظم الاجتماعية.³

¹ جرائم الإعتداء على حرمة الحياة الخاصة للأشخاص ، مقال منشور على الموقع الإلكتروني : <https://scholarworks.uaeu.ac.ae/cgi/viewconte> اطلعنا عليه يوم 2023/08/24 .

² المادة 303 مكرر من القانون 06-23 المعدل والمتمم لقانون العقوبات.

³ نايري عائشة: الجريمة الإلكترونية في التشريع الجزائري ، مذكرة لنيل الماستر في القانون ، تخصص قانون ، جامعة أحمد دراية ، كلية الحقوق ، أدرار، 2016-2017، ص 26.

ويشترط القانون في غالبه للقول بوجود جريمة معلوماتية ماسة بالآداب العامة أن تستوفي جملة من الشروط الأساسية وهي أن تكون علنية أي أن تترتب نتائج يعترف بها القانون ويرتب عليها آثاره، إضافة إلى أن تكون معروضة على الجمهور.

وقد تعرض المشرع الجزائري لمفهوم هذه الجرائم في بعض نصوص قانون العقوبات دون أن يحدد نطاقها المتصل بتقنية المعلوماتية، إلا أنه يمكن لنا إعمال هذه النصوص على جرائم المعلوماتية بالنظر إلى عمومية وشمولية النصوص، فنجد نص المادة 333 ق.ع.ج تشير إلى عقاب كل شخص ارتكب فعلا مخلا بالحياء بصفة علنية وذلك بالحبس من شهرين (02) إلى سنتين (02) وبغرامة من 500 إلى 2000 دج، إضافة إلى النص المادة 333 مكرر التي تنص على نفس المقدار من العقاب في حق كل من صنع أو حاز أو استورد أو سعى إلى ذلك، أو وزع أو أجر أو ألصق أو أقام معارض أو عرض أو شرع في ذلك أو باع أو شرع في البيع أو وزع أو شرع في ذلك، كل مطبوع أو محرر أو رسم أو إعلان أو صور أو لوحات زيتية أو صور فوتوغرافية أو أنتج أي شيء مخل بالحياء¹.

من خلال استقراء نصوص المواد السالفة الذكر نجد أن المشرع الجزائري لم يذكر بالتخصيص الجرائم التي تقع بواسطة النظم المعلوماتية والتي تستهدف المساس بالآداب العامة وإنما يمكن تطبيق نصوص هذه المواد على الجريمة المعلوماتية باعتبارها وفي الوقت الراهن من أبرز الوسائل الإجرامية المستعملة من قبل مجرمي المعلوماتية الذين وجدوا في هذه التقنية وسيلة ذات كفاءة عالية لأجل نشر إعلاناتهم الإلكترونية التي تمس بالآداب العامة، فيمكن تصنيع وتركيب الأفلام والصور بواسطة الحاسوب، وكذلك تخزينها وتعديلها ونشرها إما على شبكة المعلومات أو على وسائط تخزين خارجية كالأقراص المضغوطة، وبالتالي إتاحتها

¹ إبراهيمي سهام: الأساس القانوني للتنظيم الإداري في ظل التشريع الجزائري، الشخصية المعنوية أو الاعتبارية، مجلة القانون والعلوم السياسية، المركز الجامعي صالحى أحمد بالنعامة، جامعة الجزائر 1، كلية الحقوق، العدد 07، 2018، ص 19.

للجمهور والتأثير على قيمهما الاجتماعية، خصوصاً بالنسبة للمجتمعات العربية الإسلامية وهو الأمر الذي شددت عليها الاتفاقية العربية لمحاربة جرائم التقنية المعلوماتية وفق ما جاء في نص المادة 12 بوصفها لهذه الجرائم بجرائم الإباحية والتي صاغها المشرع السعودي أحسن صياغة في نص المادة 06 الفقرة 10 من قانون مكافحة الجرائم المعلوماتية السعودي بقولها: يعاقب بالسجن لمدة لا تزيد عن 05 سنوات وبغرامة لا تزيد عن 03 ثلاث ملايين ريال ، أو بإحدى العقوبتين كل شخص يرتكب الجرائم إنتاج ما من شأنه المساس بالنظام العام أو القيم الدينية أو الآداب العامة¹.

2: الجرائم الماسة بالنظام العام.

إن التطرق لمسألة تحديد نوع هذه الجرائم، والتي تكون الجريمة المعلوماتية وسيلة أساسية في ارتكابها، أمر في غاية الصعوبة بالنظر إلى معيار الخطورة ومدى تهديدها للمصالح العامة للأفراد، غير أن أغلب التشريعات قد وضعت ترسانة قانونية عقابية في مواجهة كل ما من شأنه المساس بأمن وسلامة مواطنيها ومؤسساتها الحيوية، وقبل التطرق إلى ذلك يمكن الإشارة إلى مفهوم الجرائم المعلوماتية الماسة بالنظام العام من خلال ما أورده المادة 15 و16 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية بشأن نوع هذه الجرائم وحصرتها فيما يلي:

- نشر أفكار ومبادئ الجماعات الإرهابية والدعوة لها.
- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين المنظمات الإرهابية.
- نشر طرق صناعة المتفجرات.
- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

¹ . دردور نسيم: جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة لنيل شهادة الماجستير، تخصص القانون الجنائي، جامعة منثوري قسنطينة، 2012-2013، ص 44.

– القيام بعمليات غسل الأموال أو نشر طرق غسل الأموال¹.

– الترويج للمخدرات والمؤثرات العقلية.

أما على مستوى التشريع الوطني وبالرغم من كون الجزائر من أول الدول التي أمضت على مضمون هذه الاتفاقية بتاريخ 21 ديسمبر 2010 إلا أنها لم تبذل المجهود الكافي لأجل تجريم هذه السلوكات في قانون العقوبات، ولا زلنا نعتمد على النصوص التقليدية في شاكلة نصوص المواد من 65 إلى 96 من قانون العقوبات المتعلقة بتجريم الأفعال الموصوفة بأنها جرائم تعدي على الدفاع الوطني والاقتصاد الوطني، وجرائم التآمر ضد الدولة إضافة إلى الجرائم الإرهابية ... وغيرها من النشاطات الإجرامية، ولكن دون تحديد مظهرها الإلكتروني، ويبقى الجهد التشريعي البارز في هذا المجال هو ما تضمنته المادة 394 مكرر 3 قانون 04-05 من قانون العقوبات الجزائري²، التي تنص على مضاعفة عقوبة مرتكب الجرائم المعلوماتية المنصوص عليها في هذا القسم إذا ما استهدفت الأنظمة المعلوماتية الخاصة بهيئات الدفاع الوطني والهيئات والمؤسسات الخاضعة للنظام العام، وهو ما يعني وحسب رأينا استثناء تطبيق نص المادة 96 من نفس القانون، وحصر نطاق التجريم فيما تنص عليه المواد 394 مكرر إلى 394 مكرر 2 من نفس القانون، بالرغم من إمكانية تطبيق عقوبات أشد، كل ذلك يشكل تعارضا بين النصوص وغموضا في تطبيقها، وهو ما يستوجب علينا توجيه عناية المشرع الجزائري إلى ضرورة الإقتداء بالتوجيهات التي تقترحها الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لوضع نصوص خاصة تسد هذا الفراغ التشريعي³.

¹ محمد عبد الرحيم الناغي: الحماية الجنائية للرسوم والنماذج الصناعية (دراسة مقارنة)، د. ط. دار النهضة العربية، القاهرة، 2009، ص. 12.

² المادة 394 مكرر 3 من قانون 04-05، المرجع السابق.

³ محمد عبد الرحيم الناغي: المرجع السابق، ص 13.

الفرع الرابع: الجرائم المعلوماتية الواقعة على الأموال

يمكن تعريف المال الإلكتروني المشمول بالحماية القانونية بأنه "كل مال إلكتروني قابل للنقل والتملك" أو بأنه "المال الموجود على الحاسوب، سواء في صورة معلومات أو بيانات إلكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أو دعامات تخزين خارجية، فهو بذلك كل المدخلات الإلكترونية التي لها من القيمة المادية مما يجعلها قابلة للتملك وتكتسي الحماية القانونية".¹

أما تعريف المجلس الأوروبي لغش الحاسوب فهو: " تغيير أو محو أو كبت معطيات أو بيانات أو برامج الحاسوب، أو أي تدخل في مجال انجاز أو معالجة البيانات من شأنه التسبب في ضرر اقتصادي أو فقد حياة ملكية شخص آخر، أو بقصد الحصول على مكسب اقتصادي غير مشروع له أو لشخص آخر".²

ويعود الانتشار المتزايد لجرائم الاحتيال الإلكتروني إلى انتشار تقنية المعاملات المالية الإلكترونية خصوصا في العشر (10) سنوات الأخيرة، بفضل المزايا التي أضحت توفرها البنوك والمؤسسات المالية لزبائنهم، كمزايا التوقيع الإلكتروني، خدمة الاطلاع على الرصيد عبر الخط، تبادل ونقل الأموال عبر الشبكات والنظم المعلوماتية، كل هذه الظروف أدت وبشكل منطقي إلى استقطاب اهتمام محترفي الإجرام الإلكتروني، الذين أضحت جل اهتماماتهم منصبه حول كفاءات الحصول على الأرقام السرية لزبائن البنوك أو شفرات الدخول إلى نظم المؤسسات المالية بهدف تحويل الأموال إلى حساباتهم الشخصية.³

¹ . نايرنبيل عمر : الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية ، د.ط، دار الجامعة الجديدة، مصر، 2012 ص 32.

² . نايرنبيل عمر، المرجع نفسه، ص 33.

³ . Joël Rivière et Didier Lucas – « Criminalité et internet une arnaque à bon March » – Article publier dans la revus de la securité Globale– numero 06– année 2008– p 69–70.

أولاً: الجرائم التحويلية المشروعة للأموال أو جرائم الاحتيال الإلكتروني.

يعرف النصب أو الاحتيال على أنه من جرائم الاعتداء على ملكية مال منقول يلجأ فيها الجاني بواسطة إحدى وسائل الاحتيال المعينة قانوناً، إلى حمل المجني عليه على تسليم المال المنقول، وقد عرفها آخرون بأنها الاستيلاء على الحياة الكاملة عمداً بطريق الحيلة أو الخداع على مال مملوك للغير¹.

وقد نص المشرع الجزائري على مفهوم جريمة النصب في نص المادة 372 من قانون العقوبات الجزائري والتي تقابلها المادة 313-1 من قانون العقوبات الفرنسي بالقول: "كل من توصل إلى استلام أو تلقي أموال أو منقولات أو سندات أو تصرفات أو أوراق مالية أو وعود أو مخالصات أو إبراء من الالتزامات أو إلى الحصول على أي منها أو شرع في ذلك، وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء أو صفات كاذبة أو سلطة خيالية أو اعتماد مالي خيالي أو بإحداث أمل في الفوز بأي شيء أو في وقوع حادث أو أية واقعة أخرى وهمية أو الخشية من وقوع شيء منها يعاقب بالحبس من سنة 01 على الأقل إلى خمس 05 سنوات على الأكثر وبغرامة من 500 إلى 20.000 دج.

ثانياً: جرائم الاستخدام غير المشروع لأدوات الدفع الإلكتروني.

شاعت وانتشرت التجارة الإلكترونية التي تتيح لرجال الأعمال تجنب مشقة السفر والانتقال من بلد لآخر من أجل لقاء شركائهم وعملائهم، وأصبح بمقدورهم توفير الوقت والجهد والمال، كما أصبح في متناول المستهلك الحصول على ما يريده من دون التنقل أو استخدام الأموال النقدية للدفع، وكل ما يحتاجه هو جهاز حاسوب موصول بشبكة الأنترنت

Disponible sur site :www.cairn.info – Fond documentaire (S.N.D.L) Système national de documentation en ligne – Algérie – Date de consultation 28/03/2014

¹. نايرنبيل عمر، المرجع السابق، ص 34.

،ويمكن تشبيه التجارة الإلكترونية بسوق إلكتروني يتقابل فيه البائعون والموردون والزبائن، وتقدم فيه الخدمات في صورة إلكترونية ويتم الدفع في مقابلها بالنقود الإلكترونية¹.

وقد قدرت حجم الأموال المتداولة في إطار عمليات البيع والشراء على شبكة الانترنت يوم 08 ديسمبر 2007 وحده 320 مليون جنيه إسترليني في المملكة البريطانية مع توقع بلوغ سقف 5,13 مليار جنيه إسترليني قيمة المبادلات المالية الإلكترونية في الثلاثي الأخير لسنة 2008.²

الفرع الخامس: الجرائم الواقعة على امن الدولة.

تقوم جريمة الواقعة على الأسرار باستعمال النظام الإلكتروني لإفشاء الأسرار، سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة. ويتخذ هذا النوع من الجرائم صورتين، الأولى تتعلق بالجرائم الواقعة على أسرار الدولة، حيث أتاح الانترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على الأسرار العسكرية والاقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو جماعة 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 الامتناع عن القيام بعمل³.

¹. محمد عبد الرحيم الناغي: المرجع السابق، ص 13.

² Charlie Abrahams – « La Cybercriminalité un Business Croissant lié à l'effondrement des crédits » Article publié dans la revue de la sécurité Globale- numero 06- année 2008 – p 30 Disponible sur site : www.carin.info – Fond documentaire (S.N.D.L) Système national de documentation en ligne – Algérie- Date de consultation 28 /03/2014

³. نايرنبيل عمر، المرجع السابق، ص 36.

وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح 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 أشد¹".

المطلب الخامس: الجرائم الواقعة علي النظام الالكتروني.

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 04 - 15 الصادر في 10 نوفمبر 2004، المتضمن قانون العقوبات بتجريم كل أنواع الاعتداءات 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 الاعتداء صورتين وهما: الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش، وهذا ما سنتناوله في الفروع التالية.

الفرع الأول: الجرائم الواقعة علي المكونات المادية للنظام.

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 الالكتروني فإن العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة

¹ . الأمر رقم 04-15، المتضمن قانون العقوبات، المرجع السابق.

المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام¹.

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 يطبع² 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 عرضية³.

الفرع الثاني: الجرائم الواقعة علي المعلومات المدرجة بالنظام.

لما كانت الحاجة ملحة وضرورية لحماية المال الإلكتروني قد استقر الفكر القانوني على ضرورة وجود نصوص قانونية لهذا الغرض وقد استجابت عدة دول ومنها الجزائر. فبالنسبة للتشريع الجزائري تدارك المشرع الجزائري مؤخرا الفراغ القانوني في مجال الإجرام

¹أمال قارة: الجريمة المعلوماتية ، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر 1 ، الجزائر ، 2013 ، ص 23.

²تايرنبيل عمر: المرجع السابق، ص 38.

³. محمد عبد الرحيم الناغي، المرجع السابق، ص 16.

الإلكتروني وذلك باستحداث نصوص تجرّيمية لقمع الاعتداءات الواردة على الإلكترونيّة ضمن نصوص قانون العقوبات، قانون الملكية الفكرية والصناعية.

أولاً: أركان جريمة إتلاف المعلومات.

إن لجريمة إتلاف المعلومات عدة أركان تتمثل في:

1: الموضوع. إن الموضوع الذي ينصب عليه فعل الجاني في جريمة الإتلاف المعلومات هي المعلومات ويقصد بالمعلومات البيانات التي تتم معالجتها وترتيبها وتنظيمها وتحليلها بغرض الاستفادة منها والحصول على نتائج معينة من خلال استخدامها.

ويشترط كي تتمتع هذه المعلومات بالحماية أن تكون موجودة داخل النظام الإلكتروني أما إذا كانت هذه المعلومات خارج النظام سواء قبل دخولها أو بعد خروجها من هذا النظام ، كان يقع فعل الاعتداء، على المعلومات الموجودة على قرص أو شريط مغنط خارج الخدمة فإن الإتلاف الإلكتروني تتحقق في هذا الفرض¹.

2: الركن المادي: ويأخذ في جريمة إتلاف المعلومات إحدى الصور الثلاثة:

أ: الإدخال : ويقصد به عملية إدخال إضافة معطيات جديدة على المعلومات الموجودة داخل النظام، ويتحقق هذا الفعل في الفرض الذي يتم فيه إدخال أي فيروس معلوماتي في النظام حتى ولو لم يحدث أي ضرر فمجرد إدخال هذا الفيروس، يحقق الركن المادي لهذه الجريمة.

ب: المحو أو الإلغاء : ويقصد به إفناء أو شطب المعلومات الموجودة داخل النظام كلياً أو جزئياً، ومن الأمثلة الواقعية على هذا الفعل ما قم به احد العاملين في شركة السمسة

¹ . أنور الحربي نثروبييل، القبلة الإلكترونية الموقّعة تنفجر في الكويت ، مجلة آفاق الانترنت، السنة الثانية العدد 14 ، 1999، ص 38.

والتأمين على الحياة في فورت ورثبولاية تكساس الأمريكية 1985 بعد فصله من العمل باختراق النظام الإلكتروني للشركة لمذكورة بهدف الانتقام، حيث تمكن من محو أكثر من مائة وثمان وستين ألف من سجلات الشركة عن طريق زرع فيروس معلوماتي وقد حكم عليه بالمراقبة لمدة سبع سنوات، ودفع تعويض قدره أحد عشر ألف وثمان مائة دولار.¹

ج: تعديل المعلومات : ويقصد به تغيير المعطيات الموجودة داخل النظام ولاستبدالها بمعطيات أخرى ولا تتطلب هذه العملية تغييرا في المعلومات أو استبدالها بمعلومات أخرى، بل يتحقق الركن المادي لهذه الجريمة بمجرد إجراء تعديل داخلي ومن الأمثلة الواقعية على هذه الصورة، قيام صبي ألماني عمره 16 سنة بزرع فيروس معلوماتي في شبكة المعلومات الخاصة لمستخدمي النظام videotext مهمته النقاط وجمع بيانات ذات طبيعة شخصية بالإضافة إلى قيام هذا الفيروس بالتلاعب في هذه البيانات بالتعديل والتغيير والمحو وتغيير مفاتيح السر.²

3: الركن المعنوي : ويتخذ صورة القصد الجنائي ويقوم على عنصري العلم والإرادة فيجب تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، وأن يعلم بأن نشاطه جرمي³.

الفرع الثالث: الجرائم الواقعة علي البرامج الالكترونية.

أولا: الفيروسات:

وهو برنامج معلوماتي أعطي تسمية فيروس لتشابهه الكبير مع الفيروس البيولوجي من حيث الانتقال والتكاثر ووظائفه التدميرية لأنظمة الالكترونية والقدرة على تعديل البرامج

¹ . إبراهيمي سهام، المرجع السابق، ص 28.

² . أنور الحربي نثرنوبيل، المرجع نفسه، ص 39.

³ أنور الحربي نثرنوبيل، المرجع نفسه، ص 39.

الأخرى التي يرتبط بها، كما يستطيع الفيروسات التمييز بين البرامج السليمة ولبرامج التي سبق وأن أصبحت بالفيروس.¹

ثانيا: القنبلة الإلكترونية.

و تنقسم إلى قسمين :

1: القنبلة المنطقية: ويهدف هذا الفيروس إلى تدمير المعلومات عند حدوث ظرف معين مثل تدمير نظام تسيير الموارد البشرية لمؤسسة معينة عند شطب اسم أحد الموظفين من القائمة.

2: القنبلة الزمنية: يعمل هذا الفيروس في ساعة محددة من يوم معني ومن ابرز الأمثلة عن ذلك فيروس anglo Michael مايكل انجلوا وفيروس Macmag وفيروس شرنوبيل shernobel ويتميز هذا الأخير بأنه فيروس الأول الذي يصيب المكونات المادية بالخراب والتلف إلى جانب المكونات المعنوية (المعلومات) حيث اكتشف هذا الفيروس سنة 1998.

ثالثا: الدودة الإلكترونية: هي عبارة عن نظام معلوماتي يمتاز بقدرته على التنقل عبر شبكات نقل المعلومات بهدف إعاقة عملها، والتشويش عليها عبر شل قدرتها على التبادل الخ وأهم ما تتميز به هذه الفيروسات ، الانتشار ، عبر الشبكات عن طريق توليد نفسها ومن أشهرها الدودة التي أطلقها الطالب الأمريكي في جامعة كورنال universityCornell، روبيرت موريس سنة 1988 عبر شبكات الجامعات والشبكات العسكرية في الولايات المتحدة بتدمير الآلاف من الحواسيب وتعطيل الشبكات وكان هدفه من هذا هو إظهار ضعف مقاييس امن الشبكات قائلا " أردت أن أعرف إذا كان بإمكانني كتابة برنامج يستطيع قدر

¹ . عامر بزرا فايز ، أبو علي : فيروساتالكمبيوتر، ط 1، دار ضنين للنشر، عمان، 1994،ص 55.

الإمكان الانتشار بشكل واسع على شبكة الانترنت " وقد حكم على روبرت سنة 1995
بالمراقبة لمدة ثلاثة سنوات وبالععمل بالخدمة الاجتماعية لمدة 400 ساعة.

ولقد أصبح مجرمو الالكترونية يتفخرون باستخدامها كوسيلة لاختراق الأنظمة ومن
الأمثلة الواقعية على ذلك ما حدث في صفحة إدارة الدفاع الأمريكية DOD الخاصة بالقوات
الجوية الأمريكية التي تعرضت واجهتها المرحة بزوار الموقع إلى اعتداء أجبر المسؤولين
على إغلاق المواقع التي تملكها إدارة الدفاع الأمريكية ، ليتم تريب برنامج وقاية اشد أمنًا.¹

¹ محمد عبد الرحيم الناغي: المرجع السابق، ص 22.

الفصل الثاني:

أساليب ردع الجريمة الالكترونية

المبحث الاول: أساليب وتقنيات إرتكاب الجرائم الالكترونية

يحتاج مرتكب الجريمة سواء كانت تقليدية أو معلوماتية إلى استخدام وسائل وأساليب غير مشروعة لتحقيق أغراضه ، إلا أن الجريمة الالكترونية تتميز بكونها تنصب حول التأثير سلبا على الحاسب الالى وإتالف وتدمير أنظمتها الالكترونية.

فالمجرم الالكتروني يحتاج إلى الاستعانة بأدوات معينة يفرض وجودها هذا النوع من الجرائم ، وبسبب إعتبار الجريمة جريمة تقنية ترتكب بوسائل فنية وتقنية تتناسب وطبيعة المعلومات محل الجريمة الالكترونية ، فإنها بالضرورة تجعل مرتكبها يلجأ في تنفيذ جرائمه إلى إستعمال تقنيات مختلفة تتميز بالتغير والتطور المستمر ، ولذا فرغم محاولة حصرها فإنه بالمقابل ال يمكن التنبؤ بالوسائل الفنية والتقنية التي قد أستحدثت في مجال تكنولوجيا المعلومات.

و لعل من أهم هذه التقنيات ما يسمى بالاختراق وإستعمال البرامج الخبيثة والتي سنتناولها من خالل مايلي:

المطلب الاول: أدوات الجرائم الالكترونية

حتى يتمكن الجاني من تنفيذ جريمته الالكترونية يستلزم توفر أدوات لذلك ومن أبرزها مايلي:

- الاتصال بشبكة الانترنت بإعتبارها أداة رئيسية لتنفيذ الجريمة .
- توفير برمجيات خاصة لنسخ المعلومات المخزنة عند المستخدم على جهاز الحاسوب ووسائل التجسس ومنها ربط الكاميرات بخطوط الاتصال الهاتفي

- توفير ما يسمى بالباركود وهي عبارة عن أدوات تستخدم لمسح الترميز الرقمي وفك تشفير الرموز .
- توفير طابعات .
- أجهزة الهاتف النقال والهواتف الرقمية الثابتة .

المطلب الثاني: الاختراق

(Haking) عبارة عن تقنية يتم بها الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات، كونه يمثل القدرة على الوصول إلى هدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير قانونية.

و قد عرفه القانون العربي النموذجي الموحد في جرائم إساءة إستخدام تقنية المعلومات بأنه :

الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق إنتهاك الاجراءات الأمنية".

و عملية الاختراق الالكتروني تتم عن طريق تسريب البيانات الرئيسية والرموز الخاصة ببرامج شبكة الانترنت من أي مكان في العالم ، بحيث الأهمية للبعد الجغرافي في الحد من الاختراقات الالكترونية التي ال تزال نسبتها كبيرة ، ومنها لم تكتشف بعد بسبب تعقيد نظم تشغيل الحاسبات الالكترونية والشبكات الالكترونية

1/أنواع الاختراق :

لهذا الاسلوب التقني الاجرامي أنواع تتمثل في:

- أ- إختراق مزودات الخدمة أو الاجهزة الرئيسية للشركات أو المؤسسات أو الجهات الحكومية ، عن طريق إختراق الجدران النارية الموضوعه لحمايتها والذي غالبا ما يتم بإستخدام المحاكاة الممثلة لمصطلح يطلق على إنتحال شخصية للدخول إلى النظام.
- ب- التعرض للبيانات أثناء إنتقالها والتعرف على شفرتها من أجل كشف كل من بطاقات الائتمان والارقام السرية للبطاقات البنكية.
- ت- إختراق الاجهزة الشخصية وهي الطريقة الاكثر شيوعا ، نظرا لتوفر العديد من برامج الاختراق سهلة الاستخدام.

2/وسائل الاختراق

: يتم إختراق جهاز الضحية دون علمه عن طريق عدة أدوات ووسائل منها:

- أ- الاختراق بإستعمال نظم التشغيل المليئة بالثغرات من خلال البروتوكولات التي يستخدمها نظام التعامل مع شبكة الانترنت ، فيقوم المخترق بالبحث عن ضحية من خالل (Internet Protocol IP) به الخاص. معرفة رقم
- ب- الاختراق بإستخدام البرامج وهي الطريقة التي تتطلب وجود برنامجين ، حيث الاول يسمى برنامج الخادم Server الموجود في جهاز الضحية والثاني يسمى بالبرنامج المستفيد العميل Client الموجود بجهاز المخترق ، ومن أخطرها برنامج حسان طروادة المتميز بالقدرة على الاختراق دون إمكانية كشفه وال تتبعه وحذفه من البرنامج المصاب ، الذي بمجرد عمله لمرة واحدة يسهل له القيام بمهامه ويمكن إرساله للضحية عن طريق الرسائل الالكترونية وإستخدام برامج الدردشة
- ت- الاختراق بإستخدام أسلوب التنقيش عن مخالقات التقنية ، بالبحث في مخالقات الحواسيب من قمامات ومواد متروكة على مستوى الجهاز تسهل إختراق النظام مثل الب ارمج المدون عليها كلمة السر أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة.
- ث- الاختراق بإستعمال أسلوب المحاكاة بواسطة التخفي بإنتحال شخصية وصالحيات شخص يمكنه الدخول إلى نظم الالكترونية بإستخدامه وسائل التعريف الخاصة به .

ج- الاختراق باللجوء إلى إنتحال شخصية الموقع عن طريق قيام المخترق بوضع نفسه في موقع بيني، بين البرنامج المستعرض للحاسب الخاص بأحد مستخدمي الانترنت وبين الموقع (WEB) ، (و به يتمكن من خال جهاز حاسوبه مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه ، وبالتالي سرقتها أو تغييرها

ح- الاختراق بواسطة تشتم كلمات السر وجمعها وإلتقاطها، عن طريق إستخدام برمجيات يمكنها تشتم أو إلتقاط كلمات السر خال تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة

خ- الاختراق بواسطة المسح والنسخ الذي هو عبارة عن أسلوب يستخدم فيه برنامج الماسح ، وهو برنامج إحتتمالات يقوم على فكرة تغيير التركيب أو تبديل إحتتمالات المعلومة المتعلقة بكلمة السر أو رقم هاتف الموزع.

فقد تستخدم قائمة الاحتمالات لتغيير رقم الهاتف بمسح قائمة أرقام كبيرة للوصول إلى ما يستخدمه الموزع ، أو إجراء مسح إحتتمالات عديدة لكلمة السر للوصول للكلمة الصحيحة التي تمكن المخترق من الدخول للنظام

د- الاختراق بواسطة هجمات إستغلال المزايا الإضافية والتي هي عبارة عن أسلوب لا يمكن مخترق النظام من تدمير معطيات المستخدم والتلاعب بها فقط ، وإنما يسهل له تدمير مختلف ملفات النظام حتى الغير متصلة بالمدخل الذي دخل منه، لأنه إستثمر المزايا الإضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخله.

الاختراق عن طريق إستراق الامواج والهندسة الاجتماعية ، حيث يتم إستراق الامواج بإستخدام لواقظ تقنية لتجميع الموجات المنبعثة من النظم المختلفة ، كإلتقاط كل من موجات شاشات الكمبيوتر الضوئية أو الموجات الصوتية من أجهزة الاتصال.

أما الهندسة الاجتماعية فهي تسمية الأسلوب شخصي في الحصول على معلومة الاختراق ، وليس لها أي أبعاد تقنية حيث يلجأ المخترق فيها لإستعمال أسلوب الكذب والخداع للحصول على معلومات ذات طابع تقني ، مثل الحصول على كلمة المرور أو سر النظام عن طريق

إيهام الضحية بأنه شخص مساعد له تابع مثال لقسم الصيانة أو قسم التطوير، ويحتاج هذه المعلومات التي تمكنه من ارتكاب جريمته.

3/الحماية الفنية من الاختراق:

لكي يتم الحد من عملية الإختراق وما يترتب عليها من آثار فإنه يتوجب إتباع الطرق المتمثلة في:

أ- **إتباع إجراءات وقائية:** كإخفاء الملفات المهمة وإغالقها بكلمات سرية وعدم تركها على الجهاز، بل تحفظ في إسطوانة وتشغل عند الحاجة ، مع ملاحظة أنها إجراءات غير كافية لأنها تجرد المستخدم من منافع الحاسب الالى.

ب- **تثبيت برامج حماية على الحاسب :** بحيث تنقسم إلى نوعين الاولى برامج مضادات للفيروسات والثانية الجدران النارية ، بحيث تقوم الاولى بمراقبة أي ملف يقوم المستخدم بإستخدامه للتأكد من خلوه من الفيروسات مثل فيروس أحصنة طروادة ، أما الثانية فهي برامج صغيرة تثبت داخل النظام من أجل مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الانترنت ، بحيث تقوم بالسماح أو الاعتراض على دخول هذه البيانات أو خروجها وتنبه المستخدم بذلك ليقوم بالسماح بذلك أو عدمه.

ث- **الاستعانة بخبرات محترفي التسلل :** عملية يقوم بها المسؤولين عن أمن الحاسبات الالية وشبكات الانترنت وكذلك رجال الامن ، من أجل تطوير نظم الحماية ضد المتسللين لأجهزة الحاسوب ومعطيائهم والذين يملكون مهارات متقدمة ويطورون تقنياتهم لإختراق بشكل مستمر .

المطلب الثالث : الفيروسات البرامج الخبيثة المدمرة:

ترتكب الجريمة الالكترونية المتسببة في إتلاف البيانات والبرامج عن طريق برامج مدمرة تقوم بخداع مستخدم الحاسب ، حيث تظهر على شكل برامج مفيدة وآمنة فيؤدي تشغيلها إلى تعطيل الحاسب المصاب وتدمير برامجه.

فهي برمجيات مكررة يمكن تصنيفها إلى أربعة أنواع رئيسية هي الفيروسات والديدان وأحصنة طروادة وبرامج الانزال إضافة لبرامج القنبلية الالكترونية ، وهي أنواع يتفق الفقهاء في كل من إنجلترا والولايات المتحدة على أن المشاكل الناشئة عنها واحدة.

1- الفيروسات :

فيروسات الحواسيب موجودة منذ أواخر الثمانينات ويزداد عددها وتأثيرها باستمرار، وأصلها عبارة عن برامج أعدها شخص أو أشخاص بهدف تخريب وشتبب البيانات من ذاكرة الحاسوب ، وهي مبرمجة على أن تعمل من خلال برامج أو برنامج آخر ولها القدرة على نسخ ذاتها ، وأبرز طرق إنتشارها البريد الإلكتروني أو البرامج المحملة من الانترنت. ويمكن تعمد أشخاص معينون نشرها بإضافتها مع ملفات ترسل بالبريد الإلكتروني الذي بمجرد فتحه من المرسل إليه تفتح هذه الملفات وينتشر الفيروس ويبدأ عمله في التخريب.

أ- تعريفها وخصائصها : الفيروسات هي برامج يتم إنتاجها خصيصا لكي تلحق نفسها ببعض البرامج المشهورة عن طريق تزيف أو تعديل بسيط للتوقيع الخاص بالبرنامج الاصلي المتمثل في مجموعة الارقام الثنائية ، وتتمكن هذه البرامج من تدمير البرامج والمعلومات أو إصابة الاجهزة بالخلل بعدة طرق ، فمنها ما يبدأ بالعمل مباشرة عند الاصابة ، وبعضها عند تنفيذ بعض الاوامر، متميزة بقدرتها على التكاثر والانتقال من جهاز إلى آخر عن طريق الملفات المتبادلة بين المستخدمين.

و فيروسات الحاسب الالى عبارة عن برامج خبيثة تسلسل إلى البرمجيات بحيث تدخل إليها وتتنسخ نفسها على ب ارمج أخرى وهذا من أجل التخريب وبالتالي الحصول على منافع شخصية، وتكون هذه الفيروسات مخزنة على البرامج التطبيقية وبرامج التشغيل وتنشط في حالة نسخ البرامج من جهاز إلى آخر وعن طريق شبكة الانترنت انطالقا من رسائل البريد الالكتروني والوثائق والمعلومات التجارية والمالية المنقولة عبر شبكة الانترنت .

و عند الحديث عن الفيروس الالكتروني فإننا نقصد الفيروس المتعلق بالحاسب الالى والمتعلق بالانترنت المختلفين عن بعضهما من حيث الانتشار والدور، بحيث يتميز فيروس الإنترنت بانتشاره الكبير والمستمر رغم إغلاق الحاسب أو النظام كله ، كما أنه يقوم بدور المخرب والمختلس للمعلومات خالفا لفيروس الحاسب الالى الذي يقتصر دوره على التخريب فقط ، كما أن له قدرة أكبر من قدرة الحاسب الالى بحيث يقوم بدوره طالما كانت شبكة الانترنت تعمل ولو تم إغلاق أجهزة الحاسب ، بعكس فيروس الحاسب الذي يبقى في الجهاز المصاب به ولا ينتقل إلى الجهاز الاخر الا بالعدوى عن طريق ملف أو برنامج من الجهاز المصاب أو عن طريق القرص المرن أو الصلب أو القرص المنضغط أو جهاز USB.

و يتميز الفيروس الالكتروني بعدد من الخصائص التقنية ، والمتمثلة في كونه عبارة عن برنامج صغير يختفي بسهولة في النظام الالكتروني وبالتالي يصعب على البرامج المضادة للفيروسات العثور عليه، إضافة لقدرته الهائلة على مهاجمة المكونات المعنوية لجهاز الحاسب الالى والشبكات الالكترونية التي تربطها فيما بينها مما يزيد في قدرته على الانتشار والسرعة في تنفيذ أهدافه.

ب- أنواع الفيروسات : تتميز الفيروسات بكثرة العدد والتنوع ،لذا لقد حدد الفقه العديد من الفيروسات المختلفة اعتمادا على كل من تكوينها وأهدافها وكذا شكلها ومكانها كالتالي:

1/ أنواع فيروسات الحاسب الالى من حيث تكوينها وأهدافها:

1- فيروس عام العدوى : ينتقل إلى أي برنامج أو ملف بهدف تعطيل نظام التشغيل بكامله

2- فيروس محدود العدوى : يستهدف مهاجمة نوع معين من النظام ويتميز ببطء الانتشار وصعوبة الاكتشاف .

3- فيروس عام الهدف : يتميز بسهولة إعداده واتساع مدى تدميره وتندرج تحته أغلب الفيروسات .

4- فيروس محدد الهدف : يقوم بتغيير هدف البرامج دون تعطيلها، ويحتاج إلى مهارة عالية بالتطبيق المستهدف

2/ أنواع الفيروسات حسب شكلها ومكانها:

1- الفيروس المتعدد الاجزاء: يقوم بإصابة الملفات مع قطاع الاقالع في نفس الوقت ويكون مدمرا في الكثير من الاحيان إذا لم يتم الوقاية منه.

2- الفيروس المتطور: يتميز بكونه يغير الشفرة كلما إنتقل من جهاز لآخر، وبتطور مضادات الفيروسات يتناقص خطره .

3- الفيروس المخفي : هو فيروس يخفي نفسه بحيث يجعل الملف المصاب سليما لخداع مضادات الفيروسات ، التي أصبح من السهل عليها كشف هذا النوع من الفيروسات.

4- فيروس بدء التشغيل : هو فيروس يصيب قطاع الاقالع في الجهاز ، مما قد يمنع المستخدم من إقلاع الجهاز وكذا الوصول إلى النظام .

5- فيروس الملفات : هو فيروس عامة ما يصيب البرامج ، وينتشر بين الملفات الاخرى والبرامج الاخرى عند تشغيله.

3/ أنواع أخرى من الفيروسات حسب كثرة عددها المتسارع:

إضافة لأنواع الفيروسات السالفة الذكر فقد أكد البعض بأن الفيروسات كثيرة جدا ولا يمكن حصرها ، إذ أنها آخذة في التزايد بشكل متسارع وأهمها : الفيروسات المقيمة ، الفيروسات النائمة ، الفيروسات الاستعراجية ، فيروسات الثغرات...

ج- **كيفية الإصابة بالفيروسات والاثار المترتبة على ذلك:** عندما يقوم الفيروس بإصابة برنامج معين فإنه يقوم بربط نفسه في بداية البرنامج أو في منتصفه أو في نهايته ، بحيث يبدأ عمله بإنطالق عمل البرنامج .

و من الاثار التي يخلفها الفيروس والتي تختلف حسب نوعه ما يلي:

- البطء الشديد في الحاسب مما يجعل التعامل معه مستحيال.
- عدم القدرة على تشغيل معظم التطبيقات وظهور رسالة خطأ كلما تمت محاولة تشغيلها .

- إمتلاء القرص بما لا يتناسب مع عدد وحجم الملفات الموجودة عليه.
- مسح الملفات التنفيذية وكذا حذف جميع المعطيات الموجودة داخل القرص الصلب .
- ظهور مربعات حوار غريبة أثناء العمل على الجهاز.
- إضاءة لمبة القرص الصلب أو القرص المرن دون أن تقوم بعملية فتح أو حفظ ملف.
- إصابة أحد أجزاء المكونات الصلبة ، مثل ما يحدث مع فيروس "تشير نوبل" الذي يصيب نظم الادخال والاخراج الاساسية مما يؤدي إلى توقف الحاسب بالكامل

ذ- الحماية من الفيروسات

مادامت الفيروسات عبارة عن وسيلة تستخدم لتدمير المعلومات والبيانات والبرامج وتعطيل شبكة المعلومات ، فإنه يتوجب على صاحب الحاسب الالي ومستعمل الانترنت سواء كان شخصا طبيعيا أو معنويا ، وخاصة إذا كان معتادا على تبادل الاقراص المرنة والملفات عبر الانترنت ، أن يلتزم بإتباع خطوات الحماية المتمثلة فيما يلي :

- توفير برنامج حماية من الفيروسات في جهاز الحاسب الالى مع ضرورة تحديثه بشكل دوري.
- عدم فتح المرفقات في أي إيميل مجهول المرسل أو في إيميلات أصدقائك إذا كانت تنتهي بexe أو bat أو أي إمتداد لا تعرفه.
- عدم قبول ملف من شخص مجهول بعكس الشخص المعروف لديك، ففي حالة قبولك ملف منه فافحصه ببرنامج الحماية لأنه قد يكون هو أيضا ضحية للفيروسات.
- وجوب فحص جميع البرامج المنزلة من الانترنت أو تم تشغيلها من قرص مرن أو CD قبل التشغيل .
- لذا من الضروري مراعاة عملية الاحتفاظ دائما بنسخ بديلة للمعلومات المهمة تفعيل لفكرة ضرورة الاخذ بالاعتبار كون أن النظام الوحيد الامن تماما هو المكتوب باليد أو المحفوظ الوقاية خير من العالج.

2- برامج الدودة:

أطلقت سنة 1988 عبر شبكة الانترنت الولايات المتحدة الامريكية برنامج يعرف بالدودة، والذي يسبب لأجهزة الحاسب الالى خالل الشبكة انهيار في قيادة وتوجيه الجامعات والمعاهد العسكرية ومنشآت الابحاث الطبية .

و يقوم برنامج الدودة بالاستغلال أي فجوة في نظام التشغيل كي ينتقل من حاسوب آخر أو من شبكة لأخرى عبر الوصلات الرابطة بينها، حيث تتكاثر أثناء انتقالها بإنتاج نسخ منها وتسبب بالتخريب الفعلي للملفات والبرامج ونظام التشغيل. وقد أطلقت هذه الدودة من طرف طالب أمر يكي يسمى روبرت موريس بقسم علوم الكمبيوتر بجامعة كورنيلبواليةنيويورك ، حيث قام ببث الدودة لإثبات عدم مائتمة أساليب ووسائل الامان في شبكات الكمبيوتر ، ولكنه تسبب في تدمير الألاف من شبكات الحاسب الالى.

المنتشرة في الولايات المتحدة وإعاقة طريق ومسلك الشبكات إضافة لخسائر مالية كبيرة لمواجهة دودة الانترنت ، لذا أدين بإنتهاك قانون الاحتيال وإساءة إستخدام الكمبيوتر وحكم

عليه بالحبس لمدة ثالث سنوات وبالعامل أربعمئة ساعة في الخدمة الاجتماعية وغرامة مالية تقدر بعشرة الاف وخمسين دولار أمريكي إضافة لتكاليف المراقبة .

و من المهم الاشارة إلى أن الديدان التي تنتشر عن طريق الايميل ، فإنه يرفق بالرسالة ملفا يحتوي على دودة ، وعندما يشغله المرسل إليه تقوم الدودة بنشر نفسها إلى جميع الايميلات الموجودة في دفتر عناوين الضحية.

3- حصان طروادة :

جاءت تسميته تأثرا بتلك الاحصنة التي إستعملتها الجنود اليونانية عندما حاصرت مدينة طروادة ، حيث تخفوا داخل أحصنة خشبية عندما أدخلت إلى داخل المدينة فقفزوا منها وتمكنوا من مهاجمة وهزيمة عدوهم.

و بنفس الطريقة يعمل برنامج حصان طروادة ، بحيث يختفي هذا البرنامج داخل برنامج حاسوبي عادي ولكن عند تنفيذه يتسبب في الكثير من المشاكل الناتجة عن نشاطه التدميري والمتمثلة في تعديل البرامج وتزوير المعلومات ومحو بعضها.

و مما يميز حصان طروادة كونه يقوم بالتخفي داخل الملفات العادية ، ويحدث ثغرة أمنية في الجهاز المصاب تسهل دخول المخترقين إليه والعبث بمحتوياته ، عن طريق نقل أو محو الهام منها أو إستخدام هوية هذا الجهاز في الهجوم على أجهزة أخرى.

4- برامج الانزال:

هي برامج صممت لمراوغة مكافحة الفيروسات ، وتعتمد على التشفير غالبا لمنع إكتشافها. ووظيفة هذه البرامج عادة نقل وتركيب الفيروسات ، فهي تنتظر لحظة حدوث أمر معين على الحاسب الالي لكي تنطلق وتلوته بالفيروس المحمول في طياتها

5- القنبلة الالكترونية :

و تنقسم إلى قسمين الاولى منطقية والثانية زمنية

أ- القنبلة المنطقية : عبارة عن برامج صغيرة يتم إدخالها بطرق غير مشروعة ومخفية مع برامج أخرى ، بهدف تدمير وتغيير برامج ومعلومات النظام في لحظة محددة أو في فترة زمنية منظمة عند انجاز أمر معين.

و للقنابل المنطقية فيروس يعمل كالقنبلة إذ يظل في حالة سكون حتى يتم تفجيره في الوقت المناسب ، إذ يظل البرنامج موجودا ولا تأثير له حتى يجد بيانات مخزنة في مكان محدد لها قيمة معينة أو بعد تشغيل البرنامج لعدة مرات معينة وفي المرة التالية يبدأ الفيروس في العمل.

و مثالها زرع القنبلة المنطقية التي سوف تعمل عند إضافة سجل موظف بحيث تنفجر لتمحو سجلات الموظفين الموجودة أصل في المنشأة.

ففي ولاية لوس أنجلس بالولايات المتحدة الامريكية تمكن أحد العاملين بإدارة المياه والطاقة من وضع قنبلة منطقية في نظام الحاسب الالي الخاص بها ، مما أدى إلى تخريب هذا النظام عدة مرات .

ب- القنبلة الزمنية :

سميت كذلك لقيامها بالعمل التخريبي في وقت محدد سلفا، بحيث تختلف عن القنبلة المنطقية المرتبطة بالقيام بنشاط معين ، أم الزمنية فهي مرتبطة بلحظة زمنية محددة بالساعة واليوم والسنة .

و مثالها يمكن للمخرب كتابة برنامج وظيفته مسح الكشوفات التي تحمل أسماء الموظفين وبياناتهم الالزمة لدفع رواتبهم قبل إستالم رواتبهم بساعة ، مما يؤدي إلى تأخير عملية الدفع وإرباك أعمال الشركة والاساءة لسمعتها .

و من أمثلتها الواقعية قيام محاسب خبير في نظم المعلومات بدافع الانتقام بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة التي يعمل بها وقامت بفصله ، حيث انفجرت بعد ستة أشهر من رحيله من المنشأة ورتبت إتالف كل البيانات المتعلقة بها.

المبحثالثاني: آليات مكافحة الإجرام الإلكتروني.

المطلب الأول: الأجهزة المختصة في مكافحة الجريمة الإلكترونية

أصبحت الجريمة الإلكترونية أشد خطورة على الفرد والمجتمع وعلى الفرد بصفة خاصة.

ومن أجل الحفاظ عليها وضعت أغلب التشريعات وأجهزة مختصة في مكافحتها بما في ذلك التشريع الجزائري.

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.

يقصد بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال وجرائم المساس بأنظمة المعالجة الآلية للمعطيات أو أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية وأنشأت بموجب القانون رقم 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ومن مهام الهيئة الوطنية:

-تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق عمليات الوقاية والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية.

وهناك الحالات التي تسمح بمراقبة الاتصالات الإلكترونية لأغراض وقائية كالوقاية من جرائم الارهاب والجرائم الماسة [أمن الدولة بإذن من النائب العام لدى مجلس قضاء الجزائر لمدة 06 أشهر قابلة للتجديد والوقاية من اعتداءات على منظومة معلوماتية على نحو يهدد

مؤسسات الدولة أو الدفاع الوطني أو المصالح الاستراتيجية بإذن من السلطة القضائية المتخصصة⁽¹⁾.

الفرع الثاني: الهيئات القضائية الجزائرية المختصة.

أنشأت هذه الأقطاب بموجب القانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الاجراءات الجزائية.

وتختص الجهات القضائية المختصة بالجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات طبقا للمواد 37-329-40 قانون إ ج.

إمكانية قيام اختصاص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الاعلام والاتصال المرتكبة في الخارج حتى ولو كان مركبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 قانون رقم 90./04

2/ توسيع صلاحيات الضبطية القضائية:

عند معاينة الجرائم الماسة بأنظمة المعالجة الآلية كما يمكن تمديد الاختصاص المحلي إلى كامل الإقليم الوطني المادة 16 قانون إ ج كما يمكن تمسح المحلات السكنية وغير السكنية في كل ساعة من ساعات الليل والنهار بإذن من وكيل الجمهورية حسب المادة 47 قانون الاجراءات الجزائية.

3/ أساليب التحري الخاصة: اعتراض المراسلات الالكترونية المادة 65 مكرر 06 قانون إ ج المدرجة بموجب القانون 06-22 المؤرخ في 20/12/2006

• تفشي المنظومة الالكترونية المادة 05 من القانون رقم 04/09.

(1)- سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائرية في مجال الجريمة المعلوماتية بمحكمة سيدي محمد، ص 11-12.

• حجز المعطيات الالكترونية المادة 06 رقم 04/09.

• نسخ المعطيات على دعامة تخزين الكترونية.

• منع الاطلاع على المعطيات التي يشكل محتواها جريمة⁽¹⁾.

الفرع الثالث: المعهد الوطني للأدلة الجنائية وعلم الإجرام (بوشاوي):

يتكون المعهد الوطني للأدلة الجنائية وعلم الاجرام من احدى عشرة دائرة متخصصة في مجالات متخصصة، جميعها تضمن انجازه الخبرة، التكوين والتعليم لتقديم المساعدات التقنية والبحوث والدراسات والتحليل في علم الجريمة، دائرة الاعلام الآلي والتكنولوجي مكلفة بمعالجة تحليل وتقديم كل دليل رقمي وتمثالي للعدالة كما تقدم مساعدة تقنية للمحققين في التحقيقات المعقدة، أفراد لدائرة يسهرون على تأمين اليقظة التكنولوجية من أجل تحسين المعارف، التقنيات والطرق المستعملة في مختلف الخبرات العلمية لإنجاز المهام المنوط بها، تنقسم الدائرة إلى 3 مخابر وذلك حسب نوع المعلومات (سمعية، بصرية، اعلام آلي) كل مخبر مزود بقضية مهمتها إنشاء المعطيات من حوامل المعلومات وضمان نزاهة وشرعية الدليل وهذه المخابر هي مخبر (الإعلام الآلي، مبر الفيديو، مخبر الصوت).

أولاً:

مخبر الإعلام الآلي: من مهامه:

- تحليل ومعالجة حوامل المعطيات الرقمية (الهاتف، الشريحة، القرص الصلب، ذاكرة الفلاش).

- تحديد التزوير الرقمي للبطاقات البنكية.

ومن تجهيزاته:

(1)-مولود ديدان، قانون العقوبات، قانون رقم 09-01 المؤرخ في 25 فبراير، 2009، د. ط، ص120.

- محطة ترميم وتصليح الأجهزة والحوامل المعطلة الشبكات الاعلامية (خبرات الاعلام الآلي والتجهيزات البيانية).

- محطة ثابتة ومحمولة لإجراء خبرات الإعلام الآلي.

- جهاز اقتناء معلومات الهواتف والحواسب.

والقاعدة التي يحتوي عليها: 07/ قاعات (مكتب التوجيه، فصيلة الأنظمة المشحونة، فصيلة

تحليل المعطيات، فصيلة الهواتف، فصيلة اقتناء المعطيات، قاعة موزع وقاعات تخزين)⁽¹⁾.

مخبر الفيديو: تختص مخبر الفيديو بمقارنة الأوجه وشرعية الصورة والفيديو وإعادة بناء مسرح الجريمة بالشكل الثلاثي الأبعاد

وتحسين نوعية الصورة (فيديو، صورة) بمختلف التقنيات.

ومن تجهيزاته: جهاز فيديو بوكس وحوامل الفيديو الرقمية والممغنطة وحبكات اعلامية (كونيكتك ستوديو، ماكب ثلاثي أبعاد) وموزع لحفظ شرائح الفيديو.

أما بالنسبة للقاعات يحتوي مخبر الفيديو على 04 قاعات (قاعتان للتحليل، قاعة التخزين، وقاعة موزع).

مخبر أصوات: من مهامه التي يؤديها: تحسين نوعية إشارة الصوت بنزع التشويش وتعديل السرعة ومعرفة وتحديد المتكلم وتحديد شرعية التسجيلات الصوتية.

ومن تجهيزاته: أجهزة الازدواجية والسماع وحبكات اعلامية (معالجة وتحسين التسجيلات الصوتية، نسج الأقراص المضغوطة وأجهزة التصليح والتعبير).

(1)-جواهري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال جمع المعلومات، المعهد الوطني للأدلة الجنائية وعلم الاجرام (الجزائر) جامعة بسكرة، كلية الحقوق، ص 3.

أما بالنسبة للقاعات فإنه يحتوي مخبر الصوت على 05 قاعات (03 قاعات التحليل، قاعة تخزين، قاعة موزع)⁽¹⁾.

المديرية العامة للأمن الوطني:

تصدت المديرية العامة للأمن الوطني للجريمة الالكترونية من مختلف الجوانب منها:

الجانب القانوني: والمتمثل في النصوص القانونية: كقانون 06-22 المؤرخ في 10-12-2006 والقانون 03-05 والقانون المدني والقانون 09-04 المؤرخ في 05/08/2009 وقانون العقوبات المواد من 394 مكرر إلى 394 مكرر 07.⁽²⁾

الجانب التنظيمي: يتمثل في التكوين المتواصل والتخصيص وتدعيم مخابر الشرطة العلمية وتدعيم المصالح الولائية شرطة القضائية وهيكله مصالح الشرطة القضائية للتصدي الجريمة.⁽³⁾

الجانب التوعوي: لم تغفل المديرية العامة للأمن الوطني عن الجانب الوقائي التوعوي يظهر ذلك من خلال برمجة المديرية لخطوات اتساقية للتصدي للجريمة الالكترونية عن طريق تنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

أما في إطار سياسة الشرطة الجوية التي تنتجها قيادة المديرية العامة للأمن الوطني بفتح موقع إلكتروني خاص بالشرطة الجزائرية على الأنترنت يستطيع من خلاله أي مواطن مهما كان مستواه العلمي أو الاجتماعي طرح انشغاله والتبليغ عن أي شيء يثير الشبهة⁽¹⁾.

(1)-سالم عبد الرزاق، مرجع سابق، ص 07.

(2)-حملاوي عبد الرحمان، مداخلة بعنوان (دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة محمد خضير، بسكرة، 2016، ص 2.

(3)-سالم عبد الرزاق، مرجع سابق، ص 09.

على المستوى الدولي:

في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم.

كما أن المديرية العامة للأمن الوطني لم تغفل في استغلال عضويتها الفعالة ففي المنظمة الدولية للشرطة الجنائية ANTERPOL هاته الأخيرة تتيح مجالات للتبادل الالكتروني الدولي وتسهل الاجراءات القضائية المتعلقة بتسليم المجرمين وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا⁽²⁾.

الفرع الرابع: التحقيق أو التحري في الجرائم الالكترونية:

تعد مرحلة التحقيق الابتدائي أو ما يطلق عليها بمرحلة جمع الاستدلالات مرحلة هامة في سبيل البحث والتحري عن الجرائم، وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة الالكترونية، لأنها تعد حجر الزاوية الذي يتم على أساسه بناء الدعوى برمتها، فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبقى متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم، ففي ثير من الجرائم الالكترونية لم يترك الجاني وراؤه سوى ذلك التعبير الذي يعترى وجوه القائمين على تعقبه الممزوج بالإحباط والإعجاب معا⁽³⁾.

أولا: خصائص التحري في الجرائم الالكترونية:

(1)-حملاوي عبد الرحمان، مرجع سابق، ص 06.

(2)-عبد الرحمان خليفي، اجراءات جزائية في التشريع الجزائري المقارن، ط1، دار بلقيس للنشر والتوزيع، الجزائر، 2005، ص 120.

(3)-نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، باتنة، 2012-2013، ص 109.

التحقيق الجنائي عموماً يخضع لما يخضع له سائر أنواع لعلوم الأخرى فلا قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة.

وهذه القواعد إما قانونية وإما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئاً سوى الخضوع والامتثال، أما الثانية فتتميز بالمرونة التي يضيف عليها المحقق من خبرته وفطنته ومهارته الكثير.

وذلك أن الفكر البشري المتعلق بالمجرم الإلكتروني يجب أن يقابله فكر بشري من قبل المحقق الجنائي، وبالتالي فإن أسلوب التحقيق وفكر التحقيق الجنائي يجب أن يتغير ويتطور أيضاً، وذلك كنتيجة طبيعية لمواجهة فكر المجرم الإلكتروني⁽¹⁾.

1) منهج أو أسلوب التحقيق الابتدائي في الجريمة الإلكترونية:

عموماً هو مجموعة الإجراءات التي يقوم بها المحقق وتؤدي إلى اكتشاف الجريمة ومعرفة مرتكبها تمهيداً لتقديمهم إلى المحاكمة.

وقد تكون هذه الإجراءات عملية كالتفتيش أو فنية كمظاهرات البصمات أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في النظام الإلكتروني.

والهدف من التحقيق الابتدائي هو التأكد أولاً من وقوع جريمة يعاقب على القانون، ومن ثمة معرفة نوع هذه الجريمة، ومن هو الجاني ومن هو المجني عليه، وكذا معرفة وقوعها وما هي الوسائل التي استعملت في ارتكابها ويكون ذلك في الجريمة الإلكترونية وفقاً لمنهج تحقيقي يختلف عن غيره من الجرائم الأخرى⁽²⁾.

أ/ وضع خطة عمل التحقيق:

(1) -نعيم سعيداني، المرجع السابق، ص 109.

(2) -نعيم سعيداني، المرجع السابق، ص 110.

يبدأ المحقق عمله عند تجميع الاستدلالات المتعلقة بالجريمة الالكترونية بوضع خطة العمل اللازمة على ضوء المعلومات المتوفرة لديه، وتحديد الفريق الفني الازم للقيام بمساعدته في أعمال التحقيق وذلك على النحو التالي:

-وضع الخطة المناسبة والتي لا تبدء إلا بعد معاينة مسرح الجريمة والتعرف على أنظمة الحماية وتحديد مصدر الخطر ووضع التصورات الكفيلة للتصدي للجريمة.

- عمل دراسة وافية وجادة لكافة اجراءات التحقيق ضمن الخطة المسبقة التي تم وضعها وناقشها العاملون في فريق التحقيق.

- التخطيط الفني للتحقيق وذلك من أجل الوصول إلى أفضل الطرق والأساليب للتعامل مع هذه الجرائم بالتفصيل والوضوح.

- تنسيق جهود الفريق القائم بالتحقيق لتسهيل مهمتهم وعملهم وتقليل الآثار السلبية والإسراع في انجاز العمل وهو ما يؤدي إلى ضمان مستوى جيد من الأداء.

- تحديد الاجراءات المسبقة والتي من شأنها التقليل من الأخطاء الفردية التي قد تنتج عن قلة الخبرة أو نقص المعرفة، وبالتالي تساعد على ايجاد درجة جيدة من التقيد بالمستوى المطلوب مع ضمان أو 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 الارتكاز عليها أثناء تنفيذ الخطة وهي أن يتم تعيين الأشخاص الذين سيتم معهم وتحديد النقاط التي يجب استضاحها معهم وتقدير مدى الحاجة للاستعانة ببعض الفنيين اللازم توافرهم لاستكمال التحقيق، بالإضافة إلى مراعاة الظروف والملابسات المحيطة بالواقعة ذلك أم من هذه الظروف ما يشمل عوامل مهمة يجب مراعاتها عند وضع خطة العمل ومنها:

- مدى أهمية الأجهزة والشبكات المتضررة لعمل المنظمة.

- مدى حساسية البيانات التي يحتمل سرقتها أو اتلافها.

- مستوى الاختراق الأمني الذي تسبب فيه الجاني.

ثم بعد ذلك وضع الأسلوب الأمثل لعملية التفتيش وذلك من خلال تحديد نوع الأدلة التي يريد فريق التحقيق البحث عنها⁽¹⁾.

ب/ تشكيل فريق التحقيق:

إن التحقيق الابتدائي في الجرائم المتعلقة بالإنترنت يكون غالبا أكبر من أن يتولاه شخص واحد بمفرده، حتى ولو كانت المضبوطات هي مجرد حاسبا شخصي واحد، ولذلك فإنه يفضل أن يتعاون عدة محققين في انجاز مهمة التحقيق والعثور على الأدلة.

ويجب أن يتشكل فريق التحقيق من فنيين أو أخصائيين ذوي خبرة في مجال الحاسوب والإنترنت، ويمتازون بمهارات في التحقيق الجنائي بشكل عام والتحقيق الجنائي الإلكتروني بشكل خاص، ولهؤلاء المحققين أن يستعينوا بخبراء في مجال الحاسوب والإنترنت ليتمكنوا من فك التعقيدات التي تفرضها ظروف وملابسات كل جريمة.

وإن كان أسلوب العمل الفريق يستخدم في التحقيق في كثير من أنواع الجرائم إلى أنه يأخذ أهمية خاصة في الجرائم المتعلقة بالإنترنت لما تتطلبه من مهارات فنية وخبرات متنوعة قد لا تتوفر لدى المحققين وبذلك يكون تشكيل فريق خاص بالتحقيق في هذا النوع من الجرائم أمرا ضروريا، ومن الناحية العملية غالبا ما يتكون فريق التحقيق في الجرائم المتعلقة بالإنترنت من:

- المحق الرئيسي ويكون ممن لهم خبرة في التحقيق الجنائي.

(1)-نعيم سعيداني، المرجع السابق، ص 111.

- خبراء الحاسوب وشبكات الأنترنت الذين يعرفون ظروف الحادث وكيفية التعامل مع هذه الجرائم.

- خبراء ضبط وتحليل الأدلة الرقمية العارفين بأمور التفتيش للحاسوب.

- خبراء أنظمة الحاسوب الذين يتعاملون مع الأنظمة البرمجية.

- خبراء التصوير والبصمات والرسم التخطيطي.

وفي هذا الإطار نجد أن المشرع الجزائري قد أشار إلى مسألة إمكانية استعانة الجهات المكلفة بالتحقيق بالخبراء المتخصصين في مجال الحاسوب والنظم الالكترونية، ومن الذين لهم دراية بعمل المنظومة الالكترونية أم ممن لهم دراية بالتدابير المتخذة لحماية المعطيات الالكترونية، وذلك بغرض المساعدة جهات التحقيق في انجاز مهمتها وتزويدها بالمعلومات الضرورية لذلك⁽¹⁾.

(2) العناصر الأساسية للتحقيق الابتدائي في مجال الجريمة الالكترونية:

ونقصد بها تلك الاجراءات التي تستعمل من طرف جهات التحقيق أثناء تنفيذ طرق التحقيق الثابتة والمحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، وهناك اجراءات يتعين على الضبطية القضائية مراعاتها أثناء التحقيق الابتدائي.

أ/ الاجراءات التي يجب مراعاتها قبل البدء في التحقيق:

يمكن أن نرد الأهم فيها كما يأتي:

- تحديد نوع نظام المعالجة الآلية للمعطيات فهو كمبيوتر معزول أن متصل بشبكة الأنترنت.

- وضع مخطط تفصيلي للمنشأة التي وقعت بها الجريمة مع كشف تفصيلي عن المسؤولين بها ودور كل منهم.

(1)-نعيم سعيداني، المرجع السابق، ص 112.

- إذا وقعت الجريمة على شبكة فإنه يجب حصر طرفيات الاتصال بها أو منها الريقة التي تمت بها عملية الاختراق من عدمه، وهل هناك حواسيب آلية خارج هذه المشكلة ولها امكانية الاتصال بها أم لا؟.

- مراعاة صعوبة بقاء الدليل فترة طويلة في الجريمة الالكترونية.

- مراعاة أن الجاني قد يتدخل من خلال الشبكة لإتلاف كل المعلومات المخزنة.

- يجب فصل التيار الكهربائي على موقع المعاينة أو جمع الاستدلالات لشل فاعلية الجاني في أن يقوم بطريقة ما بمحو آثار جريمته.

- فصل خطوط الهاتف حتى لا يسيء الجاني استخدامها، والتحفظ على الهواتف المحمولة من قبل الآخرين الذين لا علاقة لهم بعملية التحقيق لأنهم قد يسيئون استخدامها لطمس البيانات.

- التأكد من أن خط الهاتف يخص الحاسوب محل الجريمة، ذلك أنه من الخدع التي يستعملها الجاني عند الاختراق أن يتم ذلك بخط هاتفي مسروق عن طريق الدخول إلى شبكة الهاتف والتلاعب فيها وتضليل أجهزة المراقبة وأجهزة التحقيق بعد ذلك.

- ابعاد الموظفين عن أجهزة الحاسب الآلي بعد الوصول منهم على كلمة السر وكذا الشفرات في حالة وجودها.

- تصوير الأجهزة المستهدفة (التي وقعت بها أو عليها الجريمة) من المام والخلف وذلك لإثبات أنها كانت تعمل وكذلك للمساعدة في اعادة تركيبه من أجل البدء في اجراءات التحقيق⁽¹⁾.

(ب) الاجراءات التي يجب مراعاتها أثناء التحقيق:

عند البدء في عملية التحقيق الابتدائي سيما عند القيام بعملية تفتيش جهاز الحاسوب

فإنه على رجال الضبطية القضائية وبرفقتهم الخبراء الذين يستعينون بهم مراعاة ما يلي:⁽¹⁾

(1)-نعيم سعيداني، المرجع السابق، ص113.

- عمل نسخة احتياطية من القرص الصلب أو الأسطوانة المرنة قبل استخدامها والتأكد فنيا من دقة النسخ عن طريق الأمر (Diskcomp).
- نزع غطاء الحاسب الآلي المستهدف والتأكد من عدم وجود أقراص صلبة إضافية.
- أن يكون الهدف من نسخ محتوى الأسطوانة والأقراص تحليل المعلومات الموجودة بها بغرض التوصل إلى معرفة الملفات الممسوحة، ويمكن استعادتها من سلة المهملات مع ملاحظة أن هناك بعض الملفات التي إن مسحت وضغط على أزرار معينة مثل Shift delete وفي وقت واحد لا يمكن استعادتها وكذا من أجل معرفة الملفات الخفية المخزنة في ذاكرة الحاسوب.
- العمل على فحص البرامج وتطبيقاتها مثل البرامج الحسابية التي تكون قد استخدمت في جريمة اختلاس معلوماتي.
- العمل على فحص العلاقة بين برامج التطبيقات والملفات خاصة تلك التي تتعلق بدخول المعلومات وخروجها.
- حفظ المعدات التي تضبط بطريقة فنية وسليمة(2).

المطلب الثاني: اثبات في المادة الالكترونية.

الفرع الأول: طرق اثبات تقليدية:

أولاً: الشهادة:

أ) تعريف الشهادة وأنواعها:

(1)-نعيم سعيداني، المرجع السابق، ص 113.

(2)-نعيم سعيداني، المرجع السابق، ص 114.

الشهادة تقرير يصدر عن شخص في شأن واقعة عاينها بحاسة من حواس بحيث قد تكون الشهادة مباشرة بواسطة احدى حواس خمس لشخص أو غير مباشرة مثل شهادة السماع أو نقل عن غير، وتكون قيمتها أقل من شهادة مباشرة⁽¹⁾.

(ب) الشهادة في مرحلة التحقيق الابتدائي والتحقيق النهائي:

بحيث يشترك كلاهما في جل النقاط إلا أن هناك فروق هامة نذكر منها:

- شهادة تؤدي سرا أمام قاض تحقيق، وبصورة علنية أمام المحاكم.
- اختيار الشهود في مرحلة التحقيق من حق قاضي التحقيق وقاضي احالة، أما في مرحلة التحقيق النهائي فإن دعوة الشهود من حق الخصوم والنيابة العامة.
- شهادة مؤداة أمام قاض التحقيق لا تعتبر من عناصر القناعة في المحاكم أما شهادة أمام المحاكم فهي من أدلة التي يستند عليها الحكم.
- يستمع قاضي التحقيق إلى الممنوعين من شهادة أمام المحاكم في حين أن شهادة هؤلاء ممنوعة أمام المحاكم⁽²⁾.

(ج) شروط الشهادة: ومن أهم الشروط واجب توفرها لقيام شهادة نذكر:

التمييز: حيث يجب أن يبلغ الشاهد سنة خمسة عشر سنة من عمره وقت إدلاء الشهادة ويمكن سماع شهادة أقل سن منهم على بيل معلومات دون أداء اليمين⁽³⁾.

تحليف اليمين: حيث أوجب القانون أطول المحاكمات الجزائية في المواد 77، 192، 286 ق. إ. ج تحليف الشاهد باليمين وإلا بطلت شهادته.

أن لا يكون الشاهد من الممنوعين: فحسب المادتين 193، 192 ق. إ. ج هم:

(1)- عبد الوهاب حومد، أصول محاكمات جزائية، طبعة 4، مطبعة جديدة دمشق، 1990، ص 576.

(2)- عبد الوهاب حومد، المرجع السابق، ص 577.

(3)- محمد نجيب حسن، شرح قانون الجنائية، طبعة ثانية، دار نهضة عربية، القاهرة 1988، ص 441.

- أصول المتهم وفروعه من أب، أم، ابن، ابنة وغيرهم.

- اخوته وأخواته.

- قرابة الصهرية.

- زوج زوجة بعد طلاق⁽¹⁾.

(د) الشاهد في الجريمة الالكترونية:

بحيث أنه من الممكن أن يكون الشاهد في الجريمة الالكترونية صاحب الخبرة والتخصص في تقنية وعلوم الحاسوب الذي يملك الخبرة للولوج إلى نظام المعالجة آلية للبيانات إذا كانت مصلحة تحقيق تقضي ذلك بحيث يرى الفقه أن شاهد الالكتروني يمكن أن يكون من احدى الطراف التالي:

- القائم على تشغيل الحاسوب.

- المبرمج.

- المحلل الذي يقوم بتحليل خطوات البرنامج وتجميعها.

- مدير النظام والذي يوكل إليه إدارة في النظام الالكتروني⁽²⁾.

(هـ) الشهادة عبر الأنترنت:

من شهادات الفورية يتم الحصول عليها في مرحلة التحقيق النهائي أمام محكمة الموضوع، حيث يكون الشاهد غير حاضر جسدياً أمام المحكمة وإنما يتم سماع شهادته عبر الأنترنت بشكل سمعي ومرئي بحيث يظهر الشاهد بهيئته كاملة في الفيديو من دون أي اشكال⁽³⁾.

ثانياً: القرائن:

(1)-محمد نجيب حسن، المرجع السابق، ص 441، 442، 443..

(2)-جميل عبد الباقي صغير، أدلة اثبات الجنائي في تكنولوجيا حديثة، دار نهضة قاهرة 2002، ص 104 وما بعدها.

(3)-جميل عبد الباقي صغير، المرجع السابق، ص 104 وما بعدها.

أولاً: تعريف القرائن:

القرينة هي استنتاج الواقعة المطلوب اثباتها من واقعة أخرى قام عليها دليل اثبات، وتعتبر قرائن من طرق اثبات الغير مباشرة، يعتبرها لا ترد على واقع مطلوب اثباتها عكس طرق اثبات أخرى كشهادة⁽¹⁾.

ثانياً: أنواع قرائن وقوتها بالإثبات:

بحيث أنه يوجد نوعين مهمين من القرائن وهما:

أ) القرائن القانونية: هي القرينة التي نص عليها القانون، وتعنى من تقررت لمصلحته عن أي طريقة أخرى من طرق اثبات، ويلزم قاضي بلا خذيتها بحيث تنقسم قرائن قانونية إلى قرائن قانونية قاطعة ومطلقة وهي قرائن لا يجوز اثبات عكسها، وقرائن قانونية بسيطة ومؤقتة وهي قرائن تجيز للمتضرر منها اثبات عكسها بإقامة دليل يعاكس مضمونها.

ب) القرائن القضائية أو الموضوعية: هي القرائن التي لم ينص عليها قانون ويمكن للقاضي أن يستخلصها من ظروف الدعوى مثل أسلحة، بصمات، شعر⁽²⁾.

ثالثاً: دور القرائن في اثبات جريمة احتيال عبر الأنترنت:

بحيث أنه يمكن للقاضي أن يختار ما يشاء من القرائن القضائية لإثبات جريمة الاحتيال عبر الأنترنت ما دامت هذه القرائن تشكل القناعة لديه على ارتكاب المدعى عليه لهذه الجريمة⁽³⁾.

ثالثاً: الاعتراف:

(1)-حسين بن سعيد الغافري، سياسة جنائية في مواجهة جرائم الأنترنت، دار نهضة عربية، القاهرة 2009، ص 243.

(2)-حسين بن سعيد الغافري، مرجع سابق، ص 235.

(3)-محمد نجي حسن، مرجع سابق، ص 451.

أ) تعريف الاعتراف:

اعتراف هو اقرار المدعى عليه على نفسه بصدور الواقعة، بحيث يكون للاعتراف دور حاسم في الدعوى الجزائية، حيث يتم استجواب المدعى عليه وفق أساليب مختلفة، ليصرح مدعى عليه بارتكابه للجريمة⁽¹⁾.

ب) أنواع الاعتراف:

حيث قد يكون اعتراف قضائياً عندما يصدر عن المدعى عليه في مجلس القضاء أثناء النظر في دعوى متعلقة بالجريمة قد يكون اعتراف غير قضائي عندما يصدر عن مدعى عليه خارج مجلس القضاء، أو في مجلس القضاء في غير الدعوى متعلقة بالجريمة⁽²⁾.

ج) شروط اعتراف: يشترط لصحة اعتراف توافر الشروط التالية:

- أن يكون اعتراف صادر عن شخص يتمتع بالوعي أو ادراك.
- أن يكون اعتراف صادر عن ادارة حرة فلا يصح اعتراف تحت صائلة اكرام مثل الضرب، التعذيب وغيرها.

كما يعتبر تحليف اليمين للمدعى عليه غير جائز كونه يعتبر من تعذيب نفسي⁽³⁾.

د) قيمة قانونية للاعتراف: اعتراف الصحيح هو مجرد دليل اثبات في دعوى ويخضع تقديره لقاضي الموضوع حسب قناعته الشخصية فله أن يأخذ به أو يهمله، واعتراف النظري

(1)-عبد الوهاب حومد، المرجع السابق، ص 580.

(2)-عبد الوهاب حومد، المرجع السابق، ص 582.

(3)-حسن بن سعيد الغافري، المرجع السابق، ص 240

للمدعى عليه أمر يرفض منطق السليم ما لم يقترن بالاعتراف العملي الذي يؤكد صحة ما جاء به على لسان المدعى عليه⁽¹⁾.

رابعاً: الدليل الكتابي: (الضبوط)

أ) تعريف الضبط أو المحضر:

الضبط هو المحرر الذي يدونه الموظف المختص لإثبات ارتكاب الجرائم أو إجراءات التي اتخذت بشأنها وفق أشكال محددة قانوناً⁽²⁾.

ب) القيمة الإثباتية للضبوط: حيث نجد ثلاث أنواع من الضبوط وهي:

1) الضبوط التي يعمل بها ما لم يثبت تزويرها: نصت عليها مادة 182 قانون أصول المحاكمات الجزائية بقولها: "لا يسوغ تحت طائلة البطلان إقامة البيانات الشخصية على ما يخالف أو يجاوز مضمون المحاضر التي يوجب القانون اعتبارها والعمل بها حتى ثبوت تزويرها"⁽³⁾.

وتعتبر من أقوى أنواع الضبوط من حيث اثبات لأن قاضي ملزم بالأخذ بها إلا إذا استطاع المدعى عليه إثبات تزويرها.

2) الضبوط التي يعمل بها حتى يثبت العكس: مادة 178 قانون أصول محاكمات جزائية بقولها: "يعمل بالضبط الذي ينظمه ضباط الضابطة عدلية ومساعد والنائب العام في الجرح والمخالفات مكلفون بتثبيتها حتى يثبت العكس ويشترط في اثبات العكس إما بينة كتابية أو

(1)-حسن بن سعيد الغافري، المرجع السابق، ص 242

(2)-جميل عبد الباقي الصغير، مرجع سابق، ص 122.

(3)-محمد نجيب حسن، مرجع سابق، ص 482.

بواسطة الشهود". وهدف ضبط تساعد عمل القضاء في اثبات الجرائم الجنحية والمخالفات ويدخل في هذا النوع الضبوط التي تنظمها شرطة السير لإثبات المخالفات المرورية⁽¹⁾.

3) الضبوط التي لا تعدوا أن تكون معلومات عادية:

مادة 180 قانون أصول المحاكمات الجزائية يقولها حد لا قيمة لضوابط أخرى إلا كمعلومات عادية والقانون لم يحدد طبيعة هذا النوع، لذلك فهذا الضبط لا يخل في النوعين أول وثاني ومن أمثلة هذا الضباط الضبوط التي ينظمها موظفو الضابطة العدلية في الجنايات، فهي مجرد اخبار عن ارتكاب جرائم⁽²⁾.

ج) الشروط الشكلية للضباط: حتى يكون للضبوط المذكورة قوة في إثبات يجب أن تتوفر فيها الشروط الشكلية منصوص عليها في مادة 179 قانون أصول المحاكمات الجزائية وهي:

- أن يكون الضبط قد نظم ضمن حدود اختصاص موظف أثناء قيامه بوظيفته.
- أن يكون الموظف قد شهد الواقعة بنفسه أو سمعها شخصيا.
- أن يكون الضبط صحيحا في الشكل بأن يتضمن الضبط اسم من نظمه وصفته⁽³⁾.

د) القيمة اثباتية لضبوط جريمة احتيال عبر الأنترنت:

بناء على ما سبق، يمكن لضبوط تنظيم إثبات الجرائم المنصوص عليها في مشروع قانون جريمة الكترونية إما أن يعمل حتى ثبوت العكس عندما تكون جريمة جنحة وصف، وهناك من يرى أن تخصص رجال الضابطة العدلية في مجال تقنية المعلومات أمر تفرضه طبيعة جرائم الانترنت فلذلك يجب أن يكون عمل رجال الضبط القضائي أقرب إلى الخبير التقني،

(1)-محمد نجيب حسن، مرجع سابق، ص 485.

(2)-حسن الحو خدار، مرجع سابق، ص 338.

(3)-حسن الحو خدار، مرجع سابق، ص 340.

بحيث يكون مستعدا دائما للتعامل مع هذه الجرائم ومدربا على فن تنظيم محاضر والضبوط متعلقة بها(1).

خامسا: الخبرة:

أ)تعريف الخبرة: الخبرة هي ابداء رأي في من شخص مختص فنيا في شأن واقعة أهمية في الدعوى الجزائية(2).

ب) القوة إثباتية لخبرة:

لا يلزم تقرير الخبرة القاضي الجزائي لأنه يحكم حسب قناعاته الشخصية فالمحكمة هي التي تقدر قيمة النتائج التي توصل إليها الخبير في تقريره فلها أن تأخذ به كله أو تجزئه، فتأخذ منه الجزء التي تقنع به(3).

ج) الخبرة التقنية في جريمة احتيال عبر الأنترنت:

حيث تعتبر الخبرة تقنية في جريمة احتيال عبر الأنترنت م أكثر الطرق إثبات أهمية إذ أنها تؤدي دورا لا يستهان به في إثبات هذه الجريمة بحيث أصبح يطلق عليه في الفقه المقارن مصطلح الالكترونية شرعية ويقصد به استخدام الطرق العلمية لجمع وتحليل الدليل الرقمي مأخوذة من مصادر رقمية واحتفاظ به وتوثيقه على نحو يسهل بناء الحوادث التي تؤدي إلى اكتشاف الجريمة(4).

(1)-حسن الحو خدار، مرجع سابق، ص 341.

(2)-محمد نجيب حسني، مرجع سابق، ص 462.

(3)-محمد نجيب حسني، مرجع سابق، ص 462.

(4)-محمد نجيب حسني، مرجع سابق، ص 464.

د) كيفية اختيار الخبير القضائي: أطلق المشرع الجزائري في استعانة بالخبرة لتكوين قناعته الشخصية فله مطلق الصلاحية في اختيار الخبير الالكتروني، فمن الممكن أن يكون شخصاً طبيعياً أو اعتبارياً⁽¹⁾.

ج) آلية عمل البير الالكتروني: يقوم الخبير بفحص أجهزة الرقمية متعلقة بالجريمة سواء أكانت حواسيب شخصية وغيرها من أجهزة خدمات الالكترونية، بحيث يجب على الخبير أن يكون على قيام بمهامه التالية:⁽²⁾

1- حجز البيانات: استناد لمبدأ لوكارد التبادلي الذي يرى أن أي شخص يدخل إلى مسرح الجريمة يجب أن يأخذ منه شيئاً أو يترك شيئاً خلفه فيجب على الخبير أن يقوم في البداية بعملية حجز البيانات متعلقة بالجريمة اضافة إلى حجز أجهزة التي تحتوي هذه بيانات لمدى مشتبه به⁽³⁾.

2- حفظ البيانات: يقوم الخبير بنسخ البيانات التي تم حجزها وتصبح لديه نسختين الأولى يتم تخزينها في أجهزة رقمية وثانية تتم اجراء عملية اختبار والفحص عليها كونها تعد نسخة طبق الأصل.

3- استعادة البيانات: حيث يجب على الخبير استعادة البيانات المحذوفة وهو أمر ضروري من أجل إعادة بناء القضية وذلك عن طريق جهاز التخزين.

4- تحليل البيانات: بحيث يقوم الخبير بتقييم محتوى البيانات الرقمية بفحصها بدقة لتحديد وسائل الجريمة ودوافعها والغرض منها.

(1)-محمد نجيب حسني، مرجع سابق، ص 591.

(2)-عبد الفتاح بيومي الحجازي، مرجع سابق، ص 407.

(3)-عبد الفتاح بيومي الحجازي، مرجع سابق، ص 409.

5- اعادة بناء قضية: فبعد تجميع وتحليل البيانات من طرف الخبير يتم حصول على نتيجة للوصول إلى ما حصل بين المجرم والضحية إثناء ارتكاب الجريمة.

6- كتابة تقرير: يتضمن التقرير النتائج التي توصل إليها الخبير من خلال عملية البحث استناد في ذلك إلى خطوات من أول مرحلة إلى آخر مرحلة قام بها الخبير، سلسلة ومترابطة.(1)

الفرع الثاني: طرق اثبات حديثة

اولا: الدليل الرقمي

1. تعريف الدليل الرقمي:

هو مجموعة معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في اجهزة النظم الالكترونية وشبكات الاتصال ويمكن استخدامها في اي مرحلة من مراحل التحقيق او المحاكمة لإثبات وملحقاتها حقيقة فعل او شيء او شخص له علاقة بجريمة، او جاني او مجني عليه(2).

2. خصائص الدليل الرقمي:

الدليل الرقمي هو دليل علمي: إن الدليل الرقمي يحتاج إلى بيئته التقنية التي يتكون فيها، لكونه من طبيعة تقنية المعلومات ذات المبنى العلمي ومن ثمة فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الرقمي، فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة ان القانون مسعاه العدالة واما العلم فمسعاه الحقيقة.

(1)-عبد الفتاح بيومي الحجازي، مرجع سابق، ص 601.

(2)-ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم أنترنت، دار فكر قانونية، مصر 2006، ص 88.

الدليل الرقمي من طبيعة تقنية: إن الطبيعة التقنية للدليل تقتضي أن يكون هناك توافق بين الدليل المرصود، وبين البيئة التي يعيش فيها فلا تنتج سكيناً يتم به اكتشاف القاتل، أو اعترافاً مكتوباً أو مالا في جريمة الروشة، وإنما ما تنتجه التقنية هو نبضات رقمية تشكل قيمتها في إمكانية تعاملها مع القطع الصلبة التي تشكل الحاسوب على أية شاكلة يكون عليها، ومثل هذا الأمر يجعلنا نقرر أنه لا وجود للدليل الرقمي خارج بيئته التقنية وأنه لكي يكون هناك دليل رقمي يجب أن يكون مستوحاً أو مستتباً من البيئة الرقمية أو التقنية.

الدليل الرقمي دليل متنوع ومتطور: يشمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقمياً، على الرغم من أن الدليل الرقمي في أساسه متحد التكوين بلغة الحوسبة والرقمية إلا أنه مع ذلك يتخذ أشكالاً مختلفة يمكن أن يظهر عليها، كأن يكون بيانات غير مقروءة وقد يكون بيانات مفهومة كما لو كان معدة بنظام المعالجة الآلية، كما من الممكن أن يكون صورة ثابتة أو رقمية أو معدة بنظام التسجيل السمعي البصري أو يكون مخزناً في البريد الإلكتروني.

وأما عن كون الدليل الرقمي دليلاً متطوراً فهي خاصية تكاد تكون تلقائية، نظراً لارتباطه بالطبيعة حركة الاتصال عبر الإنترنت والعالم الافتراضي اللذان لا يزالان في بدايتهما ولم يصلا بعد إلى منتهاهما ولن يكون من السهل احتوائهم.

الدليل الرقمي صعب التخلص منه: كما حدث اتصال بتكنولوجيا المعلومات في معنى ادخال بيانات إلى ذلك العالم فإنه من الصعب التخلص منها ولو كان ذلك باستخدام أعتى أدوات الالغاء، كونها لا تعد من العوائق التي تحول دون استرجاع الملفات المذكورة إذ تتوفر برمجيات ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم الغاؤها أو ازلتها من الحاسوب.

الدليل الرقمي ذو طبيعة رقمية ثنائية (1.0): ان الآثار التي يتركها مستخدم النظام الالكتروني والتي تشمل الرسائل المرسله منه او التي استقبلها وكافة الاتصالات التي تمت من خلال الحاسب الآلي وشبكة الاتصالات تكون على الشكل الرقمي، البيانات الموجودة داخل الحاسب الآلي سواء كانت في شكل نصوص او حروف او ارقام او صور از فيديو تتحول الى نظام ثنائي في تمثيل الأعداد يفهمه الحاسب الآلي، قوامه الرقمان (0.1).⁽¹⁾

3. أشكال الدليل الرقمي: بحيث نجد الدليل الرقمي في عدة اشكال اهمها:

الصورة الرقمية: وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة في شكل ورقي او في شكل مرئي باستخدام الشاشة المرئية، والصورة الرقمية تمثل تكنولوجيا بديلة للصورة التقليدية.

التسجيلات الصوتية: وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل

النصوص المكتوبة: المحادثات الصوتية على الأنترنت وتشمل النصوص التي يتم كتابتها بواسطة الآلة الرقمية ومنها الرسائل عبر البريد الإلكتروني والبيانات المسجلة بأجهزة الحاسب الآلي⁽²⁾.

4. أنواع الدليل الرقمي: حيث يأخذ الدليل الرقمي نوعين رئيسيين هما:

أدلة أعدت لتكوين وسيلة اثبات ومن امثلتها نجد:

- السجلات التي تم انشاؤها بواسطة الجهاز تلقائياً، وتعتبر هذه السجلات من مخرجات الجهاز ولم يساهم الانسان في انشائها.

(1)-رشيدة بو بكر، جرائم اعتداء على نظام معالجة آلية لجرائم أنترنت، منشورات حلبي حقوقية، ط 2012، ص 385.

(2)-ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 93.

- السجلات التي جزء منها تم حفظه بالإدخال وجزء تم انشاؤه بواسطة الجهاز.

ومن أمثلة ذلك البيانات التي تم ادخالها الى الأدلة وتتم معالجتها من خلال برنامج خاص.

أدلة لم تعد لتكوين وسيلة اثبات اي الأدلة الرقمية التي لم تعد لتكوين وسيلة اثبات فهي تلك الأدلة التي تنشأ دون ارادة الشخص بمعنى أن أي أثر يتركه دون أن يكون راغبا في وجودها، ويسمى هذا النوع من الأدلة بالبصمة الرقمية أو الآثار الالكترونية الرقمية.

حيث تتجسد في الآثار التي يتركها مستخدم النظام الالكتروني بسبب تسجيل الرسائل المرسله منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال النظام الالكتروني وشبكة الاتصالات.

وتبدو أهمية التمييز بين هذين النوعين في كون أن النوع الاول من الأدلة الرقمية قد أعد سلفا كوسيلة لإثبات بعض الوقائع التي يتضمنها، لذلك فإن عادة ما يعتمد الى حفظه للاحتجاج به لاحقا وهو ما يقلل من امكانية فقدانه كما يكون من السهل الحصول عليه، بينما النوع الثاني من الأدلة الرقمية فلكونه لم يعد أصلا ليكون أثرا لمن صدر عنه لذا فهو في الغالب ما يتضمن معلومات تغيد في الكشف عن الجريمة ومرتكبها ويكون الحصول عليه باتباع تقنيات خاصة لا تخلو من الصعوبة والتعقيد⁽¹⁾.

(5) مصادر الحصول على الدليل الرقمي:

بحيث تتمثل هذه المصادر في اجهزة الحواسيب الخاصة بالجاني والمجني عليه وكذا اجهزة مقدم الخدمة، وهذه مصادر ذكرت على سبيل المثال لا الحصر.

أ. فحص جهاز الحاسوب الخاص بالجاني والمجني عليه:

(1)-ممدوح عبد الحميد عبد المطلب، مرجع سابق، ص 97.

إن فحص جهاز الحاسوب الخاص بالجاني يمكن من التحقق من طريقة التي قام بها هذا الأخير في ارتكاب الجريمة، وبالتالي فإن فحص جهاز الحاسوب الخاص به يمكن المحقق من معرفة الدخول وتتبع مصدره، ويمكن الوصول إلى الدليل الرقمي متعلق بالجرائم الالكترونية من خلال اجهزة الحاسوب سواء الخاصة بالجاني او المجني عليه عن طريق البحث في المصدرين التاليين:(1)

أنظمة الحاسوب وملحقاته:

تعد الحواسيب مصدر غنيا بالأدلة الرقمية خاصة تلك الحواسيب الشخصية التي تعد بمثابة أرشفة سلوكية للفرد وتعتمد عملية الفحص على الحاسوب بالفحص الذاتي من خلال قيام الحاسوب ذاته بفحص مكوناته وتقديم تقرير كامل بذلك الى صاحب الفحص، ويتم الفحص باستعمال مهارات عالية اضافة الى استعانة بجهاز آخر وأجهزة تقنية للبحث في جزئيات الحاسوب ويجب ان تشمل عملية الفحص على ما يلي:

● فحص القرص الصلب: وذلك من خلال البحث عن مجموع البيانات الرقمية ذات الطابع الثنائي، ويتم الفحص قرص الصلب اما جزئيا او كليا بالإضافة إلى امكانية معرفة ما تم حذفه من بيانات وكل ذلك يتوقف على مهارة الشخص القائم باستخلاص البيانات الرقمية من القرص الصلب.(2)

● فحص البرمجيات: حيث يستوجب في هذه الحالة الفحص الداخلي والخارجي للبرمجيات، فلفحص الداخلي يتم بالبحث عن مصدر ملفات الموجودة في هذا الاطار، اما الفحص الخارجي والذي يتم اللجوء فيه الى النسخة الأصلية للمقارنة بينها وبين النسخة محل اشتباه لدلالة على ثبوت ارتكاب جريمة.

(1)-عبد الفتاح بيومي، الجريمة في عصر العولمة، دراسة لظاهرة اجرامية معلوماتية، دار الفكر الجامعي، طبعة 01، ص102.

(2)-عمر محمد بن يونس، المرجع السابق، ص991.

• فحص النظام الالكتروني: ان مهام اساسية لكل نظام معلوماتي هو تحقيق فرضية تنفيذ الأوامر التي يمكن ان يقوم مستخدم الحاسوب، وتعني عملية فحص النظام الالكتروني ضبط كافة ما يحتويه جهاز الحاسب الآلي من معلومات.

ب. فحص أنظمة الاتصال بالإنترنت:

ويقصد بذلك⁽¹⁾ تلك الاجراءات او المراحل متبعة حال استخدام اتصال بالإنترنت سعيا للبحث عن الدليل بتحديد مكان وقوع الجريمة او جهاز الحاسب الذي انطلق منه النشاط الاجرامي من خلال تتبع للمسار عكسي للأنترنت، فالحاسوب بمجرد ان يتم تعرف على مسار يقوم تلقائيا باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات وباستخدام في عملية تتبع حركة مسار الأنترنت نظام فحص الكتروني يطلق عليه اسم البصمات المعاصر.⁽²⁾

6) القواعد الاجرائية في استخلاص الدليل الرقمي:

1-القواعد الاجرائية التقليدية لاستخلاص الدليل الرقمي:

يصعب حتى هذه اللحظة في غالبية الأنظمة التقليدية لإجراءات جمع الأدلة من أجل مباشرة القانونية ان نحدد الى اي مدى تكفي الأساليب مما لا شك فيه ان المشرع لم يجر استخلاص الدليل من تحقيقات ناجحة في مجال الجرائم الالكترونية غير ضوابط تحكم ذلك عن طريق قواعد اجرائية معينة أهمها: المعاينة، الخبرة، التفتيش وضبط الأشياء ومما لا شك فيه أيضا ان هذه القواعد عامة النطاق تنظم استخلاص الدليل في جميع الجرائم، تقليدية كانت ام مستحدثة الا في الثانية قد تكون بحاجة الى تطوير لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثبات وهو ما سوف نعرفه من خلال ما يلي:

(1)-خالد ممدوح ابراهيم، المرجع السابق، ص182.

(2)-خالد ممدوح ابراهيم، المرجع السابق، ص202.

أولا/ التفتيش وضبط الدليل الرقمي:

يجمع الفقه الجنائي على أن التفتيش هو اجراء من اجراءات التحقيق يباشره موظف مختص دف البحث عن أدلة لجناية او جنحة، تحقق وقوعها في محل يتمتع بحرمة، وذلك وفقا للضمانات والقيود القانونية المقررة وأن ضبط الأدلة هو النتيجة الطبيعية التي ينتهي إليها التفتيش والتي يتم الحصول عليها أثناءه، وعلى ذلك فإنه يتضح لنا ان هذين الإجراءين ما هما الا وسيلة للإثبات المادي، ذلك أن التفتيش يستهدف ضبط أشياء مادية تساعد في اثبات وقوع الجريمة واسنادها الى المتهم المنسوب اليه ارتكا. كما ان رجال الضبطية القضائية قد تعودوا في الجرائم التقليدية على ضبط الا الأشياء المادية.(1)

ثانيا: ضبط الدليل الرقمي:

إن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها أثناءه فالضبط اذن هو غاية التفتيش القريبة والأثر المباشر الذي يسفر عنه الإجراء والأساس القانوني للضبط هو العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق والتي تفيد في كشف الحقيقية ما كان منها ضد المشتبه فيه أو ما كان من مصلحته وقد تعودت جهات التحقيق في الجرائم التقليدية ان يقع الضبط على الأشياء المادية فقط بوصفها أدلة بوصفها أدلة مادية للجريمة التي يجري التفتيش بشأن، لكن في مجال الجرائم الالكترونية الطبيعية العلمية المعقدة للدليل الرقمي الذي يوجب التفتيش عنه وضبطه لإثبات هذا النوع من الجرائم ليس كالدليل التقليدي، فالبيئة الافتراضية لا تنتج سكيناً او سلاحاً نارياً وإنما تنتج نبضات رقمية تشكل قيمة وجوهر الدليل الرقمي.

2- اجراءات ضبط الدليل الرقمي:

(1)-محمد خليفة، حماية جنائية، لمعطيات الحاسب الآلي في فنون الجزائري المقارن، دار الجامعة الجديد، 2007، ص93.

يصعب اقامة الدليل على الجرائم التي تقع على العمليات الالكترونية المختلفة وذلك بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة لأن محل تلك الجرائم كما عرفنا سابقا هو جوانب معنوية تتعلق بالمعالجة الآلية للمعطيات والتي تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغطة لا يمكن للإنسان قراءتها أو ادراكها إلا من الحواسيب التي تحفظها، لأجل ذلك فإن القواعد التقليدية في اثبات لا تكف لضبط مثل هذه البيانات لذلك فإن طريقة ضبط المعلومات المعالجة آليا تختلف عما هي عليه عند ضبط المكونات المحسوسة كالأقراص المرنة، المودم، والخادم.....ومن خلال دراستنا للقانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نجد ان المشرع وضع طريقتين لضبط الأدلة الرقمية، الأولى وتكون عن طريق نسخ المعطيات محل البحث علة دعامة تخزين الكترونية تكون هذه الأخيرة قابلة لحجزها ووضعها في أحرار حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون⁽¹⁾ الاجراءات الجزائية، والطريقة الثانية تكون باستعمال التقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة الالكترونية من الوصول الى المعطيات التي تحويلها هذه المنظومة او القيام بنسخها ويكون ذلك في حالة ما اذا استحال لأسباب تقنية ضبط هذه المعطيات وفق الطريقة الأولى وان كان الدليل الرقمي يخضع في ضبطه الى قواعد تحريز الأدلة الجنائية عموما الا انه ونظرا الى الطبيعة الخاصة له فإن عملية ضبطه وتحريزه تحتاج الى بعض الاجراءات الخاصة لحمايته فنيا والحفاظ عليه وصيانته من امكانية العبث به، وهو ما نوه عليه المشرع في المادة السادسة الفقرة الثالثة من القانون 04/09 حينما اوجب على السلطات التي تقوم بعملية ضبط الدليل الرقمي ان تسهر على سلامة المعطيات في المنظومة الالكترونية التي تجري العملية، وان لا يؤدي استعمال الوسائل التقنية في ذلك الى المساس بمحتوى هذه المعطيات ومن هذه الاجراءات الخاصة

(1)- شيماء عبد الغاني، محمد عصا الله، حماية جنائية للتعاملات الكترونية، دار جامعة الجديدة، 2007، ص358.

في هذا الاطار نذكر على سبيل المثال عدم اخذ نسخة احتياطية عن المعطيات والعمل عليها لضمان عدم المساس بالدليل الأصلي تنفيذ برامج على الحاسوب مسرح الجريمة خوفا من اتلاف الموجودة عليه او محو الذاكرة او الملفات وعدم السماح للمشتبه به بالتعامل مع الحاسوب ضبط الدعائم الأصلية للمعلومات وعدم الاقتصار على ضبط نسخها عدم ثني القرص لأن ذلك يؤدي الى تلفه وفقدانه للمعلومات المسجلة عليه.(1)

القواعد الاجرائية الحديثة لاستخلاص الدليل الرقمي:

بحيث يعتبر تطور التكنولوجيا اتصالات ومعلومات معضلة حتمت على معظم التشريعات ايجاد طرق جديدة وملائمة تتناسب وطبيعة التقنية للجريمة الالكترونية والدليل الرقمي، ومن ضمن المقومات التشريعية التي ارساها المشرع الجزائري ضمن خطته في مكافحة الجريمة الالكترونية ما جاء به في القانون 22/06 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الاجراءات الجزائية (امر 155/66) من خلال اجرائي التسرب واعتراض المرسلات، ومن خلال قانون 04/09 استحدث اجرائين جديدين هما المراقبة الالكترونية وحفظ المعطيات المتعلقة بحركة السير.(2)

التسرب واعتراض المرسلات:

يتم اللجوء اليهما في الجرائم الالكترونية فنجد المشرع الجزائري قد حدد التسرب على سبيل الحصر في المادة 65 مكرر 5 من ق.إ. ج منها الجرائم الماسة بأنظمة معالجة الآلية للمعطيات بحيث يعتبر التسريب ممارسة غير مألوفة قانونيا، واجراء من أخطر اجراءات انتهاك لحرمة الحياة الشخصية للمشتبه به، فنجد المشرع الجزائري قد احاط اجراء التسريب بجملة من الشروط يتعين مراعاتها في تحقيق فنجد الشروط شكلية اجراء انن فلا

(1)-شيماء عبد الغاني محمد عطا الله، مرجع نفسه، ص360.

(2)-رشيدة بو بكر، المرجع السابق، ص397.

يمكن لضباط الشرطة القضائية ولوج عملية التسريب بمفرده دون أن يكون متصل على اذن بذلك من الجهات القضائية المختصة مادة 65 مكرر 11 قانون الاجراءات الجزائية "يجوز لوكيل جمهورية او لقاضي التحقيق بعد اختصار وكيل جمهورية ان يأذن له⁽¹⁾ حسب الحالة بمباشرة عملية التسريب" حيث يجب أن يكون اذن مكتوبا والا كان الاجراء باطلا مادة 65 مكرر 15، ذلك ان اذن يتضمن مجموعة من الشروط كذكر هوية ضابط الشرطة القضائية التي تتم عملية التسريب تحت مسؤوليته، اضافة الى تحديد المدة المطلوبة في عملية التسريب والتي يجب أن لا تتجاوز اربعة أشهر.

أما الشروط الشكلية فقد نظمها المشرع الجزائري في شطرين أساسيين يتمثل الأول في تحديد نوع الجريمة محصورة في مادة 65 مكرر 05 "جرائم مخدرات، جريمة المنظمة العابرة للوطنية، جرائم تبييض أموال، جرائم ارهابية، جرائم الفساد، جرائم متعلقة بالتشريع الخاص بالصرف والجرائم ماسة بأنظمة المعالجة الآلية للمعطيات"

ويتمثل الشرط الثاني ان يكون اذن بالتسريب مسببا بعناصر تقنع جهات قضائية المختصة منح الاذن لإجراء التسريب.

• ومن أهم طرق التسريب في مجال الجرائم الالكترونية دخول ضباط او اعوان شرطة قضائية إلى عالم افتراضي وذلك باختراق مواقع معينة وفتح ثغرات الكترونية، أو اشتراك في محادثات غرف الدردشة أو حلقات الاتصال المباشر فيهم والظهور بمظهر كما لو كان فاعلا مثلهم مستخدما في ذلك اسماء وصفات وهمية ومستعارة للاستفادة من كيفية اقتحام الهاكر لمختلف مواقع.⁽²⁾

اعتراض المرسلات السلكية واللاسلكية:

(1)-شيماء عبد الغاني محمد عطا الله، المرجع السابق، ص365.

(2)-شيماء عبد الغاني محمد عطا الله، المرجع السابق، ص366.

وتعرف بأنها عملية مراقبة شرية لشبكات سلكية ولاسلكية في اطار اجراءات البحث والتحري عن الجريمة الالكترونية حول أشخاص المشتبه فيهم أو مشاركتهم في الجريمة استحدث المشرع الجزائري هذا النمط بموجب قانون 22/06 المؤرخ في 2006/12/20 معدل والمتمم لقانون الاجراءات الجزائية من خلال الفصل الرابع من باب ثاني من كتاب الأول تحت عنوان "اعتراض مرسلات وتسجيل أصوات والنقاط والصور" تضمنه ستة مواد من مادة 65 مكرر إلى مادة 65 مكرر 10، بحيث نجد ان اجراء اعتراض المرسلات السلكية واللاسلكية يتم بدون علم اصحابها أوجب أن يتم هذا الاجراء بصدور ترخيص من السلطة القضائية ومراقبتها لعملية التنفيذ طبقا للمادة 65 مكرر 05 فلا يمكن لضباط الشرطة اعتراض المرسلات إلا بإذن مكتوب ومسبب من طرف وكيل الجمهورية او قاضي التحقيق في حالة فتح تحقيق قضائي، وعلى وكيل جمهورية او قاضي التحقيق قبل منح الاذن تقدير فائدة اجراء اعتراض وجديته وملائمته لسير الدعوى العمومية، ونصت مادة 65 مكرر 07 ان يتضمن الاذن اعتراض المرسلات كل العناصر التي تسمح بالتعرف على اتصالات مطلوب اعتراضها واقصى مدة لذلك مقدرة بأربعة أشهر قابلة للتجديد حسي تقدير سلطة مصدرة للإذن وفقا لمقتضيات التحري والتحقيق وتتم عملية اعتراض المرسلات على البريد الالكتروني، فكل رسالة تحمل معلومات عامة مثل تاريخ انشاء رسالة وتاريخ تلقيها عنوان مرسل والمرسل اليه⁽¹⁾ رغم امكانية انشاء حسابات وهمية او ارسال رسالة دون اظهار عنوان بريد الالكتروني صحيح، وللحصول على مزيد من المعلومات في حاشية البريد الالكتروني بإجراء بعض خطوات للحصول عليها وغيرها من التقنيات والبرامج التي تكشف اصل هذه الرسالة وتمكن من اطلاع عليها دون علم مرسلها.⁽²⁾

(1)-شيماء عبد الغاني محمد عطا الله، المرجع السابق، ص367.

(2)-شيماء عبد الغاني محمد عطا الله، المرجع السابق، ص368.

المراقبة الالكترونية وحفظ المعطيات:

ونعني بها مجموعة الأجهزة المتكاملة مع بعضها البعض بغرض تشغيل مجموعة من بينات داخلية وفق لبرنامج موضوع مسبقا قصد الحصول على نتائج المطلوبة حيث نجد ان المشرع الجزائري لم يعتبر هذا اجراء من ضمن طرق الحصول على الدليل الرقمي فقط بل ادرجه ضمن التدابير الوقائية من الجرائم التي يمكن ان ترتكب بواسطة الالكترونية، بحيث نجد ان اجراء مراقبة اتصالات الكترونية في اطار التحريات وتحقيقات قضائية لا تتم الا بواسطة هذا الاجراء وهو ما قررته المادة الرابعة من قانون 04/09 بأنه يمكن القيام بعملية مراقبة الكترونية للاتصالات للوقاية من افعال موصوفة بجرائم ارهاب او التخريب والجرائم الماسة بأمن الدولة أو في حالة اعتداء على منظومة معلوماتية تهدد نظام العام او الدفاع الوطني ومن اهم شروط مراقبة الكترونية للاتصالات ان يتم هذا الاجراء تحت سلطة القضاء وبإذن منه، ان تكون هنالك ضرورة تتطلب هذا الاجراء وهو ما أكده المشرع الجزائري في المادة الرابعة من القانون 04/09.⁽¹⁾

7) القيمة القانونية للدليل الرقمي وحجيته في مجال اثبات جنائي

أ. القيمة القانونية للدليل الرقمي في مجال اثبات الجنائي:

إن مجرد وجود دليل يثبت وقوع الجريمة ونسبها إلى شخص معين لا يكفي لتعويل عليه، إذ يلزم أن يكون لهذه أدلة قيمة قانونية وقيمة الدليل الرقمي الجنائي تتوقف على مسألتين رئيسيتين هما:

مشروعية الدليل الرقمي:

(1)-محمد خليفة، المرجع السابق، ص102.

تعرف المشروعية بأنها التوافق والتعقيد بأحكام القانون في اطاره مضمونه الخاص، فهي تهدف لحماية حريات وحقوق اشخاص ضد تعسف السلطة من التطاول عليها، فلا شك ان مشروعية الجرائم والعقوبات ينعكس على قواعد اثبات الجنائي ويفرض خضوعها هي الأخرى لمبدأ الشرعية، وتثبت مشروعية وجود الدليل الرقمي ان يعترف المشرع بهذا الدليل ويجيز للقاضي ان يستند اليه في تكوين عقيدته وفقا لطبيعة اثبات السائد في الدولة.(1)

1. موقف المشرع الجزائري من الدليل الرقمي: لقد عرفت تشريعات اجرائية نظامين للإثبات
 - نظام اثبات المقيد: وفيها يقوم المشرع بتحديد ادلة اثبات حصرا وكذا قوة اثباتية لكل دليل بناء على قناعة المشرع بها وهو ما يعرف بنظام الأدلة القانونية.
 - نظام اثبات الحر: والذي يقوم على اساس حرية الاثبات فلا يقوم المشرع بتحديد الأدلة وتقدير الثبوتية حسب قناعته بها فلا يلزمه المشرع بأدلة معينة يستند اليها كون ادلة تتساوى في قيمة اثبات.(2)

واسترشادا بما سبق ذكره فإن النظم القانونية التي تتبنى نظام ادلة القانونية لا يمكن في ظلها اعتراف للدليل الرقمي بأي قيمة اثباتية ما لم ينص قانون عليه صراحة ضمن قائمة أدلة اثبات، ففي نظام اثبات الحر في القانون الجزائري (مادة 212 قانون الاجراءات الجزائية) فإن مشروعية الدليل الرقمي لا تثور من حيث الوجود، اعتمادا على اساس حرية اثبات فمسألة قبول الدليل الرقمي لا تتطلب سوى اقتناع القاضي به، كون المشرع الجزائري لم يقيد قاض بنصوص قانونية تلزمه بقبول أو رفض الدليل الرقمي حيث نجد أن الحصول على الدليل الرقمي يجب أن يكون مشروعاً وأن لا يخالف مبدأ مساس بحرية افراد وذلك من خلال أن يتم البحث عن الدليل بعد اخذ اذن من القضاء أو الجهات المختصة والا اعتبر

(1)-هلاي عبد الله احمد، حجية مخرجات كميوترية في المواد الجنائية، طبعة الثانية، دار النهضة العربية، 2008، ص104.

(2)-محمد خليفة، المرجع السابق، ص112.

هذا الدليل باطلا مادة 191 قانون الاجراءات الجزائية التي نصت على أنه تنظر غرفة اتهام في صحة اجراءات مرفوعة اليها اذا اكتشفت سبب لبطلانه قضت ببطلان اجراء المشوب ببطلان اجراءات تالية كلها او بعضها.(1)

المطلب ثالث: حجية الدليل الرقمي في اطار نظرية الاثبات الجنائي.

إن مسألة تقديم الدليل الجنائي في اثبات الواقعة اجرامية هي مسألة موضوعية محضة للقاضي ان يمارس سلطته للتقديرية فيها حيث لا يشترط ان يكون الدليل الذي استند اليه القاضي صريحا دالا على واقعة مراد اثباتها بل يكفي ان نستخلص من ظروف وقرائن الدعوى.

الفرع أول: شروط وآثار الدليل الرقمي

1-شروط قبول الدليل الرقمي:

باعتبار الدليل الرقمي تطبيق من تطبيقات الدليل العلمي وحجية اثبات القضاء في تقليل من الأخطاء واقترب أكثر إلى تحقيق عدالة وتوصل للحقيقة إلا أن ذلك لا ينف استبعاد كونه موضع شك من حيث امكانية خضوعه للعبث والخروج به على نحو يخالف الحقيقة من جهة، ومن جهة اخرى ان يتم حصول خطأ اثناء الحصول على الدليل الرقمي، وعليه وحتى يتم اعتبار الدليل الرقمي حجية قاطعة يجب أن تكون هذه ادلة رقمية غير قابلة للشك اضافة إلى قيام بتقييم الدليل الرقمي لتحقق من سلامته باستخدام عمليات حسابية خاصة تسمى الخوارزميات وتتم هذه عملية في حالة عدم الحصول على النسخة أصلية للدليل الرقمي.

(1)-محمد خليفة، المرجع السابق، ص113.

1. آثار القيمة العلمية للدليل الرقمي في مجال اثبات الجنائي:

حيث يرى البعض انه ليس بشرط ان يكون اقتناع القاضي يقينيا بذلك لأن القاضي لا يملك وسائل ادراك اليقين كحالة ذهنية تلتصق دون ان تختلط بأي شك على المستوى الشخصي.(1)

لاكن ثمة رأي آخر يرى ان وسائل العلمية في أغلب حالاتها ليست دليلا مستقلا في ذاته وانما هي قرائن يتم دراستها لاستخلاص دلالاتها وهي غير مستقلة عن القرائن، وذلك لأنها لا تصلح في ذاتها كدليل وحيد في اثبات الجنائي، وانقاض باعتماده على خبير في مسائل الفنية، فمن الغير مقبول ان يتخلى القاضي عن حقه لأي سبب من اسباب ذلك ان توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم بموجبها سواء بالأدلة او البراءة ليس معدة لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة بل تعتبر دليل يقتنع ارادة القاضي اما بالحكم بالإدانة او بالبراءة.(2)

الفرع الثاني: موقف المشرع الجزائري من الدليل الرقمي وأنظمة اثبات في الجرائم الالكترونية في مجال اثبات الجنائي

إن اثبات في المواد الجنائية هو النتيجة التي تتحقق باستعمال وسائل وطرق مختلفة للوصول لدليل يستعين به القاضي لاستخلاص حقيقة وقائع.

أولا: أنظمة اثبات الجنائي: حيث نجد نظامين هما:

1-نظام اثبات المقيد او نظام ادلة قانونية:

(1)-عمر محمد بن يونس، المرجع السابق، ص301.

(2)-عمر محمد بن يونس، المرجع السابق، ص302.

مفاد هذا النظام ان يتقيد القاضي في حكمه سواء بالإدانة او البراءة بأنواع معينة من الأدلة طبقا لما يرسمه المشرع، لفكرة اساسية لهذا النظام تقوم على أن المشرع له الدور الأساسي في الاثبات من خلال تحديده للأدلة المقدمة في الدعوى والذي يستند اليها القاضي في حكمه، ولا سبيل له أن يستند إلى أي دليل ما لم ينص عليه القانون صراحة ضمن ادلة اثبات فهنا نجد ان دور القاضي سلبي نظرا لتقيد سلطة القاضي في تقدير عناصر ادلة معروضة عليه، وفي ذلك اخراج للقاضي من وظيفته الطبيعية التي تتمثل في فحص الدليل وتقديره.(1)

2- نظام اثبات الحر أو نظام اقناع الشخص للقاضي الجزائي:

وفقا لهذا النظام لا يرسم القانون طرقا محددة للإثبات، اذ يتمتع القاضي جزائي في هذا النظام بحرية مطلقة في تكوين اعتقاده من أي دليل يطرح امامه فنجد أن حرية اثبات القاضي الجزائي بأي دليل مادي أو نفسي بالإضافة لحرية اقتناعه بكلفة ادلة مطروحة عليه.(2)

وعلى هذا الأساس يكون للقاضي الجزائي دور فعال حيال الدليل الذي يوضع امامه، وله كافة صلاحيات في اتخاذ الاجراءات التي يراه مناسبا ويخدم اظهار الحقيقة.(3)

ثانيا: موقف المشرع من انظمة الاثبات والدليل الرقمي

نصت المادة 212 قانون الاجراءات الجزائية على أنه يجوز اثبات الجرائم بأي طريق من طرق الاثبات وللقاضي ان يصدر حكمه تبعا للاعتقاد شخصي"

(1)-محمد عيد الغريب، حرية قاضي الجنائي في اقتناع اليقيني واثره في تسبب احكام

(2)-زبدة مسعود، اقتناع الشخصي للقاضي الجزائي، مؤسسة وطنية للكتاب، طبعة أولى، ص80.

(3)-زبدة مسعودة، المرجع السابق، ص81.

نصت مادة 307 قانون الاجراءات الجزائية ان قانون لا يطلب من قضاة ان يقدموا حسابا على الوسائل التي بها قد وصلوا الى تكوين اقتناعهم وان يبحثوا بإخلاص ضمائرهم في ادلة مسندة اليهم.

1. أساس موقف المشرع الجزائري من أنظمة اثبات:

استنادا إلى المادتين سابقتي الذكر يتضح أن المشرع الجزائري قد تبنى كقاعدة عامة نظام اقتناع الشخص للقاضي الجزائي، وتحليل المادة 212 قانون الاجراءات الجزائية نجده كرس قاعدتين تكمل احدهما الأخرى قاعدة اقتناع الحر للقاضي الجزائي من جهة وقاعدة اختيار وسائل اثبات من جهة اخرى، حيث نجد أن الدليل الرقمي يجب أن يخضع لسلطة القاضي الجزائي في تقديره والحكم عليه فالمشرع الجزائري منح حرية أدلة إلا في بعض الجرائم التي تتطلب ادلة معينة، ومنح قاضي جزائي سلطة تقدير الدليل والحرية في تكوين اقتناعه من أي دليل يطمئن إليه.⁽¹⁾

(1)-محمد خليفة، المرجع السابق، ص193.

الخاتمة :

إن قيام المشرع باستحداث هذا النوع من الجرائم إنما يكون قد فهم الوضع القائم على المستوى الدولي وهو ظهور أدوات جديدة تساهم في التطور التكنولوجي وتطور تكنولوجيات الإتصال والمكالمات والتواصل الإجتماعي ، وهذا ما أدى إلى ظهور إجرام جديد يتلاءم مع هذه الأدوات واستدعى تدخل المشرع لحماية البرامج من كل أنواع الدخول غير المشروع إلى هذه البرامج والبقاء فيها والولوج إليها وكذا إدخال أية وسيلة من شأنها إعاقة عمل هذه البرامج والمعطيات .

إن هاذا التعديل القانوني جاء نتيجة لفهم المشرع الجزائري للتطور التكنولوجي الذي سيحدثه جهاز الإعلام الآلي ولذلك اعتبره بأنه من قبيل المال المنقول المعنوي وهو ما يجعلها قد وردت تحت عنوان المساس بالأموال .

و الملاحظ من جهة أخرى هو أن قانون العقوبات الجزائري وكان مثله مثل القوانين المقارنة إلا أنه يسعى جاهاذا للحاق بالركب والتطور التكنولوجي الحاصل على المستوى الدولي حتى لا يبقى خارجه .

قائمة المراجع

- نبيلة هبة هروال، الجوانب الإجرامية لجرائم الانترنت، فيم رحلة جمعاستد لالات، دراسة مقارنة، دارا لفكر الجامعي 30 شارع سويتير - الإسكندرية، 2013.
- عبد الفتاح مراد، دور الكمبيوتر في مجاز ارتكاب الجرائم الإلكترونية، شرح جرائم الكمبيوتر والانترنت، دار الكتب والوثائق المصرية.
- ماشوش مراد، مكافحة جرائم المعلوماتية في التشريع الجزائري، مذكرة لاستكمال المتطلبات لتأهيل شهادة ما ستر أكاديمي في مسار الحقوق، تخصص قانون جنائي، سنة 2013-2014.
- (1) مولود ديدان، قانون العقوبات، قانون رقم 09-01 المؤرخ في 25 فبراير 2009، د. ط.
- هبة نبيلة هروال، جرائم الانترنت، دراسة مقارنة، أطروحة دكتوراه، تخصص القانون، كلية الحقوق وعلوم السياسية، جامعة تلمسان، الجزائر، 2013/2014.
- يوسف صغير، الجريمة المرتكبة عبر الانترنت، رسالة لنيل شهادة الماجستير، تخصص القانون الدولي لأعمال، كلية الحقوق وعلوم السياسية، جامعة تيزي وزو، الجزائر، 2013 .
- - محمد علي العريان: "الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004.
- محمد حموني، خصائص الجريمة الإلكترونية ومجالات استخدامها، مجلة الحقيقة، العدد 41، 2018.

- القانون رقم 04-15 المؤرخ في 10 نوفمبر يعدل ويتمم الأمر 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، ج.ر، ج.ج.د.ش، العدد 71 الصادر في 10 نوفمبر 2004.
- - القانون 04-09
، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا اتصالات وعلامات الاتصال ومكافحتها، ج،ر، العدد 47، الصادر في 16 أوت 2009.
- - محمد سامي الشوا: "ثورة المعلومات وانعكاساتها على قانون العقوبات". دار النهضة العربية، القاهرة. 1994.
- عبد الله حسين محمود: سرقة المعلومات المخزنة في الحاسبات الآلي، دار النهضة العربية، ط 2، القاهرة 2002.
- وانظر كذلك: محمد سامي الشوا:
ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998.
- د. عمر محمد أبو بكر بنونس: الجرائم الناشئة عن استخدام الإنترنت، دار النهضة العربية، 2004.
- د. سعيد عبد اللطيف حسن: اثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، ط 1، دار النهضة العربية، القاهرة، 1999.
- وانظر: د: هشام رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة. بأسويط، 1994.
-
- اسامة احمد المناعسة: جلال محمد الزعبي، صايفاضا لهواوشة : جرائم الحاسبات الآلي والإنترنت، دراسة تحليلية مقارنة، دار وائل للنشر، عمان، الأردن، الطبعة الأولى، 2001 .

- د. نائلة عادل محمد فريدقورة :
- جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، دار النهضة العربية، القاهرة، 2003 .
-
-
- - أشار اليه جميل عبد الباقي الصغير : "القانون الجنائي والتكنولوجيا". الكتاب الأول:
الجرائم الناشئة عن استخدام الحاسب الآلي. دار النهضة العربية سنة 1992. القاهرة.
- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هو مه الجزائر، ط10، 2011.
- أحسن بوسقيعة الوجيز في القانون الجزائي العام، دار هو مه الجزائر، 18، 2019.
- القانون رقم 06-23 المؤرخ في 24 ديسمبر 2006، يعدل ويتمم الأمر رقم 66-156 الصادر في 08 جوان 1966، المتضمن قانون العقوبات، ج. ر . العدد 84.
- إيمان بنغادي، أثر تعديل قانون العقوبات الجزائري في التصدي للجريمة الإلكترونية، مجلة أفاق للبحوث والدراسات المركز الجامعي، اليزي، الجزائر، العدد 04، جوان 2019
- بوضياف استمها ن الجريمة الإلكترونية والإجراء التشريعية لمواجهة لها، مجلة الأستاذ الباحث للدراسات القانونية والسياسية جامعة محمد بوضياف المسيلة، العدد 11 سبتمبر 2018.
- د. حمود بن محسن الدعجاني، الجريمة الإلكترونية
(دراسة فقهية تطبيقية)، مجلة الجامعة الإسلامية، ملحق العدد 183.558 ج16.
- خالد حسن أحمد لطفي : جرائم الأنترنت "
- بينا القرصنة الإلكترونية وجرائم إبتزاز الإلكترونية، دار الفكر الجامعي، ط1، مصر، 2018 .
- المادة 144 من القانون 11-14 المؤرخ في 2/08/2011 معدل ومتمما لأمر 66-156، المتضمن قانون العقوبات، ج. ر، عدد 44.
- المادة 303 مكرر من القانون 06-23 المعدل والمتمما لقانون العقوبات.

- ناير عائشة:
الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل لياسترفيا القانون، تخصص قانون، جامعة
أحمد دراية، كلية الحقوق، أدرار، 2016-2017.
- إبراهيم يسها م:
الأساس القانوني للتنظيم الإداري في ظل التشريع الجزائري، الشخصية المعنوية أو الاعتبارية، مجلة
القانون والعلوم السياسية، المركز الجامعي صالح أحمد بالنعامة، جامعة الجزائر 1
، كلية الحقوق، العدد 07 ، 2018.
- در دور نسيم:
جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، رسالة لنيل شهادة الماجستير، تخصص القانون
ن الجنائي، جامعة منثوريقسنطينة، 2012-2013.
- محمد عبد الرحيم الناغي: الحماية الجنائية للرسوم والنماذج الصناعية
(دراسة مقارنة)، د. ط، دار النهضة العربية، القاهرة، 2009 .
- ناير نبيل عمر :
الحماية الجنائية للمحالات الإلكترونية في جرائم المعلوماتية، د. ط، دار الجامعة الجديدة، مصر ،
2012 .
- •
• أمال قارة:
الجريمة المعلوماتية، رسالة لنيل درجة الماجستير في القانون الجنائي والعلوم الجنائية، جامعة الجزائر
1 ، الجزائر ، 2013.
- • أنور الحربين نوبيل، القبلة الإلكترونية الموقوتة تنفجر في الكويت، مجلة آفاق الانترنت، السنة الثانية
العدد 14 ، 1999 .

- عامر بزر فايز، أبو علي : فيروسات الكمبيوتر، ط 1، دارضنين للنشر، عمان، 1994.
- -
- سالم عبد الرزاق، ملتقى حول المنظومة التشريعية الجزائية في مجال الجريمة المعلوماتية بمحكمة سيد
ي محمد.
- مولود ديدان، قانون العقوبات، قانون رقم 09-01 المؤرخ في 25 فبراير، 2009، د. ط.
- جواهر يعياش، مداخلة حول مسارات التحقيقات الجنائية في مجال المعلومات، المعهد الوطني لأدلة ال
جنائية وعلم الاجرام (الجزائر) جامعة بسكرة، كلية الحقوق.
- حملاوي عبد الرحمان، مداخلة بعنوان
(دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة محمد خضير، بسكرة،
2016، ص 2.
- عبد الرحمان خليفي، اجراءات جزائية في التشريعات الجزائرية المقارن، ط 1، دار بلقيس للنشر والتوزيع، الجز
ائر، 2005.
- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهاد
ة الماجستير في العلوم القانونية، باتنة، 2012-2013.
- عبد الوهاب حومد، أصول محاكمات جزائية، طبعة 4، مطبعة جديدة دمشق، 1990.
- محمد نجيب حسن، شرح قانون الجنائية، طبعة ثانية، دار نهضة عربية، القاهرة 1988.
- جميل عبد الباقي صغير، أدلة اثبات الجنائيات في تكنولوجيا حديثة، دار نهضة القاهرة 2002.
- حسين بن سعيد الغافري، سياسة جنائية في مواجهة جرائم الأنترنت، دار نهضة عربية، القاهرة 2009.
- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الأنترنت، دار فكر قانونية، مص
ر 2006.
- رشيدة بوبكر، جرائم اعتداء على نظام معالجة آلية لجرائم الأنترنت، منشورات اتحاد بحقوقية، ط
2012.

- عبد الفتاح بيومي، الجريمة في عصر العولمة، دراسة نظاهرة إجرامية مع معلوماتية، دار الفكر الجامعي، طبعة 01.
- محمد خليفة، حماية جنائية، لمعطيات الحاسب الآلي في فنون الجزاء المقارن، دار الجامعة الجديد، 2007.
- شيماء عبد الغاني، محمد عصا الله، حماية جنائية للتعاملات الكترونية، دار جامعة الجديدة، 2007.
- هلال عبد الله حامد، حجية مخرجات كمبيوترية في المواد الجنائية، طبعة الثانية، دار النهضة العربية، 2008.
- محمد عيد الغريب، حرية قاضي الجنائي في اقتنا عال يقيني واثره في تسيب احكام
- زبدة مسعود، اقتنا عال شخصيل لقاضي الجزائي، مؤسسة وطنية للكتاب، طبعة أولى.

systeme de traitement automatisé de données (ou STAD)

La loi Godfrain du 5 janvier 1988, ou Loi no 88-19 du 5 janvier 1988 relative à la fraude informatique, est la première loi française réprimant les actes de criminalité informatique et de piratage

Voir : https://fr.wikipedia.org/wiki/Loi_Godfrain .

Catala, la propriété de l'information, p : 97 et masse : la deliquance informatique aspects de droit pénal international in le criminel. Dr.

la criminalité éinformatiques url' internet. : Mohammed boBuzubar University. No1 Journal of law academic publication council Kuwait vol. 26 – march 2002 pp.41.4

Analyse Philippe Rose. La criminalité informatique à l'horizon prospective. Le harmattan 1992 جرائم الإعتداء على حرمة الحياة الخاصة

للأشخاص ، مقال منشور على الموقع الإلكتروني :

اطلعنا عليه يوم <https://scholarworks.uaeu.ac.ae/cgi/viewconte>

. 2023/08/24

. Joël Rivière et Didier Lucas –« Criminalité et internet une arnaque à bon March » – Article publier dans la revus de la securité

Globale– numero 06– année 2008– p 69–70. Disponible sur site

:www.cairn.info – Fond documentaire (S.N.D.L) Système national

de documentation en ligne – Algérie –Date de consultation

28/03/2014.– Charlie Abrahams – « La Cybercriminalité un

Business Croissant lié à l’effondrement des crédits » Article publier

dans la revus de la securité Globale– numero 06– année 2008 –p

30 Disponible sur site : www.carin.info – Fond documentaire

(S.N.D.L) Système national de documentation en ligne – Algérie–

Date de consultation 28 /03/2014.

– Computer Hackers : Tomorrows Tarrarts Dynamics, News for and about members of the American society for in dustrialseturdy jam varylfebrauary. 1990. p: 7.

الفهرس

1	مقدمة :
2	الفصل الاول: ماهية الجريمة الالكترونية
3	المبحث الأول: تطور الجريمة الإلكترونية.....
3	المطلب الاول: تطور الجريمة الإلكترونية في التشريعات المقارنة:
6	المطلب الثاني: تطور الجريمة الإلكترونية في التشريع الجزائري:
9	المبحث الثاني: طبيعة الجريمة الالكترونية:
9	المطلب الاول: الطبيعة الخاصة للجرائم الالكترونية.
9	الفرع الاول: تعريف الجريمة الالكترونية.
14	الفرع الثاني: موضوع الجريمة الالكترونية
15	الفرع الثالث: خصوصية الجريمة الالكترونية.
17	المطلب الثاني: الطبيعة القانونية للجريمة الالكترونية.
17	الفرع الاول: المعلومات لها طبيعة قانونية من نوع خاص.
18	الفرع الثاني: المعلومات مجموعة مستحدثة من القيم.
20	المطلب الثالث: خصائص الجريمة الالكترونية
20	الفرع الأول : أنها تتركب من مجرم غير تقليدي
21	الفرع الثاني : صعوبة اكتشاف اثبات الجرائم الالكترونية
22	الفرع الثالث : الجرائم الالكترونية للضحية دور مهم فيها
23	الفرع الرابع : الجرائم الالكترونية ناعمة مغرية للمجرمين
23	الفرع الخامس : الجرائم الالكترونية جرائم معابرة للحدود
25	المبحث الثاني: الأسس التي تقوم عليها الجريمة الالكترونية

25	المطلب الأول : أطراف الجريمة الالكترونية .
25	الفرع الأول: المجرم الالكتروني.
29	الفرع الثاني: ضحايا الإجرام الالكتروني.
31	المطلب الثاني: أركان الجريمة الإلكترونية.
31	الفرع الأول: الركن الشرعي:
32	الفرع الثاني : الركن المادي
33	الفرع الثالث: الركن المعنوي.
36	المبحث الثالث: أنواع الجرائم الالكترونية .
36	المطلب الأول: الجريمة الواقعة على الأشخاص
36	الفرع الأول: جرائم السب والقذف في صورتها الالكترونية
36	الفرع الثاني: جرائم الإعتداء على حرمة الحياة الخاصة.
37	الفرع الثالث: الجرائم الماسة بالحريات العامة.
41	الفرع الرابع: الجرائم المعلوماتية الواقعة على الأموال
43	الفرع الخامس: الجرائم الواقعة علي امن الدولة.
44	المطلب الخامس: الجرائم الواقعة علي النظام الالكتروني.
44	الفرع الأول: الجرائم الواقعة علي المكونات المادية للنظام.
45	الفرع الثاني: الجرائم الواقعة علي المعلومات المدرجة بالنظام.
47	الفرع الثالث: الجرائم الواقعة علي البرامج الالكترونية.
50	الفصل الثاني:
50	أساليب ردع الجريمة الالكترونية
51	المبحث الأول: أساليب وتقنيات إرتكاب الجرائم الالكترونية
51	المطلب الأول: أدوات الجرائم الالكترونية

52	المطلب الثاني: الاختراق.....
56	المطلب الثالث : الفيروسات البرامج الخبيثة المدمرة:
63	المبحث الثاني: آليات مكافحة الإجرام الإلكتروني.
63	المطلب الأول: الأجهزة المختصة في مكافحة الجريمة الالكترونية.....
74	المطلب الثاني: اثبات في المادة الالكترونية.....
96	المطلب ثالث: حجية الدليل الرقمي في اطار نظرية الاثبات الجنائي.....
100	الخاتمة :