جامعة ابن خلدون ـ تيارت ـ

كلية الحقوق و العلوم السياسية

قسم الحقوق

الموضوع:

التحري والتحقيق الابتدائي في جرائم الأنترنت

مقدم ضمن متطلبات نيل شهادة الماستر في الحقوق

تخصص: علوم جنائية

من إعداد الطالبتين:

- غـــلام نصيـــرة
- فـــــلاح فاطمـــة

إشراف الدكتـــور:

- بن أحمـــد محمد

أعضـــاء لجنـــة المناقشـــة

أعضاء اللجنة	الرتبـــة	الصفة
د.بن عمارة محمد	أستاذ محاضر "أ"	رئيسا
د.بن أحمـــد محمد	أستاذ مساعد "أ"	مشرفا مقررا
د.عبد الصدوق خيرة	أستاذ محاضر "أ"	عضوا مناقشا

السنة الجامعية: 2018م/ 2019م

الحمد لله سبحانه وتعالى، له عظيم الشكروالحمد بنعمته أتممنا هذا العمل

اعترافاً بالفضل والجميل نتوجه بخالص الشكروعميق التقدير والامتنان

إلى الأستاذ: بن أحمد أحمد الذي تفضل علينا بالإشراف على هذا العمل

فله منا كل التقديروالامتنان .

كما نتقدم بخالص شكرنا إلى أعضاء لجنة المناقشة على قبولهم تقييم هذا العمل ومناقشته .

كما نشكركل من قدم لنا يد العون لإنجازهذا العمل

إهداء

إلى الذي أفنى عمره محترقا شامخا لكي يريني النور،

إلى ذلك الوجه المكابر إلى تلك الهمة العالية

إلى أبي الحبيب .

إلى روضة الأمل المعطاء وجداول الحنين المتدفقة

إلى التي الجنة تحت إقدامها إليك أيها الملاك السماوي

إلى أمي الحبيبة .

إلى من أوقدوا بنور قلوبهم شموع ليلي الغريب

إلى أختي وأولادها وإخوتي .

أهدي ثمرة جهدي

فاطمة

إهداء

إلى من علمني النجاح والصبر، وافتقدته في مواجهة الصعاب

فلم تمهلني الدنيا لأرتوي من حنانه

إلى روح أبي الطيبة " الحاج" رحمه الله .

إلى زوجي العزيز الذي كان عونا وسندا لي "عبدالقادر"

إلى القلوب الطاهرة والنفوس البريئة

إلى رياحين حياتي أولادي" زهرة وسعيد"

إلى كل من عرفتني بهم الحياة، وكل من عرفتني بهم الدراسة...

أهدي ثمرة جهدي

نصيرة

قائمة المختصرات:

باللغة العربية:

ص: صفحة.

ط: طبعة.

ق.إ.ج: قانون الإجراءات الجزائية الجزائري.

ق.ع: قانون العقوبات الجزائري.

باللغة الفرنسية:

IP :Adresse internet protocole
TCP :Trams commission protocole

مُقَدِّمَةٌ

مقدمة:

ظهرت الجريمة مع بداية البشرية وقد حاربها الإنسان منذ اللحظة الأولى عندما أحس فيها بخطر يهدد كيانه واستقراره بل ويهدد حياته، وهي مظهر من مظاهر المجتمع ، لأنها ناتجة عن ما يحويه السلوك الإنساني في علاقاته المتداخلة لعنصري الخير والشر المتصارعين على مر السنين، وعليه فالمجتمع هو صاحب الحق في توقيع العقاب على الأفراد بمجرد ارتكابهم الأفعال المجرمة بنصوص قانونية تنظمها السلطة التشريعية لكل دولة، ولا يمكن معاقبة الشخص إلا إذا سبق ارتكابه للفعل نص قانوني يجرم سلوكه و هذا ما كرسته المادة الأولى من قانون العقوبات الجزائري حيث نصت على أنه " لا جريمة ولا عقوبة أو تدابير أمن بغير نص" كما أنه لا تنفذ العقوبة إلا بعد صدور حكم نهائي بالإدانة فالمتهم بريء حتى تثبت إدانته وهذا ما بينته المادة 38 من الدستور ويسبق الحكم بالإدانة عدة إجراءات تباشرها سلطة مختصة بالتحري والتحقيق عند وقوع جريمة بهدف البحث عن الأدلة التي تساعد على كشف الحقيقة التي تقودنا إلى المتهمين ومن ثم توقيع العقاب عليهم.

وقد شهد العقد الأخير من القرن العشرين غزوا تكنولوجيا أدى إلى ظهور اختراعات هائلة على المستوى التقني، من بينها ظهور الحاسبات الآلية التي أصبحت لها قيمة لما تحتوي عليه من معلومات يمكن تخزينها واسترجاعها في ثوان معدودة، مما سهل مختلف المعاملات التي شملت مختلف الميادين منها الميدان الاقتصادي، الاجتماعي، السياسي....الخ

إلا انه مع التقدم العلمي والتكنولوجي الذي مس مختلف مجالات الحياة، وجعل من العالم خلية مترابطة بشبكات إلكترونية حطمت الحواجز أمام التواصل بين الشعوب وسهلت المعاملات بين الأفراد من مختلف مناطق العالم، ظهر نوع جديد من الإجرام حيث أصبحت التقنيات الحديثة وسيلة لارتكاب مختلف الجرائم التقليدية في أسرع وقت دون أن تترك أي اثر يدل على المجرم وقد مرت هذه الجريمة بتطور تاريخي مصاحبا لتطور التقنية واستخداماتها حيث ظهر هذا النوع من الجرائم في بداية الستينيات بأول معالجة لما يسمى بالجريمة الإلكترونية على المقالات والمواد الصحافية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر، وقد ثار جدل حول ما إذا كانت هذه الأفعال مجرد سلوكيات غير أخلاقية في بيئة الحوسبة، أم أنها تكتسب الصفة الجرمية وبالتالي تعتبر أفعال يعاقب عليها القانون، ومع بداية السبعينيات اكتسبت الصفة

الإجرامية وذلك بعد إجراء عدة دراسات مسحية وقانونية اهتمت بالجرائم الإلكترونية وعالجت عددا من القضايا الفعلية.

وتكمن أهمية الموضوع في أن الجريمة الإلكترونية من الجرائم المستحدثة التي توجب الدراسة والتحليل أكثر، والتحقيق فيها يتطلب مهارات فنية وتقنية والخبرة في مجال الحاسب الآلي والانترنيت اللذين اعتبرا وسيلتين أساسيتين لارتكاب الجريمة الإلكترونية، وما يزيد الموضوع أهمية هو خطورة هذه الجريمة وانتشارها بسرعة رهيبة وعجز القوانين التقليدية على مواكبة هذه السرعة.

ومن الدراسات السابقة التي تناولت هذه الجريمة من حيث مفهوم الجريمة الالكترونية كتاب "الجريمة الالكترونية" للدكتورة غنية باطل، دراسة مقارنة لسنة 2015، حيث تناولت هذا الموضوع بشكل موسع وتطرقت إلى صور الجريمة وأركانها والعقوبات المقررة لها.

وكتاب الجوانب الاجرائية لجرائم الأنترنت للأستاذة نبيلة هبة هروال سنة 2007 حيث تناولت فيه ماهية جريمة الأنترنت واختصاصات الضبطية القضائية في مكافحة جريمة الأنترنت.

وكتاب مبادئ الإجراءات الجنائية لجرائم الكمبيوتر والانترنت للدكتور عبد الفتاح بيومي حجازي، الطبعة الأولى، 2006 وتناول هو الأخر موضوع إجراءات التحقيق في الجريمة الإلكترونية تفصيلا وتحليلا، حيث تطرق لمختلف المشكلات المتعلقة بالدليل الإلكتروني والمتعلقة بسلطات الاستدلال والتحقيق .

وبناءا على ما سبق فإن ما دفعني لاختيار هذا الموضوع هو رغبتي في التعرف على هذا النوع المستحدث من الإجرام الذي انتشر بصورة ملفتة في المجتمع الجزائري مؤخرا، ولأنها ترتبط بالتقنية الحديثة وتعتبر من سلبياتها لابد من أنها تتميز بمجموعة من الخصائص مقارنة مع باقي الجرائم التقليدية، مما يستدعي الوقوف ومعرفة إن كانت هناك إجراءات خاصة في مجال البحث والتحري، ومدى إمكانية تطبيق القوانين التقليدية لمواجهة الجريمة الإلكترونية كذلك دفعني الفضول لمعرفة بما يحكم به القاضي في مثل هذه الجرائم، إن كان يستعين بالنصوص التقليدية أم أن هناك قوانين خاصة يلجأ إليها ورغبتي في إزالة الغموض عن هذه الجريمة.

وتكمن إشكالية البحث في ما مدى قابلية تطبيق القواعد التقليدية لإجراءات التحقيق في جرائم الانترنيت ؟

- هل توجد أجهزة خاصة بالتحقيق فيها ؟

وللإجابة عن هذه الإشكالية قسمت البحث إلى فصلين:

الفصل الأول بعنوان: الأحكام العامة في الجرائم المعلوماتية (الأنترنت) حيث عالجنا فيه ماهية الجريمة المعلوماتية في المبحث الأول، والذي قسمناه بدوره إلى مطلبين خصصنا المطلب الأول لدراسة مفهوم الجريمة المعلوماتية وعرضنا أنواع الجرائم المعلوماتية في المطلب الثاني، أما المبحث الثاني من هذا الفصل فقد تناولنا فيه المواجهة الجنائية لجرائم الأنترنت، من حيث أركان جريمة الأنترنت في المطلب الأول وقمع الجريمة المعلوماتية في المطلب الثاني.

الفصل الثاني بعنوان: إجراءات المتابعة الجزائية في جرائم الأنترنت بينا في المبحث الأول، مرحلة البحث والتحري (مرحلة جمع الاستدلالات) من خلال الاجراءات التقليدية لجمع الدليل في المطلب الأول، والمطلب الثاني عالجنا فيه الإجراءات الحديثة لجمع الدليل الالكتروني، من التسرب واعتراض المراسلات والمراقبة الالكترونية، والمبحث الثاني لهذا الفصل تطرقنا إلى مرحلة التحقيق، حيث تكلمنا عن مفهوم التحقيق الجنائي وخصائه في الجريمة المعلوماتية، أما المطلب الثاني تناولنا فيه اجراءات التحقيق في الجريمة المعلوماتية.

وقد اعتمدنا على المنهج التحليلي المقارن في دراستنا هذه، لتبيان مفهوم كل من الجريمة الإلكترونية والتحقيق، ومناقشة الإجراءات المتخذة للتصدي لهاته الجريمة المستحدثة.

الفصل الأول

الأحكام العامة في جرائم الأنترنت

يشهد العالم الحديث تحديات كبيرة ومتزايدة نتيجة التطورات السريعة في شتى الميادين وعلى وجه الخصوص الميدان العلمي والتكنولوجي خلال الربع الأخير من القرن الماضي حيث أصبح الحاسب الآلي ركيزة أساسية في عصرنا الذي تطور دوره بحيث تعدى إجراء العمليات الحسابية المعقدة ليشمل قضايا في شتى مجالات الحياة المختلفة، فقد ترتب على هذه الآلة المتقدمة الكثير من الأمور والتطورات الايجابية حيث جعل العالم بمثابة قرية صغيرة لا يعترف فيها بالحدود الجغرافية وذلك من خلال استغلال الشبكات المتصلة بها حول المعمورة خاصة شبكة الانترنت، حيث سمحت هذه الأخيرة للناس بتبادل أخبارهم والحصول على أية معلومات يريدونها بسرعة فائقة وبدون صعوبات وفي منتهى السرية[1].

إلا أن هذه التقنية الحديثة لم تسلم من الاستغلال غير الشرعي لها، مما أدى إلى ظهور نوع جديد من الإجرام يسمى "الإجرام الالكتروني" والذي تنبثق عنه عدة تسميات من بينها: الجريمة الإلكترونية، المجرم الإلكتروني، الأدلة الرقمية، الجريمة المعلوماتية...الخ.

وهذه التقنية أدت إلى ثورة هائلة وانقلاب خطير لمفهوم الجريمة والجزاء في النظرية التقليدية، فقد ساعدت الأشخاص على ارتكاب جرائمهم بطرق ووسائل جديدة ، دون ترك أي أثر لهم ودون معاناة.

هذه الجريمة هي من الجرائم المستحدثة، التي توجب التنبه لمخاطرها وحجم الخسائر الناتجة عنها، وعليه سنتطرق لماهية الجريمة الإلكترونية في المبحث الأول مما يستوجب تحديد مفهوم الجريمة المعلوماتية وذلك من خلال تبيين أنواع الجرائم المعلوماتية وخصائصها.

أما المبحث الثاني فسأتعرض إلى المواجهة الجنائية لجرائم للأنترنت بالتطرق إلى أركانها وقمع الجريمة المعلوماتية.

[1] – بخيتي فاطمة الزهراء، إجراءات التحقيق في الجريمة الالكترونية، مذكرة ماستر في الحقوق، جامعة المسيلة، سنة 2004، ص6

المبحث الأول: ماهية جرائم الانترنت

أبرز القرن 20 من نوع آخر تتعلق بوسائل الاتصال وكسب المعلومات نتيجة التقدم الذي أحدثه العلماء والمكتشفون لوسيلتين هما: جهاز الكمبيوتر ووسيلة أخرى لكسب المعلومة والاتصال وهي الأنترنت، ويعبر عنه الفقهاء بقرن المعلوماتية نتيجة تدفق هذه المعلومات وانسيابها ووفرتها ولعل الجريمة الالكترونية واحدة من المتغيرات الكبيرة التي طرأت نتيجة التزاوج بين وسائل الاتصال والتكنولوجيا الحديثة[1] وفيما يلي تفصيل لمفهوم هذه الجريمة من حيث التعريف والخصائص والأركان.

المطلب الأول: مفهوم جرائم الانترنت

ظهرت تعابير كثيرة حول تعريف الجريمة الإلكترونية ما بين مضيق لمفهومها وموسع كما تعددت المصطلحات المستخدمة للدلالة عليها فالبعض استخدم مصطلح جرائم أو إساءة استخدام الحاسبات أو جرائم المعالجة الآلية للبيانات والبعض الآخر أطلق عليها اسم الإجرام المعلوماتي.

الفرع الأول: تعريف جرائم الانترنت

تعتبر الجريمة المعلوماتية من الظواهر الحديثة وذلك لارتباطها بتكنولوجيا حديثة، ولقد تعددت الجهود الرامية إلى وضع تعريف محدد جامع مانع لها، حيث لم يتفق الفقه على تعريف محدد بل إن بعض الفقهاء ذهب إلى ترجيح عدم وضع تعريف بحجة أن هذا النوع من الجرائم ما هو إلا جريمة تقليدية ترتكب بأسلوب الكتروني[2].

أولا/ تعريف جرائم الانترنت: قبل التعرف على **جرائم الانترنت** يجدر الإشارة إلى تعريف الجريمة العامة.

[1] – محمد أمين شوابكة، جرائم الحاسوب والأنترنت، ط1، دار الثقافة، عمان، 2004، ص06.

[2] – خالد ممدوح، امن الجريمة الإلكترونية، دار الجامعية الاسكندرية، 2008، ص41.

1-تعريف الجريمة العامة لغة:

الجريمة لغة: مأخوذة من الجرم وهي الذنب والجناية، جمعها جرائم، وجرم الشيء قطعه و جريمة الرجل على قومه وإليهم: أذنب وجنى جناية[1].

2- جريمة الانترنت:

الأنترنت في اللغة هي كلمة جديدة في القاموس اللغوي لمختلف لغات وهي كلمة انجليزية حركة مختصرة من مقطعين (Inter) وهي اختصار (International) ، وتعني دولي، و(net) وهي اختصار لكلمة (net work) وتعني الشبكة. وبجمع الكلمتين أي (international net work) فإن المعنى الكامل المتحصل عليه هو الشبكة الدولية، والأنترنت وفقا لبروتوكول مشترك، يسمح بسيرورة إرسال الوسائل المنقسمة إلى طرود مستقلة [2].

ثانيا: تعريف جريمة الانترنت فقها

انقسم الفقه إلى عدة آراء منهم من ضيق من مفهوم الجريمة الإلكترونية ومنهم من وسع من مفهومها.

أ/الفقهاء الذين ضيقوا من مفهوم جريمة الانترنت: ومن أنصار هذا الرأي مارو Merwe الذي عرف جريمة الانترنت بأنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"[3].

وعرفها ر. توت و أهردكتس Ahradcatst و R.tott " تلك الجرائم التي قد حدث في مراحل ارتكابها بعض عمليات فعلية داخل الحاسب"[4].

ب/الفقهاء الذين وسعوا من مفهوم جريمة الانترنت: ومن أصحاب هذا الرأي ميشال وكريدو Credo و Michal حيث عرفا الجريمة الإلكترونية بأنها "سوء استخدام الحاسب أو أنها جريمة تسهل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة إلى الحالات المتعلقة بالولوج غير

[1]-علي بن هادية، بلحسن البليشي، الجيلالي بن الحاج يحيى، القاموس الجديد للطلاب، الشركة الوطنية، الشركة التونسية الجزائر، تونس، ط1، 1979، ص251.

[2] - نبيلة هبة هروال ، الجوانب الاجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، 2007، ص06.

[3]-محمد أمين الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة ، عمان، ط1 ، 2007 ، ص08.

[4]-سميرة معاشي، ماهية الجريمة الالكترونية، مجلة المنتدى القانوني، العدد السابع، جامعة بسكرة، ص276.

المصرح به لحاسب المجني عليه أو بياناته، كما تمتد الجريمة الإلكترونية لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان وانتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق الكترونية وتزيف المكونات المادية والمعنوية للحاسب بل وسرقة جهاز الحاسب في حد ذاته أو أيا من مكوناته[1] ".

تعريفات تستند إلى موضوع الجريمة:

يرى أصحاب هذا الاتجاه أن جريمة الانترنت ليست هي التي يكون النظام المعلوماتي أداة ارتكابها بل هي التي تقع على النظام أو داخل نطاقه ومن أنصار ذلك التعريف روزن بلات الذي عرف جريمة الانترنت بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول للمعلومات المخزنة داخل النظام أو التي تحول عن طريقه[2] ".

4-تعريفات تستند إلى معرفة المفاعل بتقنية المعلومات:

كما عرفها دافيد تونبسون david thopson الذي عرفها بأنها " جريمة تتطلب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية النظام المعلوماتي[3] " .

ثالثا: التعريف القانوني لجريمة الانترنت

تطرقت معظم التشريعات الوطنية لتعريف جريمة الانترنت وفيما يلي ذكر لبعض التعريفات على سبيل المثال:

أ.تعريف المشرع الجزائري:

تبنى المشروع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة ويمثل نظام المعالجة الآلية للمعطيات المسألة الأولية أو الشرط الأولي الذي لابد من تحققه حتى

[1]- سميرة معاشي، المرجع السابق، ص276.

[2]-أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط2، 2006، ص85-86.

[3]أحمد خليفة الملط، المرجع السابق، ص86.

يمكن البحث في توافر أو عدم توافر أركان الجريمة من جرائم الاعتداء على هذا النظام فإن ثبت تخلف هذا الشرط الأولي فلا يكون هناك مجال لهذا البحث.

لم يتخلف المشرع الجزائري بدوره عن ركب التشريعات التي وضعت تعريفا لنظام المعلومات حيث أنه عرف من خلال نص المادة 2 من الفقرة من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مسميا إياه "المنظومة المعلوماتية" وهي أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة ، يقوم واحد منها أو أكثر معالجة الآلية للمعطيات تنفيذا لبرنامج معين".

جرم المشرع الجزائري الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثر الجزائر بالثورة المعلوماتي من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل وهذا 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 والذي خصص القسم السابع مكرر منه تحت عنوان : المساس بأنظمة المعالجة الآلية للمعطيات والذي تضمن 08 مواد من المادة 394 مكرر وحتى المادة 394 مكرر 7[1].

ب.تعريف المشرع الفرنسي:

عرف القانون الفرنسي رقم 19 لسنة 1988 أنماط الجريمة الإلكترونية وميز بين الاعتداء على برامج ومعلومات الحاسب الآلي، وبين الاعتداء على أدواته وآلاته و لم ينص على تجريم سرقة البرامج والمعلومات واعتبرها مالا معلوماتيا حيث حدد في جريمتي :

1- جريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات[1].

2-جريمة إتلاف برامج ومعلومات الحاسب الآلي الرقمي وبذلك تكون هذه الجرائم متعلقة بمحتوى الاسطوانة المغنطة أو الشريط المغنط.

[1] – بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائر، مذكرة لنسل شهادة ماستر، حقوق، جامعة بسكرة، سنة 2015-2016، ص31.

ج. تعريف المشرع الأمريكي :

حصر المشرع الأمريكي الجرائم الإلكترونية في الأفعال التالية:

1-**العبث بالحاسب الآلي** : حيث يرتكب الشخص جريمة العبث بالحاسوب الآلي إذا قام عن علم وبدون إذن من مالك الحاسوب الآلي بما يلي: يدخل أو يسبب الدخول إلى حاسوب أو أي جزء منه أو برامج أو بيانات، يدخل أو يسبب الدخول إلى حاسوب إلى أو أي جزء منه أو برامج ويحصل على بيانات أو خدمات، يدخل أو يسبب الدخول في حاسوب آلي أو أي جزء منه أو برامج أو بيانات ويتلف ويحطم الحاسوب الآلي أو يعدل أو يمحو أو يسحب برامج الحاسب الآلي أو البيانات[1]، وقد اصدر المشرع الأمريكي عدة قوانين في مواجهة الجريمة الإلكترونية من بينها قانون آداب الاتصالات 1996 يجرم فيه القذف والسب عبر شبكة الانترنيت كما وسع نطاق وحماية الأطفال بإصدار قانون لحمايتهم ضد الاستغلال الجنسي سنة 1998[2].

الفرع الثاني: تعريف شبكة الأنترنت

أنترنت كلمة انجليزية حركية مختصرة مكونة من مقطعين (Inter) وهي اختصار (International) ، وتعني دولي، و(net) وهي اختصار لكلمة (net work) وتعني الشبكة وبالتالي الأنترنت هي شبكة عالمية للمعلومات.

والأنترنت أو الشبكة العالمية للمعلومات عبارة عن شبكة ضخمة من الحواسب المتصلة فيما بينها حول العالم التي تتم من خلالها تبادل المعلومات، قد تكون هذه الشبكات محلية (Intra local) تربط مجموعة حواسيب قريبة من بعضها البعض وتشترك في المعدات المادية وتشترك أيضا في البرامج والبيانات فقد تجمع كل إدارة من إدارة المؤسسة أو شركة ضخمة حواسيبها في شبكة محلية وترتبك الحواسب المحلية عن طريق حاسوب واحد على الأقل يمتاز بالسرعة العالية وقدرة تخزين كبيرة.

[1]- سمير معاشي، المرجع السابق، ص277.

[2]- محمد أمين الشوابكة، المرجع السابق، ص18.

وهناك شبكات موسعة او عامة تربط طرفيات حواسيب منتشرة في مناطق جغرافية واسعة كالمدن والدول والقارات، وترتبط هذه الحواسيب مع بعضها عن طريق قنوات الاتصال مثل خطوط التلفون والمكروويف والأقمار الصناعية ويطلق عليها اسم شبكات تحمل البيانات العمومية[1].

أولا: الحواسيب ونظام الحواسيب (الكومبيوتر)

يعرف الحاسوب على أنه جهاز إلكتروني مصنوع من مكونات يتم ربطها وتوجيهها باستخدام أوامر خاصة لمعالجة وإدارة المعلومات بطريقة ما، وذلك بتنفيذ ثلاث عمليات أساسية هي استقبال البيانات المدخلة (الحصول على حقائق المجردة).

ومعالجة البيانات إلى معلومات (إجراء الحسابات والمقارنات ومعالجة المدخلات، وإظهار المعلومات المخرجة (الحصول على نتائج).

ونظام الحاسوب يمكن تعريفه على أنه مجموعة من الأجهزة المتكاملة تعمل مع بعضها البعض بهدف تشغيل مجموعة من البيانات المدخلة وفقا لبرنامج موضوع مسبقا للحصول على نتائج معينة.

وهناك تعريف أخر (مجموعة من الأجهزة الالكترونية تقوم بصورة أوتوماتيكية باستقبال البيانات وخزنها ومعالجتها واستخراج النتائج تحت سيطرة تعليمات مخزنة فيها).

ويطلق على مجموعة الأجهزة التي تشكل الكيان المادي الملموس لنظام الحاسوب لفظ (Hardware) أي المعدات ويطلق على مجموعة الأوامر والتعليمات لفظ (software) أي البرمجيات، وهذه المعدات والبرمجيات لا قيمة لها دون وجود المستخدمين وهم الأشخاص الذين يتعاملون مع البرمجيات لتحقيق أهداف خاصة[2].

ثانيا: نظام المعلوماتية

تأخذ المعلومات عدة معاني منها:

[1] – نهلة عبد القادر مامون، الجرائم المعلوماتية، دار الثقافة، ط2، الأردن، 2010، ص34.

[2] – نهلة عبد القادر مامون، مرجع سابق، ص20.

1- المعلومات هي المعنى الذي يستخلص من البيانات عن طريق العرف أو الاتفاق أو الخبرة أو المعرفة. وقد اقترح الأستاذ catala تعريف للمعلومات بأنها : رسالة ما يعبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير.

وعرفها المشرع الفرسي وفقا للقانون 82-652 الصادر في 26 جويلية 1982 بأنها " صوت أو صورة أو مستند أو معطيات أو خطايا أيا كانت طبيعتها"[1]

ويرى البعض أنها على أنها أحد عناصر المعرفة التي يتصل بها الغير من خلال وسيلة مناسبة لنقله أو تسجيلها أو معالجتها وتأخذ شكل رسالة يمكن نقلها إلى الغير من خلال وسيلة معينة[2].

المطلب الثاني: تصنيف الجرائم (أنواع الجرائم)

من الصعب تصنيف الجرائم الالكترونية نظرا لاختلافها من مجتمع لآخر من حيث تطوره، ومدى استخدامه للحاسوب، ودرجة اعتماده عليه في مختلف جوانب الحياة، وقد أوجد مشروع الاتفاقية الأوروبية لعام 2001 تقسيما جديدا نسبيا لجرائم الكمبيوتر والانترنت يقسمها إلى أربع طوائف، مع ملاحظة أنها تستثني الجرائم المتعلقة بالخصوصية لوجود اتفاقية أوروبية مستقلة.

1-الجرائم التي تستهدف سلامة وسرية عناصر المعطيات والنظم: وتضم (الدخول غير القانوني، الاع تراض غير القانوني، تدمير المعطيات، اعتراض النظم).

الجرائم - المرتبطة بالكمبيوتر وتضم (التزوير المرتبط بالكمبيوتر، الاحتيال المرتبط بالكمبيوتر).

3-الجرائم المرتبطة – بالمحتوى: وتضم (طائفة واحدة وفق هذه الاتفاقية، وهي الجرائم المتعلقة بالأفعال الإباحية وغير الأخلاقية).

4- الجرائم المرتبطة بالأشخاص والأموال: وتضم (السرقة والاحتيال والتزوير، والإطلاع على البيانات الشخصية، المعلومات المضللة والزائفة، أنشطة الاعتداء على الخصوصية، إساءة

[1] – بعرة سعيدة، مرجع سابق، ص08.

[2] – غنية باطلي، الجريمة الالكترونية دراسة مقارنة، منشورات الدار الجزائرية، الجزائر، 2005، ص59.

استخدام المعلومات، القرصنة، بث البيانات من مصادر مجهولة، الإرهاب الالكتروني ...وغيرها من الجرائم.

ويصنف الفقهاء والباحثون جرائم الحاسوب والانترنت ضمن فئات عديدة، ولكن على العموم يمكن تقسيمها إلى مجموعتين أساسيتين:

المجموعة الأولى :جرائم تقع على الانترنت .

المجموعة الثانية :جرائم تقع بواسطة الانترنت

الفرع الأول: تصنيفات الجريمة المعلوماتية

المجموعة الأولى: الجرائم التي تقع على الانترنت

أي أن الشبكة تكون عنصر سلبي في الجريمة أي محل للجريمة فقط، فإن هدف المجرم ينصب حول البيانات والمعلومات المخزنة والمنقولة عبر قنوات الانترنت الخاصة أو العامة أو اختراق الحواجز الأمنية إن وجدت والاعتداء على الأموال...الخ.

1 الكسب السهل:

أصبح لبرامج المعلومات قيمه غير تقليديه لاستخداماتها المتعددة في كافة المجالات الاجتماعية، والاقتصادية فهذه القيمة المميزة لبرامج المعلومات تجعلها محلا للتداول، وهنا تبدو أهمية الإنترنت بصفته مصدرا للمعلوماتية، مما أدى إلى ظهور قيمة اقتصاديه جديدة وأموال جديدة، عرفت بالأموال المعلوماتية، وصاحب ظهور هذا المال المعلومات جرائم جديدة عرفت بالجرائم المعلوماتية وهذه الجرائم يمكن تصورها من زاويتين[1]:

الأولى: تكون المعلوماتية أداة أو وسيلة للاعتداء.

الثانية: تكون المعلوماتية موضوعا للاعتداء (أي سرقة تلك المعلومات).

كما تتضمن جرائم نظم المعلومات كذلك جريمة إساءة استخدام المعلومات، والمقصود بها الأذى الذي يتم تحقيقه باستخدام هذه المعلومات، مثل عدم تمكين المستفيد من الوصول إليها، أو

[1] – غنية باطلي، المرجع السابق، ص61.

كشفها، أو استغلالها في إلحاق الضرر بمصالح صاحب المعلومات وتشمل جرائم الملكية الفكرية نسخ البرامج غير القانوني، والسرقة والاتجار بالأسرار التجارية، كما تشمل جرائم النسخ غير القانوني للمعلومات أو حيازة المعلومات بطريقة غير قانونية، وتوزيع المواد ذات حقوق النشر بما في ذلك الصور في الصيغة الإلكترونية والمطبوعة، والمواد المرئية والسمعية والمخزنة على شرائط أو أقراص مرنة، أو أقراص مدمجة أو على الحاسب.

الدخول على المواقع المحجوبة باستخدام (البروكسي):

"البروكسي" هو برنامج وسيط يقوم بحصر ارتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز موحد، والمعنى المتعارف عليه لدى مستخدمي الانترنت" للبروكسي "هو ما يستخدم لتجاوز المواقع المحجوبة، والتي عادة ما تكون إما مواقع جنسية أو سياسية.

جرائم الاختراق:

هي عملية اقتحام الأنظمة أو الشبكات الخاصة بأفراد أو منظمات خاصة أو حكومية بمساعدة بعض البرامج المتخصصة في فك وسرقة كلمات السر، وتصريحات الدخول بهدف الاطلاع على المعلومات أو تخريبها أو سرقتها أو تخريب الأجهزة وتعطيلها كما أن أبرز ضحايا الاختراق هي مواقع الأنترنت التي يقوم المخترقون بتحريف تصاميمها ومعلوماتها وهذه العملية تسمى Defacing وهناك أساليب المستخدمة في عمليات الاختراق[1].

الاقتحام أو التسلل:

يشمل الاختراقات سواء للمواقع الرسمية أو الشخصية، أو اختراق الأجهزة الشخصية واختراق البريد الإلكتروني، أو الاستيلاء عليه، والاستيلاء على اشتراكات الآخرين وأرقامهم السرية.

ب–الاغراق بالرسائل: سرعة وسهولة إرسال المعلومات والبيانات بواسطة الشبكة العنكبوتية إلى عدد هائل من المستقبلين سهل كثيرا من أنواع الاحتيال، وأصبح البريد الإلكتروني أكبر وسيلة لانتشار الشائعات في الانترنت عن طريق ما يسمى بالرسائل المتسلسلة.

[1] – بعرة سعيدة، مرجع سابق، ص13.

ج–الفيروسات: الفيروسات هي في الأصل برامج أعدها شخص أو أشخاص بهدف تخريب وشطب البيانات من ذاكرة الحاسوب، وهي مبرمجة بحيث تعمل من خلال برامج أو برنامج آخر ولها القدرة على نسخ ذاتها، وأبرز طرق انتشارها البريد الإلكتروني أو البرامج التي يتم تحميلها من الانترنت، ويمكن أشخاص نشر الفيروسات بأصنافها مع ملفات ترسل بالبريد الالكتروني بهدف التخريب[1]

ويمكننا تصنيف البرمجيات الماكرة إلى أربعة أنواع رئيسية هي:

1- الفيروسات viruses

2- الدود: Worms

3- أحصنة الطروادة: Trojan horses

4- برامج الانزال: Droppers

4–المواقع المعادية:

أ/المواقع السياسية المعادية: الغرض من إنشائها هو معارضة النظام السياسي القائم في بلد ما والهدف منها تسبيب الفرقة بين الشعب ونظامه السياسي ويتم تلفيق أخبار ومعلومات غير حقيقة ويعمد أصحاب هذه المواقع إلى إنشاء قاعدة بيانات بعناوين أشخاص يحصلون عليها من الشركات التي تبيع قواعد البيانات.

ب–المواقع الدينية المعادية: بعض المواقع التي تدعي أنها مواقع دينية اسلامية ولكن ما إن يدخل المستخدم إلى الموقع حتى يفاجأ بأنه موقع إباحي، أو موقع تنصيري ويبث أفكارا هدامة مخالفة للشريعة وتسيء للدين.

ج–المواقع المعادية للأشخاص أو الجهات: وهي المواقع التي تمس رموز الشعوب سواء كانت تلك الرموز فكرية أو سياسية ودينية وتشكيك الناي في مدى مصداقية هؤلاء الأفراد وذلك بالتشهير والسب والقذف والتصنت والتقاط الصور للأشخاص من مختلف القطاعات الاجتماعية والفكرية والدينية دون رادع أو خوف.

[1] – ياسمينة بونعارة، الجريمة الالكترونية، بحث (شبكة الأنترنت)، جامعة الأمير عبد القادر للعلوم الاسلامية، ص 14-16.

5-جرائم القرصنة: يشير مفهوم القرصنة إلى ممارسات غير مشروعة تستهدف التحايل على نظام المعالجة الآلية للمعطيات بغية اتلاف المستندات المعالجة إلكترونيا وذلك من خلال قرصنة الكتابة أو استخدام برامج الكمبيوتر الجاهزة وهدف القرصنة الالكترونية تحقيق مكاسب مالية شخصية مثل سرقة معلومات بطاقات الائتمان تحويل الأموال من حسابات مصرفية إلى حساب المقرصنين.

6-جرائم التجسيس الالكتروني: التجسيس الالكتروني هو اختراق أجهزة ويقوم بعمليات الحسيس على المستخدم بطرق غير شرعية ولأغراض غير سوية لسرقة معلومات تتعلق به سواء على الصعيد الشخصي او السياسي أو لسرقة حسابه او بهدف معرفة معلومات تتعلق بالجانب المادي[1].

7- **الإرهاب الإلكتروني:** يعرف الإرهاب الإلكتروني بأنه العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه أو عرضه أو عقله أو ماله، فتكنولوجيا المعلومات أفادت الجماعات الارهابية وذلك من خلال تبادل المعلومات بين المنظمات الارهابية المختلفة وكذلك أنشأت مواقع لتعليم صناعة متفجرات، طرق اختراق البريد الالكتروني وكيفية دخول إلى المواقع المحجوبة وطريقة نشر الفيروسات.

ثانيا: المجموعة الثانية: جرائم تقع بواسطة الأنترنت: أي أن الشبكة تكون أداة إيجابية لارتكاب الجريمة فتسهل للمجرم المعلوماتي تحقيق غايته، ويلاحظ أن أغلب صورها في هذه الحالة تشكل جرائم الواقعة على الأشخاص.

1-الجرائم الجنسية والممارسات غير الأخلاقية: تستهدف هذه الجرائم فضح الأسرار الشخصية أو القذف أو تشهير بشركات أو أشخاص بقصد الاضرار بالسمعة الشخصية أو المالية، إما بسبب المنافسة أو بداعي الانتقام بالإضافة إلى تجارة الدعارة والصور الخليعة لمشاهير وكذلك أطفال.

[1] - ياسمينة بونعارة، المرجع السابق، ص 16-20.

2-الجرائم المالية:

أ/جرائم السطو على أرقام البطاقات الائتمانية:

ومن الجرائم التي ترتكب باستخدام التكنولوجيا سرقة الأقراص الصلبة والمرنة بغرض الحصول على المعلومات التي تحويها ويتولى قراصنة المعلومات بيعها، وتعد عمليات سطو على بطاقات الائتمان أحدث أنماط السلوك الاجرامي التي ارتبطت بشبكة الأنترنت من بنوك مؤسسات مالية وأفراد[1]..

ب-القمار عبر الأنترنت: مع ظهور شبكة الأنترنت ظهرت صيحات القمار يتمثل في مواقع ويب تم تصميمها على طراز كازينوهات لاس فيغاس أمريكية وتتوفر على جميع أنواع القمار وأنواعه، وقد حاول المشرع الأمريكي تحريك مشروع قانون لمنع المقامرة عبر الأنترنت[2]،

ويقوم بها رجال الأعمال.

ج-تزوير البيانات: يتم تزوير البيانات الحاسب إما بإدخال بيانات مغلوطة إلى قواعد البيانات أو بتعديل البيانات الموجودة عمدا مثل أرصدة الحسابات وتزويد المعاملات والتخريب والسرقة المخزون والمرتبات، باستخدام بعض البرامج المساعدة الجاهزة المصممة خصيصا لتعديل البيانات في مكانها مباشرة.

د-الجرائم المنظمة: الجريمة المنظمة هي عنف منظم قصد الحصول على مكاسب مالية بطرق وأساليب غير مشروعة وتمارس الجريمة المنظمة على شكل نصب واحتيال وتزوير وسطو وخطط من أجل الابتزاز والقتل وتنفذ بعد تدبير وتنظيم.

هـ-تجارة المخدرات عبر الأنترنت: يتم استخدام الأنترنت في مختلف المجالات ومنها المجال الأمني وكذلك سعن جماعات الإجرام المنظم عبر العالم لاستغلال الأنترنت في مختلف أنشطتها[3].

[1] - سعيد مبروك ابراهيم، المكتبة الجامعية وتحديات مجتمع المعلومات، دار الوفاء للطباعة والنشر، الاسكندرية، ط1، 2009، ص88.

[2] - محمد علي قطب، موقف الشارع الاسلامي من جرائم الأخلاق عبر الأنترنت، مركز الاعلام الأمني، جامعة نايف العربية للعلوم الأمنية، ص4 www.nauss.adu.sa

[3] - ياسمينة بونعار، مرجع سابقن ص25.

2-غسيل الأموال: ويعد غسيل الأموال إحدى صور الجرائم الاقتصادية وهو ظاهرة ترتبط بالجريمة العالمية المنظمة وعلى الأخص جرائم المتاجرة بالمخدرات، الإرهاب الدولي، تهريب الأسلحة، الغش والتزييف، الفساد السياسي والفساد الإداري والمالي، وتعد جريمة غسيل الأموال اليوم من المشاكل العالمية التي تحظى باهتمام معظم الدول المتقدمة والنامية على حد سواء وإن كان بدرجات متباينة في الأهمية.

3-قيادة الجماعات الإرهابية عن بعد: إن من أهم دوافع الجرائم المعلوماتية التي برزت بشكل كبير في العصر الحديث هي الدوافع الإرهابية، نظرا لسهولة استخدام التقنيات الحديثة، وخدمتها للمنظمات الإرهابية عن طريق تسهيل الاتصال والتواصل بين قياداتها وأعضائها، ونقل الأفكار والمعتقدات والآراء، وتلقي الأوامر وتمرير المعلومات والتعليمات، والوسائل الأخرى التي تساعد على ارتكاب الجرائم الإرهابية.

كما استغلت مواقع التواصل الاجتماعي لتمرير بعض الرسائل والخطابات، تويتر مثلا كانت أداة فعالة في يد الإرهابيين استخدموه كوسيلة للحصول على معلومات حول ما تم إعداده لهم من طرف القوات الأمنية، ووسائل التواصل الاجتماعي الجديدة يمكن أن تستغل من طرف الإرهابيين في التخطيط لهجماتهم الإرهابية.

5-البطاقات البنكية:

إن الأشخاص الذين يقومون بالتحايل واستخدام الحاسب الإلكتروني للسرقة تنقصهم الأمانة، حيث يعمدون إلى استخدام الحاسبات العائدة لأصحاب العمل لارتكاب جرائمهم، فقد يقومون مثلا بتغيير أرقام سجلات الحسابات بحيث تصبح أقل من المجموع الفعلي للحسابات الموجودة، ثم يتم الاستيلاء على المبلغ الذي يتم طرحه من هذه الحسابات، أو استخدام بطاقات مزورة يتم عند استخدامها نقل الأموال من حسابات الزبائن الآخرين إلى حساب سارق الأموال، عمليات الاحتيال هذه لا تكون مقصورة على المصارف أو مؤسسات الأعمال، وإنما يمكن أن تحصل في أية جهة تعتمد في عملها على الحاسب[1].

[1] - ياسمينة بونعارة، المرجع السابق، ص 25-27.

الفرع الثاني: خصائص جريمة الانترنت والمجرم المعلوماتي

أولا: خصائص جريمة الانترنت:

جرائم الانترنت كما سبق ذكره هي تلك الجرائم العابرة للحدود والتي تقع إما على شبكة الأنترنت او بواسطتها من قبل شخص على دراية فائقة بها.

باستقرائنا لهذا التعريف تتضح لنا الخصائص التي تتميز بها جرائم الأنترنت والتي يمكن حصرها فيما يلي:

أولا: الحاسب الآلي هو أداة ارتكاب جرائم الأنترنت

تعتبر هذه الخاصية من أهم الخصائص التي تميز جرائم الأنترنت عن غيرها من الجرائم الأخرى لا سيما التقليدية، ذلك لأن شبكة الأنترنت هي احدى التقنيات الحديثة التي أفرزها تطور الحوسبة، ولذلك فإن ارتباطها بالحاسب الآلي هو أمر لا مفر منه، باعتباره النافذة التي تطل بها تلك الشبكة على العالم الخارجي، وإن كنا اليوم تعاصر إمكانية استعمال الأنترنت عبر الهاتف الخلوي.

ثانيا: الجرائم ترتكب عبر شبكة الأنترنت او عليها

تعد شبكة الأنترنت الحقل الذي تقع فيه جرائم الأنترنت، وذلك لأنها تمقل حلقة وصل بين كافة الأهداف المحتملة لتلك الجرائم، كالبنوك والشركات الصناعية وغيرها من الأهداف التي تكون غالبا الصحية لها، إلا أنها وبالرغم من كونها الوسيلة لارتكاب جرائم الأنترنت إلى جانب الحاسب الآلي، فإنها كذلك لم تنج من يد المجرمين، لأنه هي الأخرى قد تكون محلا لاعتداءات[1].

ثالثا: مرتكب جرائم الأنترنت هو شخص ذوي خبرة فائقة في مجال الحوسبة

تتطلب جرائم الأنترنت على غرار الجرائم التقليدية فرقة فنية عالية سواء عند ارتكابها أو عند العمل على عدم اكتشافها من الشخص الذي يرتكبها، أي يجب أن يكون ذلك الشخص خبيرا بالقدر اللازم والكافي بأمور الحوسبة والأنترنت.

[1] نبيلة هبة هروال، الجوانب الاجرائية لجرائم الأنترنت، دار الفكر الجامعي، 2007، ص35-40

ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي وان الشرطة تبحث أو ما تبحث عن خبراء الكمبيوتر عند ارتكابها هذا النوع من الجرائم.

رابعا: جريمة الأنترنت جريمة عابرة للحدود الدولية

لقد سبق وان ذكرنا ان شبكة الأنترنت لها طابع دولي ، إذ أنها لا تعترف بتلك الحدود القائمة بين الدول سواء الجغرافية أو السياسية، وهذا ما أدى إلى اعتبار الجرائم المعلوماتية من الجرائم الدولية، وكذا من الجرائم ذات البعد الدولي، وتأخذ جرائم الأنترنت بعدا دوليا، من حيث امكانية أن يكون العمل الاجرامي عبر الأنترنت من طبيعة عالمية، وذلك حينما يرتبك داخل دولة إلا أنها تمتد إلى خارج اقليم تلك الأخيرة، مما يعني خضوعها لأكثر من قانون جنائي كما هو الشأن في جرائم المخدرات والإرهاب والتجسس الاقتصادي وغسيل الأموال.

كما أنها قد تأخذ ذلك البعد في الحالة التي يعترف بها المشرع الدولي بأن العدوان يمكن أن تقوم به دولة ولو في صيغة تأييد، مثلما قامت به عصابات الكيان الصهيوني من دعوة لاجتماع الهكرة في مؤتمر عالمي في شهر ماي سنة 2000 في فلسطين المحتلة.

وتعتبر جريمة الأنترنت جريمة دولية في الحالة التي يكون أحد أطرافها شخصا دوليا كما حدث في التجسس الذي قامت به الولايات المتحدة إذ استخدمت الأسلحة المعلوماتية وذلك عن طريق انتهاك انظمة حاسوب أعدائها أثناء القصف الجوي للحلف الأطلنطي **Nato** في كوسوفو[1].

ثانيا: المجرم المعلوماتي:

تتطلب الجريمة الإلكترونية مهارة فنية عالية على عكس الجرائم التقليدية التي يمكن أن يرتكبها أي شخص وحتى الأمي، ذلك أنه لا يرتكب الجريمة الإلكترونية إلا شخصا ذو خبرة بأمور الحاسب الآلي والانترنيت وقبل التطرق لخصائص الجريمة الإلكترونية، يجدر ذكر خصائص المجرم الإلكتروني التي تميزه عن المجرم العادي.

[1] نبيلة هبة هروال، مرجع سابق، ص40.

1-خصائص المجرم المعلوماتي:

حتى يحقق الجزاء الجنائي غايته سواء في مجال الردع العام أو الخاص لا بد من ان يوضع في الحسبان شخصية المجرم الذي ينبغي إعادة تأهيله اجتماعيا حتى يعود مواطنا صالحا للمجتمع، ويمكن القول أن الجاني في الجريمة المعلوماتية يتمتع بقدرة كبيرة من الذكاء.

وما يميز المجرم الإلكتروني عن المجرم العادي أنه عائد للإجرام، حيث يعود كثير من مجرمي المعلومات إلى ارتكاب جرائم أخرى في مجال الكمبيوتر انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم وتقديمهم إلى المحكمة في المرة السابقة، مما يؤدي إلى العود.

كما يتميز المجرم الالكتروني بأنه غير عنيف ذلك أنه ينتمي إلى إجرام الحيلة فهو لا يلجأ إلى العنف في ارتكابه للجرائم[1]، بالإضافة إلى ذلك هناك سمات خاصة بالمجرم المعلوماتي.

حيث يتمتع بالمهارة والمعرفة بتقنيات الحاسوب والأنترنت، بل إن بعض مرتكبي هذه الجرائم هم من المتخصصين في مجال معالجة المعلومات آليا فتنفيذ الجريمة المعلوماتية بتطلب قدرا من المهارة لدى الفاعل التي قد يكتسبها عن طريق الخبرة أو الدراسة في هذا المجال[2].

المجرم المعلوماتي انسان اجتماعي:

فهو عادة اجتماعي قادر على التكيف في بيئة اجتماعية ويتمتع بثقة كبيرة في مجال عمله، فالمجرم المعلوماتي يتميز بأنه لا يخضع نفسه في حالة عداء مع المجتمع المحيط به.

المعرفة: تتمثل في معرفة كافة الظروف التي تحيط بالجريمة المراد ارتكابها وكذا امكانية نجاحها واحتمالات فشلها، فالجناة عادة يمهدون بأشياء غير متوقعة من شأنها افشال افعالهم والكشف عنهم[3].

السلطة: المجرم المعلوماتي يتمتع بسلطة تجاه النظام المعلوماتي ويقصد بالسلطة الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي فالكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشر

[1] – عبد الفتاح بيومي حجازين مكافحة جرائم الأنترنت، دار الفكر الجامعي، الاسكندرية، ط1، 2006، ص83-86.

[2] – محمد امين شوابكة، جرائم الحاسوب، مرجع سابق، ص77.

[3] – بخيتي فاطمة الزهرة، المرجع السابق، ص16.

في مواجهة المعلومات محل الجريمة، وقد تتمثل هذه السلطة في الشيفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة، كفتح الملفات وقراءتها وكتابيتها ومحتوى المعلومات أو تعديلها[1].

[1] – محمد أمين الشوابكة، مرجع سابق، ص79.

المبحث الثاني: المواجهة الجنائية لجرائم الأنترنت

إن الجريمة هي نتيجة الأفعال المادية الصادرة عن الإنسان وهذه الأفعال تختلف حسب نشاطات الإنسان، وهذا ما جعل المشرع يتدخل لتجريم الأفعال الضارة بموجب نص قانونية يحدد فيه الفعل الضار أو المجرم والعقوبة المقررة لارتكابه[1]

وفي هذا المبحث نتطرق إلى أركان الجريمة المعلوماتية التي تنقسم بدورها إلى 03 أركان، الركن الشرعي، الركن المادي والركن المعنوي، هذا في المطلب الأول، أما فيما يخص العقوبات فقد أدرجناها ضمن مطلب ثان تحت عنوان قمع الجريمة المعلوماتية.

المطلب الأول: أركان الجريمة

لا تختلف جريمة الأنترنت عن أي جريمة أخرى، إذ أنها تتطلب لتحقيقها الأركان المتفق على ضرورة توفرها في أي جريمة لكي تتواجد على أرض الواقع، بالإضافة إلى ضرورة تواجد الشرط المبدئي في كل جريمة أي النص الشرعي المجرم أو الصفة غير مشروعة، فإنه لا بد من وجود الركنين: اللذين تتألف منهما كل جريمة الركن المادي والركن المعنوي[2].

الفرع الأول: الركن الشرعي لجريمة الأنترنت

إن ظهور شبكة الأنترنت ادى إلى تطور ظاهرة الإجراء بشكل خطير في تفشي جريمة الالكترونية وازداد هذا الوضع خطورة خاصة حيث أصدر المجلس الأوربي سنة 1989 توصية لتشجيع دول الأعضاء على تبني نصوص عقابية خاصة بجريمة المساس بأنظمة المعالجة الآلية للمعطيات وقد اختلفت في اختبار التقنية التشريعية المناسبة، فمنها من قام بإدماج النصوص العقابية المتعلقة بالإجرام المعلوماتي في قانون العقوبات التقليدي، ومنها من قام بوضع قانون جنائي مستقل للمعلوماتية يدخل في القانون الجنائي التقني وتستمد الجرائم المعلوماتية شرعيتها من مختلف التشريعات الوطنية الصادرة بشأن الجريمة المعلوماتية فقد بذلت هيئة الدول بوضع تشريعات لتصدي ومواجهة ومكافحة جرائم الإلكترونية[3] وتعزيز التعاون الدولي في هذا المجال ومثال ذلك:

---

[1] – أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة ، الجزائر، طبعة 2010-2011، ص27.

[2] – نبيلة هبة هروال، المرجع السابق، ص41.

[3] – بعرة سعيدة، المرجع السابق، ص44.

أ/على المستوى الوطني:

لقد تناولت معظم التشريعات الوطنية نصوص مستحدثة تكفل مواجهة هذا التطور من الإجرام ومنها على سبيل المثال:

1- **التشريع الفرنسي:** تناول المشرع الفرنسي جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في الباب الثالث من القسم الثاني من قانون العقوبات الجديد وهي تضم المواد 1/323 إلى 7/323.

2- **التشريع التونسي:** أصدر سنة 2000 قانون التجارة والمبادلات الإلكترونية حيث عالج أحكام العقد والمعاملات الإلكترونية، كما عالج الجرائم التي تقع على هذه التجارة والمعاملات الإلكترونية، حيث جاء في الباب الأول منه أحكام عامة للمبادلات والتجارة الإلكترونية ، والباب الثاني تناول أحكام تخص الوثيقة الإلكترونية والإمضاء الإلكتروني، أما الباب الثالث فقد بين فيه المشرع الوكالة الوطنية للمصادقة الإلكترونية، والباب السادس منه تناول حماية المعطيات الشخصية.

3- **التشريع الجزائري:** نظرا لأن المعلوماتية أصبحت من وسائل ارتكاب الجرائم، تدخل المشرع الجزائري لمواكبة هذا التطور بأن عدل قانون العقوبات من خلال القسم السابع منه، حيث تناول جرائم المساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 39 مكرر7 من قانون العقوبات[1].

ب/على مستوى الدولي:

التوصية رقم 9 (89) R المتعلقة بالجرائم المرتبطة بالحاسب الآلي التي أصدرها المجلس الأوربي والاتفاقية التي تخص الإجرام المعلوماتية أو السيبيري الموقعة في نوفمبر سنة 2001 ببودابست ، ودخلت حيز التنفيذ في جويلية سنة 2004 وصادقت عليها بعض أعضاء المجلس الأوربي بالإضافة إلى كندا واليابان والولايات المتحدة الأمريكية وجنوب إفريقيا حيث جعل منها وثيقة دولية ملزمة بالنسبة للدول الأطراف فيها.

[1] - يحي فاطمة، مرجع سابق، ص 32-34.

مؤتمر الأمم المتحدة السابع الذي انعقد في ميلانو ايطاليا 1985 حيث قام بدراسة حماية نظم المعلومات والاعتماد على الحاسب الآلي وتوصل إلى مجموعة من المقترحات والتوصيات لمكافحة الجريمة (الالكترونية) فقد أكد المؤتمر على وجوب تطبيق تطورات جديدة في مجال العلم والتكنولوجيا واتخاذ تدابير ملائمة ضد حالات اساءة استعمال تكنولوجيا وأكد المؤتمر عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي ترم الجريمة الالكترونية باعتبارها نمطا من انماط الجريمة المنظمة كغسيل الأموال، الاحتيال المنظم، حيث تضمن عمل لبرنامج عالمي لمنع الجريمة المنظمة وتقديم المساعدة التقنية للبلدان النامية[1].

ج/على مستوى الجهود العربية:

فقد اعتمد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد ًقانونا نموذجيا بموجب القرار 229 لسنة 1996 حيث تناول الجريمة الإلكترونية في الفصل التاسع منه بعنوان الاعتداء على حقوق الأشخاص الناتج عن المعالجات المعلوماتية، حيث جاء في المادة 461 من هذا الفصل صور للجريمة الإلكترونية وعقوبة التحريض على هاته الجريمة في الفقرة الأولى والثانية، والفقرات الثالثة والرابعة من نفس المادة والمواد 462-463 أما المادة 465 عاقبت على الاشتراك في الأفعال تشكل الجريمة الإلكترونية بنفس عقوبة الفاعل الأصلي، والمادة 466 عاقبت على الشروع في ارتكاب الجريمة الإلكترونية بذات عقوبة الفاعل الأصلي[2].

ويطرح الركن الشرعي عدة إشكالات قانونية هامة منها ما يتعلق بالموقع أي مكان هذه الجرائم وكذا إشكالية الطريقة أو المصطلحات التقنية التشريعية المناسبة لها[3].

إشكالية المكان (الموقع): والمقصود من ذلك هو هل يوجد مكان لهذه الجرائم في القانون الجنائية التقليدي؟ أم أن الأمر يحتاج إلى قانون خاص؟

فيما يتعلق بدمج النصوص الجديدة في القانون الجنائي التقليدي وتبعا للطريقة المستعملة من طرف مراجعي القانون الجنائي والذين اتفقوا على الإلمام بكل الجرائم في الوسيلة الوحيدة المتمثلة

[1] - http://www.moi.gov-qa/unccpckdoha/arabic/previous congresses: html أطلع عليه بتاريخ 2019/03/03 الساعة 19.11

[2] – مذكرة توضيحية للقانون الجزائي العربي الموحد، جامعة الدول العربية، ج2، رقم 292 بتاريخ 1996/11/19.

[3] – الأمر رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 156/66 الموافق لـــ 08 جوان 1966 المتضمن قانون العقوبات.

في القانون الجنائي الفرنسي، إلا أنه غيروا الصياغة فيما بعد بحيث أنهم لم يتفقوا على دمج هذه الجرائم ضمن الكتاب الثالث المخصص (للجنايات والجنح ضد الأموال) أو إحالة كل النصوص الجنائية إلى الكتاب الخامس تحت عنوان "الجنايات والجنح الأخرى).

إن الحل المتمثل في قانون خاص – أي الكتاب الخامس من القانون الجنائي – يترتب عليه وبدون شك الحد من هذه الجريمة، والذي يعد ظاهرة جديدة للقانون الجنائي التقني – بعض التشريعات تركت قمع هذه الجريمة خارج القانون الجنائية.

ولكن أغلب التشريعات أدمجت النصوص الجديدة في قوانينها الجنائية سواء في الولايات المتحدة الأمريكية وكندا.

وللدمج ضمن النصوص الجنائية القديمة لدينا عدة فرضيات وآراء:

فهناك من يقول بإدماجها ضمن جرائم الأموال باعتبارها أنه يمكن اصباغ صفة المال على الكيانات المادية والمعنوية للحاسوب.

والبعض الآخر فضل إدماجها في إطار الجزء الخاص بالجرائم ضد الملكية أن الكيان المادي للحاسوب قابل للتملك، كما ان الكيان المعنوي يدخل الملكية الفكرية.

وهناك من يرى بإضافة جزء خاص بالجرائم الالكترونية مستقل عن الأجزاء التقليدية باعتبار أن هذه الجرائم تتعلق بقيمة اقتصادية جديدة لها طابع خاص، وهناك من يرى أنه من الأفضل إلحاق كل جريمة الكترونية بما يقابلها في قانون العقوبات التقليدي مثلا: جرائم التزوير المعلوماتي في باب تزوير المحررات والاعتداء على المعطيات ضمن جريمة الاتلاف[1].

اشكالية الطريقة (المصطلحات): تعتبر الطريقة أو المصطلحات التقنية من الاشكاليات الصعبة والمعقدة التي تطرحها مواجهة أو قمع الجريمة الالكترونية نظرا لغموض مفهومها باعتبارها مصطلح غريب عن لغة القانون.

بالنسبة للإشكالية التي يطرحها الركن الشرعي لجريمة الأنترنت يختلف موقف التشريعات في تحديد تعريف المصطلحات التقنية في الدول الانجلوساكسونية التي تعتمد على طريقة إعطاء

[1] – غنية باطلي، المرجع السابق، ص147-148.

تعريفات في صلب القانون ، أما الطريقة الفرنسية توكل مهمة تحديد المعاني المصطلحات التقنية للقضاء وهي الطريقة المفضلة نظرا لسرعة تطور تقنيات الإعلام الآلي إمكانية مواكبة القانون الجنائي لهذا التطور، وعلى اثر ذلك ادمج المشرع الجزائري هذه الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات ضمن قانون العقوبات التقليدي و لم يستحدث قانونا خاصا ضمن القسم السابع مكرر شمل 8 مواد من المادة 394 مكرر إلى 394 مكرر 07[1].

الفرع الثاني: الركن المادي

إن الركن المادي لجريمة الأنترنت يقوم على صورتين أساسيتين:

الصورة الأولى: متمثلة في الاعتداء على نظام المعالجة الآلية وهذه الأخيرة تحتوي على نوعين من الاعتداء.

النوع الأول: وهو الدخول والبقاء غير مشروع في نظام المعالجة الآلية وهو ينطوي على 3 أفعال: فعل الدخول، البقاء، عرقلة (التعطيل).

النوع الثاني: متمثل في الاعتداء العمدي على نظام المعالجة الآلية للمعطيات وهو ينطوي على 3 أفعلا: فعل الإدخال، المحو، التعديل.

الصورة الثانية: متمثلة في الاعتداء على المنتجات الإعلام الآلي، ويحتوي هذه الصورة على فعل التزوير المعلوماتي[2].

أولا: سنتطرق إلى دراسة الدخول أو البقاء غير مشروع في نظام المعالجة الآلية للمعطيات نصت المادة 394 مكرر من قانون العقوبات الجزائري على أن:" يعاقب بالحبس من ثلاث (3 أشهر) إلى سنة (1) وبغرامة من 50.000دج إلى 200.000دج كل من يدخل او يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

[1] – مولود ديدان، قانون العقوبات الجزائري، قانون رقم 01/09 المؤرخ في 29 فيفري 2009، د.ط، ص120.

[2] – بعرة سعيدة، المرجع السابق، ص51.

تضاعف العقوبة على الأفعال المذكورة أعلاه تحريب أو تغيير لمعطيات المنظومة وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين(2) وبغرامة من 50.000دج إلى 300.000دج".

تقابلها المادة 323 ف1 من قانون العقوبات الفرنسي والتي تنص على أن "عقوبة فعل الحضور أو البقاء وغير المشروع في نظام المعالجة الآلية للمعطيات هي الحبس لمدة سنة وبغرامة 100000أورو.

أما إذا انتج عن فعل الدخول او البقاء محو أو تغيير في المعطيات الموجودة داخل النظام أو تعيب تنظيم تشغيل النظام فالعقوبة تشدد وتصبح الحبس لمدة سنتين وبغرامة تصل إلى 200.000 أورو.

نستنتج من هاتين المادتين أن لهذه الجريمة صورتين ففي الفقرة الأولى تتوافر أركان الجريمة في صورتها البسيطة وعقوبتها وفي الفقرة الثانية أركان الجريمة في صورتها المشددة وعقوبتها ضعف عقوبة الجريمة في صورتها البسيطة.

جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة:

نستنتج من الفقرة الأولى من المادة 394 مكرر أن أركان هذه الجريمة وحسب القواعد العامة يجب أن يتوافر على السلوك الإجرامي المتمثل في الدخول أو البقاء سواء في صورتها البسيطة أو المشددة وهذا هو الركن المادي.

الركن المادي: السلوك الاجرامي لهذه الجريمة نوعان ايجابي وسلبي.

فالأول يتمثل في فعل الدخول والثاني يتمثل في الامتناع عن الخروج.

المقصود بفعل الدخول: يقصد به الولوج إلى المعطيات المخزنة داخل نظام الحاسب الآلي بدون رضا المسؤول عن هذا النظام أو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له استخدامه والدخول إلى المعلومات[1].

[1] – غنية باطلي، الجريمة الالكترونية، المرجع السابق، ص150-151.

أما بالنسبة للتشريعات المختلفة فقد تباين موقفها تجاه تحديد محل الركن المادي في جريمة الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات وبذلك يمكن أن نميز 3 صور محل هذه الجريمة وهي كالآتي:

الصورة الأولى: تتمثل في المعلومات في ذاتها.

الصورة الثانية: انظمة المعالجة الآلية للمعطيات التي لا ترتبط من خلال شكة الاتصال.

الصورة الثالثة: شبكة المعلومات.

فهذا التباين والاختلاف حول محل ركن المادي لهذه الجريمة أورد 3 اتجاهات:

الاتجاه الموسع: يجمع بين الصور الثلاث ويتخذها جميعا كمحل الجريمة وهي المعلومات الواسعة للمعالجة الآلية وشبكات المعلومات . وتبنى هذا الاتجاه المشرع الفرنسي واقتدى به المشرع الجزائري.

الإتجاه الثاني: استبعد شبكات المعلومات من نطاق التجريم ، ويتبنى هذا الاتجاه المشرع الانجليزي.

الاتجاه الثالث: جرم فعل دخول عبر شبكات المعلومات وتبني هذا الاتجاه الشرع السويسري.

إن جريمة دخول غير مصرح إلى نظام المعالجة الآلية للمعطيات يعد في التشريع الجزائري جريمة شكلية لأنها لا تشترط تحقق النتيجة ، يكفي الوصول إلى المعلومات المخزنة بداخل النظام، فبمجرد الوصول إليها تقوم الجريمة، يرتكب فعل دخول بأية طريقة أو وسيلة كانت لأن المشرع الجزائري لم يحددها[1].

ويستوي أن يتم الدخول بطريق مباشر يستطيع الجاني للوصول إلى المعلومات المخزنة لدى الأنظمة المعالجة الآلية باستخدام الشاشة النظام والاطلاع بالقراءة على ما هو مكتوب عليه

[1] – نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، المنشورات الحلبية الحقوقية، ط1، 2005، ص323-324.

وباستخدام آلة طباعة مرفقة بجهاز الحاسب الآلي استخراج قائمة البرامج الموجودة داخل النظام المعلوماتي أو بطريق غير مباشر ويكون ذلك بالالتقاط المعلوماتي.

ولا تهتم صفة الشخص الذي يدخل النظام، المهم أن يكون من الأشخاص الذين ليس لهم الحق في الحضور إلى النظام مخالفا بذلك إرادة من له حق السيطرة على النظام سواء نص على ذلك القانون أو الاتفاق وسواء كانت هذه الأنظمة تتعلق بأسرار الدولة أو دفاعها أو تتضمن معطيات شخصية تتعلق بحرمة الحياة الخاصة وعليه نطرح التساؤل التالي: من يملك الحق بإعطاء الترخيص بالدخول وما هي الحالات التي يكون فيها الدخول غير مصرح به.

الشخص الذي يمكنه التحكم في الدخول أو البقاء: هو هيئة أو شخص يسمح بالدخول أو عدم الدخول إلى النظام وعرفته الاتفاقية الخاصة بحماية الأفراد في مواجهة نظم المعالجة الآلية للمعطيات 1989/01 "كل شخص طبيعي او معنوي او سلطة عامة أو كل مؤسسة او جهاز يكون لهم التصرف في نظام الحاسب الآلي التابع لهم وتقرير مضمونه أو محتواه وكيفية تنظيمه والهدف منه" وفي حالة تعدد المسؤولية يجب تحرير المسؤول على منح هذا الترخيص للدخول إلى النظام فإذا لم يتم تحديده فيعتبر الكل مسؤول[1].

حالات عدم الترخيص: ترى المادة 1/323 من قانون جنائي الفرنسي الجديد أن هناك طريقتين للدخول:

–حالة عدم وجود الترخيص مطلقا: لا يكون للشخص أية علاقة بالنظام كان يكون ضمن احد العاملين لا نخول له وظيفة الاتصال بهذا النظام.

–حالة وجود ترخيص: يكون الدخول مرخص ولكن في حدود معينة ولكن الفاعل يتجاوز وذلك كأن يكون مرخص له أن التجول في جزء ولكنه يتعدى ذلك إلى كل النظام عن قصد أو عن غير قصد أما في حالة الشخص يملك تصريحا بالدخول لكن هذا التصريح غير شامل لكل النظام بل مقتصرا على بعض المناطق فقط، وعليه فإن الدخول إلى هذه المناطق يعد مشروعا والمناطق الأخرى غير مشروعة وتجاوز التصريح الذي نقصده هو التجاوز في لمكان وليس الزمان وهناك تساؤل فيما يخص الدخول قد استخدم لغرض غير الذي منح لأجله الترخيص فهل يعد هذا

[1] – غنية باطلي، المرجع السابق، ص153.

تجاوز للتصريح وأثار هذا الاشكال آراء متضاربة وبقرار الصادر عن محكمة الاستئناف (RENNES) الصادر في 06 فيفري 1996 التي اعتبرت أن مجرد الدخول البسيط دون الأخذ في الاعتبار الغرض أو الهدف من الدخول والنتائج الممكنة يعتبر جريمة، إذا فمجرد الدخول البسيط إلى داخل النظام يمكن ان يقع تحت طائلة القانون الجنائي لأن الدخول غير الصريح بع أو التصريح تم وفقا لتعليمات القائم على النظام والذي ينتج أن يتم باستعمال كلمة مرور مسروقة تقنيتا يعتبر الدخول مشروعا أما قانونا غير مشروع لأنه بشكل انتحال للشخصية[1].

البقاء: هو "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام" وهو " عدم وضع حد للتشعب داخل النظام مع الاعتقاد بأن ذلك يشكل خطأ" وهو "الدخول عن طريق الخطأ ولكن البقاء داخل النظام عن إرادة ووعي"

ويتحقق فعل البقاء غير المشروع سواء كان مستقلا عن الدخول غير المشروع وهي الحالة الأولى أو مقترنا بفعل الدخول غير المشروع وهي الحالة الثانية.

الحالة الأولى: حالة استغلال فعل البقاء عن الدخول غير المشروع.

قد يكون الدخول مسموحا به او مصرحا به ومع ذلك فغن الفاعل لا يقطع الاتصال عند إدراكه ان وجوده داخل النظام والبقاء فيه غير مشروع، فهو يبدأ في اللحظة التي كان يجب على الشخص المغادرة والخروج من النظام ومن صور البقاء غير المشروع.

- بقاء الجاني داخل النظام بعد المدة المحددة له.
- البقاء فيما يتعلق بالخدمات الهاتفية المفتوحة على الجميع والحصول على خدمة لمدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل او عمليات غير مشروعة.
- طبع المعلومات أو المعطيات والتي كان من المفترض أن يطلع عليها بالرؤية.

وقد يكون الدخول إلى النظام قد تم بالخطأ أو الصدفة أو السهو بدون إرادة من الداخل ولكن عند إدراكه واكتشافه بأنه داخل النظام يبقى فيه ولا يخرج منه في الوقت المحدد للخروج،

[1] – محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، دون سنة نشر، ص141.

فالبقاء يبدأ من للحظة التي يعلم فيها الجاني أنه داخل نظام غير مصرح له بدخوله، ورغم ذلك لا يضع حدا لتجوله وبقائه داخل النظام فيعاقب الفاعل على جريمة البقاء غير مشروع إذا ما توفر الركن المعنوي[1].

الحالة الثانية: حالة اجتماع كل من فعل البقاء والدخول غير المشروع

غالبا ما يجتمع فعل الدخول ولبقاء غير المشروع كان يكون الفاعل غير مصرح له بالدخول إلى النظام وبالرغم من ذلك يدخل إلى النظام ضد إرادة من له حق السيطرة عليه ويبقى فيه بعد ذلك، ويتحقق هنا الركن المادي للجريمتين معا فتثور مسألة هامة وهي كيفية الفصل بين الجريمتين؟ أي متى تبقى جريمة الدخول غير المشروع وتبدا جريمة البقاء غير المشروع؟

ولعل هذه الاشكالية اختلفت فيها الآراء حيث يرى.

الرأي الأول: جريمة الدخول تتحقق منذ اللحظة التي يتم فيها الدخول إلى البرنامج أي يفترض البقاء لفترة قصيرة، لكن يؤخذ على هذا الرأي أنه لم يحدد هذه الفترة بطريقة حاسمة ولحظة بداية جريمة البقاء.

الرأي الثاني: لحظة الدخول تتحدد في الوقت الذي يعلم فيها المتدخل أن بقاءه داخل النظام غير مشروع ولكن يؤخذ على هذا الرأي صعوبة اثبات علم المتدخل.

الرأي الثالث: جريمة البقاء داخل النظام تبدأ من اللحظة التي ينذر فيها المتدخل بانه متواجد بطريقة غير مشروعة ولكن يؤخذ على هذا الرأي أنه لا بد من وجود جهاز انذار يقوم بهذه المهمة إذا أمكن تحقيقه في المؤسسات والشركات الكبرى إذ يعتقد أن الرأي الصائب هو الذي يرى أن جريمة البقاء تبدأ من الوقت الذي يبدأ فيه المتدخل بالتجول داخل النظام بعد انتهاء الوقت المحدد ففي هذه الحالة التي يكون فيها الدخول غير مشروع ودخل الجاني وظل ساكنا (أي لم يبدأ بالترك والتجول بعد) لا تقوم جريمة البقاء غير المشروع بل تظل جريمة الدخول غير المشروعة قائمة ويكفي في جريمة البقاء غير المشروع حتى ولو لم يتم التقاط المعلومات أي لا يشترط أي نتيجة فيكفي البقاء المجرد.

[1] – محمد خليفة، المرجع السابق، ص 133.

يجتمع فعل البقاء مع فعل الدخول غير المشروع إلى نظام المعالجة الآلية للمعطيات مثل أن لا يكون للجاني حق الدخول ويدخل عن طريق الغش حيث نصت م 394 مكرر من قانون العقوبات الجزائري على فعل البقاء غير المشروع على غرار القانون الفرنسي في المادة 323 ف 1 من القانون العقوبات الفرنسي يصعب تطبيق النص في قراءته الأولى لأنه بنص على الدخول أو البقاء غير المشروع داخل نظام المعالجة الآلية للمعطيات مع تأثير على البيانات التي يحتويها النظام أي يشترط تحقيق نتيجة.

جرمت محكمة استئناف باريس في حكمها في 1994/04/05 البقاء الغير مشروع سواء تم بطريقة خطأ أو بطريقة مشروعة داخل نظام المعالجة الآلية للمعطيات إلا أنه اكتسب بعد ذلك صفة عدم المشروعية[1].

الصورة المشددة: نصت المادة 394 مكرر ف2، ف3 من قانون العقوبات الجزائري على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هاذين الفعلين إما محو أو تحوي للمعطيات التي يحتويها النظام وإما عدم صلاحية النظام لأداء وظائف النتيجة تخريب وإشتغاله.

إن ظرف التشديد ظرف مادي تربط بينه وبين الجريمة العمدية الأساسية علاقة سببية لكي نقول ان الشرط متوفر.

وفي المادة 394 مكرر من الفقرة الأخيرة شدد المشرع عقوبة المحو وتعديل المعطيات كل واحد على حدى تجريب نظام اشتغال المنظومة من جهة أخرى وعقوبة هذه الأخيرة أشد لأن عقوبة المحو أو التغيير هي ضعف عقوبة الدخول والبقاء غير المشروعين، أما بالنسبة للمشرع الفرنسي فجمع بين طريفين في فقرة واحدة وفي عقوبة واحدة في المادة 1/323 قانون العقوبات الفرنسي[2].

[1] – غنية باطلي، المرجع السابق، ص152.

[2] – غنية باطلي، المرجع نفسه، ص168-169.

النوع الثاني: الاعتداء العمدي على نظام المعالجة الآلية للمعطيات

نصت على هذه الصورة المادتين 5 و 8 من الاتفاقية الدولية للإجرام المعلوماتي والمادة 2/323 من قانون عقوبات الفرنسي نصت على "كل من قام بإعاقة او افساد وظيفة نظام المعالجة الآلية للمعطيات يعاقب بالحبس لمدة 3 سنوات وغرامة 300.000 أورو أما المشرع الجزائري فلم ينص عليها وذلك للتشابه الكبير بينها وبين جريمة الدخول أو البقاء غير المشروع واستبعدها كجريمة قائمة بذاتها[1].

وفقد اختلف الفقه حول ما إن كان الاعتداء وسيلة أم غاية؟

فإن كان الاعتداء الذي وقع على المعطيات مجرد وسيلة فإن الفعل بشكل جريمة الاعتداء العمدي على المعطيات ومع عدم وجود نص خاص بالاعتداءات العمدية على نظام المعالجة الآلية للمعطيات، فإن الاعتداءات على سير النظام الناجمة عن الدخول المشروع للنظام تفلت من العقاب وتتمثل السلوكات الإجرامية في هذه الاعتداءات في فعل عرقلة (التعطيل) والافساد.

التعطيل (العرقلة): إن المشرع لم يشترط الوسيلة التي يتم بها فعل التعطيل سواء كانت مادية اقترنت بعنف، أم لا لكسر الأجهزة المادية للنظام او تحطيم الأسطوانة أو منع العمال من الوصول إلى النظام او المكان الذي يوجد به النظام.

وتكون معنوية إذا وقعت على الكيانات المنطقية للنظام مثل البرامج والمعطيات باتباع التقنيات التالية: كإدخال برنامج فيروسي، استخدام قنابل منطقية يجعل النظام بتباطئ اداءه لوظائف إلى غيرها من التقنيات[2].

الافساد: يقصد به هو كل فعل يؤدي إلى جعل نظام المعالجة الآلية للمعطيات غير صالح للاستعمال السليم وبالتالي يعطي نتائج غير تلك التي كان من الواجب الحصول عليها ومن تقنيات الافساد استخدام القنبلة المعلوماتية التي يمكن من خلالها إدخال معلومات تتكاثر داخل النظام وتجعله غير صالح للاستعمال[3].

[1] – عبد الفتاح بيومي حجازي، مرجع سابق، ص39.

[2] – أمال قارة، المرجع السابق، ص113.

[3] –محمد أمين احمد الشوابكة، مرجع سابق، ص238.

الإعتداءات العمدية على المعطيات:

نصت عليها المواد 3،4، 8 من الاتفاقية الدولية للإجرام المعلوماتي وكذلك كذلك المادة 323من قانون العقوبات الفرنسي بنصها:" كل من أدخل بطرق الغش المعطيات بنظام المعالجة الآلية للمعطيات أو محا أو عدل، ونصت على الاعتداءات تلك المعطيات بعقوبة الحبس تصل إلى 03سنوات وبعقوبة الغرامة تصل 300 ألف أورو.

وبالإضافة إلى ذلك نصت المادة 394 مكرر 2 قانون العقوبات الجزائري على الاعتداءات العمدية بنصها:" يعاقب بالحبس من شهرين 02 إلى ثلاثة (3) سنوات وبغرامة من 1.000.00 إلى 10.000.000 دج كل من يقوم عمدا أو عن طريق الغش بما يلي:

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

- حيازة أو إفشاء أو نشر واستعمال لأي غرض كل المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم، ومن هنا أن نشاط إجرامي لجريمة الاعتداء العمدي للمعطيات يتجسد في صورتين هما:

الصورة الأولى: الاعتداءات العمدية على المعطيات الموجودة: تتجسد هذه الاعتداءات العمدية على المعطيات في ثلاث أفعال هي: الإدخال والمحو والتعديل.

الإدخال: هو إضافة معطيات جديدة على الدعاية الخاصة سواء كانت خالية، أم كانت يوجد عليها معطيات من قبل، ونكون أمام فعل الإدخال في حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة أو التزوير[1].

وقد يكون التدخل في المعطيات بإدخال معطيات وهمية إلى النظام المعلوماتي لم تكن موجودة من قبل او يقصد التشويش على صحة البيانات القائمة (الموجودة) وبالتالي يكون من السهل تغذية الحساب بمعلومات مغلوطة ووهمية وزائفة ويقوم بتنفيذ الأوامر بحيث يخزن المعلومات سواء كانت

[1] - بعرة سعيدة، المرجع السابق، ص56.

صحيحة او خاطئة وتعتبر من أهم الأساليب المستعملة في الاحتيال الالكتروني لاسيما في المنشآت ذات الأموال لأنه لا يتصور ارتكابها إلا من قبل أشخاص ذوي دراسة واسعة بالإعلامية وتقنياتها[1].

2-فعل المحو او الإزالة: يقصد بها إزالة جزء من معطيات المسجلة داخل النظام وتحطيم تلك الدعامة او نقل أو تخزين جزء من معطيات في ذاكرة مختلفة.

3-فعل التعديل: يقصد بفعل التعديل تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى ويتحقق ذلك عن طريق برامج تتلاعب في المعطيات سواء بالمحو الكلي أو جزئي.

الصورة الثانية: المساس العمدي بالمعطيات خارج النظام.

نص المشرع الجزائري على صورتين للمساس العمدي بالمعطيات خارج النظام

1-تتعلق بحماية المعطيات من استعمالها في الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات.

2-تتعلق بحماية المعطيات المتحصل إليها من هذه الاعتداءات وذلك في نص المادة 394 مكرر2 قانون العقوبات وتهدف هذه الحماية إلى الوقاية من ارتكاب جريمة أخرى تتمثل في:

حيازة أو إفشاء أو نشر أو استقبال هذه المعطيات المتحصل عليها من احدى هذه الاعتداءات.

II-الاعتداءات على منتوجات الاعلام الآلي (التزوير المعلوماتي): يعد هذا الفعل من أخطر صور الغش والمعلوماتي نظرا لما يتمتع به الحاسب الآلي من خطورة[2].

ولقد خصص المشرع الجزائري في جريمة التزوير فصل كامل من مواد 197- 241 قانون العقوبات الجزائري وبالرغم من ذلك لم يجرم عملية التزوير التي تقع على دعائم معنوية كالمستندات الرقمية أو المعلوماتي مثلا (معطيات معلوماتية، مستندات معلوماتية، برامج معلوماتية، و لم يعرف بصفة عامة جريمة، التزوير إلا أنه في نص المادة 441 من قانون العقوبات الفرنسي، عرف التزوير وجميع بين تعريف جريمة التزوير التقليدية (على دعامة مادية) وجريمة التزوير

[1] – محمد أمين أحمد شوابكة، المرجع السابق، ص 231- 232.

[2] – أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائر، دار هومة، الجزائر، ط2، 2007، ص133.

المعلوماتية (على دعامة معنوية كالمستندات المنطقية والمعلوماتية)، أما فيما يخص وسائل مستعملة لتزوير معطيات المعلوماتية لم يحددها المشرع الفرنسي إلا أنه يشترط تحقيق النتيجة المتمثلة في تزوير معطيات من خلال تغيير الحقيقة واحداثها ضرر الغير[1].

وتضاربت الآراء حول امكانية تطبيق او عدم تطبيق النصوص العقابية التقليدية على جريمة المعطيات المعلوماتية وانقسمت هذه الآراء إلى مؤيد ومعارض.

الفريق المؤيد: لتطبيق النصوص التقليدية على التزوير المعلوماتي، يرى هذا الفريق بان هناك علاقة وثيقة بين العقاب على التزوير ونظام الاثبات فطبقا لمبدأ الاثبات الحر في المعاملات التجارية فإن الوثائق الالكترونية تصلح للإثبات وبالتالي اعتمادها في جرائم التزوير أما الفريق المعارض فيردى أن جريمة التزوير في المحررات تستلزم ان تكون كتابة وهو ما يتعارض في مجال المعلوماتية التي تتطلب معالجة آلية للمعطيات وجريمة التزوير تبين إمكانية استعمال الوثيقة المزورة كوسيلة اثبات ولكن الوثائق والسجلات أو المستندات ليس لها أهمية في ميدان الاثبات.

وللتغلب على الصعاب في مجال المحررات المعلوماتية وفي سبيل تحديد الحماية من جريمة التزوير في محيط المعلوماتية، عمدت التشريعات في الكثير من الدول باستخدام وتعديل نصوصها العقابية حيث اتبع المشرع التونسي في المشرع الفرنسي في هذا المجال من خلال تجريم كل أنواع التزوير المعلوماتي[2].

أما المشرع الجزائري ورغم تداركه من خلال القانون 15/04 المتضمن قانون العقوبات الفراغ القانونية في مجال الاجرام المعلوماتي قام بتجريم الاعتداءات الواردة على منتوجات الاعلام الآلي فلم يستحدث نصا خاصا بالتزوير المعلوماتي، ولم يتبنى الاتجاه الذي تبنته التشريعات التي عملت على توسيع مفهوم المحدد ليشمل كافة صور التزوير الحديث[3].

الركن المعنوي: يعد الركن المعنوي للجريمة عنصرا أساسي لقيام المسؤولية الجزائية وبدونه لا تقوم الجريمة إذ لا يسأل شخص عن جريمة ما لم تقم علاقة بين ماديتها ونفسية الجاني وسيطرة

[1] – دردور نسيم، جرائم الالكترونية على ضوء القانون لجزائري والمقارن، مذكرة لنسل شهادة ماجستير، سنة 2013/2012، ص56.

[2] – المرجع نفسه، ص57- 59.

[3] – أمال قارة، المرجع السابق، ص140.

الإرادة الجرمية للجاني على ماديات الجريمة وبالتالي تحدد صورة القصد الجرمي للجريمة مقصودة أم تأخذ صورة الخطأ الذي تكون به الجريمة غير المقصودة.

فالركن المعنوي للجريمة هو الوجه الباطني النفسي للسلوك الذي قام به الجاني والنص القانوني هو الذي يحدد الوجه الباطني النفسي ونوعه، لكن في بعض الأحيان يتعدى السلوك الاجرامي نفسية صاحبه او مرتكب الجريمة لأسباب خارجة عن إرادته ضغطت علبه ودفعته لارتكاب الجريمة كأن يكره شخص على التوقيع بإمضاء في سند مرور وفي هذه الحالة فإن الجاني لا يسأل جزائيا عن السلوك الذي قام به.

تعد جرائم الأنترنت كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام (العلم والارادة) لتحديد المسؤولية الجنائية ولا يمكن تصور وجود قصد خاص بالجريمة دون أن يسبقه القصد العام، أما القصد الخاص في الجرائم المعلوماتية فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة بدى الجاني من وراء القيام بالفعل غير المشروع أو ارتكاب الجريمة، فكل جريمة معلوماتية تختلف عن الأخرى من حيث أركانها وماهيتها وطبيعتها.

ويرى اتجاه من الفقه أن القضاء الأمريكي لم يستقر على حال بالنسبة لبعض الجرائم التي ترتكب باستخدام الأنترنت من حيث مدى تحديد ما إذا كانت تتطلب قصدا عاما او خاصا ويلاحظ الباحث أن القصد الخاص يتوافر في بعض الجرائم المعلوماتية سيما وأن معظم الجرائم المعلوماتية تقوم بتوافر القصد العام، وهو علم الجاني بمضمون الفعل الذي قام او سيقوم به بان هذا الفعل غير مشروع وكذلك ارتباط هذا العلم بالإرادة[1].

فمثلا في جريمة سرقة المعلومات من الحاسب الآلي او البريد الالكتروني يعد فعل غير مشروع ويجب أن يرتبط هذا العلم مع الإرادة وهي الحالة النفسية التي تعكس قيام الجاني بالسلوك ويتوافق مع القصد العام الذي ذكرناه سابقا في جريمة سرقة المعلومات (نية التملك) للمعلومة التي تم سرقتها والتي تعكس (القصد الخاص) في مثل هذا النوع من الجرائم ومثال ذلك ضرورة توافر نية التملك للأموال المتحصل عليها من سرقة بطاقات الائتمان وتحويلها إلى حسابه الخاص (القصد الخاص).

[1] – لورنس سعيد الحوامدة، الجرائم المعلوماتية وأركانها وآلية مكافحتها، جامعة طيبة، السعودية، 2016-2017، ص23

وكخلاصة قول فإن القصد العام والخاص في جرائم الأنترنت هو أساسي لتحديد المسؤولية الجزائية، والذي يحدد وجود قصد خاص في بعض الجرائم المعلوماتية هو طبيعة الجريمة ونية الإضرار أو النية الخاصة للجاني والتي يمكن استخلاصها من مكونات كل جريمة على حدى ويشكل مستقبل وبالتالي فجرائم الأنترنت والجرائم المستحدثة هي كغيرها من الجرائم التقليدية يشترط وجود الركن المعنوي لقيام الجريمة.

أما عن الإثبات في توافر الركن المعنوي في جرائم الأنترنت فهو يقع على عاتق النيابة العامة والمحكمة المختصة بالنظر في مثل هذا النوع من القضايا والمحكمة صاحبة الصلاحية بتقدير وجود سوء النية من عدمها[1].

المطلب الثاني: قمع جريمة الأنترنت

الفرع الأول: قمع الجريمة بالنسبة للشخص الطبيعي

لقد قرر المشرع الجزائري وكذا الفرنسي عقوبات أصلية وأخرة تكميلية للشخص الطبيعي، وتختلف العقوبات الأصلية بحسب الجريمة المرتكبة المنصوص عليها في القسم السابع مكرر أما العقوبات التكميلية من الأحكام المشتركة في جرائم هذا القسم وعليه سنتطرق في:

أولا: العقوبات الأصلية

ثانيا: العقوبات التكميلية

أولا: العقوبات الأصلية

أ-عقوبة جريمة الدخول أو البقاء غير المشروع

عقوبة الجريمة في صورتها البسيطة

يعاقب المشرع الجزائري على هذه الجريمة بالحبس من 3 أشهر إلى سنة وبغرامة 50.000 إلى 200.000دج وترك المشرع للقاضي السلطة التقديرية في تقدير العقوبة بحسب الوقائع المعروضة امامه.

[1] – لورنس سعيد الحوامدة، المرجع السابق، ص25.

أما المشرع الفرنسي حيث يعاقب بالحبس من شهرين إلى سنة وبغرامة 100.000 فرنك وبصدور قانون عقوبات الفرنسي سنة 1994 يشدد في العقوبة ويجعل لها حدا واحدا هو سنة ولغي الحد الادنى وهو شهرين وبالتالي سلب القاضي السلطة التقديرية في تقدير العقوبة أما بالنسبة للغرامة فرفعها إلى 15.000 أورو اما في سنة 2004 أصبحت العقوبة 02 سنتين وغرامة 30.000 يورو.

عقوبة الجريمة في صورتها المشددة: نصت المادة 394 مكرر ف2ن ف3 من قانون العقوبات الجزائري على جريمة الدخول او البقاء في المشروع إذا ترتب حذف او تغيير المعطيات 6 أشهر إلى 02 سنتين وبالنسبة للغرامة 100.000دج إلى 200.000دج أما إذا حدث تخريب لنظام المعالجة الآلية بالعقوبة تكون: الحبس من 6 أشهر و 02 سنتين اما الغرامة من 50.000دج إلى 300.000دج، أما القانون العقوبات الفرنسي فرفع عقوبة إلى 3 سنوات والغرامة 45.000 يورو.

ب–عقوبة جريم الإفساد أو تعطيل سير النظام:

نلاحظ أن المشرع الفرنسي قد نص على عقوبة موحدة لجريمة الاعتداء العمدي[1] سواء على المعطيات أو على سير النظام أي الحبس حتى 3 سنوات والغرامة حتى ثلاثة مئة ألف فرنك (300.000 أورو) وفي سنة 2004 اصبحت العقوبة هي 5 سنوات لكلا الجريمتين وغرامة 75000 أورو.

أ/1–عقوبة جريمة الاعتداء العمدي على المعطيات الموجودة داخل النظام:

نصت المادة 394 مكرر 1 قانون العقوبات الجزائري على هذه الجريمة الحبس 6 أشهر إلى 3سنوات وعقوبة الغرامة 500.000دج إلى مليون دينار 4.000.000 دج أما القانون الفرنسي 2004 فقد شدد ألأكثر في العقوبة إذ رفع عقوبة الحبس إلى 5 سنوات وغرامة 75.000 اورو.

[1] غنية باطلي، المرجع السابق، ص207-210.

ب/1 عقوبة جريمة التعامل غير المشروع بالمعطيات: نصت المادة 394 مكرر 4 من القانون 15/04 على عقوبات أصليتان هما الحبس والغرامة وهذه العقوبة مقررة لكل من الصورتين.

*عقوبة الصورة الأولى: تتمثل العقوبة الأصلية في الحبس من 02 شهرين إلى 3 سنوات والغرامة من مليون (1000.000 دج) إلى خمس ملايين (5000.000دج)

*عقوبة الصورة الثانية: هي نفس العقوبات التي أقرها المشرع الجزائري للصورة الأولى المتمثلة في التعامل الغير مشروع في المعطيات لارتكاب احدى الجرائم المنصوص عليها في هذا القسم وهي الحبس من شهرين إلى 03 سنوات وغرامة من مليون إلى 5 ملايين دج واضافة إلى هذه العقوبات الأصلية اشترط عقوبات تكميلية تشترك فيها جميع جرائم هذا القسم[1].

ثانيا: العقوبات التكميلية

بالإضافة إلى العقوبات الأصلية المفروضة على مرتكبي جرائم المساس بأنظمة المعالجة الآلية للمعطيات قرر المشرع عقوبات تكميلية تتمثل في المصادرة والغلق بالنسبة للقانون الجزائري أما بالنسبة للقانون الجزائري أما بالنسبة للقانون الفرنسي فكانت العقوبة التكميلية المطبقة على الأشخاص الطبيعية المدانة بجنح الاعلام الآلي وهي نفس المادة من القانون العقوبات الفرنسي لسنة 2004.

المصادرة: المصادرة هي الايلولة النهائية إلى الدولة لمال أو مجموعة من الأموال معنية (م 15 ق.ع.ج) وقد تكون:

المصادرة العامة: أي أيلولة كل أموال المحكوم عليه واضافتها إلى ملكية الدولة.

أ-المصادرة الخاصة: أي أيلولة مال من أموال المحكوم عليه وإضافتها إلى ملكية الدولة ولقد نصت المادة 394 مكرر06 بقوله "مع الاحتفاظ بحقوق الغير حسني النية يحكم بمصادرة الاجهزة البرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا للجرائم المعاقب عليها وفقا لهذا القسم، علاوة على اغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعمل مالكها"

[1] - باطلي غنية، نفس المرجع، ص213.

إلا أن الصادرة هي نقل ملكية شيء مادي أو عيني ممتلك للمحكوم عليه ونقله إلى الدولة أما الغرامة هي تحميل ذمة المحكوم عليه يدين لها والمصادرة في جرائم الإلكترونية الاعتداء على أنظمة المعالجة الآلية للمعطيات هي عقوبة تكميلية وجوبية أي ليس للقاضي السلطة التقديرية في الحكم بها اولا ومن خلال نص المادة 394 مكرر 6 ق.ع.ج نستنتج لا بد من تعيين شروط لتضييق عقوبة المصادرة.

1-ان يحكم على المتهم بالعقوبة الأصلية بإحدى الجرائم المنصوص عليها في القسم الخاص بالاعتداء على أنظمة المعالجة الآلية للمعطيات.

2-الأشياء التي تمت مصادرتها قد استخدمت في ارتكاب الجريمة سواء كانت هذه الأشياء والوسائل معلوماتية او غير معلوماتية.

الوسائل المعلوماتية تتمثل في انظمة الحاسب الآلي والأنترنت والأقراص المضغوطة وقد تكون كتب او وثائق[1].

3-يجب ان تكون الأشياء المستخدمة مضبوطة حتى يمكن مصادرتاه سواء قدمها الجاني من تلقاء نفسه او ضبطتها الشرطة، فلا يمكن مصادرة شيء غير مضبوط والحكم على الجاني بدفع قيمته او يجب أن لا تخل المصادرة بحقوق الغير حسن النية، والغير هنا كل أجنبي عن الجريمة تماما أي ليس فاعلا ولا شريكا وتثبت ملكيته للشيء المضبوط وبشرط أنه يجهل أن هذه الوسائل قد تستخدم في ارتكاب جريمة أو أنه بذل ما في وسعه لعدم استعمالها إلا أنها استعملت فعلا في ارتكاب الجريمة، وحقوق الغير حسن النسبة تمتد لتشمل حق عيني على الشيء كحق الانتفاع أو الرهن مثلا، أما الحقوق الشخصية فلا تحول دون المصادرة لأن محلها ذمن المدين وليس مالا معينا من أمواله حتى ولو كان الشيء المضبوط هو الضمان الوحيد للمدين، ولا يهم إذا كان حق الغير حسن النية قد نشأ قبل أو بعد ارتكاب الجريمة مادامت نيته حسنة النية وقت ارتكابه الجريمة أو وقت نشأة حقه، وعليه فإذا كان للغير حسن النية حق على الأشياء المضبوطة مثلا حق انتفاع أو رهن فلا يمكن الحكم بمصادرتها وتحل الدول محل المتهم فيصبح الغير حسن النية مالك على الشيوع مع الدولة او تنتقل الملكية للدولة محملة بحق الرهن أو الانتفاع.

[1] – محمد خليفة، المرجع السابق، ص121.

ب/الغلق: نصت عليه المادة 394 مكرر06 قانون العقوبات الجزائري وتشمل غلق المواقع التي تكون محلا لجريمة من جرائم المعاقب في هذا القسم والتي تقدم خدمات تسمح بالدخول غير المشروع لمختلف الأنظمة أو تسمح بالتلاعب بالمعطيات هناك مواقع تقوم بتعليم كيفية تصميم المعطيات غير المشروعة ونشرها والاتجار بها ويقع الغلق كذلك بالنسبة للمحل ومكان الاستغلال أي المكان الذي استعمله الجناة لارتكاب الجريمة والذي يحوي على الأجهزة المستعملة في الدخول غير المصرح به أو التلاعب في المعطيات أو التعامل في معطيات غير مشروعة وبالنسبة لمدة الغلق المادة 394 مكرر قانون العقوبات الجزائري لم تحدد مدة معينة قد تكون مؤبدة او مؤقتة مثلما هو منصوص عليه في الأحكام العامة لقانون العقوبات المادة 16 مكرر 1 مضافة بالقانون 23/06 "يجوز أن يؤمر بإغلاق المؤسسة نهائيا أو مؤقتا في الحالات وبالشروط المنصوص عيليها في القانون ونصت المادة 5/323 من القانون الجنائي الفرنسي على عقوبة الغلق في البند الرابع منها وكانت محددة بـــ 5 سنوات على الأكثر وتوقع هذه العقوبة على المؤسسات أو على فرع المشروع الذي استخدم في ارتكاب الجريمة[1].

الفرع الثاني: العقوبات المقررة للشخص المعنوي

لقد تضمن تعديل قانون العقوبات الجزائري لسنة 2004 اقرار للمسؤولية الجنائية للأشخاص المعنوية بنص المادة 18 مكرر من القانون 15/04 ومن بين الجرائم التي يعاقب عنها الشخص المعنوي هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

وقد شدد في عقوبة هذه الجرائم إذا ارتكبها شخص معنوي او كانت موجهة ضد الجهات العامة (أي إذا كانت هذه المعطيات تابعة للدولة ونفس الأمر نص عليه المشرع الفرنسي في المادة 6/323 من القانون الجنائي وفقا للشروط المنصوص عليها في المادة 2/121.

نصت المادة 394 مكرر 4 من قانون العقوبات الجزائري:" يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمسة (5) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي" ونصت المادة 6/323 من القانون الجنائي الفرنسي "يمكن للأشخاص المعنوية أن يسألوا جنائيا عن الجرائم المرتكبة في هذا القسم طبقا للمادة 2/121"

[1] – محمد خليفة، المرجع السابق، ص122.

والمادة 7/121 تنص" على أنهم يسألوا في الحالات التي نص عليها القانون أو اللائحة عن الجرائم التي ارتكبوها لحسابهم او من طرف أعضائهم او ممثليهم، أما الجماعات المحلية والتجمعات التابعة لها يسألون جنائيا إذا كانت الجرائم التي ارتكبوها أثناء ممارستهم نشاطهم.

أولا: شروط تقرير المسؤولية الجزائية للشخص المعنوي

والمسؤولية الجنائية للأشخاص المعنوية لا تستبعد الأشخاص الطبيعية فاعلين أو مساهمين الذين ارتكبوا نفس الوقائع و المادة 51 من قانون 51/04 توضح أن المشرع الفرنسي أراد أن يشرك، الأشخاص الطبيعية في المسؤولية مع الأشخاص المعنوية مقتصرة على الحالات وحدهم نتائج فعل مرتب عن الإرادة الجماعية، وهذه المسؤولية مقتصرة على الحالات التي نص عليها القانون أو اللوائح وهي مسؤولية مرتبطة بتوافر شروط:

1-أن ترتكب الجريمة من أحد أعضاء الشخص المعنوي أو ممثليه

2-يجب أن تركب الجريمة لحساب الشخص المعنوي

3-يسأل الشخص المعنوي بصفته فاعلا أصليا او مساهما.

تنعقد المسؤولية الجنائية للشخص المعنوي عند قيامه بجرائم لها علاقة بالمجال الالكتروني وفي إطار الاقتصاد الحالي تقوم الشركات بالبحث عن المعلومات بأية وسيلة وهذا البحث يمكن أن يكون عن طريق الدخول او البقاء غير المشروع في النظام المعلوماتي لشركة أخرى منافسة والاطلاع على ملفاتها وخططها، وبالتالي تكون هذه المنافسة غير مشروعة عن طريق ارتكاب جرائم الكترونية، ولقد شدد المشرع العقوبة على الشخص المعنوي لان الكثير من الأشخاص المعنوية تنشأ بغرض تحقيق الربح[1].

ثانيا: عقوبات على الشخص المعنوي: (التكميلية) المادة 18 مكرر قانون العقوبات الجزائري.

-حل الشخص المعنوي.

-غلق المؤسسة أو فرع من فروعها لمدة لا تتجاوز خمس5 سنوات.

[1] - محمد خليفة، المرجع السابق، ص124.

-الإقصاء من الصفقات العمومية لا تتجاوز خمس 5 سنوات.

-المنع من مزاولة نشاط أو لمدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر ، نهائيا أو لمدة لا تتجاوز خمس 5 سنوات.

-مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها.

- نشر وتعليق حكم الإدانة

أ-الوضع تحت الحراسة القضائية لمدة لا تتجاوز عدة خمس السنوات وتنصب الحراسة على ممارسة النشاط الذي أدى إلى الجريمة أو الذي ارتكبت الجريمة بمناسبته[1]. أما إذا كانت الجريمة موجهة ضد الأشخاص المعنوية فقد قرر المشرع تشديد العقوبة في حالة ما إذا كان الضحية جهات عامة، التي شغلت بالدفاع الوطني أو الهيئات أو المؤسسات الخاضعة للقانون العام وهذا ما جاءت به المادة 394 مكرر 4 من القانون 15/04.

[1] – غنية باطلي، المرجع السابق، ص214.

الفصل الثاني

إجراءات التحقيق في جريمة الأنترنت

التقدم التكنولوجي الذي يشهده العصر الحديث يحتم ضرورة وجود قانون حديث يسايره ويتصدى للتطورات الإجرامية التي تصاحبه، محاولا حماية هذه التقنية الحديثة من الانتهاكات الخطيرة التي تهدد سلامة الأفراد، سواء في أموالهم، أعراضهم، حرياتهم الشخصية، وغيرها من الحقوق التي أصبحت مهددة مع انتشار استخدام الكمبيوتر والانترنيت من مختلف فئات المجتمع، فرغم ما قدمه التقدم التكنولوجي من تسهيلات في مختلف الميادين إلا انه أصبح أداة لأخطر الجرائم، وتكمن خطورتها في سهولة ارتكاب الجرائم التقليدية مع صعوبة اكتشافها، دون اللجوء إلى الوسائل التقليدية في ذلك، لأن الجرائم باتت ترتكب بواسطة التقنيات الحديثة كجرائم السرقة، الاختلاس ، القذف ، السب ....الخ .

وعليه فان هذا النوع من الجرائم يستوجب تحديث القوانين والتعليمات، وكذا خلق جهات أمنية متخصصة للتحقيق فيها، ومن خلال هذا الفصل سنتطرق إلى مرحلة البحث والتحري كمبحث اول يتضمن دور الضبط القضائي في المطلب الأول، وتطرقنا في المطلب الثاني إلى الاجراءات الحديثة لجمع الدليل الالكتروني، أما عن المبحث الثاني فيتضمن مرحلة التحقيق والتي هي محور دراستنا، قسمناه إلى مطلبين، المطلب الاول مفهوم التحقيق الجنائي في الجريمة المعلوماتية، أما المطلب الثاني تحدث عن إجراءات التحقيق.

المبحث الأول: مرحلة جمع الاستدلالات (البحث والتحري)

إن هذه المرحلة من اختصاص ضباط الشرطة القضائية وهم نوعان النوع الأول: هم الذين يتمتعون باختصاص عام ويختصون بإجراءات الاستدلال بشان الجرائم المنصوص عليها في قانون العقوبات أما النوع الثاني فهم ذو الاختصاص النوعي المحدد بخصوص نوع معين من الجرائم حددها القانون على سبيل الحصر المادة 21 ق.إ.ج وسلطتهم محددة لا تمتد إلى مرحلة التفتيش ودخول المنازل والمعامل والمباني والأماكن المحاطة بأساور إلا بحضور أحد ضباط الشرطة القضائية ومن بين هؤلاء رؤساء الأقسام المهندسون وأعوان الغابات وحماية الأراضي وما يهمنا في هذه الدراسة دور الضبطية القضائية ومجال اختصاصها فيما يتعلق بالجريمة المعلوماتية.

المطلب الأول: الإجراءات التقليدية لجمع الدليل الالكتروني

سنتطرق في هذا المطلب إلى إجرائين:

الفرع الأول: الاجراءات المادية

تتمثل في المعاينة والتفتيش والضبط.

أولا: المعاينة: يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيها الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف عن الجريمة وعن مرتكبيها[1] .

وبالتالي يجب على السلطات المختصة بإجراء المعاينة الانتقال إلى أماكن وقوع الجريمة وإجراء المعاينة التي تسمح للجاني بتغيير او إزالة كل او بعض الآثار المادية للجريمة التي تساعد في التنقيب عن الحقيقة وحتى لا يقع الشك في الدليل المستنبط منه وهذا ما أكدته المادة 42 من ق.إ.ج.ج.

أ/شروط صحة معاينة مسرح جرائم الأنترنت:

حتى تتحقق المعاينة الغرض المرجو منها في كشف الحقيقة يجب التقيد بعدّة شروط وهي:

1-على السلطة المختصة بالتحقيق الانتقال فور وصول خبر وقوع الجريمة إلى مكان الواقعة[2].

2-السيطرة والتحكم على مكان وقوع الجريمة المعلوماتية، عند وصول سلطة التحقيق لمكان الحادث لمعاينة وجب السيطرة عليه وذلك يمنع أي شخص من مبارحة مكان الواقعة ريثما تنتهي الشرطة القضائية من تحرياتها وكذلك منع أي شخص بداخل مسرح الجريمة حتى لا يؤدي إلى تغيير آثار والأدلة المستمدة من الواقعة سواء بقصد أو بخطأ.

3-قيام الخبراء محل حسب اختصاصه بدفع أثار.

4- الضمان إجراء معاينة بصورة مرتبة ومتسلسلة ينبغي على السلطة المختصة الالتزام بالطرق التالية:

-تحديد نقاط بدء في المعاينة.

[1] – بعرة سعيدة، المرجع السابق، المرجع السابق، ص75.

[2] – بعرة سعيدة، المرجع نفسه، ص76.

-عدم الانتقال من مكان لآخر إلا بعد التأكد من معاينته تمام.

5-الدقة والعناية الفائقة في معاينة مسرح الجرائم المعلوماتية وذلك بوصف المنطقة التي ارتكبت فيها الجريمة (يجب معاينة كل المنافذ الدخول والخروج) وكذا وصف المحويات فيما هو مرتبط بالجريمة، كأجهزة الكمبيوتر والماسح.

6-التحفظ على مسرح الجرائم المعلوماتية بعد المعاينة لأن الهدف من الحفاظ على أثار الجريمة بعد انتهاء من المعاينة هو من أجل إمكانية العودة إليه كلما أراد المحقق او القاضي كشف غموض أو التأكد من آثار معينة.

7-تدوين المعاينة ويكون ذلك كتابيا ورسميا وتصويريا[1].

باعتبار المعاينة من أهم اجراءات التحقيق الجنائي فإن أهميتها تتجسد سواء من:

-**الناحية القانونية**: تبدوا اهميتها من عدة اتجاهات منها تأكيد وقوع الجريمة وقف ارتكاب الواقعة الاجرامية، كما تساعد القاضي في تكوين قناعته.

الناحية العملية: فهي تساعد المحقق على تحديد وقت ارتكاب الواقعة الإجرامية ومعرفة علاقة الجاني بالمجني عليه، وتحديد الأسلوب الاجرامي المستعمل، فالانتقال للمعاينة في الجريمة المعلوماتية لا يكون إلى العالم المادي بل إلى العالم الافتراضي أو العالم الفضاء الإلكتروني cyber space والذي يكون عادة الموقع او المكتب الذي توجد فيه مكونات الحاسب الآلي المادية والمعنوية والتي تكون محلا للجريمة أو ادلتها وهي تتمثل في الأجهزة والأنظمة والبرامج، وعليه يتم طرح الاشكال التالي كيف يتم الانتقال والمعاينة إلى العالم الافتراضي؟

يستطيع عضو سلطة التحقيق او مأمور الضبط القضائي ان ينتقل إلى العالم الافتراضي لمعاينته من مكتبه من خلال الحاسوب الموضوع في ذلك الأخسر، كما يمكنه اللجوء إلى مقهى الأنترنت أو إلى بيت الخبرة القضائية او إلى الخبرة الاستشارية وأيضا يجوز له اللجوء إلى مقر مزود الانترنت الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة.

وللمعاينة في جرائم الأنترنت أشكال مختلفة، تختلف بحسب نوعية الجريمة المرتكبة، على أن هناك طرقا عامة تتوافق مع طبيعة الاتصال بالأنترنت أو الوسيلة التي يتم بها ذلك الاتصال فمثلا

[1] - نبيلة هبة هروال، المرجع السابق، ص217- 218.

هناك وسيلة تصوير شاشة الحاسوب والتي قد تكون بواسطة آلة تصوير تقليدية او عن طريق استخدام برمجية حاسوب متخصصة في أخذ صور لما يظهر على الشاشة وهذا ما يصطلح عليه "تجميد مخرجات الشاشة" أو عن طريق حفظ الموقع باستخدام خاصية الحفظ المتوافرة في نظام التشغيل[1].

الخطوات الواجب اتباعها قبل التحرك والانتقال إلى مسرح الجريمة:

وتجدر الإشارة إلى أنه يجب تتبع خطوات معينة قبل التحرك والانتقال إلى مشرح الجريمة ومنها:

1-توفير معلومات مسبقة عن مكان الجريمة، وعن نوع وعدد الاجهزة المتوقع مداهمتها وشبكاتها، لتحديد إمكانيات التعامل معها فنيا من حيث الضبط والتأمين وحفظ المعلومات.

2-إعداد خريطة للموقع الذي تتم الإغارة عليه وإعداد خطة للهجوم على ذلك الماكن.

3-الحصول على الاحتياجات الضرورية من الأجهزة وبرامج صعبة ولينة للاستعانة بها في الفحص والتشغيل.

4-تأمين التيار الكهربائي بحيث لا يتم التلاعب او التخريب عن طريق قطع التيار أو تعديل الطاقة الكهربائية.

5-إعداد فريق تفتيش من المتخصصين وإعداد الأمر القضائي اللازم للقيام بالتفتيش.

كما يجب اتباع الخطوات التالية عند الوصول إلى مسرح الجريمة .

1-تصوير شاشة الحاسب الآلي.

2-عدم نقل أية مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط لموقع الحاسب الآلي من أية مجالات لقوى مغناطيسية (ممرات مغناطيسية) يمكن أن تتسبب في محو البيانات المسجلة.

9-البحث عن خادم الملف لتعطيل حركة الاتصالات

[1] – نبيلة هبة هروال، المرجع السابق، ص218.

4-التحفظ على محتويات بسلة المهملات، والقيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطمة المتواجدة فيها، ورفع البصمات التي قد تكون لها صلة بالرجيمة المرتكبة.

5-الاستعانة بأهل الخبرة عند الضرورة[1].

نطاق إعمال المعاينة الإلكترونية: يعتمد المحقق الجنائي لإجراء المعاينة الالكترونية بحثا عن الأدلة الرقمية على فحص مجموعة مصادر الدليل في البيئة الإلكترونية التي ارتكبت فيها الجريمة المعلوماتية والمتمثلة عادة في مكونات اجهزة الحواسيب الخاصة بالجاني والمجني عليه وملحقاتها وكذا انظمة الاتصال بالأنترنت.

أولا: معاينة مكونات الحاسب

تعتبر الحواسيب مصدرا غنيا بالأدلة الإلكترونية خاصة الحواسيب الشخصية التي تعد بمثابة أرشيف لسلوك الأفراد ونشاطاتهم وخفايا الجريمة الالكترونية باعتبار هذه الاجهزة وسيلة تنفيذها او محل وقوعها والمعروف أن الحاسب الآلي يقوم في تركيبته على ثلاث عناصر أساسية هي القطع الصلبة (hard ware) والقطع المرنة او البرمجيات (soft ware) وكذا المعطيات المعلوماتية أو البينات (données informatique) لذلك فمعاينة هذا الحاسب يستلزم الفحص المادي والمعنوي لكل هذه العناصر نظر للارتباط الطبيعي بين بعضها البعض وقد تعتمد عملية الفحص هنا على طريقتين أساسيتين:

الأولى: هي الفحص الذاتي من خلال قيام الحاسب ذاته بفحص مكوناته وتقديم تقرير كامل إلى طالب الفحص ومثل هذه العملية تتطلب من القائم بها معرفة تقنية ومهارة فنية عالية.

ثانيا: فهي الفحص بواسطة حاسب آلي آخر أو أجهزة تقنية عالية للبحث في جزئية أو جزئيات عبر الحاسب وعادة ما تشمل عملية فحص المكونات الحاسب الآلي العناصر التالية:

ثانيا: معاينة القرص الصلب :يتم معاينة القرص الصلب للحاسب الآلي بالفحص الجزئي أو الكلي للبيانات الرقمية ذات الطابع الثنائي المتواجدة بداخله يقوم المحقق بترع القرص من الحاسب المراد فحصه بكل عناية وحذر من أي ارتجاج أو اصطدام بأي شيء تفاديا لإتلافه أو تعطيله أو فقد أية بيانات، ثم يقوم بفحص وتحليل النسخ التي تصدر من القرص بنفسه أو بواسطة الخبير

[1] - نبيلة هبة هروال، مرجع سابق، ص219- 220.

المختص، والفحص الجزئي للقرص الصلب يسمح للمحقق التعرف على محتوى البيانات ثنائية الرقم التي يؤدي التعامل معها إلى الكشف عن القيمة الاستردادية للبيانات المخزنة فيه سواء كانت محتويات مكتوبة[1] او بصورة مسجلة وكذا استرجاع ما تم حذفه من بيانات ومعلومات وبرامج بالاستعانة ببرمجيات مخصصة لهذا الأمر، فعملية فحص القرص الصلب تساعد المحقق عادة على جمع البيانات والمعطيات المخزنة فيه بشكل آلي او إرادي التي كان يستخدمها الجاني من معلومات او صفحات وعناوين الأنترنت أو رسائل البريد الالكتروني المرسلة وكذا استرجاع ما تم حذفه من بيانات ومعلومات وبرامج بالاستعانة ببرمجيات مخصصة لهذا الأمر، وتجدر الإشارة إلى أن عملية فحص القرص الصلب كي تكون مجدية لا بد من مراعاة مسائل عدة منها كيفية التي يتم ضبط الحاسب وفحص القرص الصلب عنه ومهارة الشخص القائم لاستخلاص البيانات دون العبث بمحتوياتها وكذلك مراعاة شرط سلامة الحاسب الآلي، الذي يعني صحة حركة القطع الصلبة فيه لتجنب رفض المحكمة الاعتداء بالدليل المنبثق عنه.

2-معاينة البرمجيات: بتبع المحقق في هذه العملية طريقتين هما:

الفحص الداخلي: تّبع المحقق في هذه العملية طريقتين هما، الفحص الداخلي للبرمجيات والفحص الخارجي لها. فأما الفحص الداخلي، فيتم من خلال البحث عن البناء المنطقي للبرمجية بما يكشف عن وجود مجهودا في إعداده للعمل حين إنزاله في جهاز الحاسب الآلي، وذلك بتتبع الخطوات المنطقية التي تعبر عن هذا الجهد، ولعل أكثر ما يسعى المحقق الوصول إليه في إطار الفحص الداخلي هو مصدر الملفات الموجودة داخل البرمجيات التي تفيد في ترتيب حدوث الجريمة الالكترونية، والتع رف على الكيفية التي تم الإعداد لها. علما أن النسخ عبر الانترنت يختلف عن النسخ باستخدام برمجيات المعالجة فالأول نسخ عبر العالم الافتراضي أما النسخ الثاني فيتم لاستخدام مصنف متداول في العالم المادي.

الفحص الخارجي: فيتم بواسطة البحث عن البناء المنطقي للبرمجية للتأكد مما إذا

كانت هذه الأخيرة منسوخة أم لا، ثم مقارنة النسخة الأصلية بالنسخة محل الاشتباه للدلالة على ثبوت ارتكاب الجريمة بدرجة مقنعة.

[1] – خالد ممدوح إبراهيم، المرجع السابق، ص215.

3-**معاينة النظام المعلوماتي:** المقصود به هو قيام المحقق بفحص وضبط كافة المعلومات المخزنة في ذاكرة تخزين الحاسب على شكل ملفات والتي يمكن استردادها عبره بأية حركة استردادية ممكنة، ما دام موضوعها يشكل جريمة ...وقد اكد المختصون في مجال تكنولوجيا الاعلام والاتصال بأن نظام التخزين في ذاكرة الحاسب يعد مصدرا مهما للدليل الالكتروني، لأنه يسمح للحاسب الآلي بالاحتفاظ بصفة آلية بنسخة كاملة مما اطلع عليه المشتبه فبيه من مواقع وصفحات الأنترنت أثناء ايجاره عبر العالم الافتراضي[1].

ثانيا: التفتيش

يعتبر التفتيش من إجراءات التحقيق بمعناه الفني القانوني الدقيق يجريه ضابط الشرطة القضائية لإثبات الجريمة او نفيها سواء كان التفتيش متعلقا بشخص او مكان او شيء حسب طبيعته لضبط الأدلة ويعتبر هذا الإجراء من أهم الإجراءات لأنه يمس حق الإنسان في احترام شخصيته كإنسان وكفالة حياته الخاصة من حرية الأفعال وحرية اختيار المسكن ومن ان يكون آمنا في مسكنه (حرمة المسكن) وفي حرية وسرية اتصالاته ومراسلاته، ولهذه الأهمية حرصت الدساتير على صبانة حرمة الأشخاص والمساكن واتصالاتهم ومراسلاتهم وعدم جواز المساس بها إلا بأمر قضائي مسبب او في حالة التلبس بالجرم المشهود[2].

لا يختلف معنى التفتيش في الجريمة التقليدية عن الجريمة المعلوماتية وبالتالي يقصد به إجراء من إجراءات التحقيق الذي يهدف إلى إظهار الحقيقة، حيث تباشر السلطة المختصة بالدخول إلى نظم المعالجة الآلية للمعطيات.

أ/خصائص التفتيش:

-إجراء من إجراءات التحقيق الابتدائي والذي يدخل ضمن الاختصاصات العادية لقاضي التحقيق وهذا ما نصت عليه المادة 68 ف1 ق.إ.ج واستثناء يجوز لضباط الشرطة القضائية القيام بهذا الإجراء بناءا على شروط وهذا ما تبينه المادة 17 ق.إ.ج.

[1] – خالد ممدوح إبراهيم، المرجع السابق، ص62.

[2] – مصطفى محمد موسى، المرجع السابق، ص190.

-انه يهدف إلى البحث عن ادلة مادية للجريمة والتي تؤثر في اقتناع القاضي (قد يترك الجاني وسائل وادوات التي استخدمها في ارتكابه للجريمة او بصمات الأصبع).

-أن تكون الأدلة ناشئة عن جنائية او جنحة تحقق وقوعها، باعتبار التفتيش عمل من أعمال التحقيق فلا يجوز إجراءه إلا إذا وقعت الجريمة بالفعل وكانت مما يصفها القانون بجناية أو جنحة وبالتالي لا يجوز التفتيش في المخالفات نظرا لضآلتها ولعدم خطورتها[1].

أن يقع التفتيش على محل يتمتع بحرمة المسكن أو الشخص:

يقع التفتيش على حرمة المسكن أو الشخص، ذلك أن قيام ضابط الشرطة القضائية بالبحث والتحري في الطرق العامة أو في الغابات...الخ، لا يعد تفتيشا لانتفاء حرمة المكان، وعليه فهو إجراء

من إجراءات الاستدلال والذي يدخل في اختصاصاتهم العادية.

5-أن يتم التفتيش وفقا للإجراءات القانونية المقررة:

يتم القيام بإجراء التفتيش وفقا للشروط القانونية، بحيث يجب مباشرته طبقا لإجراءات صحيحة فإذا شاب التفتيش الواقع على نظم الحاسوب عيب فإنه باطل، لأن التفتيش الذي يقوم به المحقق بغير الشروط المنصوص عليها في القانون يعتبر باطل بطلان مطلق، وبالتالي لا يجوز التمسك بما ورد في محضر التفتيش وكما لا يجوز للمحكمة الاعتماد عليه في إصدار حكمها[2].

ب-شروط تفتيش جرائم الأنترنت:

يعتبر التفتيش انتهاك على الحق في الخصوصية الفردية، ومن ثم يعد التفتيش أحد مظاهر تقييد الحريات الإنسانية، لذا عمدت الدول على إحاطته بالضمانات القانونية والضوابط التي يجب على المحقق احترامها والتقيد بها قبل وأثناء قيامه بعملية التفتيش منها ما يتعلق بمحل التفتيش وما هو اجرائي.

محل التفتيش: يقصد به المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره وخصوصيته والسر الذي يحميه القانون هو ذلك الذي يودع في محل له حرمة كالمسكن أو سيارة

[1] - بعرة سعيدة، المرجع السابق، ص 79.

[2] - براهيمي جمال، المجرع السابق، ص 15.

او رسائل وبالتالي فمحل التفتيش قد يكون أحد المواقع المذكورة مع مراعاة الاجراءات والشروط القانونية المقررة للموقع على حدى.

ولما كان المستودع في الجرائم المعلوماتية هو الحاسب الآلي الذي يقوم في تركيبه على مكونات (Hard -ware) كوحدات المعالجة المركزية، وجدات الادخال والاخراج ووحدات التخزين، ومكونات أخرى منطقية كبرامج النظام الأساسية، البرامج التطبيقية والبيانات المعالجة آليا.

تفتيش المكونات المادية للحاسب: ليس هناك خلاف أن الولوج إلى المكونات المادية للحاسب الآلي بحثا عن أدلة مادية تكشف عن حقيقة الجريمة الالكترونية[1] ومرتكبيها بخضع لإجراءات التفتيش هذه الكيانات المادية يتوقف أساسا على طبيعة المكان الذي يتواجد فيه ما إن كان عاما او خاصا فغن كانت موجودة في مكان خاص لمسكن المتهم أو أحد ملقحاته كان له حكمه بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المساكن وملحقاتها وبإجراءات والضمانات المقررة قانونا في التشريعات.

ففي القانون الجزائري يشترط المواد من (44-47 ق.إ.ج) للقيام بإجراء تفتيش مسكن في الجرائم المتلبس بها الحصول مسبقا على إذن قبل الدخول إلى المسكن والشروع في التفتيش، على أن يكون التفتيش نارا في الفترة الممتدة من 05 صباحا إلى 08 مساءا بحضور صاحب السكن أو ممثله، وإن تعذر استدعى ضابط الشرطة القضائية القائم بالتفتيش شاهدين من غير الموظفين الخاضعين لسلطته.

وينبغي التمييز داخل المكان الخاص بين ما إذا كانت مكونات لحاسب منعزلة أم أنها متصلة بحواسيب أو أجهزة متواجدة في مكان آخر كمسكن الغير، ففي هذه الحالة يجب على المحقق مراعاة القيود والضمانات التي يشترطها القانون لتفتيش هذه الأماكن، ولكن وبتعديل قانون الاجراءات الجزائية بالقانون 22/06 المؤرخ في 2006/12/20 استفى بموجب الفقرة الأخيرة من المادة 45 ق.إ.ج والفقرة الثانية من المادة 47 ق.إ.ج والفقرة الثالثة من المادة 64 عن تطبيق كل الضمانات المقررة لتفتيش المساكن عندما يتعلق الأمر بالتفتيش في الجرائم الالكترونية بحيث

[1] – بن مكي نجاة، السياسة الجنائية لمكافحة الجرائم المعلوماتية، مذكر مقدمة لنيل شهاد الماجستير في القانون الدولي، زواقري، الطاهر، معهد العلوم القانونية والإدارية، مدرسة الدكتوراه، قطب خنشلة، 2008-2009، ص15.

أصبح من الممكن القيام بتفتيش مسكن المتهم في الجريمة الالكترونية في أي ساعة من الليل أو النهار ودون حاجة لرضائه ولا لحضوره أثناء التفتيش.

اما إذا كانت المكونات المادية للحاسوب متواجدة في أماكن عامة سواء اكانت عامة بطبيعتها كالحدائق العامة أو الطرق العامة، أم أماكن عامة بالتخصيص كما هي الأنترنت ومحلات بيع وصيانة الحواسب، فإجراءات تفتيشها تكون وفقا للإجراءات الخاصة بتلك الأماكن وكذلك بالنسبة للمكونات الموجودة بحوزة شخص ما، بغض النظر إن كان مبرمجا او عامل صيانة أو موظفا في شركة تنتج الحاسب الآلي، فإن التفتيش هذه المكونات يخضع لأحكام تفتيش الأشخاص وبالشروط والضمانات القانونية المحددة لذلك[1].

تفتيش المكونات المعنوية للحاسوب: مكونات المعنوية للحاسوب متمثلة في المعلومات والبيانات المعالجة آليا، فهي محل خلاف باعتبارها غير مادية وقد نص المشرع الجزائري في المادة 81 ق.إ.ج على عبارة "أشياء" فهذه العبارة يدخل في مضمونها الأشياء المادية والمعنوية وهذا ما أدى ببعض الفقهاء الفرنسيين بالتفسير إلى أن برامج الحاسب الآلي ذات كيان مادي يشمل على نبضات وذبذبات إلكترونية ممغنطة قابلة للتخزين داخل الجهاز أو على الأقراص الصلبة، كما يجب الأخذ بعين الاعتبار القيمة التي يتمتع بها شيء محل الحماية الجنائية والتي قد تكون غالبا مصلحة اقتصادية يصل إليها صاحبها لذلك فالأشياء المعنوية مثلها مثل الأشياء المادية إلا أن العائق يكمن في صعوبة إجراء التفتيش والتحري عن الأدلة الإلكترونية وذلك راجع إلى:

-نقص المعرفة والدراية في فن التعامل مع البرامج والبيانات المخزنة أليا من قبل السلطات المختصة بالتفتيش .

-صعوبة تحديد أو تخصيص محل التفتيش والأشياء التي يهدف إلى ضبطها، نظرا لارتباطها بالجوانب التقنية والفنية التي تتطلب من المختصين بالتفتيش على العلم بكيفية التعامل مع الأرقام السرية والبرامج والسجلات المخزنة في الحاسب الآلي.

[1] – براهيمي جمال، المرجع السابق، ص16.

-وجود صعوبة في التحكم بالأجهزة التي يستهدف تفتيش النظام المعلوماتي فيها خاصة عند وجود جهازين في مكانين مختلفين[1].

مدى خضوع شبكات الحاسب الآلي للتفتيش:

قد يكون حاسب المتهم متصل بغيره من الحواسيب عبر الشبكة الإلكترونية، وهنا يجب التمييز بين ما إذا كان حاسوب المتهم متصلا بآخر داخل إقليم الدولة، أو كان متصلا بحاسوب يقع في نطاق إقليم دولة أخرى.

أ -حالة وجود جهاز متصل بجهاز المتهم داخل الدولة نفسها

تتحقق هذه الحالة حينما يقوم المتهم بتحويل عبر الأنترنت معلومات أو بيانات متعلقة بجريمة إلكترونية من حاسبه إلى حاسب أو منظومة معلوماتية مملوكة للغير متواجدة في مكان آخر وتخزينها فيها، ففي هذه الحالة تواجه السلطات التحقيق مشكلة تجاوز الاختصاص المكاني من ناحية والاعتداء على حرمة خصوصية الغير من ناحية أخرى لاسيما في الدول العربية التي لم تفصل قوانينها الاجرائية في هذه المسألة.

نتيجة لذلك عمدت بعض التشريعات الاجرائية إلى تنظيم هذه المسألة وإزالة الابهام عنها، بالنص صراحة على إمكانية وجوزا امتداد الحق في التفتيش عند الحاجة ليشمل أجهزة الحاسب أو أية منظومة معلوماتية مرتبط بحاسب المتهم الجاري تفتيشه، وضبط كل البيانات الضرورية لإثبات الجريمة دون التقيد بالحصول على إذن مسبق آخر من السلطات القضائية المختصة بخصوص هذا الامتداد، فالمشرع الجزائري نص في المادة 05 ف 02 من قانون 04/09 لسنة 2009 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها في حالة تفتيش منظومة او جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الاولى، يجوز تحديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك...".

[1] - بن مكي نجاة، المرجع السابق، ص220-222.

حالة وجود جهاز متصل بجهاز المتهم داخل اقليم دولة أجنبية:

تتحقق هذه الحالة حينما يقوم المجرم الالكتروني بتخزين بيانات أو معلومات تفيد اثبات الجريمة في حاسب أو منظومة متواجدة خارج اقليم الدولة التي يقيم فيها عن طريق شبكة الأنترنت بهدف عرقلة سطات التحقيق مشكلة كبيرة تتمثل في مدى جواز تمديد إجراءات البحث والتفتيش إلى خارج اقليم الجغرافي للدولة التي صدر من جهتها المختصة الإذن بالتفتيش والحضور في المجال الجغرافي لدولة أخرى، وهو ما يسمى بالتفتيش العابر للحدود.

يجوز للسلطات التابعة لدولة ما اللجوء إلى التفتيش الإلكتروني العابر للحدود لاسترجاع بيانات مخزنة في الخارج إلا في إطار اتفاقيات تعاون خاصة ثنائية او جماعية تجيز هذا الامتداد ولكن بحسب الطابع السرعة الفائقة الذي يجري عليه نقل المعلومات الاجرامية وتهريبها للخارج قصد تخزينها واخفائها وما يستدعيه من الاستعجال في التعقب أثارها للقيام بتفتيش الأنظمة حتى ولو كانت بالخارج[1].

خوّل المشرع الجزائري على غرار التشريعات الأخرى سلطات التحقيق الحق بالتفتيش عن بعد الأنظمة المعلوماتية ولو كانت متواجدة خارج الاقليم وذلك بنصه في المادة 05 ف 03 من قانون 04/09.[2]

ثالثا: الضبط

يقصد بالضبط في جرائم المعلوماتية ضبط الأشياء لأنها من اجراءات جمع الأدلة وهو جائز سواء اكان الشيء مملوكا للمتهم أو لغيره من الأشخاص.

تعريف الضبط: هو العثور على أدلة في الجريمة التي يباشرها التحقيق بشأنها والتحفظ عليها والضبط هو الغاية من التفتيش ونتيجة المباشرة المستهدفة وذلك يتعين عند اجراءاته أن تتوفر فيه نفس القواعد التي تنطبق بشأن التفتيش ويؤدي بطلان التفتيش إلى بطلان الضبط ويترتب على هذا الارتباط بين التفتيش والضبط أن الضبط لا يجوز أن يقع على شيء إلا وصفه دليلا من أدلة الجريمة التي يجري التفتيش بشأنها، ولذلك فإنه يباشر من أجل الحقيقة المطلقة بمعنى أنه ما دام

[1] –براهيمي جمال، المرجع السابق، ص27.

[2] – المادة 05 ف 03 من القانون 04/09 المتعلق بالوقاية من جرائم المتصلة وتكنولوجيا الاعلام والاتصال.

التفتيش يستهدف ذات الحقيقة فيتعين أن يباشر ضبطها يتعلق بها من أدلة سواء كانت للإدانة أم للبراءة[1].

الأشياء محل ضبط في الجرائم المعلوماتية: يقع الضبط على الأشياء المادية وهذه قد تكون منقولة أو عقارية.

الأشياء المنقولة في الجرائم المعلوماتية: يشمل المنقول بطبيعته وهو ما يمكن نقله من مكان لآخر بدون تلف، كالحاسب الآلي الرقمي المحمول والنقال وأثاث مقهى الأنترنت ويشمل العقار بالتخصيص مثل الحاسب الآلي بمقهى الأنترنت وملحقاته من طابعات وتصوير (سكانير) وكذلك الأشياء الثابتة إذا نزعت عن أصلها المثبتة به مثل الكالات الموصولة للحاسب الآلي الرقمي.

المقصود بالعقار في الجرائم الالكترونية: يقصد بالعقار في الجرائم الالكترونية المكان مثل مقاهي الأنترنت التي قد تترك الجريمة المعلوماتية أثارا بمكان أو خلفت فيه أشياء تفيد التحقيق وتقتضي الكشف عنها مما يستدعي ضبط العقار لمصلحة التحقيق وذلك يوضح الأختام عليه وغلقه وإقامة حراس عليه[2].

ومنه بالأشياء التي يتم ضبطها في مجال الجرائم المعلوماتية والتي لها قيمة في الاثبات هي:

1-ضبط جهاز الحاسوب وملحقاته

2-ضبط المعدات المستعملة في شبكة الانترنت

3-ضبط وسائل التخزين المتحركة كالأقراص المدمجة والأقراص المرنة والأشرطة المغناطيسية

4-ضبط البرمجيات

5-ضبط البريد الالكتروني والذي يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الوسائل الالكترونية[3].

مدى صلاحية الضبط في الجريمة المعلوماتية: محل الضبط في الجريمة المعلوماتية لا يرد إلا على الأشياء كما سبق وان ذكرنا اما الأشخاص فلا يصلحون ليكونوا محلا للضبط إلا في حالات

[1] – مصطفى محمد موسى، المرجع السابق، ص208-211.

[2] – مصطفى محمد موسى، المرجع نفسه، ص211.

[3] – عبد الفتاح بيومي حجازي، المرجع السابق، ص 396-401.

استثنائية وإن كانت بعض القوانين تتحدث عن ضبط الأشخاص واحضارهم فإنه يعني القبض عليهم والقبض نظام قانوني يختلف عن الضبط، نظرا لكون محل الضبط في مجال الجريمة المعلوماتية هو البيانات المعالجة الكترونيا، فقد أثارت هذه المسألة جدلا فانقسم الفقه إلى اتجاهين يرى البعض أن بيانات الحاسوب لا تصلح أن تكون محلا للضبط لانتفاء الكيان المادي عنها ولا سبيل لضبطها إلا بعد نقلها إلى كيان مادي ملموس ويستند هذا الرأي إلى النصوص التشريعي المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة اما الرأي الثاني يرى أن البيانات ما هي إلا ذبذبات الكترونية أو موجات كهرومغناطيسية قابلة للتسجل والحفظ والتخريب على وسائط مادية وبإمكان نقلها وبثها واستقبالها وإعادة انتاجها فوجودها المادي لا يمكن انكاره.

الصعوبات التي تواجه عملية الضبط: عملية ضبط البيانات المعالجة الكترونيا تواجه عدة صعوبات منها:

-حجم الشبكة التي تحتوي على المعلومات المعالجة الكترونيا والمطلوب ضبطها

- وجود بيانات في شبكات أو اجهزة تابعة لدولة أجنبية

- يشمل التفتيش الضبط أحيانا اعتداء على حقوق الغير، او على حرمة حياتهم الخاصة، فيجب اتخاذ الضمانان اللازمة لحماية هذه الحقوق والحريات[1].

الفرع الثاني: الإجراءات الشخصية

هي غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على الدليل وتتمثل في:

أولا: الخبرة التقنية في جريمة الأنترنت:

أدى التطور التقني الهائل في عالم تكنولوجيا الإعلام والاتصال إلى احداث تغيير كبير في المفاهيم المتعلقة بالدليل الجنائي، مما أدى بدوره إلى تعاظم دور الإثبات العلمي للدليل وإعلان انضمام الخبرة التقنية إلى عالم الخبرة القضائية، وأصبحت الاستعانة بخبراء مختصين لفحص الأدلة التقنية وتقويم عملية الإثبات الرقمي وتحليل الجريمة الالكترونية أمرا ملحا لا يمكن الاستغناء عنه.

أ-دور الخبرة التقنية في اثبات جريمة الأنترنت:

[1] - يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنسل شهادة الماستر، جامعة محمد بوضياف، المسيلة، 2016-2017، ص32-33.

تعرف الخبرة الفنية بأنها إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق والقضاء، من أجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشأن وقوع جريمة أو نسبتها إلى المتهم، فهي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته على نحو المسائل التي يحتاج تقديرها بمعرفة فنية و دراية علمية لا تتوفر لديه.

وللخبرة الفنية دور كبير في إثبات جريمة الانترنت، لأنها تنير الدرب لسلطات التحقيق والقضاء وسائر الجهات المختصة بالدعوى الجزائية للوصول إلى الحقيقة وتحقيق العدالة الجنائية، لذلك ومنذ تفشي الجرائم الالكترونية، تستعين سلطات التحقيق والاستدلال والمحاكمة بأصحاب الخبرة الفنية المتميزة في مجال التقنية الالكترونية من أجل كشف غموض الجريمة وتجميع أدلتها والتحفظ عنها، أو مساعدة المحقق في إجلاء جوانب، الغموض في العمليات الالكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق.

وتبرز أهمية الاستعانة بالخبير الفني لإثبات جرائم الانترنت بشكل أكبر عند غيابه، فقد تعجز سلطات التحقيق والاستدلال عن إماطة اللثام عن الجريمة وجمع الدليل بخصوصها لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل أو محوه بسبب الجهل أو الإهمال عند التعامل معه.

ولعل إدراك بعض دول العالم لهذه الأهمية، جعلها لا تكتفي بالنصوص التقليدية التي تنظم الخبرة الفنية، وإنما أسرعت إلى تدعيمها بنصوص قانونية جديدة خاصة بالخبرة في مجال جرائم التقنية العالية، نذكر في مقدمتها قانون الإجرام الالكتروني البلجيكي الصادر في 2000/11/23 الذي نص في المادة 88 "على أنه" يجوز لقاضي التحقيق والشرطة القضائية الاستعانة بخبير مختص من أجل الحصول و بطريقة مفهومة على المعلومات اللازمة عن كيفية تشغيل نظام الحاسب الآلي والولوج إلى داخله، أو الولوج إلى البيانات المخزونة فيه أو المعالجة أو المنقولة بواسطته". وتضيف نفس المادة بأنه لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو أخذ نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة، على أن يتم ذلك

بالطريقة التي تريدها جهة التحقيق، وعلى الخبير الاستجابة لطلب هيئات التحقيق والقضاء و إلا تعرض لعقوبات جزائية[1].

و لم يتخلف المشرع الجزائري عن هذه التشريعات، اذ نص في المادة 05 الفقرة الأخيرة من القانون رقم 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة تكنولوجيا الإعلام والاتصال ومكافحتها بأنه:" يمكن للسلطات المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية معطيات المعلومات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها"[2]

ب–أنواع الخبراء الالكترونيون: الخبير في جريمة الأنترنت هو الفني المتخصص وصاحب الخبرة في التقنية الالكترونية وشبكاتها ويتمثل الخبراء الالكترونيون فيما يلي:

-المبرمجون

-المحلل: هو الشخص الذي يضع خطوات العمل ويقوم بتجميع بيانات النظام المعين.

-مهندس الصيانة والاتصالات

-مشغل الحاسب الآلي وشبكاته

-مدير النظام المعلوماتي[3].

لقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة في المواد 143 إلى 156 من قانون الإجراءات الجزائية واعتبرها من اجراءات البحث عن الدليل حيث نصت المادة 143 على أنه الجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما من تلقاء نفسها أو بطلب من النيابة العامة أو بطلب من الخصوم[4].

[1] – براهيمي جمال، المرجع السابق، ص70

[2] – مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، دار الكتب والوثائق القومية، القاهرة، 2008، ص172.

[3] – أنظر المادة 05 من القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائن المتصلة تكنولوجيا الاعلام والاتصال ومكافحتها.

[4] – القانون رقم 155/66 المؤرخ في 08 يونيو 1966 المعدل والمتمم لقانون الاجراءات الجزائية، الجريدة الرسمية العدد 48.

ثانيا: الاستجواب وسماع الشهود في جريمة الأنترنت

يستدعي أشخاص للإدلاء بأقوالهم، قد يكونون مشتبه فيهم وهذا ما يطلق عليه الاستجواب، وقد يكون هؤلاء أشخاص خارجين عن الخصومة إلا أنهم يؤثرون على مسار القضية من خلال شهادتهم.

1-الاستجواب في جريمة الأنترنت:

الاستجواب هو مناقشة المتهم بالتهمة والوقائع المنسوبة إليه ومواجهته بالأدلة القائمة ضده، والمتهم حر في الإجابة عن الأسئلة الموجهة إليه ولا يعد امتناعه قرينة ضده، وهو وسيلة تمحيص للتهمة أو لنفيها عنه، والاستجواب ذو طبيعة مزدوجة، فهو أداة اتهام ووسيلة دفاع في آن واحد، وقد عرفته محكمة النقض المصرية بأنه" مناقشة المتهم مناقشة تفصيلية في أمور التهمة وأحوالها وظروفها ومجابهته بما قام عليه من الأدلة، ومناقشته في أجوبته مناقشة يراد بها استخلاص الحقيقة التي يكون كاتما لها، وكذا مجابهته بالأدلة.

وينقسم الاستجواب إلى:

أولا /الاستجواب عند الحضور الأول في جريمة الأنترنت:

وهو أن يمثل المتهم أمام المحقق لأول مرة وذلك حتى يتحقق من هويته ويحيطه علما بكل الوقائع المنسوبة إليه وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخير المتهم في أن له الحق في توكيل محام وإن كان غير قادر ماديا يجوز للمحقق أن يعين له محام من تلقاء نفسه، كما يجب على المتهم إذا ما طرا تغير على عنوانه أن يخطر المحقق[1].

ثانيا/ الاستجواب في الموضوع

ويعني الاستجواب مواجهة المتهم بالتهمة والوقائع المنسوبة إليه ومناقشته فيهما مناقشة تفصيلية ومواجهته بالأدلة القائمة ضده ومطالبته بإبداء رأيه فيها ويكون إجباري كما . هو الشأن بالنسبة للجنايات أو اختياري في الجنح.

[1] – عبد الرحمن خلفي، محاضرات في قانون الاجراءات الجزائية، دار الهدى، الجزائر، ص168.

ثالثا: الشهادة:

-سماع الشهود في جريمة الأنترنت:

سماع الشهود هو إجراء من إجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة بحيث يستدعى أشخاص ليست لهم علاقة بالجريمة إلا أن وجودهم ضروري للكشف عن الجرائم والقبض عن مرتكبيها، وتختلف الشاهد عن الحضور للإدلاء بشهادته يعرض للمسائلة الجنائية، وعليه نتطرق لتعريف الشهادة.

أولا: تعريف الشهادة وأنواعها

تختلف الشهادة في الجريمة الالكترونية عنه في الجرائم الأخرى، لاشتراط صفات خاصة بالشاهد في الجريمة المعلوماتية.

تعريف الشهادة

هناك من عرف الشهادة بأنها الأقوال التي يدلي بها الخصوم أمام سلطة التحقيق أو الحكم في شأن جريمة وقعت سواء تتعلق بثبوت الجريمة وظروف ارتكابها أو إسنادها إلى المتهم أو براءته منها، وعرفها الدكتور عاطف النقيب " إنها تقرير الشخص لحقيقة أمر كان قد رآه أو سمعه " ، عرفها الدكتور احمد فتحي السرور "إثبات واقعة معينة من خلال ما يقوله احد الأشخاص عما شاهده أو سمعه أو أدركه بحواسه عن هذه الواقعة بطريقة مباشرة كما عرفها أبو العلاء النمر بأنها التعبير الصادق الذي يصدر في مجلس القضاء من شخص:" يقبل قوله بعد أداء اليمين في شان واقعة عاينها بحاسة من حواسه"

وعرفها اليأس أبو عبيد: "الشهادة قانونا تقوم على إخبار شفوي يدلي به الشاهد في مجلس القضاء بعد يمين يؤديها على الوجه الصحيح"

وعرفها البعض الآخر بأنها:""إثبات واقعة معينة من خلال ما يقوله احد الأشخاص . "عما شاهده أو سمعه أو أدركه بحواسه عن هذه الواقعة بطريقة مباشرة"

وهناك من عرف الشهادة بأنها الأقوال التي يدلي بها الخصوم أمام سلطة التحقيق أو الحكم في شأن جريمة وقعت سواء تتعلق بثبوت الجريمة وظروف ارتكابها أو إسنادها إلى المتهم أو براءته منها.

وتخضع الشهادة إلى عدة قواعد من بينها:

تكليف الشاهد بالحضور بواسطة القوة العمومية، كما يجب أن تسلم نسخة من طلب الاستدعاء إلى الشخص المطلوب حضوره، كذلك يجب ذكر هوية الشاهد قبل سماع شهادته وعليه ذكر قرابته أو نسبه للخصوم ومن أهم واجبات الشاهد حلف اليمين، وتجدر الإشارة . إلى انه يجوز سماع شهادة القصر وذوي العاهات وذلك وفقا لإجراءات خاصة بكل حالة .

وتؤدى الشهادات بانفراد وأخيرا تدون الشهادات بمحاضر خصصت لذلك دون حشي، أو تصحيح أو تجريح، يصادق على المحضر كل من المحقق والكاتب والشاهد.

أنواع الشهادة: [1]

تقسم الشهادة إلى 03 أنواع:

1- الشهادة المباشرة: هي أن يشهد الشاهد بما شاهده أو وقع تحت سمعه.

2- الشهادة السماعية: بمعنى من علم بالأمر من الغير شهادة سماعية بحيث لا يشهد الشخص بما رآه أو سمعه مباشرة، بل يشهد بما سمعه رواية عن الغير فيشهد مثلا أنه سمع شخصا يروي واقعة معينة، وهي أقل شأنا من الشهادة الأصلية المباشرة.

3- الشهادة بالتسامع: وهذه الشهادة تختلف عن الشهادة السماعية حيث تتعلق هذه الأخيرة بأمر معين نقلا عن شخص معين قد شاهد هذا الأمر بنفسه، أما الشهادة بالتسامع فتتعلق بواقعة معينة ليست نقلا عن شخص معين بالذات ساهد الأمر بنفسه كان يقول الشاهد سمعت كذا[2].

ثانيا: الشهادة الالكترونية (الشاهد الالكتروني)

يطلق عليه اسم الشاهد المعلوماتي لأنه هو الشخص الفني صاحب الخبرة والمتخصص في التقنية وعلوم الحاسب الآلي، والذي يكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات فلذلك نجد ان الشاهد المعلوماتي له عدة طوائف تتمثل في:

-مشغل الحاسب الآلي

[1] – نجي فاطمة الزهرة، مرجع سابق، ص66.

[2] – عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر، دار شتات للنشر، مصر، 2007ن ص87.

-خبراء البرمجة

-المحللون

-مهندسو الصيانة والاتصالات.

-مدير النظم.

1-**مشغلو الحاسب الآلي**: عامل تشغيل الآلي هو ذلك الشخص المسؤول عن تشغيل الجهاز والمعدات المتصلة به حيث تكون لديه الخبرة في مجال الحاسب الآلي عن طريق استخدام البيانات واستخراجها وهو يقوم بنقل البيانات من الوثائق إلى وسائط التخزين التي تجرى معالجتها بواسطة الحاسب الآلي.

كما تكون لديه الخبرة الواسعة في الكتابة السريعة عن طريق لوحة المفاتيح الحاسب الآلي.

2-**خبراء البرمجة**: أو مخططو البرامج وهم الأشخاص المتخصصون في كتابة أوامر البرامج وينقسمون إلى فئتين الأولى هم مخططوا برامج التطبيقات والثانية هم مخططو برامج النظم.

3-**المحللون**: هم الأشخاص الذين يحللون الخطوات، ويقومون بتجميع البيانات الخاصة بنظام معين، ودراسة هذه البيانات ثم تحليل النظام -تقسيمه - إلى وحدات منفصلة واستنتاج العلاقة الوظيفية بين هذه الوحدات، كما يتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسوب.

4-**مهندسو الصيانة والاتصالات**: هم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب ومكوناته وشبكات الاتصال المتعلقة به.

5- **مديرو النظم**: هم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية[1] .

قبل التطرف إلى هذا المطلب ارتأينا ان نتطرق إلى تعريف الدليل الالكتروني وأنواعه وأشكاله.

يختلف الوسط الذي ترتكب فيه الجريمة المعلوماتية من وسط مادي إلى وسط معنوي (الوسط الافتراضي) مما ادى إلى ظهور ادلة جنائية خاصة يمكن الاعتماد عليها في الاثبات بحيث تكون من

[1] - عبد الفتاح بيومي حجازي، المرجع السابق، ص340.

ذات الطبيعة التقنية الناجمة عن النظم الالكتروني التي تنتج منها في حالة الاعتداء عليها حسب ما عبرت عنها الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية.

قبل التطرق إلى المطلب الثاني يمكننا تعريف الدليل الإلكتروني وصوره وأنواعه.

تعريف الدليل الالكتروني: عرفته المنظمة العالمية لدليل الحاسوب في قرار لها في أكتوبر 2011 بأنه:" المعلومات ذات القيمة المحملة والمخزنة أو المنقولة في صورة رقمية، وكانت قد عرفته في مارس 2000 بأنه: "المعلومات المخزنة أو المنقولة والتي يمكن الاعتماد عليها أمام المحكمة، وعلى ذلك يمكن تعريف الدليل الالكتروني في مجال التحقيق الجنائي بأنه:" المعلومات المخزنة او المنقولة بصيغة رقمية ويعتمد عليها في التحقيقات وأمام المحكمة للإدانة أو البراءة"[1]

وكذلك عرفه الفقه بانه الدليل الذي يتم الحصول عليه بواسطة التقنية الالكترونية من الحاسوب وشبكة الأنترنت والأجهزة الالكترونية الملحقة والمتصلة به وشبكات الاتصال من خلال اجراءات قانونية لتقديمها للقضاء كدليل الكتروني جنائي يصلح للإثبات الجريمة.

أشكال الدليل الالكتروني: للدليل الالكتروني صور وأشكال نذكر منها:

الصورة الرقمية:

هي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية والصورة الرقمية تمثل تكنولوجيا بديل للصورة التقليدية.

2-النصوص المكتوبة:

وتشمل الأوراق التحضيرية التي يتم إعدادها بخط اليد كمسودة أو تصور العملية التي يتم برمجتها، وكذلك نصوص أساسية وقانونية محفوظة في الملفات العادية وتكون لها علاقة بالجريمة.

التسجيلات الصوتية:

وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الانترنت[2].

[1] – مصطفى محمود موسى، المرجع السابق، ص213-217.

[2] – يوسف جفال، المرجع السابق، ص26.

ثالثا :أنواع الدليل الالكتروني

يأخذ الدليل الإلكتروني نوعين رئيسيين :أدلة أ عدت لتكون وسيلة إثبات، وأدلة لم تعد لتكون وسيلة إثبات.

1-أدلة أعدت لتكون وسيلة إثبات:

وهي السجلات التي تم إنشاؤها بواسطة الجهاز تلقائيا، وتعتبر هذه السجلات من مخرجات الجهاز و لم يساهم الانسان في إنشائها، وكذلك السجلات التي تم حفظ جزء منها بالإدخال وجزء تم انشاؤه بواسطة الجهاز.

2-أدلة لم تعد لتكون وسيلة إثبات:

هذا النوع من الأدلة الإلكترونية نشأ دون إ ا ردة الفرد، وله أثر يتركه الجاني دون أن يكون ا رغبا في وجوده ويسمى بالبصمة الإلكترونية وتتجسد في الآثار التي يتركها مستخدم شبكة الانترنت بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسوب أو شبكة الانترنت[1].

المطلب الثاني: الاجراءات الحديثة لجمع الدليل الالكتروني:

الفرع الأول: التسرب

نص المشرع الجزائري على اجراءات خاصة تهدف إلى ضبط الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم الأخرى، وتتمثل هذه الإجراءات في التسرب واعتراض المراسلات وكذلك من خلال القانون 09/ 04 المتضمن القواعد التقليدية الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المراقبة الالكترونية.

أولا: التسرب:

تعتبر الجريمة الإلكترونية من بين الج ا رئم التي يمكن اللجوء فيها إلى إجراء التسرب واعتراض المراسلات إذا اقتضت ذلك ضرورات التحري والتحقيق بشأنها.

[1] – يوسف جفال، المرجع السابق، ص36-37.

1-التسرب (الاختراق).

نضم المشرع الجزائري أحكام التسرب في الفصل الخامس من قانون الإجراءات الجزائية من المادة 65 مكرر 11 إلى مكرر 18 ، حيث بين كيفية القيام بعملية التسرب وكذا ش روط

القيام بهذا الإجراء، وكذلك الأحكام الجزائية لمن تسبب في الكشف عن هوية الضابط أو العون المتسرب، ويتم الاستماع إلى الضابط المتسرب بوصفه شاهدا عن الجرائم المرتكبة بعد انتهاء المهلة المحددة في رخصة التسرب.

أ -مفهوم التسرب:

المقصود بالتسرب: هو قيام ضابط أو عون الشرطة القضائية بمراقبة الاشخاص المشتبه في أنهم ارتكبوا الجريمة بإظهار أنه مساهم معهم أو شريك، بحيث يستعمل الضابط أو العون

هوية مستعارة وذلك إذا ما ارتبط البحث والتحري واحدة من الجرائم التالية:

-1-جرائم المخدرات.

2-الجريمة المنظمة العابرة للحدود الوطنية.

3-الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

4-جرائم تبييض الأموال.

5-الجرائم الموصوفة بأفعال إرهابية أو تخريبية.

6-الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد.

ب -طرق التسرب في مجال جريمة الأنترنت:

يمكن تصور عملية التسرب في نطاق الجرائم الإلكترونية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي، وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها أو اشتراكه في محادثات في غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم، والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما في ذلك أسماء أو صفات هيئات مستعارة

ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام المخترق للمواقع، أو كيفية ارتكاب الجرائم وحتى المشاركة معهم في ارتكابها لتجميع كل ما يمكن جمعه من الأدلة[1].

الضوابط التي تحكم التسرب في جرائم الأنترنت:

نظرا للخطورة التي يشكلها إجراء التسرب على حرمة الحياة الخاصة للمشتبه فيه، فقد قيده المشرع بجملة من الشروط والضوابط الواجب مراعاتها قبل وأثناء مباشرته وهي كالتالي:

أولا-الضوابط الإجرائية: تتلخص الضوابط الإجرائية للتسرب الالكتروني في الإذن القضائي وكل ما يجب أن يتضمنه من أحكام، إذ لا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة والمتمثلة حسب أحكام المادة 65 مكرر 11 ق.إ.ج في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه على أن تتم العملية تحت الرقابة المباشرة للجهة الصادرة للإذن حسب الحالة لتلافي حدوث تجاوزات و تعسف في استعمال هذا الحق.

ولا يكفي أن يصدر الإذن بالتسرب من الجهة المختصة فحسب، بل لابد أن يكون مكتوبا وإلا كان هذا الإجراء باطلا، لأن الأصل في العمل الإجرائي الكتابة، وهو ما أكدته المادة 65 مكرر 15 من ق.إ.ج بنصها " يجب أن يكون الإذن المسلم طبقا للمادة (65 مكرر 11) مكتوبا تحت طائلة البطلان.

كما يشترط أن يتضمن الإذن بالتسرب جملة من البيانات التي يتوقف على تحديدها صحة الإجراء ذاته، كذكر نوع الجريمة محل عملية التسرب واسم ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، وتحديد المدة المطلوبة لهذه العملية، والتي يجب ألا تتجاوز أربعة أشهر قابلة للتجديد حسب مقتضيات التحري والتحقيق ضمن الشروط نفسها. وفي الوقت ذاته يجوز للقاضي الذي أذن بهذا الإجراء أن يأمر بوقفه في أي حين قبل انقضاء الآجال المحددة.

ثانيا-الضوابط الموضوعية :إلى جانب الضوابط الإجرائية المذكورة أعلاه أحاط المشرع عملية التسرب بضوابط أخرى موضوعية يمكن إيجازها في عنصرين أساسين هما:

[1] – المادة 65 مكرر 11 من ق.إ.ج.، ص85.

-الأول هو عنصر التسبيب، تضمنته المادة 65 مكرر 15 ق.إ.ج ويتمثل في المبر ا رت والحجج التي أقنعت الجهات القضائية المختصة لمنح الإذن بإجراء التسرب، وكذا الدوافع والأسباب التي جعلت ضابط الشرطة القضائية يلجأ إلى هذه العملية المتمثلة عادة في ضرورة التحقيق والتي تكون ضمن موضوع طلبه الإذن.

-أما العنصر الثاني، فيتعلق بتحديد نوع الجريمة التي ينصب عليها الإذن بالتسرب والتي يجب ألا تخرج عن نطاق الجرائم السبع التي حددتها على سبيل الحصر المادة (65 مكرر 5)[1].

الفرع الثاني: اعتراض المراسلات والمراقبة الالكترونية:

كان المشرع الفرنسي سباقا إلى تبني عملية اعتراض ومراقبة الاتصالات الالكترونية ضمن إجراءات التحري و التحقيق الجنائي من خلال قانون الاجراءات الجزائية لعام 1991 ثم تلاه المشرع الأمريكي في عام 2000 بمناسبة تعديل القانون الاتحادي الإجرائي الأمريكي، أين تم توسيع مجال تطبيق إجراء الاعتراض والمراقبة ليشمل كل المراسلات السلكية واللاسلكية، ونظرا لثبوت نجاعة هذا الإجراء في تعقب الدليل و إثبات الجرائم الالكترونية، فقد أوصت الاتفاقية الأوروبية حول الجرائم الالكترونية لعام 2001 من خلال نص المادة 21 جميع الدول الأعضاء بضرورة تبني اعتراض المراسلات والمراقبة الالكترونية للاتصالات في تشريعاتها الإجرائية الداخلية ضمن إجراءات البحث والتحقيق الأمر الذي لقي استجابة واسعة من طرف غالبية الدول الأوروبية.

و لم يتخلف المشرع الجزائري عن هاته الدول، بل تدخل بموجب قانون الإجراءات الجزائية رقم 22/06 المؤرخ في 2006/12/20 المعدل و المتمم فاستحدث لهذا الإجراء الفصل الرابع كاملا تحت عنوان " اعتراض المراسلات وتسجيل الأصوات والتقاط صور"

تناول فيه المقصود بهذا الإجراء، نطاقه وضمانات استخدامه. ثم عززه بالقانون رقم 04/09 المؤرخ 5 أوت2009 .

[1]- علاوة عوام، التشرب كآلية للكشف عن الجرائم في القانون الجزائري، مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012، ص03.

مفهوم الاعتراض المراسلات والمراقبة الإلكترونية

عرفت لجنة خبراء البرلمان الأوروبي بمناسبة اجتماعها المنعقد في 2006/10/06 لدراسة أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية عملية اعتراض المراسلات بأنها "عملية مراقبة سرية المراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو مشاركتهم في ارتكاب جريمة".

أما في القانون الجزائري استحدثت بموجب المادة 65 مكرر إلى 65 مكرر 10 ق.إ.ج إمكانية قاضي التحقيق أن يأمر ضابط الشرطة القضائية بترخيص كتابي وتحت اشرافه مباشرة القيام باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية، ووضع الترتيبات التقنية دون موافقة الشخص المعني من أجل القيام بالتقاط وتثبيت وتسجيل وبحث بسرية وفي أي مكان عام أو خاص والتقاط الصور لأي شخص.

وتجدر الإشارة في هذا الصدد إلى أن المراسلات التي يمكن اعتراضها يجب أن تتسم بالخصوصية ولكي تكون كذلك يلزم أن يتوافر فيها عنصران أساسيان هما:

-عنصر موضوعي يتعلق بموضوع ومضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي وسري.

-عنصر شخصي والمراد به إرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون الرسالة لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي.

ويعتبر البريد الإلكتروني أهم وسيلة تقنية في مجال التراسل الالكتروني ومن ثمة فعملية الاعتراض تنصب عليه، ومن المعلوم أن كل رسالة إلكترونية تظهر فيها معلومات عامة مثل تاريخ إنشاء الرسالة وتاريخ تلقيها وكذا عنوان المرسل وعنوان المرسل إليه، وهذه المعلومات ليست كافية لمعرفة المرسل.

تحديد الجرائم محل الاعتراض:

استعانة بعملية اعتراض أو مراقبة المراسلات الالكترونية غير مسموح في كافة الجرائم إنما في الجرائم المذكورة على سبيل الحصر في نص المادة 65 مكرر 5 من ق.إ.ج (جرائم المخدرات،

الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال أو الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد وجرائم الماسة بأنظمة المعالجة الآلية وجرائم المنصوص عليها في الفقرات أ، ب، ج، د من المادة 04 من القانون 04/09 المتمثلة في الأفعال الموصوفة بجرائم الإرهاب والتخريب، الاعتداءات على منظومة معلوماتية الماسة بأمن الدولة بما فيها التي تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني.

مفهوم الرقابة الالكترونية للاتصالات: نجد المشرع الجزائري على غرار العديد من المشرعين لم يقم بتعريف عملية مراقبة الاتصالات الإلكترونية، لكن بعض التشريعات قد قامت بتعريفها مثل التشريع الأمريكي الذي عرفها على أساس أنها: "عملية الاستماع لمحتويات أسلاك أو أي اتصالات شفوية عن طريق استخدام جهاز إلكتروني أو أي جهاز آخر".

إلا أننا يمكن أن نعرفها على أساس أنها إجراء تحقيق يباشر خلسة، وتنتهك فيه سرية الأحاديث الخاصة، تأمر السلطة القضائية في الشكل المحدد قانون يهدف الحصول على دليل غير مادي للجريمة المعلوماتية، ويتضمن من ناحية استراق السمع إلى الأحاديث ومن ناحية أخرى حفظه بواسطة أجهزة متخصصة لذلك.

ونجد أن المشرع من خلال قانون 06-01 قد أشار إلى هذا الإجراء دون تقديم تعريف له. بينما في بينما في القانون 04/09 في المادة 3 منه قد حدد كيفية مراقبة الاتصالات الالكترونية على النحو الآتي: مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو المستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في القانون الإجراءات الجزائية وفي هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية و تجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

وبالتالي فإن مراقبة الاتصالات حددها القانون على سبيل الاستثناء وفي الحالات المحددة حصريا في المادة 4 من القانون 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال[1].

[1] – موساوي سهام، الاطار القانوني للجريمة الالكترونية، مذكرة لنيل شهادة الماستر، جامعة عبد الرحمن ميرة، بجاية، 2017-2018، ص81

المبحث الثاني: مرحلة التحقيق

إذا كان التحقيق يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا تطويرا لأساليبه.

المطلب الأول: مفهوم التحقيق الجنائي في جريمة الأنترنت

تعد مرحلة التحقيق مرحلة هامة في سبيل البحث والتحري عن الجرائم، وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة المعلوماتية لأنها تعد حجر الزاوية التي سوف تأسس عليه مباشرة الدعوى.

الفرع الأول: تعريف التحقيق في جريمة الأنترنت

أولا: تعريف التحقيق والمحقق

عامة يعرف التحقيق إتخاذ جميع الاجراءات والوسائل المشروعة التي يتوصل إلى كشف الحقيقة وإظهارها.

وهو كذلك مجموعة من الاجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع التي يحددها القانون بهدف البحث عن الأدلة وتقديمها والكسف عن الحقيقة في شان الجريمة.

يعرف التحقيق في الجريمة المعلوماتية بأنه عمل قانوني يقوم به الشرطة القضائية لضبط الجرائم الالكترونية الرقمية من فاعل ودليل الكتروني رقمي لتقديمه إلى سلطات التحقيق القضائي في هذه الجرائم لإقامة العدل[1].

تعريف المحقق: هو الشخص القائم بأعمال إجراءات التحقيق الجنائي، وعرف أيضا أنه كل من عهد إليه القانون بتحري التحقيق في البلاغات والحوادث الجنائية، ويساهم بدوره في كشف غموضها وصولا إلى معرفة حقيقة الحادث وكشف مرتكبي هذه الجرائم.

[1] – مصطفى محمود موسى، المرجع السابق، ص23-24.

ثانيا: خصائص التحقيق والمحقق

1-خصائص التحقيق في الجريمة المعلوماتية:

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة وراسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة وهذه القواعد إما قانونية و إما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والامتثال أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته الكثير.

خصائص المحقق في جريمة الأنترنت:

أمام التطور التقني والتكنولوجي الذي صاحب الجريمة المعلوماتية، فإن المتخصصين بالتحقيق في هذا النوع من الجرائم المستحدثة يختلفون عن أولائك المختصين بضبط الجرائم التقليدية من حيث الخصائص وطريقة التكوين، ذلك أن التحقيق في هذه الجرائم لا يعتمد على

التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية وإنما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمة البحث والتحري عن الجرائم المعلوماتية وكشف النقاب عنها[1].

الخصائص الفنية للمحقق:

يجب أن تتوافر بعض الأمور في المحقق ليقوم بعمله على أحسن وجه.

- معرفة الجوانب الفنية والتقنية لأجهزة الحاسوب والانترنت والتي تتعلق بالجريمة المرتكبة.

- وصول الاختبارات والبلاغات عن الجرائم الواقعة على الحاسوب والانترنت من الفنيين الذين يعملون على هذه الأجهزة.

- إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية التي تدل على وقوع الجريمة، وتخزينها في الأقراص المعدة لذلك ومنع حذفها.

- تشكيل فريق تحقيق فني، وإعطاء كل واحد منهم مهمة معينة من خلال عملية التفتيش في مسرح الجريمة.

- البحث عن الأدوات المستخدمة في ارتكاب الجريمة وطرق الدخول إلى البرامج المخزنة

[1] - يوسف جفال، المرجع السابق، ص23.

وكيفية الحصول على الأرقام السرية والشفرات التي تمكنهم من الدخول إلى الحاسوب.

- وضع خطة عمل مع جميع أعضاء فريق التحقيق، والتشاور معهم لمعرفة جميع الجوانب الفنية للجريمة التي يجري التحقيق بشأنها[1].

الفرع الثاني: معوقات التحقيق الجنائي في جرائم الأنترنت

تواجه المحقق الكثير من المشاكل والمعوقات التي تؤثر في نفسيته، حيث تفقده ثقته في نفسه وأدائه، كما تؤثر على المجتمع حيث تفقده الثقة في أجهزة تنفيذ القانون، غير القادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، كما تؤثر على المجرم الذي يستغل عدم قدرة الجهات الأمنية على اكتشاف أمره، مما يعطيه ثقة في ارتكاب المزيد من هذه الجرائم ومن بين هذه المعوقات.

أولا /معوقات تشريعية

يؤدي عدم وجود التشريعات الرادعة لمجرمي الجريمة الإلكترونية إلى تفاقم نسبة الإجرام الإلكتروني لتصل إلى مرحلة تصبح فيها عملية العلاج صعبة وغير مجدية، فالقوانين التشريعية لم تتناول كل الصور التي ترتكب في مجال المعلوماتية هذا لأن التكنولوجيا في تطور مستمر عكس القوانين التي تستدعي إجراءات خاصة ومطولة للتعديل والتجديد، وهذا ما يترك المجال لمجرمي الجريمة الإلكترونية التملص من المسؤولية الجزائية لأن القوانين التقليدية غير كافية.

ثانيا: المعوقات المتعلقة بجريمة الأنترنت والجهات المتضررة

أ/المعوقات المتعلقة بجريمة الأنترنت تتمثل في:

- خفاء الجريمة وغياب الدليل المرئي وصعوبة التعرف عليه.
- الإعاقات المتعلق بالوصول إلى الدليل لإحاطته بوسائل الحماية الفنية.
- سهولة محو الدليل أو تدميره في زمن قصير جدا.

الجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدا بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعمل بها فإنه

[1] - يوسف جفال، المرجع السابق، ص27.

يستهدف بالمحو السريع عدم استطاعة السلطات إقامة الدليل ضده، وبالتالي تملصه من مسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسوب الآلي أو الشبكة أو في الأجهزة[1].

ب–المعوقات المتعلقة بالجهات المتضررة:

وهي عدم إدراك خطورة جرائم الحاسوب والانترنت من قبل المسئولين بالمؤسسات المجني عليها التي تعد من معوقات التحقيق، وكذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة الجرائم المتعلقة بالانترنت، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها

واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، وهذا يؤدي إلى الإحجام

عن الإبلاغ عن الجريمة، التي تعتبر من أهم وأخطر الإشكالات التي تتعلق بعملية الإبلاغ عن الجريمة الإلكترونية، حيث يحجم البعض عن إبلاغ السلطات المختصة بالجرائم التي ارتكبت بحقهم خاصة إذا تعلق الأمر بالمؤسسات المالية أو ما شابهها[2].

المطلب الثاني: إجراءات التحقيق في جريمة الأنترنت

التحقيق هو المرحلة الأولى من مراحل سير الدعوى الجنائية وهو ينصرف إلى مجموعة من الاجراءات التي تجريها سلطات التحقيق قبل المحاكمة، ويهدف التحقيق إلى التثبيت من الادلة القائمة على نسبة الجريمة إلى فاعل معين، حتى لا تعرض على المحكمة إلا الدعاوى المسندة إلى أسس واقعية وقانونية مثبتة.

الفرع الأول: اتصال المحقق بجريمة الأنترنت والوسائل المستحدثة

القوانين التقليدية التي كانت تنظم إجراءات التحقيق كالتفتيش والمعاينة لا يمكن تطبيقها على الجريمة الإلكترونية، كونها جريمة ذات طبيعة خاصة لأنها تتعلق بالبيانات والمعلومات غير الملموسة، مما يصعب تحديد هوية وأمكنة المجرمين وملاحقتهم، وهذا ما

[1] – خالد ممدوح ابراهيم، المرجع السابق، ص65..

[2] – يوسف جفال، المرجع السابق، ص43.

يرهق المحققين الذين يصعب عليهم جمع الأدلة من خلال البيئة المعلوماتية، فقد يصل إلى علم المحققين وقوع الجرائم من جراء الدوريات التي تقوم بها الشرطة القضائية، إما تبقي البلاغات من طرف عامة الناس أو الشكاوى من الاطراف المتضررة[1].

أولا: تلقي البلاغات حول جريمة الأنترنت

أ/البلاغ: في جرائم الأنترنت يختلف عنها الحال في الجرائم التقليدية، وإن كان يتمتع بنوع من الخصوصية تتماشى مع طبيعة هذه الجرائم، فالبلاغ هو اخبار السلطات المختصة عن وقوع جريمة أو أنها على وشك الوقوع، أو أن هناك اتفاقا جنائيا أو ادلة او قرارات او عزما على ارتكابها أو وجود شك أو خوفا من أنها ارتكبت[2].

كيفية التبليغ في جريمة الأنترنت:

قد يكون اختياري في بعض الجرائم وواجب في جرائم أخرى كما هو منصوص عليه في القانون الجزائري في المادتين 32 ق.ع و 91 ق.إ.ج ويتم التبليغ بمختلف الوسائل التي توصل المعلومات إلى الجهات المختصة فقد يكون التبليغ كتابيا أو شفويا ومن أي شخص سواء كان متضررا أو غير متضرر وهذا يطلق عليه بمصطلح البلاغ المادي وقد يقدم بواسطة البريد أو التلفون أو الصحف وهذا ما يطلق عليه باللاغ المعنوي، وقد يتم عن طريق الأنترنت وهذا ما يسمى باللاغ الرقمي، وذلك إما عن طريق ارسال رسالة الكترونية إلى عنوان البريد الالكتروني للجهات المختصة بالتحقيق والتحري للإبلاغ عن وجود صفحات أو مواقع غير مشروعة، كإرسال رسالة الكترونية تتضمن التبليغ عن وجود موقع منشور فيه صور للاستغلال الجنسي، والتبليغ في الحالات الثلاثة (البلاغ الرقمي والمادي والمعنوي) الحرية في الاختيار بين الافصاح عن هويته أو ابقائها مجهولة[3] .

[1] – بخيتي فاطمة الزهراء، المرجع السابق، ص53-54.

[2] – نبيلة هبة هروال، المرجع السابق، ص177- 181.

[3] – نبيلة هبة هروال، المرجع نفسه، ص181-182.

والمعلومات التي يجب معرفتها من المبلغ والتي ينبغي ان يدونها المحقق عند تلقي البلاغ يمكن الحصول عليها من خلال طرح أسئلة عن تاريخ ووقت تلقي البلاغ المعلومات الخاصة بمبلغ، طبيعة ونوع الجريمة المعلوماتية محل البلاغ إلى غيرها من الأسئلة المتعلقة بالجريمة[1].

ب-الشكوى في جرائم الأنترنت:

يقصد بها البلاغ أو الاخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشان جرائم معينة حظر المشرع تحريكها بصددها قبل تقديمه، أي هناك بعض الجرائم حددها المشرع على سبيل الحصر، لا يمكن تحريك الدعوى العمومية فيها إلا بعد تقديم شكوى من قبل المجني عليه أو وكيله الخاص[2].

حيث نص المشرع الجزائري في المادة 72 ق.إ.ج على :"يجوز لكل شخص متضرر من جنائية أو جنحة أن يدعي مدنيا بان يتقدم بشكواه أمام قاضي التحقيق المختص"

ولا يوجب القانون للشكوى شكلا معينا وإنما يقتصر فيها المعني بالأمر على ذكر اسمه وسنه عنوانه وموجز الوقائع، والمواد القانونية التي تعاقب الفعل المرتكب، وإعطاء كافة المعلومات الخاصة بمرتكب الجريمة إذا كان معلوما.

وقد خصصت العديد من المراكز لمعالجة تلك الشكاوى من بينها:

- مركز تلقي الشكاوى عن جرائم الاحتيال عبر الانترنيت IFCC الذي تم تأسيسه في فرجينيا الغربية بالولايات المتحدة الأمريكية من طرف مكتب التحقيقات الفدرالي FBI والمركز الوطني لجرائم الياقات البيضاء NW3C من أجل مكافحة ظاهرة الاحتيال عبر الانترنيت[3] .

ثانيا: كيفية اتصال قاضي التحقيق بملف الدعوى الخاص بجريمة الأنترنت

يتصل قاضي التحقيق بملف الدعوى إما عن طريق وكيل الجمهورية بموجب إجراء تحقيق رسمي لطلب الافتتاحي لأجراء التحقيق، وإما عن طريق شكوى جزائية مقدمة من المضرور وهذا ما اكدته المادة 38 ف 3 ق.إ.ج "...يختص بالتحقيق في الحادث بناء على طلب من وكيل

[1] - بخيتي فاطمة الزهراء، المرجع السابق، ص55.

[2] - نبيلة هبة هروال، المرجع السابق، ص 189.

[3] - بخيتي فاطمة الزهراء، المرجع السابق، ص56-57.

الجمهورية أو شكوى مصحوبة بادعاء مدني ضمن الشروط المنصوص عليها في المادتين 67ن 73 ق.إ.ج.

أ/**الطلب الافتتاحي لإجراء التحقيق**: يتصل وكيل الجمهورية بملف ضباط الشرطة القضائية فيمكن لوكيل الجمهورية ان يطلب فتح التحقيق ما لم ينص القانون على وجوب التحقيق في بعض الجنح، ويمكن لوكيل الجمهورية أن يقدم طلبا اضافيا لقاضي التحقيق إذا ظهرت وقائع جديدة طبقا للمادة 67 ف 3 على أنها "لا يجوز لقاضي التحقيق أن يجري تحقيقا إلا بموجب طلب من وكيل الجمهورية لإجراء التحقيق حتى ولو كان ذلك بصدد جناية او جنحة متلبس بها"

ويتقيد القاضي التحقيق بالوقائع دون الأشخاص طبقا المادة 67 ف 3 و 4 من ق.إ.ج :"... ولقاضي التحقيق سلطة الاتهام كل شخص ساهم بصفته فاعلا أو شريكا في الوقائع المحال تحقيقها إليه"

فإذا وصلت لعلم قاضي التحقيق وقائع لم يشير إليها في طلب إجراء التحقيق تعين عليه أن يحيل فورا إلى وكيل الجمهورية الشكاوى أو المحاضر المثبتة لتلك الوقائع"

ب–الشكوى المصحوبة بالادعاء المدني: تنص عليها المادة 72 من قانون الإجراءات الجزائية " يجوز لكل شخص تضرر من جناية أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص" إن إحدى طرق تحريك الدعوى من طرف الأفراد ، وهي في نفس الوقت إحدى طرق اتصال قاضي التحقيق بملف الدعوى .

ويلجأ عادة المتضرر من الجريمة إلى هذه الطريقة تجنبا لطول الإجراءات وتقليصا للوقت ، وحرصا منه على أن يكون الإشراف على ملف من طرف قاضي التحقيق لا أن يكون من طرف الضبطية القضائية التي عادة يكون لها تأثير على مجرى التحقيق ، كما أنه يستفيد من تتبع مجريات الدعوى العمومية بنفسه طالما كان هو من حركها .

إلا أن أخطر سلبيات الإدعاء المدني يتمثل في سوء إستعمال هذا الطريق لأن من شأنه أن يعرض الطرف المدني إلى متابعة جزائية بتهمة الوشاية كاذبة إذا ما خسر دعواه ، ولهذا عليه أن يتأكد من أن اتهامه كان مبنيا على دليل قوي في الدعوى.

ج-الجهات التي تستأنف اوامر قاضي التحقيق:

النيابة العامة:

لوكيل الجمهورية أو أحد مساعديه إستئناف جميع أوامر قاضي التحقيق دون استثناء وذلك طبقا لنص المادة 170 من قانون الإجراءات الجزائية الجزائري " الوكيل الجمهورية في أن يستأنف أمام غرفة الإتهام جميع أوامر قاضي التحقيق.

ويكون هذا الاستئناف تقرير لدى قلم كتب المحكمة ويجب أن يرفع في ثلاثة أيام من تاريخ صدور الأمر".

يجوز للنائب العام الطعن في أوامر قاضي التحقيق في ظرف 20 يوما على ألا يكون لهذا الطعن أثر موقف في حالة إستئناف أمر الإفراج ظرف 20 يوما على ألا يكون لهذا الطعن أثر موقف في حالة إستئناف أمر الإفراج ويفرج على المتهم رغم إستئناف النائب العام مالم يكن وكيل الجمهورية قد استأنفه بالطبع ويجب أن يبلغ النائب

العام عند إستئنافه الخصوم في الدعوى ، وذلك خلال العشرين يوما التالية لصدور الأمر حتى يكونوا على بينة من أمرهم ولا يفاجؤا بقرار من غرفة الاتهام في غير صالحهم[1].

طبقا لنص المادة 171 من قانون الإجراءات الجزائية الجزائري " يحق الإستئناف أيضا للنائب العام في جميع الأحوال ويجب أن يبلغ إستئنافه للخصوم خلال العشرين يوما التالية لصدور أمر قاضي التحقيق ولا يوقف هذا الميعاد ولا رفع الإستئناف بتنفيذ الأمر بالإفراج المؤقت".

إستئناف المتهم:

إن المتهم لا يجوز له إستئناف جميع أوامر قاضي التحقيق و يرفع الإستئناف بعريضة تودع لدى قلم مكتب المحكمة في ظرف ثلاثة 03 أيام من تبليغ الأمر إلى المتهم طبقا للمادة 168 ق.إ.ج.

[1] – مولود ديدان، قانون الإجراءات الجزائية، ص79.

إستئناف المدعي المدني:

كما أجاز المشرع الجزائري للمدعي المدني الحق في إستئناف أوامر قاضي التحقيق التي لها علاقة بحقوقه المدنية ، وبمفهوم المخالفة لا يجوز له إستئناف الأوامر المتعلقة بالجانب الجزائي مثل الحبس المؤقت والإفراج والرقابة القضائية.

ويرفع الإستئناف خلال 3 أيام من تاريخ تبليغ الأمر المراد إستئنافه إلى المدعي المدني وذلك بتقديم عريضة لدى قلم كاتب ضبط قاضي التحقيق طبقا لنص المادة 3/173 قانون الإجراءات الجزائية.

ثالثا: الوسائل المساعدة التي يستخدمها المحقق في جرائم الأنترنت

يحتاج المحقق في تنفيذ التحقيق إلى وسائل مادية وأخرى معنوية، وذلك لما تحتاجه الجريمة الإلكترونية من معرفة تامة وإدراك لوسائل تثبت وقوع الجريمة، والوصول إلى مرتكبيها و نسبتها إليهم.

اولا: الوسائل المادية[1]

أ/عناوين الأنترنت IP و MCA والبريد الالكتروني وبرامج المحادثة "إن عنوان الانترنيت IP"" Internet Protocol Address هو المسؤول عن تراسل حزم البيانات عبر الانترنيت وتوجيهها إلى أهدافها، ويوجد عنوان IP بكل جهاز مرتبط بالانترنيت ويتكون من أربعة أجزاء الجزء الواحد له ثلاث خانات، يشير الجزء الأول من اليسار إلى المنطقة الجغرافية ويشير الجزء الثاني لمزود الخدمة والثالث لمجموعة الحواسيب المرتبطة، والرابع يحدد الكمبيوتر الذي تم الاتصال منه.

ب.البروكسي PROXY

البروكسي وسيلة لوصل مواقع الويب والشبكات المحلية للانترنيت، فهو برنامج يعالج حركة النقل إلى الأنظمة المضيفة، نيابة على البرامج المستضافة المشتغلة على الشبكة المحلية مما يعني إمكانية المستخدم الوصول إلى الانترنيت عبر الجدار الناري، لكن لا يمكن للدخلاء رؤية الداخل، وهو وسيط بين الشبكة ومستخدميها.

[1] – بخيتي فاطمة، المرجع السابق، ص59.

ج- برامج التتبع: تقوم بالتعرف على محاولات الاختراق ومن قام بها ومصمم للعمل في الأجهزة المكتبية وساكن في خلفية المكتب وعند رصده لأي محاولة قرصنة يسارع بإغلاق منافذ الدخول أمام المخترق ثم يبدأ في عملية المطاردة لاقتفاء أثر المخترق.

د-نظام كشف الاختراق: تتولى مراقبة بعض" العمليات لتي يجري حدوثها على أجهزة الحاسوب أو الانترنيت مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب.

هـ-نظام جرة العسل: مصمم خصيصا لكي يعترض لأنواع مختلفة من الهجمات عبر الشبكة دون أن يكون عليه أي بيانات ذات أهمية ويعتمد على خداع من يقوم بالهجوم وإعطائه انطباعا خاطئا بسهولة الاعتداء على النظام.

و-أدوات الضبط: هذه الأدوات تقوم بضبط ماديات الجريمة كبرامج الحماية وادوات المراجعة وأدوات مراقبة المستخدمين والتقارير التي تنتجها نظم أمن البيانات.

ي. أدوات فحص ومراقبة الشبكات

و تشمل ما يلي:

ARP1: وظيفتها تحديد مكان الحاسوب الفيزيائي على الشبكة وهو يحتفظ بجميع أرقام كروت الشبكة MCA وله عدة من المداخل المستعملة معه.

2-برامج Visual Route هو برنامج يلتقط أي عملية فحص عملت ضد الشبكة فيقوم بإعطاء أجوبة معينة تبين العمليات التي حدث فيها المسح والمناطق التي تم فيها الهجوم وبعد معرفة عنوان IP يوضح مسار الهجوم بين مصدره والجهة التي استهدفها الهجوم.

3-أدوات التتبع TRACER: ترسم مسارا بين جهازين تظهر فيها كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني، وتوجه من خلالها الوقت والقفزات، وهي تسمح برؤية المسار الذي اتخذه IP من مضيف لأخر وتستخدم هذه الأداة الخيار "Time To Live التي تكون ضمن IP لكي تستقبل من كل موجة رسالة.

4-أدوات تفحص حالة الانترنت NET STAT هي أداة لفحص حالة الاتصال الحالي للبروتوكول TCP/IP ولها عدة مهمات من أهمها عرض جميع الاتصالات الحالية ومنافذ التصنت وعرض المنافذ والعناوين بصورة رقمية .

2-الوسائل الاجرائية:

1-اقتفاء الأثر: أخطر ما يخشاه المجرم الإلكتروني هو تقصي أثره أثناء ارتكابه للجريمة، لهذا فأهمية اقتفاء الأثر في الجريمة الإلكترونية أكثر أهمية من أهمية الشهادة في الجرائم التقليدية ويمكن تقصي الأثر بطرق عدة سواء كان ذلك عن طريق بريد الكتروني تم استقباله، أو عن طريق تتبع الأثر للجهاز الذي تم استخدامه للقيام بعملية الاختراق.

2- **الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته :**على المحقق الاطلاع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، كما يجب عليه معرفة نوعية برامج الحماية وأسلوب عملها.

الاستعانة بالذكاء الاصطناعي: ويتم ذلك من خلال حصر الحقائق والاحتمالات والأسباب والفرضيات، بعدها تتم معرفة النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسوب وفق برامج تعد لذلك، والتي تعطي كافة الاحتمالات.

4- **التأكد من وقوع الجريمة :**إن توافر المعلومات المنشورة من خلال شبكة الانترنيت قد تظهر انتشار الفيروسات، أو وقوع عمليات اختراق أو قرصنة، وعند وصول الجهة المختصة بتلقي البلاغات يجب عليها التأكد من صحة البلاغ، والتحفظ على مكان الجريمة وتأمينه، وتحديد أطراف الجريمة[1].

الفرع الثاني: الأجهزة المكلفة بالبحث والتحري عن جريمة الأنترنت

يمكن القول أن المحقق هو من يتولى التحقيق من رجال الضبطية القضائية، أو من أعضاء النيابة العامة، أو قضاة التحقيق ويلحق بالمحقق الجنائي الباحث الجنائي الذي يكون غالبا من الشرطية القضائية، الذين خول لهم القانون مهمة جمع الاستدلالات عن المشتبه بهم، وسنحاول من خلال هذا الفرع استعراض أهم الهيئات المختصة في مجال مكافحة جرائم الأنترنت.

[1] -بختي فاطمة الزهراء، المرجع السابق، ص62.

اولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال:

إن الجرائم المتصلة بتكنولوجيات الاعلام والاتصال نصت عليها في قانون 04/09 المتضمن القواعد الحاصلة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها وبمكافحة هذا النوع من الجرائم على المستوى الوطنين تم انشاء هيئة وطنية هدفها مكافحة كل جريمة قد تدخل في إطار الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وتعد سلطة إدارية مستقلة يترأسها وزير العدل، وتم النص على إنشاء هذه الهيئة في المادة 13 من قانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال وجاءت المادة كالآتي (تنشا هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحته تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم.

أ/مهام الهيئة: للهيئة الوطنية للوقاية من الجرائم المتصلة تكنولوجيات الاعلام والاتصال ومكافحته دوران أساسيان هما:

-الوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال:

ويظهر ذلك من خلال مختلف الاجراءات الوقائية التي تقوم بها هاته الهيئة التوعية لمستخدمي تكنولوجيا والاتصال بمدى خطورتها هذا النوع من الجرائم واعلامهم بانهم قد يقعون ضحيا لهاته الجرائم[1].

-مكافحة الجرائم المتصلة بتكنولوجيات الاعلام والاتصال:

ويظهر ذلك من خلال المهام الموكلة لهاته الهيئة من خلال نص المادة 14 التي جاءت كالآتي:

"تولى الهيئة المذكورة في المادة 13 خصوصا المهام الآتية:

-تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها.

-مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية.

[1] – دليلة مرزوق، جرائم المساس بأنظمة المعالجة الآلية للمعطيات على ضوء الاتفاقيات الدولية والتشريع الجزائري، مذكرة لنيل شهادة ماستر علوم جنائية، جامعة العربي بن مهيدي، 2016-2017، ص48-49.

-تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.

ثانيا: الوحدات التابعة لسلك الأمن الوطني والدرك الوطني:

أ/الوحدات التابعة لسلك الأمن الوطني والدرك الوطني:

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الج ا رئم وبالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات، وقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي، بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة ومهمتها التحقيق في الجرائم الإلكترونية تعمل بالتنسيق مع هذه المخابر.

الوحدات التابعة للدرك الوطني الجزائري

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية نذكر منها:

-المصالح والمراكز العلمية والتقنية.

-هياكل التكوين.

-المصلحة المركزية للتحريات الجنائية.

-المعهد الوطني لعلم الإجرام.

يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، وإنجاز المقاربات

الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني.

وعليه فمن الضروري إنشاء وحدات أمن وأجهزة قضائية متخصصة في مكافحة جرائم الأنترنت، يكون لديها الإلمام الكافي بالجوانب التقنية والفنية لمتابعة وكشف وضبط تلك الجرائم ومرتكبيها، مع إخضاعهم لبرامج تدريبية خاصة دورية، تساعدهم على تحسين وتحديث معارفهم وخبراتهم واطلاعهم بآخر المستجدات الحاصلة في مجال التقنية المعلوماتية.

خاتمة

خاتمـــــــة:

مع التطور التكنولوجي والعلمي في عصرنا الحديث، أصبحت حياة الإنسان سهلة بكثير مما سبق وذلك بفضل التقنيات الحديثة كالكمبيوتر والانترنت ، الذين أصبحا ركيزة أساسية تقوم عليها جل المعاملات، سواء الاقتصادية، الاجتماعية، السياسية وغيرها، إلا أنه صاحب هذا التطور تطورا في الجريمة، التي اختلفت الآراء حول تسميتها فهناك من أطلق عليها اسم "الجريمة المعلوماتية "وآخرون أطلقوا عليها " جرائم الحاسب الآلي والانترنت" وهناك من اكتفى بتسميتها " جرائم الحاسب الآلي " أو " جرائم الانترنت" ، كما أطلق عليها اسم " الجريمة الالكترونية" ، وكل هذه التسميات وغيرها تطلق على جريمة واحدة تتحقق عندما يساء استخدام التقنيات الحديثة ، وقد صاحب الاختلاف في التسمية اختلاف في التعريف بالجريمة فهناك من ضيق من مفهوم الجريمة الالكترونية، وهناك من وسع في مفهومها، وهناك من عرف الجريمة الالكترونية بالنظر إلى موضوعها وآخرون ربطوا مفهوم الجريمة الالكترونية بمدى معرفة الجاني لتقنية النظام المعلوماتي والحاسب الآلي، فالجريمة الالكترونية بحسبهم لا يرتكبها إلا شخص له دراية ومعرفة بمجال التقنية الحديثة مما يسمح له بالتلاعب بالنظم المعلوماتية.

وقد تمحورت نتائج البحث في الآتي:

1-جريمة الأنترنت هي الأفعال المخالفة للقانون التي ترتكب بواسطة الكمبيوتر من خلال شبكة الانترنت.

2-مرتكب جريمة الأنترنت يتميز عن المجرم العادي بمجموعة من الصفات، منها انه اجتماعي وذكي، يتمتع بالخبرة في مجال التقنية الحديثة، بالإضافة إلى انه غير عنيف، فهذا النوع من الإجرام لا يتطلب القوة والعنف.

3-تختلف دوافع ارتكاب جريمة الأنترنت من شخص لأخر، فقد تكون دوافع شخصية هدفها تحقيق مصلحة خاصة، وقد تكون خارجية بهدف الانتقام مثلا.

4-جريمة الأنترنت كغيرها من الجرائم التقليدية تتميز بالخطورة لكونها تمس الإنسان والمؤسسات وتتعدى حتى لان تكون خطر على امن الدولة واستقرارها، وكذلك هي من الجرائم

العابرة للحدود لارتباطها بشبكة الانترنت، كما تتميز الجريمة الالكترونية بكونها تعتمد على التقنيات الحديثة، وصعوبة اكتشافها وإثباتها.

5-يواجه المحقق للكشف عن جريمة الأنترنت والقبض على مرتكبيها ونسبتها إليهم عدة معوقات، أهمها معوقات تشريعية تكمن في عدم حصر لكل صور الجريمة الإلكترونية في القوانين الجنائية.

6-الشاهد في جريمة الأنترنت شخص فني، صاحب خبرة وتخصص في مجال التقنية الحديثة وعلوم الحاسوب، كمشغلوا الحاسب الآلي وخبراء البرمجة.

7-من بين الوسائل التي تساعد المحقق في جرائم الأنترنت هي عناوين الانترنت كبرتوكول الانترنت (IP) الموجود بكل جهاز مرتبط بالانترنت والذي يساعد على تحديد مكان الحاسب الآلي..

8-المعاينة في جريمة الأنترنت اقل أهمية منها في الجرائم العادية، لقلة الآثار المادية بينما الخبرة تعتبر من أهم إجراءات التحقيق في الجرائم الالكترونية وهذا ما تستدعيه طبيعة

هذه الجريمة، كونها تعتمد بالدرجة الأولى على وسائل مستحدثة.

وبناءا على هذه النتائج اقترح التوصيات التالية:

1-إنشاء دورات تكوينية للمحققين والقضاة في مجال نظم المعلوماتية والحواسيب، فدور القاضي مهم في توجيه مسار القضايا، فإذا كان القاضي غير ملم بالجوانب الفنية للتقنية الحديثة فانه لا يستطيع تقدير مدى خطورة المجرم المعلوماتي، وهذا يؤثر على الحكم عليه كان يصدر في حقه حكم غير متكافئ مع الجريمة المرتكبة.

2-عدم حصر صور جريمة الأنترنت في المواد القانونية وفتح المجال للمحقق في أن ينظر في جميع الجرائم المتعلقة بجرائم الأنترنت التي توجه إليه، لأنه وتطبيقا لمبدأ الشرعية يبقى دور المحقق مرتبط فقط بالتحقيق في الجرائم المذكورة على سبيل الحصر في

التشريعات الوطنية، وكما ذكر سابقا فالجرائم في تطور مستمر مما يجعل القوانين التقليدية غير كافية.

3-بما أن المجرم الإلكتروني يعتمد بالدرجة الأولى على وسائل التقنية الحديثة ولأن الإجراءات التقليدية غير كفيلة بمكافحة هذه الجرائم فينبغي على المشرع وضع إجراءات حديثة تعتمد على ذات الوسائل المستخدمة في الجريمة للكشف عنها وتتبع فاعليها.

4-ينبغي على كافة الدول وخاصة العربية وضع نظام مراقبة عبر شبكة الانترنت يسمح بتتبع الملفات المدخلة والمخرجة، وتعقب الاختراقات غير المشروع للأنظمة وتخريبها وملاحقة مرتكبيها.

5-على دارس القانون البحث في موضع إجراءات التحقيق فيما يخص جريمة الأنترنت لأنه موضوع غير مستهلك بالرغم من أهميته، ولأن هذه الجريمة لاقت انتشارا واسعا على الصعيد الوطني.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

الكتب:

الكتب العامة:

1. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة ، الجزائر، طبعة 2010-2011.

2. سعيد مبروك ابراهيم، المكتبة الجامعية وتحديات مجتمع المعلومات، دار الوفاء للطباعة والنشر، الاسكندرية، ط1، 2009.

3. عبد الرحمن خلفي، محاضرات في قانون الاجراءات الجزائية، دار الهدى، الجزائر.

كتب متخصصة:

4. أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائر، دار هومة، الجزائر، ط2، 2007.

5. خالد ممدوح، امن الجريمة الإلكترونية، دار الجامعية الاسكندرية، 2008.

6. عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر، دار شتات للنشر، مصر، 2007.

7. عبد الفتاح بيومي حجازين مكافحة جرائم الأنترنت، دار الفكر الجامعي، الاسكندرية، ط1، 2006.

8. غنية باطلي، الجريمة الالكترونية دراسة مقارنة، منشورات الدار الجزائرية، الجزائر، 2005.

9. محمد أمين الشوابكة، جرائم الحاسوب والانترنت، دار الثقافة ، عمان، ط1 ، 2007 .

10. محمد أمين شوابكة، جرائم الحاسوب والأنترنت، ط1، دار الثقافة، عمان، 2004.

11. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الاسكندرية، دون سنة نشر.

12. مصطفى محمد موسى، التحقيق الجنائي في الجرائم الالكترونية، دار الكتب والوثائق القومية، القاهرة، 2008.

13. مولود ديدان، قانون العقوبات الجزائري، قانون رقم 01/09 المؤرخ في 29 فيفري 2009، د.ط.

14. نائلة عادل قورة، جرائم الحاسب الآلي الاقتصادية، المنشورات الحلبية الحقوقية، ط1، 2005.

15. نبيلة هبة هروال ، الجوانب الاجرائية لجرائم الأنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي، الاسكندرية، 2007.

16. نهلة عبد القادر مامون، الجرائم المعلوماتية، دار الثقافة، ط2، الأردن، 2010.

الأطروحات والرسائل الجامعية:

1. بختي فاطمة الزهراء، إجراءات التحقيق في الجريمة الالكترونية، مذكرة ماستر في الحقوق، جامعة المسيلة، سنة 2014.

2. بعرة سعيدة، الجريمة الالكترونية في التشريع الجزائر، مذكرة لنسل شهادة ماستر، حقوق، جامعة بسكرة، سنة 2015-2016.

3. بن مكي نجاة، السياسة الجنائية لمكافحة الجرائم المعلوماتية، مذكر مقدمة لنيل شهاد الماجستير في القانون الدولي، زواقري، الطاهر، معهد العلوم القانونية والإدارية، مدرسة الدكتوراه، قطب خنشلة، 2008-2009.

4. دردور نسيم، جرائم الالكترونية على ضوء القانون لجزائري والمقارن، مذكرة لنسل شهادة ماجستير، سنة 2013/2012.

5. دليلة مرزوق، جرائم المساس بأنظمة المعالجة الآلية للمعطيات على ضوء الاتفاقيات الدولية والتشريع الجزائري، مذكرة لنيل شهادة ماستر علوم جنائية، جامعة العربي بن مهيدي، 2016-2017.

6. مذكرة توضيحية للقانون الجزائي العربي الموحد، جامعة الدول العربية، ج2، رقم 292 بتاريخ 1996/11/19.

7. موساوي سهام، الاطار القانوني للجريمة الالكترونية، مذكرة لنيل شهادة الماستر، جامعة عبد الرحمن ميرة، بجاية، 2017-2018.

8. يوسف جفال، التحقيق في الجريمة الإلكترونية، مذكرة لنسل شهادة الماستر، جامعة محمد بوضياف، المسيلة، 2016-2017.

المجلات العلمية:

1. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، ط2، 2006.

2. سميرة معاشي، ماهية الجريمة الالكترونية، مجلة المنتدى القانوني، العدد السابع، جامعة بسكرة.

3. علاوة عوام، التشرب كآلية للكشف عن الجرائم في القانون الجزائري، مجلة الفقه والقانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012.

4. علي بن هادية، بلحسن البليشي، الجيلالي بن الحاج يحيى، القاموس الجديد للطلاب، الشركة الوطنية، الشركة التونسية الجزائر، تونس، ط1، 1979.

البحوث الجامعية:

1. ياسمينة بونعارة، الجريمة الالكترونية، بحث (شبكة الأنترنت)، جامعة الأمير عبد القادر للعلوم الاسلامية.

مواقع الأنترنت:

1.محمد علي قطب، موقف الشارع الاسلامي من جرائم الأخلاق عبر الأنترنت، مركز الاعلام الأمني، جامعة نايف العربية للعلوم الأمنية.

www.nauss.adu.sa

2-http://www.moi.gov-qa/unccpckdoha/arabic/previous congresses: html أطلع عليه بتاريخ 2019/03/03 الساعة 19.11

القوانين والأوامر:

2. الأمر رقم 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 156/66 الموافق لـــ 08 جوان 1966 المتضمن قانون العقوبات.

3. القانون 04/09 المتضمن القواعد الخاصة بالوقاية من الجرائم، المتصلة تكنولوجيا الاعلام والاتصال ومكافحتها.

4. القانون رقم 155/66 المؤرخ في 08 يونيو 1966 المعدل والمتمم لقانون الاجراءات الجزائية، الجريدة الرسمية العدد 48.

فهرس المحتويات

فهرس المحتويات

إهداء

كلمة شكر

مقدمة ..... أ

الفصل الاول:

الأحكام العامة في جرائم الأنترنت

المبحث الأول: ماهية جريمة الأنترنت 3

المطلب الأول: مفهوم جريمة الأنترنت 3

الفرع الأول: تعريف جريمة الأنترنت 3

الفرع الثاني: تعريف شبكة الأنترنت..... 7

المطلب الثاني: تصنيف الجرائم (أنواع الجرائم) 9

الفرع الأول: تصنيفات جريمة الأنترنت.....10

الفرع الثاني: خصائص جريمة الأنترنت والمجرم المعلوماتي.....16

المبحث الثاني: المواجهة الجنائية لجرائم الأنترنت.....20

المطلب الأول: أركان الجريمة 20

الفرع الأول: الركن الشرعي لجريمة الأنترنت 20

الفرع الثاني: الركن المادي 24

المطلب الثاني: قمع جريمة الأنترنت.....36

الفرع الأول: قمع الجريمة بالنسبة للشخص الطبيعي.....36

الفرع الثاني: العقوبات المقررة للشخص المعنوي 40

الفصل الثاني

إجراءات التحقيق في جريمة الأنترنت

المبحث الأول: مرحلة جمع الاستدلالات (البحث والتحري) 44

المطلب الأول: الإجراءات التقليدية لجمع الدليل الالكتروني 45

الفرع الأول: الاجراءات المادية 45

الفرع الثاني: الإجراءات الشخصية 57

المطلب الثاني: اجراءات الحديثة لجمع الدليل الالكتروني 65

الفرع الأول: التسرب.....65

الفرع الثاني: اعتراض المراسلات والمراقبة الالكترونية.....68

المبحث الثاني: مرحلة التحقيق.....71

المطلب الأول: مفهوم التحقيق الجنائي في جريمة الأنترنت 71

الفرع الأول: تعريف التحقيق في جريمة الأنترنت 71

الفرع الثاني: معوقات التحقيق الجنائي في جرائم الأنترنت 73

المطلب الثاني: إجراءات التحقيق في جريمة الأنترنت 74

الفرع الأول: اتصال المحقق بجريمة الأنترنت والوسائل المستحدثة 74

الفرع الثاني: الأجهزة المكلفة بالبحث والتحري عن جريمة الأنترنت 81

خاتمة 86

قائمة المصادر والمراجع 90

فهرس الموضوعات

ملخص:

جريمة الأنترنت من الجرائم المستحدثة، تتطلب لارتكابها وسائل ذات تقنية عالية بالإضافة إلى ذكاء وخبرة المجرم في مجال التقنية الحديثة، وعليه فإجراءات التحقيق فيها تتمتع بنوع من الخصوصية نظرا لطبيعة الجريمة الالكترونية، حيث توجد في معظم البلدان المتضررة منها أجهزة خاصة بالتحقيق فيها، يتولى البلاغات والشكاوى بشأنها عن طريق الانترنيت من خلال مواقع الكترونية مخصصة لذلك وعند تلقي المحقق البلاغات بوقوع جريمة الكترونية يستدعي المشتبه والشهود لاستجواب المشتبه فيهم وإدلاء الشهود بأقوالهم، والشهود في الجريمة الالكترونية هم أشخاص فنين، أصحاب خبرة وتخصص في تقنية وعلوم الحاسوب والانترنت وعند الانتقال إلى مسرح الجريمة يقوم المحقق بتفتيش كل مل يستدعيه الأمر للكشف عن الحقيقة، بما في ذلك النظم المعلوماتية، وعند وجود أي دليل فانه يضبط في أحراز مخصصة لذلك، أما إن كان الدليل الكترونيا فانه يضبط وفق قواعد خاصة كالتشفير مثلا، ويقوم المحقق بمعاينة مسرح الجريمة المادي و الرقمي بمعية الخبراء.