وزارة التعليم العالي و البحث العلمي
جامعة المسيلة

كليـــة الحقوق والعلوم السياسية
قسم الحقوق

إجراءات التحقيق في الجريمة الإلكترونية

مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق
تخصص قانون جنائي

إعـــــداد الطالبة :
بخي فاطمة الزهراء

إشـــــراف الدكتور :
بلواضح الطيب

السنة الجامعية : 2014/2013

شكـــــر وعرفـــــــان

الحمد لله و الشكر لله الذي وفقني لإتمام هذا العمل

أتوجه بجزيل الشكر و خالص الثناء إلى كل الأساتذة

على ما قدموه لنا من أنوار أضاءت درب مشوارنا الدراسي

و اخص بالذكر من امتدت يداه في احتضان ما أنجزته مراجعة منه و تصحيحا

و إشرافا المشرف " بلواضح الطيب "

و ما من سبيل في هذه الكلمة سوى أن اشكر كل من ساعدنا

من قريب أو من بعيد في السر و العلن و لو بكلمة ....

إهـــــــــــــداء

اهدي ثمرة جهدي إلى اللذين كانا سببا في وجودي، أمي وأبي أطال الله عمرهما، إلى كامل العائلة صغيرا وكبيرا، إلى كل أساتذة كلية الحقوق، إلى صديقاتي، وزملاء الدراسة بمختلف أطوارها

وخاصة دفعة الماستر2013 / 2014.

مقدمة

ظهرت الجريمة مع بداية البشرية وقد حاربها الإنسان منذ اللحظة الأولى عندما أحس فيها بخطر يهدد كيانه و استقراره 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 امن بغير قانون" كما انه 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 و التحقيق 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 موضوع إجراءات التحقيق في الجريمة الإلكترونية كتاب فن التحقيق الجنائي في الجرائم الإلكترونية للدكتور خالد إبراهيم، الطبعة الأولى لسنة 2009، حيث تناول هذا الموضوع بشكل موسع وتطرق للجريمة الإلكترونية الواقعة على الأموال والأشخاص وعالج بعض صور الجريمة الإلكترونية كالقذف، السب عبر الانترنت والتنصت.

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 الجريمة الإلكترونية ؟ وتتفرع عن هذه الإشكالية عدة إشكاليات أخرى :

- ما المقصود بالجريمة الالكترونية ؟

- بما تتميز الجريمة الإلكترونية عن غيرها من الجرائم ؟

- هل توجد أجهزة خاصة بالتحقيق فيها ؟

وللإجابة عن هذه الإشكالية قسمت البحث إلى فصلين:

الفصل الأول بعنوان: ماهية الجريمة الإلكترونية والتحقيق فيها، حيث عالجت ماهية الجريمة الإلكترونية في المبحث الأول منه والذي قسمته بدوره لمطلبين، خصصت المطلب الأول لدراسة مفهوم الجريمة الإلكترونية، وعرضت الأركان التي تقوم عليها الجريمة الإلكترونية في المطلب الثاني، أما المبحث الثاني من هذا الفصل فقد تناولت فيه التحقيق في الجريمة الإلكترونية من حيث المفهوم في المطلب الأول، والمطلب الثاني ذكرت فيه جهاز التحقيق الجنائي في الجريمة الالكترونية وما يواجهه من صعوبات في سبيل الكشف عنها .

الفصل الثاني بعنوان : إجراءات التحقيق في الجريمة الالكترونية، بينت في المبحث الأول كيفية اتصال المحقق بالجريمة الالكترونية من خلال آلية التحقيق في الجريمة الالكترونية في المطلب الأول، والمطلب الثاني عالجت فيه إجرائي الاستجواب وسماع

الشهود في الجريمة الالكترونية، والمبحث الثاني لهذا الفصل تطرقت للإجراءات المتبعة عند الانتقال لمصرح الجريمة، حيث تكلمت عن التفتيش وضبط الأدلة في المطلب الأول، والمطلب الثاني تناولت فيه الانتقال إلى المعاينة وندب الخبراء.

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

الفصل الأول: ماهية الجريمة الالكترونية والتحقيق فيها

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[1] وفي منتهى السرية.

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: الجريمةالإلكترونية، 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 معانات.

1 نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت، دار الفكر الجامعي، الإسكندرية،ط1، 2007، ص5.

وهذه الجريمة هي من الجرائم المستحدثة، التي توجب التنبه لمخاطرها وحجم الخسائر الناتجة عنها، وعليه سأتطرق لماهية الجريمة الإلكترونية في المبحث الأول مما يستوجب تحديد مفهوم الجريمة الإلكترونية مع ذكر أركانها، أما المبحث الثاني فسأتعرض للتحقيق في الجريمة الإلكترونية وذلك من خلال تبيين مفهوم التحقيق في الجريمة الإلكترونية والتعرف على الأجهزة التي تتولى التحقيق في الجريمة الإلكترونية وما يعرقلها عن القيام باختصاصاتها.

المبحث الأول: ماهية الجريمة الإلكترونية

إن الثورة المعلوماتية ونتيجة للتقنيات العالية التي تقوم عليها المتمثلة في استخدام الحواسيب والشبكات المعلوماتية الرابطة بينها قد خلفت أثرا ايجابيا حيث أصبحت معظم القطاعات تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية لما تتميز به من سرعة فائقة ودقة في تجميع المعلومات وتخزينها ومعالجتها ومن ثم نقلها وتبادلها بين الأفراد والجهات والمؤسسات المختلفة في الدولة الواحدة أو بين مجموعة من الدول، إلا أن عصر المعلوماتية بالرغم من الايجابيات التي جاء بها صاحب معه مجموعة من السلبيات المتمثلة في الاستغلال السيئ للأنظمة المعلوماتية مما أدى إلى ظهور نمط جديد من الجرائم الذي يعتمد فيها الجاني على الوسائل الإلكترونية ولمعرفة ماهية الجريمة الإلكترونية تطرقت لمفهوم الجريمة الإلكترونية في المطلب الأول، أما أركان الجريمة الإلكترونية في المطلب الثاني.

المطلب الأول: مفهوم الجريمة الالكترونية

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....الخ وفيما يلي تفصيل لمفهوم هذه الجريمة من حيث التعريف، الخصائص وإبراز لمختلف التقسيمات والأضرار.

الفرع الأول: تعريف الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية 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[1]، وقبل التعرف على الجريمة الإلكترونية تجدر الإشارة إلى تعريف الجريمة عامة.

[1] خالد ممدوح، أمن الجريمة الالكترونية، الدار الجامعية، الإسكندرية، 2008، ص41.

أولا/ تعريف الجريمة لغة

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

ثانيا/ تعريف الجريمة اصطلاحا

معظم الفقهاء المؤلفين في هذا الباب يردون تعريف الجريمة في الفقه إلى ما قرره الماوردي في الأحكام السلطانية بقوله " الجرائم محظورات شرعية زجر الله عنها بحد أو تعزير يعني إذا كانت ممن يتعمد ارتكابها"، أما الإمام أبو زهرة فبعدما ذكر تعريف الماوردي وأيده ساق من بين نصوصه تعريفا أخر للجريمة فقال: " هي المعصية التي يكون فيها عقاب يقرره القضاء[2]".

ثالثا/ تعريف الجريمة الإلكترونية فقها

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

[2] ضياء مصطفى عثمان، السرقة الالكترونية، دار النفائس، عمان، ط1 ، 2011، ص32.

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

أ. **الاتجاه الذي يضيق من مفهوم الجريمة الإلكترونية**: ومن أنصار هذا الرأي مارو Merwe الذي عرف الجريمة الإلكترونية بأنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب الآلي"[1].

وعرفها ر. توت و أهردكتس Ahradcatst و R.tott " تلك الجرائم التي قد حدث في مراحل ارتكابها بعض عمليات فعلية داخل الحاسب"[2].

ب. **الاتجاه الذي يوسع من مفهوم الجريمة الإلكترونية**: ومن أصحاب هذا الرأي ميشال و كريدو 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 المصرح به لحاسب المجني عليه أو بياناته، كما تمتد الجريمة الإلكترونية لتشمل الاعتداءات المادية على جهاز الحاسب ذاته أو المعدات المتصلة به، وكذالك 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[3] ".

---

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

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

[3] نفس المرجع، ص276.

وتعرف منظمة التعاون الاقتصادي والتنمية لعام1983 عند تناولهم موضوع الإجرام المرتبط بالمعلوماتية حيث ذهبوا إلى تعريف الجريمة الإلكترونية بأنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها[1] ".

ج. اتجاهات أخرى لتعريف الجريمة الإلكترونية: تعددت المعايير التي تناولت تعريف الجريمة الالكترونية و اختلفت نذكر منها:

1. تعريفات تستند إلى موضوع الجريمة:

يرى أصحاب هذا الاتجاه أن الجريمة الإلكترونية 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 الجريمة الإلكترونية بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول للمعلومات المخزنة داخل النظام أو التي تحول عن طريقه[2] ".

وهي حسب تعريف أرتور سوبك artor sobg " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات[3]".

---

[1] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان، ط1، 2005، ص30.

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

[3] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، دار الثقافة، الأردن، ط1، 2011، ص28.

2. تعريفات تستند إلى وجوب إلمام الفاعل بتقنية المعلومات:

يستند أصحاب هذا الاتجاه إلى معيار شخصي يستوجب أن يكون الفاعل ملما بتقنية المعلومات واستخدام الحاسب الآلي، وعرفها سترين سكجوبر strin sckjobrg " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكب[1] ".

كما عرفها دافيد تونبسون david thopson الذي عرفها بأنها " جريمة تتطلب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية النظام المعلوماتي[2] " .

رابعا/ تعريف الجريمة الإلكترونية قانونا

تطرقت معظم التشريعات الوطنية لتعريف الجريمة الإلكترونية وفيما يلي ذكر لبعض التعريفات على سبيل المثال:

أ.التعريف الفرنسي:

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

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

[1] سميرة معاشي، المرجع السابق، ص277.

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

2. جريمة إتلاف برامج ومعلومات الحاسب الآلي الرقمي وبذلك تكون هذه الجرائم متعلقة بمحتوى الاسطوانة الممغنطة أو الشريط الممغنط[2]، كما اصدر المشرع الجنائي الفرنسي ق.ع الجديد لسنة 1992 المعمول به منذ مارس 1994 الذي جرم فيه صور الاعتداء الناجمة عن المعالجة الآلية للبيانات مما يسمح بانطباقه على الأفعال التي تقع على الانترنيت كمحل الاعتداء أو بواسطته كوسيلة للاعتداء[3].

ب. التعريف 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[4]، وقد اصدر المشرع الأمريكي عدة قوانين في مواجهة الجريمة الإلكترونية من بينها قانون آداب الاتصالات " mirrucation 1996 "CDA decency com يجرم فيه القذف والسب عبر شبكة الانترنيت كما وسع نطاق وحماية

---

[1] محمد مصطفى موسى، التحقيق في الجرائم الالكترونية، مطابع الشرطة ، القاهرة، 2009، ص118-119.

[2] محمد مصطفى موسى، ص114-115.

[3] نفس المرجع، ص 118-119.

[4] محمد أمين الشوابكة، المرجع السابق، ص18.

الأطفال بإصدار قانون لحمايتهم ضد الاستغلال الجنسي سنة 1998 "copa" protection act child onlin[1].

د.**التعريف العماني**: لقد عدل المشرع العماني قانون الجزاء بالمرسوم السلطاني 2001/72 حيث أضاف إلى قانون الجزاء الفصل الثاني مكرر وجرم بموجب هذا التعديل جملة من التصرفات التي يتعرض لها الحاسب الآلي وحصرها في الصور التالية[2]:

-الالتقاط غير المشروع للمعلومات والبيانات – الدخول غير المشروع على أنظمة الحاسب الآلي التجسس والتنصت على البيانات و المعلومات – انتهاك خصوصيات الغير أو التعدي على حقهم في الاحتفاظ بأسرارهم- تزوير بيانات أو وثائق مبرمجة أيا كان شكلها – إتلاف وتغيير و محو البيانات والمعلومات – جمع المعلومات والبيانات وإعادة استخدامها – تسريب المعلومات و البيانات – التعدي على برامج الحاسب الآلي لما يشكل انتهاكا لقوانين حقوق الملكية و الأسرار التجارية[3].

الفرع الثاني: خصائص الجريمة الإلكترونية والمجرم الإلكتروني

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

[1] محمد أمين الشوابكة، المرجع السابق، ص18.

[2] محمد حماد مرهج الهيتي، جرائم الحاسوب، دار المناهج، عمان، ط1، 2006، ص176.

[3] نفس المرجع، ص176.

خبرة بأمور الحاسب الآلي والانترنيت وقبل التطرق لخصائص الجريمة الإلكترونية، يجدر ذكر خصائص المجرم الإلكتروني التي تميزه عن المجرم العادي .

أولا/ خصائص المجرم الإلكتروني

حتى يحقق الجزاء الجنائي غايته سواء في مجال الردع العام أو الخاص لابد وأن يوضع في الحسبان شخصية المجرم والذي ينبغي إعادة تأهيله اجتماعيا حتى يعود مواطنا صالحا للمجتمع ويمكن القول أن الجاني في الجريمة الإلكترونية يتمتع بقدر كبير من الذكاء علاوة على أنه إنسان اجتماعي[1]، حيث انه لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به، بل هو إنسان متكيف اجتماعيا وتزيد خطورته الإجرامية كلما زاد تكيفه الاجتماعي، مع توافر الشخصية الإجرامية لديه[2].

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] عبد الفتاح مراد، شرح جرائم الكمبيوتر والانترنيت، شركة البهاء للبرمجيات، ص44.

[2] عبد الفتاح بيومي حجازي، مكافحة جرائم الانترنيت، دار الفكر الجامعي، الإسكندرية، ط1، 2006 ،ص83-86.

ويرى باركر: أن المجرم الإلكتروني وإن كان يتميز ببعض السمات الخاصة، إلا أنه لا يخرج في النهاية عن كونه مرتكبا لفعل إجرامي يتطلب توقيع العقاب عليه ويرمز باركر إلى خصائص المجرم الالكتروني بكلمة سكرام SKRAM .

المهارة/SKILLS: وتعد المهارة المتطلبة لتنفيذ النشاط الإجرامي أبرز خصائص المجرم الإلكتروني، فتنفيذ الجريمة الإلكترونية يتطلب قدرا من المهارة يتمتع بها الفاعل والتي يكتسبها عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين.

المعرفة/knowledge: و تتمثل في معرفة كافة الظروف التي تحيط بالجريمة المراد ارتكابها أو تنفيذها وكذا إمكانية نجاحها واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائم بالتعرف على المحيط الذي تدور فيه، حتى لا يواجهون بأشياء غير متوقعة من شأنها إفشال أفعالهم أو الكشف عنهم.

الوسيلة/Resources: وهي الإمكانيات التي يتزود بها الفاعل لإتمام جريمته.[1]

السلطة/Authoutry : ويقصد بها الحقوق أو المزايا التي يتمتع بها المجرم التي تمكنه من ارتكاب جريمته، فكثير من مجرمي الجريمة الإلكترونية لديهم سلطة مباشرة أو غير مباشرة في مواجهة المعلومات محل الجريمة، فقد تتمثل في الشفرة الخاصة بالدخول إلى النظام الذي

[1] نائلة عادل محمد فريد قورة ،المرجع السابق، ص56-58.

يحتوي على المعلومات التي تمكن الفاعل من فتح الملفات، قراءتها، كتابتها، محو أو تعديل المعلومات التي تحتوي عليها[1].

الباعث/Motives: الدافع لارتكاب الجريمة الإلكترونية غالبا ما يكون النفع المادي الذي سيحصل عليه الجاني من سيطرته على المعلومات، غير أن هذا القول لا يعني أنه لا وجود لبواعث أخرى، كأن يقوم شخص بتدمير قاعدة البيانات لشركة ما بدافع الانتقام[2].

ويمكن تقسيم دوافع الجريمة إلى:

أ. **الدوافع الشخصية**: والتي بدورها ترد إلى دوافع مالية، ذهنية أو نمطية.

وتعتبر الدوافع المادية من أهم البواعث على ارتكاب الجريمة الإلكترونية، لما تحققه من ثراء فاحش والدليل ما حدث في فرنسا 1986 حيث كان العائد من ارتكاب جناية سرقة مع حمل سلاح هو 70000 فرنك في حين أن جريمة غش في مجال المعالجة الآلية للمعلومات حصل منها الجاني على 270000 فرنك مما يعادل أكثر من 38 مرة.

وهناك فئة من مرتكبي الجريمة الإلكترونية يرجع ارتكابهم لها إلى الديون الناتجة من المشاكل العائلية أو الخسائر الضخمة من ألعاب القمار وإدمان المخدرات[3].

ب. **الدوافع غير الشخصية**: تتمثل في دافع الانتقام، مثل قيام محاسب شاب بالتلاعب بالبرامج المعلوماتية بإحدى المنشات التي كان يعمل بها، وبعد رحيله من المنشاة بعدة أشهر

---

[1] نائلة عادل محمد فريد قورة ،المرجع السابق، ص56-58.

[2] محمد حماد مرهج الهيتي، المرجع السابق،ص 164.

[3] أحمد خليفة الملط، المرجع السابق،ص88-89.

تم تدمير البيانات الخاصة بحسابات وديون المنشأة، كما يؤدي دافع جنون العظمة أو الطبيعة التنافسية في كثير من الأحيان لمثل هذه الجرائم حيث ترتكب من طرف العاملين داخل المنشأة، وذلك لإظهار قدراتهم الفنية لإدارة المنشأة، فيتنافسون للوصول إلى مراكز مرموقة، وقد ترتكب هذه الجرائم تحت تهديد وضغط من الغير في مجالات الأعمال التجارية والخاصة بالتجسس والمنافسة.

ج. **دوافع خاصة بالمنشأة**: يعتقد بعض المتخصصين في تقنية الأنظمة المعلوماتية أن المسؤولين عن المراكز المعلوماتية بالمنشأة يستغلون مراكزهم الوظيفية، ومهاراتهم الفنية في استخدام الأنظمة وبرامجها لأغراض شخصية أو ممارسة بعض الهوايات الدائرة في فلك التقنية ومن شأن ذلك تمادى بعضهم إلى استخدام الأنظمة بصورة غير مشروعة تصل إلى حد ارتكاب جرائم خطيرة بالمنشأة لمصلحته[1].

ثانيا/ المجني عليه في الجريمة الالكترونية

المعتدى عليه في الجريمة الإلكترونية هو من يكون ضحية الاعتداءات غير المشروعة على مكونات الحاسوب، وقد يكون شخصا طبيعيا، شركة، أو مؤسسة تتعامل بمجال الحاسوب أثناء ممارسة الأعمال التجارية، الاقتصادية والسياسية التي ينبغي أن تستغل الحاسوب في إدارة أعمالها[2]، وحسب تقديرات بعض خبراء الصندوق الدولي للبنوك فإنه من المستحيل أن تحدد على نحو دقيق نطاق الجريمة الإلكترونية التي لا يعلم ضحاياها عنها

[1] أحمد خليفة الملط، المرجع السابق، ص91.

[2] خالد عياد الحلبي،المرجع السابق، ص37.

شيء إلا عندما تكون النظم المعلوماتية المملوكة لهم هدفا للجريمة الإلكترونية، حتى في حالة علمهم بذلك فهم يفضلون عدم إفشاء الفعل لأنه لا يوجد من يريد الاعتراف بأنه تم انتهاك نظامه المعلوماتي[1].

والجدير بالذكر أن سلبية المجني عليهم أو ضحايا الجريمة الإلكترونية، وخوفهم من الإبلاغ حفاظا على سمعتهم التجارية ومكانتهم المرموقة، خير معين على التمادي في اقتراف مثل هذه الجرائم[2]، وتوجه هذه الجرائم بصفة خاصة إلى البنوك، وإلى المواقع الإلكترونية للمؤسسات المالية، لأن القطاعات المستهدفة من الجريمة الإلكترونية هي التي تعتمد أكثر من غيرها على أجهزة الحاسوب، وتعتبر البنوك من أهم تلك القطاعات وأكثرها تضررا[3].

ثالثا/ أنواع المجرمين الإلكترونيين وصفاتهم

قد يكون الجاني في الجريمة الإلكترونية، إما شخص يعمل بمفرده أو ضمن منظومة بغض النظر عن هذه الأخيرة، فقد تكون تجارية، سياسية أو عسكرية[4]، ويمكن تقسيم أنواع المجرمين إلى فئتين:

[1] عبد الفتاح بيومي حجازي، مكافحة جرائم الانترنيت، المرجع السابق، ص96-97

[2] نفس المرجع، ص96-97

[3] خالد عياد الحلبي ،المرجع السابق،ص38

[4] عبد الفتاح مراد،المرجع السابق، ص45

الفئة الأولى: صغار نوابغ المعلوماتية Pranksters

ويقصد بهم البالغ المفتون بالمعلوماتية والحسابات الآلية، وكثيرا ما لفتوا النظر في الآونة الأخيرة[1]، ويرتكب هؤلاء الأشخاص الجرائم بغرض التسلية والمزاح مع الآخرين دون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم[2].

الفئة الثانية: المحترفون في الجريمة الإلكترونية Professionals in IT crimes

ويتمتع أصحابها بخبرة ودراية أكثر من الفئة الأولى، وينقسمون حسب خطورتهم إلى:

- **فئة المتسللين الهواة** Hackers : هم لا يهدفون في حربهم المعلوماتية إلا للمغامرة وإظهار القدرات أمام الأقران فلا توجد عادة عند هؤلاء أطماع مالية[3].

- **فئة القراصنة الخبيثون** Malicious harckers : هم أشخاص هدفهم إلحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مادية من ضمن هذه الأهداف، ويندرج تحت هذه الفئة الكثير من مخترعي فيروسات الحاسبات الآلية وموزعيها.

---

[1] عبد الفتاح بيومي حجازي، مكافحة جرائم الانترنيت، المرجع السابق، ص 90.

[2] نائلة عادل محمد فريد قورة، المرجع السابق، ص61.

[3] عبد الفتاح مراد، المرجع السابق، ص 46.

- **فئة حلالي المشاكل الشخصية** Personal problem solvers: هم الأكثر شيوعا يترتب على إجرامهم في الكثير من الأحيان خسائر كبيرة تلحق بالمجني عليهم، رغبة منهم في إيجاد حلول لمشكلات مادية تواجههم، والتي لا يتم حلها بالوسائل الأخرى وغالبا ما يكون المجني عليه المؤسسة التي يعملون بها[1].

- **فئة المجرمين المهنيين** Career criminals: وتظم مجرمي الجريمة الإلكترونية الذين يبتغون من وراء نشاطهم الإجرامي تحقيق الربح المادي بطريقة غير مشروعة، ويعمل المنتمون إلى هذه الفئة في أغلب الأحوال بطريقة منظمة بحيث ينطبق على أفعالهم وصف الجريمة المنظمة[2].

- **فئة أصحاب الدعوة المتطرفة** Extreme adrocate: وتدخل في عدادها الجماعات الإرهابية أو المتطرفة، والتي تتكون بدورها من مجموعة أشخاص لديهم معتقدات وأفكار اجتماعية سياسية أو دينية، يرغبون في فرض هذه المعتقدات باللجوء أحيانا إلى النشاط الإجرامي، وقد بدأ اهتمام الجماعات الإرهابية وخاصة التي تتمتع من بينها بدرجة عالية من التنظيم، يتجه إلى نوع جديد من النشاط الإجرامي، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة بأوربا باسم The Red Brigades بتدمير ما يزيد عن 60 مركز للحاسبات الآلية خلال الثمانينيات لتلفت الأنظار إلى أفكارها ومعتقداتها[3].

---

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص 62.

[2] نفس المرجع، ص62.

[3] نفس المرجع، ص63.

- **فئة الجناة المقصرين** The Criminally Neghigent : وتظم واحدة من أهم المشكلات التي تتصل بإساءة استخدام الحاسبات الآلية وهي الإهمال، ولا شك في أن الإهمال في مجال الحاسبات الآلية يمكن أن يترتب عليه في كثير من الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح ففي نيوزيلندا مثلا: قام اثنان من مبرمجي الحاسبات الآلية بتغيير في أحد البرامج التي تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائرة بهذا التغيير، مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل 60 راكبا كانوا على متنها وتمت محاكمتهما بتهمة القتل الخطأ[1].

رابعا/ خصائص الجريمة الإلكترونية

تشترك الجريمة الإلكترونية مع غيرها من الجرائم التقليدية كتبييض الأموال، الإرهاب والاختلاس ...الخ بمجموعة من الصفات وتنفرد بصفات تميزها عن هذه الجرائم، وهي كالتالي:

أ.الخصائص المشتركة مع بعض الجرائم التقليدية:

تشترك الجريمة الإلكترونية مع الجرائم التقليدية، في كونها خطيرة ومن الجرائم العابرة للحدود وفي ما يلي تفصيل لذلك..

1. **خطورة الجريمة الالكترونية** :

[1] نائلة عادل محمد فريد قورة، المرجع السابق، ص60.

تتسم الجريمة الإلكترونية بخطورتها وذلك لمساسها بالإنسان في فكره وحياته الخاصة كما تمس المؤسسات في اقتصادها، والبلاد في أمنها القومي والسياسي والاقتصادي، ومن شأن ذلك أن يضفي أبعادا خطيرة غير مسبوقة على حجم الأضرار والخسائر التي تنجم عن ارتكاب هذه الجرائم على مختلف القطاعات والمعاملات، وقد بينت إحصائيات وفقا لتقديرات المركز الوطني جرائم الحاسب الآلي في الولايات المتحدة الأمريكية حوالي 500 مليون دولار أمريكي بينما قدرتها مصادر أخرى بـــــــــ 3و5 بليون دولار في السنة[1].

2. الجريمة الإلكترونية من الجرائم العابرة للحدود:

يمكن القول أنه من أهم الخصائص التي تميز الجريمة الإلكترونية هي تخطيها للحدود الجغرافية، ومن ثم اكتسابها طبعة دولية، فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة[2].

ب. خصائص الجريمة الالكترونية التي تنفرد بها عن الجرائم التقليدية:

هناك بعض خصائص التي تنفرد بها الجريمة الإلكترونية عن باقي الجرائم التقليدية ومن هذه الخصائص ما يلي:

1. **الحاسب الآلي هو أداة ارتكابها:** فغالبا ما يكون الحاسب الآلي[1] هو الأداة التي تمكن الشخص من الدخول إلى شبكة الانترنيت وقيامه بتنفيذ جريمته أيا كان نوعها [2].

---

[1] سميرة معاشي، المرجع السابق ،ص281

[2] محمد منير الجنبيهي و ممدوح محمد ، الجوانب الإجرائية لجرائم الانترنيت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامعي، الإسكندرية، 2006، ص14.

2. **ترتكب هذه الجرائم عبر شبكة الانترنيت أو عليها**: تعد شبكة الانترنيت الحقل الذي تقع فيه الجريمة الإلكترونية، وذلك لأنها تمثل حلقة الوصل بين كافة الأهداف المحتملة لتلك الجريمة كالبنوك والشركات الصناعية وغيرها من الأهداف التي تكون غالبا الضحية لها[3].

3. **صعوبة إثباتها**: حيث تتصف الجريمة الإلكترونية بالخفاء، أي عدم وجود أثار مادية يمكن متابعتها وهي خطيرة، وصعبة الاكتشاف بسبب اتساع نطاقها المكاني وضخامة البيانات.

4. عدم وجود مفهوم مشترك لها وكذلك عدم وجود تعريف قانوني موحد.

5. وقوع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات[4].

الفرع الثالث : تقسيمات الجريمة الإلكترونية وأضرارها

تنقسم الجريمة الإلكترونية إلى نوعين من الجرائم فقد تقع على شبكة الانترنيت كالاعتداءات المنطقية وقد تقع في شبكة الانترنيت، و تتخلف عنها أضرار تختلف نسبتها من دولة لأخرى.

---

[1] يقصد بالحاسب الآلي وفقا للموسوعة الشاملة لمصطلحات الحاسب الالكتروني " كل جهاز الكتروني ، يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال "data imput" و إخراج معلومات "data out put" و إجراء عمليات حسابية او منطقية ، وهو يقوم بالكتابة على أجهزة الإخراج" out put devices" أو التخزين و يتم إدخال البيانات بواسطة مشغل الحاسب "opérator " عن طريق وحدات الإدخال أو استرجاعها من وحدة المعالجة المركزية وبعد معالجة البيانات، تتم كتابتها على أجهزة الإخراج"، انظر المرجع السابق، احمد خليفة الملط ،ص26-27.

[2] محمد منير الجنبيهي و ممدوح محمد المرجع السابق، ص14.

[3] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنت، المرجع السابق، ص 37.

[4] خالد ممدوح إبراهيم، أمن الجريمة الالكترونية، المرجع السابق، ص45-49.

أولا / تقسيمات الجريمة الإلكترونية

نظرا لصعوبة حصر أنواع الجريمة الإلكترونية، لاختلافها من مجتمع لآخر من حيث نضجه أو درجة استخدامه للكمبيوتر واعتماده عليه، ونظرا للتباين في رؤية دور الكمبيوتر ومحاولات وصف الأفعال الإجرامية بوسائل ارتكابها، فإنه يصعب وضع تقسيم يشمل كل أنواع الجريمة الالكترونية.

أ. الإجرام المعلوماتي على شبكة الانترنيت:

هناك العديد من الجرائم التي يكون ارتكابها لهدف ما ويتعلق بالمعلومات ويتمثل هذا الهدف إما بالحصول على المعلومات أو تغييرها أو حذفها نهائيا ويشتمل هذا النوع من الإجرام على الجرائم التالية:

1.**الاعتداءات المنطقية**:

وتشمل جرائم مهاجمة الشبكة بالفيروسات أو البريد الإلكتروني التطفلي، حيث تعتبر هذه الجرائم من أخطر الجرائم التي تهدد الحواسيب وشبكة الانترنيت، وتلحق بها خسائر مادية تقدر بعشرات الملايين من الدولارات ومن بينها:

القناة المخفية Canal Caché : وهو نوع خطير من الاعتداءات، يقوم على مبدأ تهريب المعلومات عبر خرق سياسة الأمن والحماية المعتمدة في الأنظمة المعلوماتية وهي في ذلك تتطلب ذكاء فائقا من المعتدي.

وكذلك هناك جريمة انتحال شخصية الفرد أو شخصية الموقع: ويعني ذلك انتحال صفة من له الحق في الدخول إلى نظام معلوماتي معين، وذلك باستغلال بياناته كعنوانه أو تاريخ ميلاده أو رقم ضمانه الاجتماعي، استغلالا سيئا من اجل الحصول على بطاقات الائتمان أو رخص القيادة بهدف تشويه سمعة صاحب الموقع[1].

2.الاعتداءات المادية:

ومن أبرزها الاعتراض المتعمد للبيانات : ويقصد به رصد إشارات الكترومغناطيسية في الأنظمة المعلوماتية وتحليلها بهدف استرجاع المعلومات المفهومة أو المقروءة منها.

ومن بين الاعتداءات المادية كذلك الاكتساح والتفخيخ : الأول يقصد به إرسال حزمة من المعلومات إلى الشبكة للتوصل إلى تحديد أي من هذه المعلومات هي الصحيحة، أما الاعتداء الثاني فهو إدخال وظائف خفية في مرحلة تصميم، تصنيع، نقل أو صيانة النظام المعلوماتي[2].

ب. الإجرام غير المعلوماتي في شبكة الانترنيت :

ويحدث عندما تستخدم الانترنيت كوسيلة لارتكابها ويشمل العديد من الجرائم كالجرائم الجنسية، الجرائم المالية، جرائم القرصنة، جرائم غسل الأموال والمخدرات ....الخ.[3]

---

[1] نبيلة هبة هروال،المرجع السابق،ص57-61

[2] نبيلة هبة هروال ،المرجع السابق،ص62.

[3] نفس المرجع، ص62.

وهناك تقسيما آخر تبعا لمساسها بالأشخاص:

1.**جرائم تستهدف الأشخاص**: معظم الجرائم التي ترتكب عبر شبكة الإنترنيت تستهدف إما أشخاص أو جهات بعينها، وغالبا ما تكون تلك الجرائم هي جرائم مباشرة ترتكب في صورة ابتزاز أو تهديد أو تشهير، أو غير مباشرة ترتكب في صورة الحصول على البيانات والمعلومات الخاصة بتلك الجهات، الأشخاص، وذلك لاستخدام تلك المعلومات والبيانات لارتكاب جرائم مباشرة ومن بين هذه الجرائم:

- **الجرائم غير الجنسية** : التي تستهدف الأشخاص وتشمل القتل بالكمبيوتر والتسبب بالوفاة جرائم الإهمال المرتبطة بالكمبيوتر، التحريض على الانتحار، التهديد عبر وسائل الاتصال المؤقتة الاطلاع على البيانات الشخصية، قنابل البريد الإلكتروني، بث المعلومات الزائفة المظلة[1].

- **الجرائم الجنسية أو جرائم الأخلاق**: لقد احتلت مشكلة الأخلاق عبر الانترنيت حيزا كبيرا في بحوث الفقه المقارن، وذلك لاختلاف الأخلاقيات من شعب لآخر، وجرائم الأخلاق هي تلك النوعية من الجرائم التي تتضمن العدوان على القيم الأخلاقية المتعارف عليها في النظم الاجتماعية والاقتصادية، ومن أهمها جرائم القذف والسب والتشهير، جرائم الاستغلال الجنسي جرائم الاعتداء على حرمة الحياة الخاصة.

[1] عبد الفتاح مراد، المرجع السابق، ص55.

2. **الجرائم المالية**: تستهدف غسل الأموال، المخدرات، الجرائم المتعلقة بالتجارة، جرائم السرقة والنصب والاحتيال عبر الانترنيت[1].

3. **جرائم التزوير**: وهو من اخطر طرق الغش التي تقع في مجال نظم المعالجة للبيانات نظرا لأن الحاسب الآلي والانترنيت أصبحا يحلان محل الأوراق في كافة المجالات، كما في عمليات الدفع و التعاقد عبر الانترنيت وتحويلات الأموال من بنك لآخر[2].

ثانيا/ أضرار الجريمة الإلكترونية

نظرا لوقوع الجريمة الإلكترونية في نطاق تقنية متقدمة، وأنها تتزايد يوما بعد يوم وأن مجالات وقوعها كثيرة، ومخاطرها عديدة نظرا لطبيعة استخدامها في المعاملات الاقتصادية والمالية الوطنية والدولية، والاعتماد عليها في تسيير شؤون الحياة اليومية للأفراد والشؤون العامة للحكومات، ومن شأن ذلك أن يضفي أبعادا غير مسبوقة على الخسائر والاضطرار التي تنجم عن هذه الجرائم[3]، ومن خلال الاعتداء على نظام المعالجة الآلية للبيانات بصورتيه العمدية وغير العمدية، التي تحمل المنشآت الصناعية والتجارية نفقات طائلة لا يمكن حصرها تنفق من أجل إعادة الحال إلى ما كان عليه كالنفقات التي توجه إلى تعويض الخسائر التي تلحق بالمعدات المادية لإصلاحها واستبدالها بأخرى[4].

---

[1] نبيلة هبة هروال، المرجع السابق، ص64-78.

[2] عبد الفتاح مراد، المرجع السابق، ص57

[3] أحمد خليفة الملط، المرجع السابق،ص 95.

[4] بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، الإسكندرية، ط1، 2008، ص35.

وقد أجريت عدة دراسات على الجريمة الإلكترونية منها تلك الدراسة التي أجرتها منظمة Alliance Business Software في الشرق الأوسط، والتي أظهرت أن هناك تباين في حجم خسائر الجريمة الإلكترونية في الشرق الأوسط حيث تراوحت بين 30 مليون دولار أمريكي في المملكة العربية السعودية والإمارات المتحدة، ومليون وأربعمائة ألف دولار أمريكي، فقط في لبنان[1].

أما في فرنسا فقد ارتفع حجم الخسائر الناشئة عن أفعال التحايل المعلوماتي على الحاسب الآلي، حيث قدرت الخسائر في هذا المجال بما يقرب المليار وسبعة من عشرة وتشكل نسبة اثنان وخمسون في المائة من إجمالي الخسائر التي تتعلق بالإجرام الالكتروني[2].

وفي السويد أظهرت دراسة ارتر سولارز Artur Solarz أن معدل الخسارة لجريمة الاختلاس التقليدي، يبلغ 137 ألف كورونة ويرتفع إلى 196 ألف في جريمة الاختلاس الذي يستخدم النظام المعلوماتي في ارتكابها[3].

المطلب الثاني: أركان الجريمة الالكترونية وصورها

اختلف الفقهاء في تعريف الجريمة الإلكترونية، كما اختلفوا أيضا في تحديد أركانها حيث ذهب بعضهم إلى القول أن الجريمة تقوم على ركنين اثنين فقط هما الركن المادي والمعنوي، ويستبعد هذا الفقه الركن الشرعي باعتبار أن الصفة غير المشروعة للفعل تتجدد

[1] منير ممدوح،محمد الجنبيهي، المرجع السابق، ص17.

[2] بلال أمين زين الدين، المرجع السابق ، ص37.

[3] احمد خليفة الملطـــ، المرجع السابق، ص100.

على ضوء نموذج الجريمة، فهي العلاقة بين الفعل المرتكب والوصف القانوني، وبالتالي فهي تكشف عن وقوع الجريمة ولا تعتبر جزءا فيها[1]، وذهب بعضهم إلى القول أن أركان الجريمة ثلاث الركن الشرعي، المادي والمعنوي وأصحاب هذا الرأي يعتبرون الركن الشرعي ركنا لازما للجريمة تحت مفهوم الصفة غير المشروعة أي التكييف القانوني للفعل بالنظر إلى نصوص قانون العقوبات[2].

والجريمة الإلكترونية لا تختلف عن أي جريمة أخرى، إذ تتطلب لتحققها الأركان المتفق على ضرورة توفرها في أي جريمة لكي تتواجد على أرض الواقع وهي الركن الشرعي، المادي والركن المعنوي.

الفرع الأول: الركن الشرعي للجريمة الإلكترونية

ينطبق مبدأ الشرعية على تعريف الجرائم وعلى تحديد العقوبات وتدابير الأمن التي تطبق على شخص معين، فلا يجوز للقاضي تجريم الفعل ما لم يجرم بنص، ولا توقيع عقوبة لم يرد بشأنها حكم، والإشكال المطروح هنا ما محل الجريمة الإلكترونية من مبدأ شرعية الجرائم والعقوبات؟

تناولت التشريعات التقليدية الجرائم التقليدية التي تقع على الأموال والأشخاص وغيرها بالتجريم إلا أنه ومع تزايد ظاهرة قرصنة برامج الحاسوب، وتعدد العمليات

[1] ومن أنصار هذا الرأي ديكوك و جانديدي الذين قالا ان النص القانوني ليس ركنا من أركان الجريمة إنما هو عامل الردع للمزيد انظر أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر، ط3، 2006 ، ص55.

[2] مروك نصر الدين ، محاضرات في الإثبات الجنائي، ، دار هومة، الجزائر، ج1 ،2003، ص236.

الإلكترونية غير المشروعة ووقوف المشرع عاجزا أمام هذه الظاهرة الخطيرة، أدى به إلى التدخل ليتناول ما يستجد من هذا الشكل الجديد للإجرام، تطبيقا لمبدأ الشرعية وفيما يلي نماذج عن بعض التشريعات:

أولا/ على مستوى الدولي :

هناك العديد من الهيئات والمنظمات التي تؤدي دورا ملحوظا في إبرام الاتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة الجريمة الإلكترونية وعلى سبيل المثال:

أ. مؤتمر الأمم المتحدة السابع الذي انعقد في ميلانو "ايطاليا" عام 1985 حيث كلف لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعلومات والاعتداء على الحاسب الآلي حيث أقرت مجموعة من المقترحات والتوصيات لمكافحة الجريمة الإلكترونية[1]، فقد أكد هذا المؤتمر على وجوب تطبيق التطورات الجديدة في مجال العلم والتكنولوجيا في كل مكان لصالح الجمهور، واتخاذ تدابير ملائمة ضد حالات إساءة الاستعمال المخلة لهذه التكنولوجيا، كذلك أكد المؤتمر عبر قواعده التوجيهية على ضرورة تشجيع التشريعات الحديثة التي تجرم وتتناول الجريمة الإلكترونية باعتبارها نمطا من أنماط الجريمة المنظمة كغسيل الأموال والاحتيال المنظم، حيث تضمن خطة عمل لبرنامج عالمي لمنع الجريمة المنظمة عبر

[1] علي جبار الحسناوي، جرائم الحاسوب و الانترنيت،دار اليازوري ، الأردن، 2009، ص 147،148.

الوطنية والإرهاب مشددة على ضرورة إجراء بحوث ذات توجه عملي وتقديم المساعدة التقنية للبلدان النامية[1] .

ب. الاتفاقية الأوروبية لمكافحة الجريمة الإلكترونية " بودبست 22 نوفمبر 2001 " : وتناولت كل ما يتعلق بالجريمة الإلكترونية، سواء ما يقع ضد الشبكات أو الجرائم التقليدية التي تستخدم في ارتكابها الشبكات المعلوماتية[2]، فقد جاء في الفصل الأول منها تعريف لبعض المصطلحات المتعلقة بالحاسوب والانترنيت، أما الفصل الثاني فتناول الإجراءات الواجب اتخاذها على المستوى المحلي، وقد وردت بعض من صور الجريمة الإلكترونية وذلك من خلال المواد 02-10، والفصل الثالث احتوى المواد 23-31 التي أوجبت التعاون الدولي لمكافحة الجريمة والقبض على المجرمين وقد أوردت بعض صور هذا التعاون.

أما على مستوى الجهود العربية فقد اعتمد مجلس وزراء العدل العرب للقانون الجزائي العربي الموحد ًقانونا نموذجيا بموجب القرار 229 لسنة 1996ً 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 فقد عاقبت على الاشتراك

[1] http://www.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congresses.html بتاريخ 2014/09/03 على الساعة 10:30

[2] خالد عياد الحلبي، المرجع السابق، ص 256.

في الأفعال التي تشكل الجريمة الإلكترونية بنفس عقوبة الفاعل الأصلي، والمادة 466 عاقبت على الشروع في ارتكاب الجريمة الإلكترونية بذات عقوبة الفاعل الأصلي[1] .

ثانيا/ على المستوى الوطني

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

أ. **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] " فعل الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات أو جزء منه، يعاقب بالحبس لمدة سنة وبغرامة 100000 فرنك، فإذا نتج عن الدخول أو البقاء سواء محو أو تغيير في المعطيات الموجودة في النظام أما تعييب تشغيل النظام، فإن العقوبة تصبح الحبس لمدة سنتين، والغرامة تصل 200000 فرنك ".

ب. **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

1 مذكرة توضيحية للقانون الجزائي العربي الموحد، جامعة الدول العربية، الجزء الثاني ، رقم 229 ، د 12 بتاريخ 1996/11/19 .

[2] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية ، بيروت،1999 ، ص 117.

الباب الثالث فقد بين فيه المشرع الوكالة الوطنية للمصادقة الإلكترونية، والباب السادس منه تناول حماية المعطيات الشخصية[1].

ج. **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[2] من قانون العقوبات.

الفرع الثاني:الركن المادي للجريمة الإلكترونية

يتكون الركن المادي للجريمة الإلكترونية من السلوك، النتيجة والعلاقة السببية ونظرا للاختلاف الفقهي القائم حول تعريف الجريمة الإلكترونية، فإنه يصعب تحديد صورة السلوك وعلى سبيل المثال صور الجريمة الإلكترونية في التشريع الجزائري، الذي حصر الركن المادي للجريمة الإلكترونية حسب نص المواد 394 مكرر إلى 394 مكرر7 والتي نستخلص من مضمونها الصور التالية:

أولا/ الدخول أو البقاء غير المشروع داخل نظام المعلوماتية، حيث نصت المادة 394 مكرر " يعاقب بالحبس من ثلاثة 03 أشهر إلى سنة وبغرامة من 50.000 دج إلى

[1] القانون المتعلق بالمبادلات والتجارة الإلكترونية، عدد83 ، لسنة 2000 المؤرخ في 9 أوت 2000 .

[2] الأمر رقم 04-15 المؤرخ في رمضان 1425 الموافق ل:10 نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات.

100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات" .

ثانيا/ الاعتداء على سير نظام المعلوماتية، حيث نصت الفقرة 3 من نفس المادة على أنه " وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة 06 أشهر إلى سنتين 02 و غرامة من 50.000 دج إلى 150.000 دج" .

ثالثا/ حذف أو تغيير لمعطيات المنظومة.

رابعا/ القيام بإدخال عن طريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها. وهذا ما نصت عليه المادة 394 مكرر1.

خامسا/ التصميم أو البحث أو التجميع أو التوفير أو النشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية.

سادسا/ حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها[1].

[1] الأمر رقم 04-15 المؤرخ في رمضان 1425 الموافق ل:10 نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات.

الفرع الثالث : الركن المعنوي للجريمة الإلكترونية

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط ماديات الجريمة وشخصية الجاني[1]، ولقيام الركن المعنوي للجريمة الإلكترونية يكفي توافر القصد العام أي توافر العلم والإرادة، والجريمة الإلكترونية كما سبق القول من الجرائم العمدية فمتى تطابق السلوك مع الصور التي تصلح لأن تشكل جريمة إلكترونية، حسب معايير كل دولة تحقق الركن المعنوي إلا أنه قد ترتكب هذه الجرائم عن غير قصد، مثلا في جريمة الدخول غير المشروع إلى النظام أو جريمة الدخول إلى النظام بطريق كأن يعتقد الجاني أنه مازال له حق الدخول إلى النظام الآلي كأن يكون قد سبق له الاشتراك في الدخول إلى البرنامج ولكن مدة الاشتراك قد انتهت ومع ذلك دخل إلى النظام استنادا إلى هذا الاعتقاد الخاطئ، لأن الغلط في أمر جوهري ينفي القصد[2].

المبحث الثاني: التحقيق في الجريمة الإلكترونية

الجريمة الإلكترونية يرتكبها جناة ذوي صفات معينة أهمها الدراية الفنية بعمل الحاسب الآلي، وكلها تقدم الجاني في فهم تكنيك العمل في الحسابات الآلية، وكيفية تصميم البرامج كلما استطاع أن يرتكب جريمته دون أن يتم الاهتداء إليه، لأنه لا يترك أي آثار يمكن أن يستدل عليه من خلالها، هذا ما يصعب على المحققين الكشف عن هاته الجرائم

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية ، دار الفكر الجامعي ،الإسكندرية ، ط1 ،2009 ، ص 53.

[2] محمد حماد مرهج الهيتي، المرجع السابق ،ص189.

وإلقاء القبض على مرتكبيها وللتعرف أكثر على الإجراءات التي تتخذ في سبيل التنقيب عن هذا النوع المستحدث من الجرائم يجدر التعرض بالدراسة للتحقيق من حيث المفهوم والتعرف على الأجهزة التي تقوم بإجراءات التحقيق، ومناقشة الصعوبات التي تواجه المحققين في سبيل الكشف عن هاته الجرائم والقبض عن مجرميها.

المطلب الأول: مفهوم التحقيق في الجرائم الإلكترونية

تحتاج الدعوى قبل دخولها المحكمة إلى جمع المعلومات عنها من حيث نوع الفعل المرتكب ومن الذي ارتكبه والأدلة التي تثبت نسبة الفعل إلى مرتكبه وهذا ما يعرف بالتحقيق[1].

والتحقيق في الجرائم الإلكترونية يختلف عن التحقيق في الجرائم العادية من حيث الإجراءات وذلك لحداثة هذه الجريمة ومهارة مرتكبيها في الإجرام ومحو الأدلة.

الفرع الأول: تعريف التحقيق في الجريمة الإلكترونية

تعريف التحقيق في الجريمة الإلكترونية لا يختلف عنه في الجرائم الأخرى وسأتناول تعريفه لغة وقانونا، وحتى يكتمل التعريف بالتحقيق يجدر التطرق إلى تعريف المحقق الذي يقوم بكافة إجراءات التحقيق، وقبل ذلك سوف أتطرق لتعريف التحقيق بصفة عامة.

[1] براء منذر عبد اللطيف، شرح قانون أصول المحاكمات الجزائية، دار الحامد للنشر، عمان، ط1 ، 2009 ، ص71 .

أولا/ تعريف التحقيق

يهدف التحقيق إلى جمع الادلة والتنقيب عنها.

أ. **تعريف التحقيق لغة**: التحقيق مأخوذ حقق يحقق تحقيقا، حقق الظن بالله صدقه، الأمر أحكمه – مع فلان - في قضيته: أخذ رأيه فيها[1].

ب. تعريف التحقيق اصطلاحا: عرف التحقيق بمعناه العام أنه: اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها[2].

وعرف التحقيق أنه: مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة، كذلك هو مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا، بغية تمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة[3].

[1] علي بن هادية ، لحسن البليش، الجيلالي بن الحاج يحيى، المرجع السابق، ص 286.

[2] عمر بن إبراهيم بن حماد العمر ، إجراءات الشهادة في مرحلتي الاستدلال و التحقيق الابتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية،2007، ص 22.

[3] عمر بن إبراهيم بن حماد العمر، المرجع السابق، ص 22-23.

وكذلك عرف التحقيق بأنه " مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهدف التنقيب عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة ارتكبت لتقرير لزوم محاكمة المدعي عليه أو عدم لزومها[1]".

وهناك من قسم التحقيق إلى:

1. **التحقيق الجنائي العملي** : يقصد به جميع إجراءات التحقيق التي يباشرها المحقق الجنائي عند وقوع جريمة أو حادث، توصلا إلى معرفة الحقيقة وقواعد أساسها التجارب العملية التي وصل إليها المحققون في تحقيق القضايا الهامة.

2. **التحقيق الجنائي الفني**: ويرتكز على الأبحاث العلمية والتجارب الفنية التي يمكن تطبيقها لاكتشاف حقيقة الحوادث الجنائية والاهتداء إلى مرتكبيها[2].

وقد عرف أيضا بأنه " التحري والتدقيق في البحث تلمسا لمعرفة الجاني في جناية ارتكبت أو شرع في ارتكابها وكذلك في ظهور ارتكابها، ومن أولى متطلبات الأساسية استعمال الوسائل المشروعة للتحقيق[3] ".

ثانيا/ تعريف المحقق

[1] حسن الجوخندار،التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، دار الثقافة، عمان، ط1 ،2008، ص11.

[2] عبد الفتاح مراد، المرجع السابق ، ص11

[3] غسان مدحت الخيري ، الطب العدلي و التحري الجنائي ، دار الراية ، المملكة الأردنية ، ط1 ،2013 ، ص17

ذهب جانب من الفقه إلى تعريف المحقق بأنه: كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية، وتحقيقها ويسهم بدوره في كشف غوامضها وصولا إلى معرفة حقيقة الحادث وكشف مرتكبه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة[1] .

كما عرف البعض المحقق أو الباحث الجنائي بأنه " الشخص الذي يتولى ويتكلف بالتحقيق والتحري والبحث وجمع الأدلة لكشف غموض الحوادث ويتحدد دوره بالعمل على منع الجريمة قبل وقوعها أو اكتشافها بعد وقوعها، وضبط مرتكبيها والأدوات التي استعملت فيها"[2].

وعرف المحقق بأنه " ذلك الشخص الذي عهد إليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل إلى علمه من جرائم بهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة[3] " .

أما المشرع الجزائري فقد وضع تعريفا لقاضي التحقيق في المادة 68 من قانون الإجراءات الجزائية حيث جاء في نصها ما يلي " يقوم قاضي التحقيق وفقا للقانون باتخاذ

1 خالد ممدوح إبراهيم،فن التحقيق الجنائي، المرجع السابق، ص 87.

2 غسان مدحت الخيري، المرجع السابق، ص 17.

3 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 87.

جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي[1]".

الفرع الثاني: خصائص التحقيق في الجريمة الإلكترونية

الجرائم التي ترتكب بواسطة الحاسوب تنشأ في الخفاء وينصب الاعتداء فيها على معطيات الحاسوب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات، وعليه فالتعامل مع مسرح الجريمة الإلكترونية والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق[2]، وقبل التطرق إلى خصائص التحقيق في الجريمة الإلكترونية تجدر الإشارة لخصائص التحقيق عامة وهي كالأتي:

أولا/ خصائص التحقيق

أ. **السرية**: يقصد بسرية الإجراءات عدم الاطلاع عليها، ويقصد بسرية التحقيق عدم علانيتها بالنسبة للغير، وهم غير أطراف الدعوى العمومية فسرية التحقيق إذا تعني إجراء التحقيق في جو من الكتمان بالنسبة للجمهور[3]، حيث أن حضور إجراءات التحقيق غير

[1] الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو1966 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم .

[2] خالد عياد الحلبي، المرجع السابق، ص 147،183

[3] عبد الله اوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، ط2 ،2011، ص336.

مسموح به للجمهور وذلك لحماية المتهم من الشهر الذي قد يصيبه بسبب التحقيق الذي قد ينتهي بإصدار قرار أن لا وجه لإقامة الدعوى ولحماية الأدلة من العبث[1].

وقد اختلف في مسالة علانية التحقيق أو سريته فظهر اتجاهان :

1. **الاتجاه المؤيد للعلنية**: وقرر هذا الاتجاه علانية التحقيق بالنسبة لعامة الناس ولأطراف الخصومة الجزائية ووكلائهم، ومثال ذلك قانون التحقيق الجنايات المصري السابق، فجعل الأصل علانية التحقيق والسرية هي الاستثناء لإحقاق الحق وللآداب ولظهور الحقيقة، كما أخذ به القانون البحريني 1966 والقانون السوداني 1984[2].

2. **الاتجاه المؤيد للسرية**: بخلاف الرأي الأول، جعل التحقيق سري بالنسبة للعامة والخصوم على حد سواء، بمن فيهم المدعى عليه وقد اعتمد هذا الاتجاه القانون الفرنسي القديم والحالي الذي أخذ بسرية إجراءات التحقيق كأصل وعلانيته كاستثناء بالنسبة للخصوم[3]، نفس الشيء بالنسبة للمشرع الجزائري فقد نص في المادة 11 من قانون الإجراءات الجزائية على " تكون إجراءات التحري و التحقيق سرية، ما لم ينص القانون على خلاف ذلك ودون إضرار بحق الدفاع"[4]

---

[1] عمر بن إبراهيم بن حماد العمر، المرجع السابق، ص 110.

[2] حسن الجوخدار، المرجع السابق، ص34-35.

[3]. نفس المرجع، ص34-35.

[4] الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو1966 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم .

ب. التدوين: لقد اوجب المشرع المختص بالتحقيق اصطحاب كاتب معه يرافقه في جميع إجراءاته ويدون المحاضر ويصادقان معا على جميع صفحات المحاضر، بحيث يجري تدوين جميع إجراءات التحقيق وإثباتها كتابة في محضر رسمي يعد لذلك، حتى يكون حجة في الإثبات[1].

ثانيا/ الخصائص الفنية للمحقق في الجريمة الإلكترونية :

إن الجريمة الإلكترونية تنبع من التطور الفني الإلكتروني وهذا للاستخدام السيئ لبعض العاملين على أجهزة الحاسوب، مما أضاف أعباء جديدة على أجهزة التحقيق، لما يتطلبه التصدي لهذه الجرائم من قدرات فنية لم يألفها المحققون ولم يتعودوا عليها، مما أدى إلى ضرورة توفير الإمكانيات والمهارات المطلوبة في هذا المجال، وعليه فالتركيز هنا سوف ينصب على الخصائص الفنية التي تتسم بالحداثة والناتجة عن التطور الإنساني في مجال تقنية المعلومات والأنظمة الإلكترونية[2]، ويمكن ذكر الخصائص الفنية للمحقق كما يلي :

أ. **أن يكون هدف المحقق دائما إلى الوصول الحقيقة** : الشرط المتطلب لنجاح المحقق في أداء رسالته إيمانه بها، وأن يكون هدفه الحقيقي الوصول إلى الحقيقة، لا العدول عنها وهذا ليس بالأمر الهين ذلك أن أساس العدالة من صفات الله تعالى فإن آمن بها المحقق حينها لن يخل بواجباته مهما لاقى من الصعوبات، وعلى المحقق أن يضل مدركا بأنه في حالة صراع

[1] محمد علي سالم الحلبي ، الوجيز في أصول المحاكمات الجزائية ، دار الثقافة ، عمان ، ط1 ، 2005 ، ص147 .

[2] خالد عياد الحلبي ، المرجع السابق ، ص 182 .

دائم بينه وبين المجرم الإلكتروني فالأول ينشد للحقيقة والثاني يجتهد في تضليل العدالة وطمس الحقائق والأدلة[1].

ب. **أن يكون لدى المحقق موهبة فن التحقيق** : إن التحقيق الفني هو إبداع، والتمكن من القدرة على التحليل ورفع الستار عن الحقيقة والغموض عن أي أمر، أو أي قضية كانت.

أما فيما يتعلق بفن التحقيق في الجريمة الإلكترونية ليس قدرة المحقق على استجلاء مدى توافر أركان الجريمة المعروضة وعناصرها، إنما هو قدرته أيضا على مناقشة الشهود لاستجلاء أقوالهم مما يكون قد شابها غموض، ففي التحقيق في الجريمة الإلكترونية، لا يجب أن يكون المحقق مجرد آلة ميكانيكية تسجل فقط الأسئلة والأجوبة بل عليه توجيه الأسئلة للمتهم والشهود[2].

ج . **أن يكون المحقق سريع التصرف في إجراءات التحقيق**: إن سرعة انجاز التحقيق تحافظ على أدلة الجريمة وآثارها، دون أن تمس أو تمحى، ويمنع من ضياعها، فالتأخير في إجراءات التحقيق قد يترتب عليه تعريض أدلة الجريمة ومعالمها لخطر الضياع، فالسرعة في إجراء التحقيق الجنائي من الواجبات الضرورية لمساس ذلك بسلطة الدولة.

[1] خالد ممدوح ابرهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص 96.

[2] نفس المرجع ، ص98-99.

وكذا حقوق الناس وحرياتهم، فسرعة التحقيق تؤدي إلى كشف حقيقة الجريمة دون أن يتمكن الجناة من طمس آثارها وأدلتها[1].

د. **قوة الملاحظة وسرعة البديهة**: ويقصد بها المعرفة الدقيقة لحقيقة أمر، أدركته أحد الحواس عما يحيط به من ظروف[2]، كما يجب عليه معرفة الجوانب الفنية والتقنية لأجهزة الحاسب والانترنيت التي تتعلق بالجريمة[3].

و. **حياد المحقق أثناء إجراء التحقيق**: يعتبر من أهم خصائص التحقيق، فيجب أن يقوم بالتحقيق شخص غير متحيز يعنى بما يفيد الدفاع عنايته بأدلة الاتهام، ولا تتحقق الحيدة التامة للمحقق إلا إذا استقلت سلطة التحقيق عن كل من سلطة الاتهام من ناحية وسلطة الحكم من ناحية أخرى، فلا يجوز للنيابة المنوط بها توجيه الاتهام أن تحقق بعدل[4].

ي. **المساواة في معاملة الحضور**: القاعدة العامة بالنسبة للمحقق يلتزم بها هي المساواة في المعاملة، حتى بالنسبة للمتهم الماثل أمامه فينبغي على المحقق المساواة بين المتهم والمجني عليه عند المثول أمامه[5].

ه. **الهدوء وضبط النفس**: يوجد في الحياة كثيرا من ذوي النشاط الإجرامي يعملون على استفزاز المحقق لتشتيت أفكاره أو بدفعه للتعدي عليهم حتى يمكنهم تبرير اعتراضهم

---

[1] محمد علي سالم الحلبي، المرجع السابق، ص153-154.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص103.

[3] خالد عياد الحلبي، المرجع السابق، ص183.

[4] فرج علواني هليل، التحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، الإسكندرية، 2006 ، ص57.

[5] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، المرجع السابق، ص103-108.

بارتكاب الواقعة وإبطالها بادعاء أنه وليد إكراه[1]، لذا يتوجب على المحقق بالإضافة إلى الهدوء إتباع الإجراءات الصحيحة والمشروعة من أجل سرعة المحافظة على الأدلة الإلكترونية، التي تدل على وقوع الجريمة الإلكترونية بتخزينها في الأقراص المعدة لذلك ومنع حذفها[2].

الفرع الثالث: معوقات التحقيق الجنائي في الجرائم الإلكترونية

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

[1] نفس المرجع، ص110.

[2] خالد عياد الحلبي، المرجع السابق، ص183.

والتجديد، وهذا ما يترك المجال لمجرمي الجريمة الإلكترونية التملص من المسؤولية الجزائية لأن القوانين التقليدية غير كافية.

ثانيا/ المعوقات المتعلقة بالجريمة الإلكترونية والجهات المتضررة

تعترض المحقق صعوبات أثناء البحث، منها معوقات متعلقة بالجريمة الإلكترونية ، وصعوبات متعلقة بالمتضررين من الجريمة، كإحجامهم عن الإبلاغ عنها.

أ. **المعوقات المتعلقة بالجريمة الإلكترونية**: نظرا لأن الجريمة الإلكترونية ترتكب في بيئة بيانية مما يسمح بإخفاء معالم الجريمة حيث يغيب الدليل المرئي الممكن بالقراءة فهمه، لأن أدلة الجريمة الالكترونية قلما تكون مادية، فالأدلة التي تخلفها غير ملموسة مما يسمح للجناة بالتخلص منها بكل سهولة وسرعة فائقة، كما يمكنهم إحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم التي تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها[1] .

ب. **المعوقات المتعلقة بالجهات المتضررة**: هي على العموم عدم إدراك المتضررين من خطورة هذه الجرائم، كذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة الجرائم المتعلقة بالإنترنيت، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز

[1] خالد ممدوح إبراهيم ، فن التحقيق الجنائي للجرائم الالكترونية ، المرجع السابق، ص65.

على الجانب الأمني مما يؤدي إلى الإحجام عن الإبلاغ عن الجريمة، خوفا من المجتمع المحيط بهم وخشية من الفضيحة أو الظهور بمظهر مشين أمام الآخرين[1].

المطلب الثاني: جهاز التحقيق الجنائي في الجريمة الإلكترونية والصعوبات التي تواجهه

لقد بدأت التكنولوجيا بالتزايد والتطور في جميع نواحي الحياة وهذا من أثار الثورة الصناعية التي قامت في منتصف القرن التاسع عشر حيث غزت التكنولوجيا العالم من خلال الوسائل الإلكترونية الحديثة، ومع اعتماد اغلب الدول هذه الوسائل زاد النمو الاقتصادي إلا أنه صاحب هذا النمو نوع أخر من التطور في الإجرام خاصة من قبل الطبقة المتعلمة التي تتعامل مباشرة مع هذه الوسائل كالحاسب الآلي الذي أصبح في يد أي شخص والركيزة الأساسية لمختلف مجالات الحياة، وما ساعد من تفشي هذه الظاهرة هو سهولة الحصول على المعلومات بشتى أنواعها وصعوبة الكشف عن هذه الجرائم، مما أدى بالدول إلى إنشاء جهاز خاص بالتحقيق في مثل هذه الجرائم ، فما هو هذا الجهاز؟

الفرع الأول: جهاز التحقيق الجنائي في الجريمة الإلكترونية و أقسامه

نظرا لانتشار الجريمة الإلكترونية بشكل ملفت للانتباه، ولأن أجهزة التحقيق في الجرائم التقليدية لم تكن كافية للتصدي لهذا النوع من الإجرام، أنشئت أجهزة خاصة بالتحقيق فيها.

[1] خالد عياد الحلبي، المرجع السابق ، ص223-224 .

أولا/ تعريف جهاز التحقيق الجنائي في الجريمة الإلكترونية

جهاز التحقيق في الجريمة الإلكترونية هو عبارة عن الوظائف المتخصصة إلكترونيا وقانونيا، التي يصدر بها قرار إداري وتشغل بنوعين من الأفراد " ضباط و ضباط الصف" والمدنيين وتحكم علاقتهم الوظيفية التسلسل النظامي للرتب العسكرية وقانون الخدمة المدنية للمدنيين وقواعد الأمن ويستخدمون التقنية الإلكترونية وضبطها والتي يكون محلها التقنية الإلكترونية الرقمية ونظمها وبرامجها وشبكاتها[1].

ثانيا/ أقسام جهاز التحقيق الجنائي في الجريمة الإلكترونية :

أصبحت الجرائم في عصر التقنية الحديثة أربعة أنواع: جرائم الاعتداء على النفس جرائم الاعتداء على المال، جرائم الاعتداء على المصلحة العامة والجرائم الإلكترونية بعد أن كانت ثلاثة أنواع فقط.

وعلى هذا الأساس قسمت الأجهزة التي تتولى التحقيق في هذه الجرائم إلى :

أ. **أجهزة الأمن العام**: وتختص بالتحقيق في جرائم الاعتداء على النفس والمال .

ب. **أجهزة التحقيق في الجرائم المخلة بأمن الدولة** :

و تنقسم إلى :

[1] محمد مصطفى موسى،المرجع السابق.ص286.

1. أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الداخل وتتولاها أجهزة متخصصة مثل مباحث أمن الدولة في مصر، فرنسا والكويت[1].

2 . أجهزة تختص بالتحقيق في الجرائم المضرة بأمن الدولة من جهة الخارج وتتولاها أجهزة متخصصة مثل المخابرات العامة في مصر.

ج. **جهاز التحقيق في الجرائم الالكترونية**: وهذا النوع من الأجهزة لم ينشأ بعد في كل الدول العربية وإن كانت بعض الدول قد أنشأته منذ أن استخدمت الحاسب الآلي وشبكات المعلومات[2]، ويرجع السبب الرئيسي لإنشاء جهاز متخصص للتحقيق الجنائي في الجرائم الإلكترونية، إلى تحقيق الضبط الاجتماعي الإلكتروني حماية للمجتمع من الجرائم الإلكترونية وذلك للحد منها وضبطها بعد وقوعها، وذلك بالعمل على الحصول على الدليل الإلكتروني من أجل إثبات الجريمة[3].

ويضاف إلى هذا السبب زيادة تفاعل المجرمين مع تقنية المعلومات، فقد وضح أن تقنية المعلومات ستزيد التفاعل بين الإرهابيين ومهربي المخدرات والأسلحة وجماعات الجريمة المنظمة، فمن خلال عالم مرتبط شبكيا سيكون هنالك مدخل للمعلومات والتقنية والتمويل وللخداع المعقد وتقنيات الأفكار الهدامة، وإذا تم استخدام ذلك سواء عن طريق

---

[1] محمد مصطفى موسى،المرجع السابق، ص 286

[2] نفس المرجع، ص 286.

[3] نفس المرجع، ص 286-287.

الدول أو فاعلين غير دوليين سيصبح ذلك بمثابة الخاصية الرئيسية لمعظم التهديدات من الداخل للدول[1].

أما الجزائر فلا زالت إلى الآن تفتقر لجهاز خاص بالتحقيق في الجريمة الإلكترونية إلا أنه انعقدت عدة ملتقيات حول مخاطر هذه الجريمة وناشدت بإنشاء جهاز خاص بالتحقيق في الجريمة الإلكترونية في الجزائر، منها الملتقى الوطني للجريمة الإلكترونية الذي نظم بدائرة ڤديل بمبادرة من نقابة المحامين لولاية وهران، حيث أختتم بمجموعة من التوصيات منها: أنه لابد من الإسراع في إنشاء الهيئة الوطنية المكلفة بتنشيط وتنسيق عمل السلطات المكلفة بمكافحة الجريمة الإلكترونية، ومدها بالمساعدة والاستشارة اللازمة، وحث الخبراء على ضرورة الإسراع في إنشاء هذه الهيئة الوطنية التي ينص على استحداثها القانون 09/04 الصادر في 5 أوت 2009 والخاص بالوقاية من الجرائم الإلكترونية ومكافحتها[2].

الفرع الثاني: صعوبات تتعلق بجهات التحقيق في الجريمة الالكترونية

إن بعض الصعوبات ترجع إلى شخصية المحقق مثل الهيبة من استخدام الكمبيوتر والانترنيت، وهناك ما يتعلق بالنواحي الفنية ونقص المهارة الفنية المطلوبة للتحقيق في هذا النوع من الجرائم، وعدم توفر المعرفة بأساليب ارتكاب الجريمة الإلكترونية وقلة الخبرة في

[1] محمد مصطفى موسى،المرجع السابق، ص 288.

[2] الملتقى الوطني حول الجريمة الالكترونية، جريدة الأمة العربية، وهران، 2013/02/01 . .

هذا المجال والمعرفة باللغة الانجليزية، خاصة وأن للعاملين في مجال الكمبيوتر مصطلحات علمية خاصة تشكل الطابع المميز لمحادثاتهم[1].

ولذلك بدأت الأجهزة الأمنية والقضائية باستقطاب المختصين في الكمبيوتر ليكونوا ضمن كوادرها كما جرى تدريب رجال الشرطة والقانون على استخدام الكمبيوتر، وقد تكون أمام أجهزة الشرطة والنيابة مجالات متنوعة ينبغي تغطيتها بالدعم والعناية، ومن هنا كانت المناداة إلى إنشاء وحدة خاصة بالجريمة الإلكترونية متفرغة لهذا النوع من الجرائم[2].

وقد يكون لحداثة هذا النوع من الجرائم وقلة المستكشف منها سبب وراء عدم اكتساب تلك الأجهزة خبرة التعامل معها، ناهيك عن الانتشار الواسع للكمبيوتر وتنوع برامجه وأنظمته مما يجعل حصر أساليب الجريمة المعلوماتية وصورها وأنماطها صعبا وبالتالي يتعذر معه تدريب المحققين[3].

---

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية ،المرجع السابق ،ص69.

[2] نفس المرجع، ص70.

[3] نفس المرجع، ص 70-71.

الفصل الثاني: إجراءات التحقيق في الجريمة الإلكترونية

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 سأتطرق لكيفية اتصال المحقق بالقضية وذلك في المبحث الأول، مما يستوجب تحديد آلية التحقيق في الجريمة الإلكترونية مع التطرق إلى إجرائي الاستجواب وسماع الشهود من الإجراءات التحقيق، أما المبحث الثاني فسأتعرض للإجراءات الأخرى التي تجرى على مسرح الجريمة وهي على الترتيب التفتيش وضبط الأدلة وأخيرا الانتقال للمعاينة وندب الخبراء.

المبحث الأول: اتصال المحقق بالجريمة الإلكترونية

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 يرهق المحققين الذين يصعب عليهم جمع الأدلة من خلال البيئة الإلكترونية ذات الطبيعة المعقدة والغامضة.

مما يستوجب على القائمين بالتحقيق الإلمام بكل الجوانب التقنية والتكنولوجية وضرورة الاستعانة بالخبرة التي تعد ضرورية في الكشف عن هذه الجرائم.

المطلب الأول: آلية التحقيق في الجريمة الإلكترونية

قد يصل إلى علم المحققين وقوع الجرائم من جراء الدوريات التي تقوم بها الضبطية القضائية و إلا فإنها تصل إلى علمهم إما بتلقي البلاغات من طرف عامة الناس أو الشكاوى من الأطراف المضرورة ، ويثار تساؤل حول ما إذا كانت هناك جهات مختصة لتلقي البلاغات والشكاوى بشأن الجريمة الإلكترونية، أم أنها تقدم أمام الجهات المختصة بتلقي البلاغات والشكاوى في الجرائم العادية؟

الفرع الأول: تلقي البلاغات والشكاوى حول الجريمة الإلكترونية

تظل الجريمة مستمرة ما لم يتم التبليغ عنها إلى الجهات المختصة بالتحقيق وبمجرد وصول نبأ وقوعها إلى تلك الجهات، فإنها تتخذ عدة إجراءات للتأكد من وقوعها وكشف مرتكبيها،و معرفة المحققين لوقوع جريمة ما يتم وفق طريقتين.

أولا/ البلاغات في الجريمة الإلكترونية

والبلاغ هو إخبار السلطات المختصة عن وقوع جريمة، أو أنها على وشك الوقوع ، أو أن هناك اتفاقا جنائيا أو أدلة أو قرائن، أو عزما على ارتكابها أو وجود شك أو خوفا من أنها ارتكبت[1].

أ. **كيفية التبليغ في الجريمة الالكترونية**: قد يكون البلاغ واجب في جميع الجرائم كما في قانون الإجراءات الجناية المصري وقد يكون اختياري في بعض الجرائم وواجب في جرائم أخرى كما هو منصوص عليه في القانون الجزائري في المادتين "32 من ق.ع و 91 من ق ا ج " ويتم التبليغ بمختلف الوسائل التي توصل المعلومات إلى الجهات المختصة بالتحقيق فقد يكون التبليغ كتابيا، أو شفويا ومن أي شخص سواء كان متضررا أو غير متضرر وهذا ما

[1] نبيله هبة هروال، المرجع السابق،ص177.

يطلق عليه مصطلح البلاغ المادي وقد يقدم بواسطة البريد أو التلفون أو الصحف وهذا ما يصطلح عليه البلاغ المعنوي، وقد يتم عن طريق الانترنيت وهذا ما يسمى بالبلاغ الرقمي[1].

كما يتم الإبلاغ عن الجريمة الإلكترونية عن طريق الانترنيت أو ما يسمى بالبلاغ الرقمي، وذلك إما عن طريق إرسال رسالة الكترونية إلى عنوان البريد الالكتروني للجهات المختصة بالتحقيق كإبلاغها عن وجود صفحات أو مواقع غير مشروعة بإرسال رسالة الكترونية مثلا، تتضمن التبليغ عن وجود موقع منشور فيه صور الاستغلال الجنسي للأطفال[2].

والمعلومات التي يجب معرفتها من المبلغ والتي ينبغي أن يدونها المحقق عند تلقي البلاغ يمكن الحصول عليها من خلال طرح أسئلة عن: تاريخ ووقت تلقي البلاغ، المعلومات الخاصة بالمبلغ، طبيعة ونوع الجريمة الإلكترونية، محل البلاغ، إلى غيرها من الأسئلة المتعلقة بالجريمة.

ب. **الجهة المختصة بتلقي البلاغات في الجريمة الإلكترونية**: الجهة المختصة بتلقي البلاغات في فرنسا في مثل هذه الجرائم هي البريد الإلكتروني للدرك الوطني الفرنسي[3] باعتبارها الجهة المختصة بالتحقيق والتحري عن الجرائم الجنسية المتعلقة بالأطفال، والجهة المختصة بتلقي بلاغات في جمهورية مصر العربية موقع شرطة إدارة مكافحة جرائم

---

[1] نفس المرجع ، ص178-180.

[2] نبيله هبة هروال، المرجع السابق ، ص182.

[3] judiciare@ gendarmeriedefense.gouv.fr. .

الحاسبات وشبكات المعلومات[1]، ويوجد موقع خصص للتضامن مع حملة الحكومة الفرنسية في مكافحتها للإجرام عبر شبكة الانترنيت، وهناك موقع أخر يختص بتلقي ومتابعة البلاغات التي تقدم إليه لدى الجهات المختصة عبر الانترنيت حول الجرائم التي ترتكب عبرها[2].

وهناك موقع أخر[3] يختص بتلقي ومتابعة البلاغات التي تقدم إليه لدى الجهات المختصة عبر الانترنيت حول الجرائم التي ترتكب عبرها [4].

ثانيا/ الشكوى في الجريمة الالكترونية

قد يترتب على الجريمة ضرر خاص قد يصيب احد الأفراد ماديا أو معنويا فينشأ له حق في تحريك الدعوى العمومية بتقديم شكوى أمام الجهة المختصة بالتحقيق حيث نص المشرع الجزائري في المادة72 من ق ا ج [5]على " يجوز لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص" وقد عرفت الشكوى بأنها البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشأن جرائم معينة، حظر المشرع تحريكها بصددها قبل تقديمه[6]، ولا يوجب القانون للشكوى شكلا معينا وإنما يقتصر فيها المعني بالأمر على ذكر

---

[1] http.//www.ccd.gov.eg.

[2] http://www.pointdecontact.net

[3] http://www.infowar.com

[4] خالد عياد الحلبي، ص182-183.

[5] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، ط2، 2009، ص28.

[6] نبيلة هبة هروال، المرجع السابق، ص189.

اسمه وسنه عنوانه وموجز الوقائع، والمواد القانونية التي تعاقب الفعل المرتكب، وإعطاء كافة المعلومات الخاصة بمرتكب الجريمة إذا كان معلوما[1].

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 المتصاعدة والموقع المخصص لتلقي الشكاوى من الضحايا تحت عنوان: http://www.ifccfbi.gov[2].

الفرع الثاني: الوسائل المساعدة التي يستخدمها المحقق في الجريمة الإلكترونية

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.

أولا/الوسائل المادية

[1] محمد حزيط، المرجع السابق، ص 30.

[2] نبيلة هبة هروال، المرجع السابق، ص 193.

أ.**عناوين الانترنيت** "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[1].

في حالة وجود أي مشكلة فان أول ما يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني، وتوجد أكثر من طريقة لمعرفة عنوان "IP" الخاص بجهاز الحاسوب منها في حالة العمل على نظام التشغيل Windows بكتابة Winipcfg في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان "IP "[2] .

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

[1] خالد ممدوح ابراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، المرجع السابق، ص303.

[2] نفس المرجع، ص304.

للدخلاء رؤية الداخل[1] ويعمل البروكسي كوسيط بين الشبكة ومستخدمها، حيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة وضمان الأمن وتوفير خدمات الذاكرة الجاهزة Cache Memory، حيث يتلقى مزود البروكسي عبر الانترنيت طلبا من المستخدم بحيث يبحث عن الصفحة المطلوبة ضمن الذاكرة المخفية Cache Memory المحلية فيتحقق البروكسي من وجودها[2] وإذا لم تكن موجودة، فإنه يعمل كمزود زبون ويرسل الطلب إلى العالمية حيث يستخدم أحد عناوين "IP" كما يمكن للذاكرة الخفية Cache Memory الاحتفاظ بالعمليات التي تمت عليها مما يجعل دورها قويا في الإثبات.

ج. برامج التتبع: هذه البرامج يمكنها أن 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 وهذا البرنامج يتكون من شاشة رئيسة تقدم للمستخدم بيانا شاملا لعمليات اختراق، وتحمل إسم الحدث وتاريخ الحدوث، عنوانه"IP" الذي تم من خلاله، والشركة المزودة لخدمة الانترنيت المستضيفة للمخترق[3]، وفور حدوث أي محاولة للاختراق تظهر أمام المستخدم شاشة صغيرة مصحوبة بتحذير صوتي يظهر على الشاشة عنوانه "IP" الخاص به.

---

[1] بلال بن جامع ، المشكلات الأخلاقية و القانونية المثارة حول شبكة الانترنيت ، ماجستير في علم المكتبات تخصص إعلام علمي و تقني، جامعة منتوري، قسنطينة، 2006، ص 163.

[2] خالد عياد الحلبي،المرجع السابق،ص 206..

[3] نفس المرجع، ص207-208.

د. نظام كشف الاختراق: يرمز له ب "IDS" وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجري حدوثها على أجهزة الحاسوب أو الانترنيت مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب، ويتم من خلال تحليل رزم البيانات أثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الأحداث فور وقوعها في الشبكة، وفي حال اكتشف النظام وجود إحدى هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة[1].

ه. نظام جرة العسل: هو 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 بهدف إغرائه بمهاجمته ليتم منعه من الاعتداء على أي جهاز آخر في الشبكة، في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء، بالتالي تحليلها واتخاذ إجرائي وقائي[2].

و. أدوات الضبط: إن جهات التحقيق وجمع الاستدلالات تحتاج إلى ضبط ماديات الجريمة وإثبات وقوعها والمحافظة على الأدلة حتى يتم نسبتها إلى الجاني، لتقديمها للنيابة العامة لكسب اعترافه ولذا يوجد أدوات تقوم بضبط ماديات الجريمة كغالبية برامج الحماية وأدوات المراجعة وأدوات المراقبة المستخدمين والتقارير التي تنتجها نظم أمن البيانات كما يمكن

[1] خالد عياد الحلبي،المرجع السابق ، ص 208-209

[2] نفس المرجع ، ص209

استخدام اغلب الأدوات المستخدمة في الجريمة كأداة ضبط مثل أدوات جمع المعلومات عن الزائرين[1].

ي. أدوات فحص ومراقبة الشبكات

و تشمل ما يلي :

1. أداة ARP وظيفتها تحديد مكان الحاسوب الفيزيائي على الشبكة وهو يحتفظ بجميع أرقام كروت الشبكة mac وله عدة من المداخل المستعملة معه.

2. برنامج 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[2].

3. أداة 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

[1] نفس المرجع ،ص210

[2] خالد عياد الحلبي،المرجع السابق ، ص211

ضمن"IP" لكي تستقبل من كل موجة رسالة، وبذلك يكون هو العدد الحقيقي للوثبات، ويتم بذلك تحديد المسار الذي تسلكه الرزمة بشكل دقيق[1].

4. أداة 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 وعرض كامل جدول التوجيه[2].

ثانيا/الوسائل الإجرائية

وتتمثل في:

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[3].

2. **الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته**: على المحقق الاطلاع على النظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، كما يجب عليه

[1] نفس المرجع، ص211

[2] خالد عياد الحلبي،المرجع السابق ،ص 212.

[3] نفس المرجع، ص212.213.

معرفة نوعية برامج الحماية وأسلوب عملها، من التقارير التي تنتجها نظم أمن البيانات وتقارير الجدران النارية[1].

3. **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، ثم أكثر الاحتمالات وصولا ثم الاحتمال الأقوى مع إعطاء الأسباب[2].

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 وكل من له صلة بها[3].

المطلب الثاني: الاستجواب وسماع الشهود في الجريمة الإلكترونية

يستدعى 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.

الفرع الأول: الاستجواب في الجريمة الإلكترونية

[1] نفس المرجع ، ص214،213.

[2] خالد عياد الحلبي، المرجع السابق، ص214،213.

[3] نفس المرجع، ص 215.

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 المختلفة قبله ومناقشته مناقشة تفصيلية كما تفيدنا إن كان منكرا للتهمة أو يعترف بها إذا شاء الاعتراف[1] ، وينقسم الاستجواب إلى[2]:

أولا/ الاستجواب عند الحضور الأول في الجريمة الالكترونية

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[3].

ثانيا /الاستجواب في الموضوع في الجريمة الإلكترونية

[1] فرج علواني هليل، المرجع السابق، ص 645.

[2] محمد حزيط، قاضي التحقيق، المرجع السابق، ص 59.

[3] عبد الرحمان خليفي، محاضرات في قانون إجراءات جزائية، دار الهدى ،الجزائر ، 2012، ص168.

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].

ثالثا/الاستجواب الإجمالي في الجريمة الإلكترونية

يهدف إلى تلخيص الوقائع وإبراز الأدلة التي سبق جمعها خلال كافة مراحل التحقيق والإشارة إلى الاستعلامات التي وردت في شأن وحياة وسلوك وشخصية والسوابق العدلية للمتهم، ويختم بطرح السؤال التالي: هذا هو استجوابك الأخير فهل لديك ما تدلي به للدفاع عن نفسك؟ ويحتوي الملف الجنائي على الوثائق التالية: شهادة الميلاد المتهم، صحيفة السوابق العدلية، تقرير البحث الاجتماعي ويقصد بهذا الأخير ندب خبير لإجراء بحث اجتماعي عن حياة المتهم، وسلوكه وأخلاقه في المحيط الذي كان يعيش فيه وكذا محيط مهنته، وكل ما يتعلق بحياته الاجتماعية، وكذا شهادة جيرانه سواء قام به المحقق بنفسه أو عن طريق إنابة قضائية لأحد ضباط الشرطة القضائية[2] .

الفرع الثاني: سماع الشهود في الجريمة الإلكترونية

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

[1] محمد حزيط ، قاضي التحقيق، المرجع السابق،ص67.

[2] محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، ط3 ، 2008 ، ص108،109.

الجرائم والقبض عن مرتكبيها، وتخلف الشاهد عن الحضور للإدلاء بشهادته يعرضه للمسائلة الجنائية، وعليه سأتطرق أولا لتعريف الشهادة ثم الشهادة في الجريمة الإلكترونية.

أولا/تعريف الشهادة وأنواعها

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

أ .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[1]، 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"

[1] عبد الله بن سعيد أبو داسر، إثبات الدعوى الجنائية، أطروحة دكتوراه في القانون، جامعة الإمام محمد بن سعود الإسلامية السعودية، 1443ه، ص 45.

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[1] ".

وعرفها اليأس أبو عبيد " الشهادة قانونا تقوم على إخبار شفوي يدلي به الشاهد في مجلس القضاء بعد يمين يؤديها على الوجه الصحيح[2]".

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[3]".

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[4] .

و تخضع 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

---

[1] عماد محمد احمد ربيع ،حجية الشهادة في الإثبات الجزائي، مكتبة دار الثقافة مركز غنيم، الأردن ، ط1 ، 1999، ص 90،92.

[2] إلياس أبو عبيد، أصول المحاكمات الجزائية، منشورات الحلبي الحقوقية، لبنان، ج1، ط1، 2006، ص 560.

[3] علي فضيل البوعينين،ضمانات المتهم في مرحلة المحاكمة،دار النهضة العربية، القاهرة، 2006، ص 351 -352.

[4] عبد الله بن سعيد أبو داسر، المرجع السابق، ص 45.

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[1].

وتؤدى الشهادات بانفراد وأخيرا تدون الشهادات بمحاضر خصصت لذلك دون حشي أو تصحيح أو تخريج، يصادق على المحضر كل من المحقق والكاتب والشاهد[2].

ب.أنواع الشهادة:

تنقسم شهادة الشهود إلى ثلاث أنواع:

1. **الشهادة المباشرة**: هي أن يشهد الشاهد بما شاهده أو وقع تحت سمعه[3].

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[4].

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

---

[1] مروك نصر الدين، المرجع السابق، ص383-384.

[2] نفس المرجع، ص385.

[3] محمد علي سكيكر، آلية المسؤولية الجنائية، دار الفكر الجامعي، الإسكندرية، ط1، 2008 ، ص 137 .

[4] العربي شحط عبد القادر، نبيل صقر، الإثبات في المواد الجزائية، دار الهدى، الجزائر، 2006، ص101.

بواقعة معينة لكنها ليست نقلا عن شخص معين بالذات شاهد الأمر بنفسه كأن يقول: الشاهد سمعت كذا، وإن الناس يقولون كذا وكذا عن هذه الواقعة أو الأمر[1].

ثانيا/ الشهادة الإلكترونية

وتفترض أن تكون في التحقيق النهائي أمام محكمة الموضوع، حيث يمكن الحصول على أقوال المتهم بشكل سمعي مرئي، وقد ظهر بعد ظهور فكرة الدوائر الاتصالية الإلكترونية المتكاملة من مغلقة ومفتوحة، ولقد كانت بدايات الأخذ بهذا النظام-الشهادة الالكترونية الفورية- في القضاء الأمريكي عندما واجه القضاء مشكلة إدلاء الشهادة من قبل أشخاص وضعوا في برنامج حماية الشهود، فقد قررت المحكمة الفيدرالية العليا الأمريكية قبولها لنظام الشهادة طالما كانت هناك أسباب في القانون تدعو إليه[2].

ويختلف الشاهد في الجريمة الإلكترونية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية وقد عرف الشاهد الالكتروني بأنه: "الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي الذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات ويمكن القول أن الشاهد الإلكتروني هو كل من:

[1] نفس المرجع، ص 101-.102

[2] خالد ممدوح إبراهيم، المرجع السابق، ص 262.

أ.**مشغلو الحاسب الآلي**: هو ذلك الشخص المسؤول عن تشغيل الجهاز والمعدات المتصلة به حيث تكون لديه الخبرة في مجال الحاسب الآلي عن طريق استخدام البيانات واستخراجها كما تكون لديه الخبرة الواسعة في الكتابة السريعة عن طريق لوحة المفاتيح.

ب.**خبراء البرمجة**: هم الأشخاص المتخصصون في كتابة أوامر البرامج وينقسمون إلى فئتين: الأولى هم مخططوا برامج التطبيقات والثانية هم مخططو برامج النظم[1].

ج.**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.

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

هـــــ. **مديرو النظم**: هم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية[2].

المبحث الثاني: الانتقال إلى مسرح الجريمة الإلكترونية:

[1] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة ط1 ، 2009.

المرجع السابق، ص612 -613.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي، المرجع السابق، ص264.

عند تلقي المحقق البلاغ أو الشكوى بوقوع جريمة ما ، فإنه ينتقل مباشرة إلى مكان وقوعها مع إخطار وكيل الجمهورية، وذلك بهدف التنقيب عن الأدلة وحمايتها، إلا انه تجدر الإشارة إلى أن مسرح الجريمة الإلكترونية بالإضافة إلى المسرح المادي يوجد مسرح إلكتروني متمثل في البيئة الرقمية التي يجد فيها المحقق صعوبة استخلاص الدليل منها، مما يدفعه إلى الاستعانة بالخبراء الفنيين في هذا المجال، ومن بين الإجراءات التي يقوم بها المحقق على مصرح الجريمة التفتيش وضبط الأدلة الذي سأتطرق لهما في المطلب الأول بالإضافة إلى المعاينة وندب الخبراء في المطلب الثاني.

المطلب الأول: التفتيش و ضبط الأدلة في الجريمة الإلكترونية

التفتيش وضبط الأدلة في الجريمة الإلكترونية يحتاجان إلى تقنيات خاصة تختلف عن حالات الجرائم التقليدية وذلك راجع لطبيعة الوسيلة المستخدمة لارتكاب الجريمة، كذلك يرجع الاختلاف إلى أن مسرح الجريمة في الجريمة الإلكترونية معلومات وبيانات غير ملموسة مما يصعب هاذين الإجراء ويستلزم وسائل خاصة مقارنة بالظروف العادية- الجرائم التقليدية - فهل يكفي التعريف التقليدي لهذا الإجراء للإلمام بكل عناصرهما الواقعة على نظم الحاسب الآلي والانترنيت؟ وما مدى قابلية التقنية العالية لهذا الإجراء؟

الفرع الأول: التفتيش في الجريمة الإلكترونية:

التفتيش في الجريمة الإلكترونية يقع على نظم الحاسوب والانترنيت، وهو إجراء يهدف إلى البحث عن الأدلة المادية والمعنوية التي تثبت ارتكاب الجريمة، ونسبتها إلى مرتكبها ويجدر التطرق إلى تعريف التفتيش عامة ثم التفتيش في الجريمة الإلكترونية.

أولا/ تعريف التفتيش

يهدف التفتيش إلى جمع الأدلة من مكان وقوع الجريمة.

أ. **تعريف التفتيش لغة** : من مصدر فتش أي بحث وسأل ، فتش الرجل عن الشيء أي تصفحه[1].

ب. **تعريف التفتيش قانونا**: هو البحث المادي في مكان ما بهدف البحث عن الأشياء المتعلقة بالجريمة الجاري جمع الاستدلالات أو حصول التحقيق بشأنها[2].

ج.**تعريف التفتيش فقها**: تعددت التعريفات الفقهية في هذا الشأن، فعرفه الفقه الفرنسي بأنه "بحث بوليسي أو قضائي عن عناصر الدليل عن جريمة ما،ويمكن وفقا لقواعد قانونية خاصة أن ينفذ في المسكن الخاص بأي شخص أو في أي مكان آخر حيث يمكن أن توجد أشياء يكون اكتشافها مفيدا في إظهار الحقيقة "[3].

[1] على بن هادية، لحسن بليش الجلالي بن الحاج يحي، المرجع السابق، ص 756.

[2] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، المرجع السابق، ص91.

[3] بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، ط1، 2011، ص 58.

وعرف التفتيش جانب من الفقه بأنه إجراء من إجراءات التحقيق تقوم به سلطة حددها القانون، يتم بالبحث في مستودع السر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة ويتمثل مستودع السر في شخص المتهم أو في المكان الذي يعمل به ويقيم فيه[1].

ويمكن تعريف التفتيش بأنه ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي الغرض منه البحث عن أدلة الإثبات المرتكبة، وكل ما يفيد للوصول إلى الحقيقة في متابعة أي شخص يشتبه في أنه مرتكب الجريمة[2].

ثانيا/ القواعد العامة لتفتيش نظم الحاسوب و الانترنيت

الغرض من التفتيش هو البحث عن الأدلة المتعلقة بالجريمة، التي تساعد في كشفها والتفتيش في الجريمة الإلكترونية ينقسم إلى تفتيش ماديات الجريمة الملموسة، والتفتيش في نظم الحاسوب الغير الملموسة والتي تخضع لقواعد عامة وهي:

أ.القواعد الشكلية لتفتيش نظم الحاسوب و الانترنيت:

الأصل أن التفتيش لا تقوم به إلا سلطة التحقيق، فيخضع التفتيش في هذه الحالة للخصائص العامة لكافة إجراءات التحقيق، المتمثلة في وجوب التدوين بمعرفة كاتب والسرية عن الجمهور وحضور الخصوم ووكلائهم كلما أمكن ذلك [1].

---

[1] علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنيت، عالم الكتب الحديث، الأردن، ط1، 2004 ص10-11.

[2] بلعليات إبراهيم ، أركان الجريمة و طرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، ط1، 2006، ص 214.

وهناك شروط للتفتيش تختص بها الجريمة الإلكترونية دون غيرها من بينها توافر الخبرة الفنية لدى القائم بالتفتيش من خلال أن يتلقى المحقق في الجريمة الإلكترونية تدريبات فنية خاصة، تعرفه كيفية التعامل مع التقنية الحديثة وكيفية ضبط الأدلة والحفاظ عليها في هذا المجال، كذلك يجب أن يتم التفتيش بصورة صحيحة من الناحيتين الموضوعية والشكلية[2].

كذلك من القواعد الشكلية التي تحكم التفتيش عدم التجاوز في التفتيش، وذلك بمنع التفتيش عندما لا توجد تحريات جدية تنبئ عن وجود دلائل قوية عن معلومات تفيد في كشف الحقيقة مع وجوب أن يكون التفتيش في حدود الإذن المكتوب، المؤرخ والموقع من الجهة التي أصدرته وإلا كان التفتيش باطلا [3].

ويجب أن يكون إذن التفتيش محدد المدة التي تحتسب من يوم الإذن إلى الجهة المأذون لها إجراء التفتيش[4]، وأضافت الجمعية الدولية لقانون العقوبات ضرورة وجود خبير معالجة بيانات يساعد في صياغة مسودة إذن التفتيش[5].

وأخيرا بما أن التفتيش عن الملفات الموجودة في جهاز الكمبيوتر من الأمور المعقدة لأنها تحوي عمليات إلكترونية غامضة يمكن تخزينها حتى على رأس إبرة وتحريكها حول

---

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، جامعة نايف العربية للعلوم الأمنية، الرياض،2007 ، ص 19.

[2] بكري يوسف بكري، المرجع السابق، ص 105-106.

[3] نفس المرجع، ص108.

[4] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص223.

[5] بكري يوسف بكري، نفس المرجع، ص 108.

العالم في أي وقت، إذا فتفتيش وضبط نظم الحاسب الآلي يعتبر فن بقدر ما هو علم مما ينبغي على رجال الضبط القضائي ورجال النيابة العامة إتباع الخطوات التالية:

- تجميع فريق عمل يتكون من رجل الضبط القضائي المكلف بالمهمة، وكيل الجمهورية، خبير فني قبل القيام بالتفتيش قدر الإمكان.

- التعرف قدر الإمكان على نظم الكمبيوتر قبل إجراء التفتيش .

- وضع خطة لتنفيذ التفتيش.

- العناية بمسودة إذن التفتيش- اشتمالها على وصف محل التفتيش- وشرح إستراتيجية التفتيش الممكنة[1].

ب.القواعد الموضوعية لتفتيش نظم الحاسوب والانترنت :

يجب مراعاة القواعد التالية حين قيام المحقق بعملية التفتيش :

1. **وجود سبب للتفتيش**: الإذن بالتفتيش لا يصح إصداره إلا لضبط ماديات الجريمة الواقعة بالفعل واتهام شخص أو عدة أشخاص بارتكابها، والمساهمة فيها مع توافر أمارات قوية على وجود أشياء تفيد فيكشف الحقيقة لدى المشتكى عليه أو غيره[2].

[1] خالد ممدوح إبراهيم، المرجع السابق، ص225-226.

[2] علي حسن محمد الطوالبة، المرجع السابق، ص 62.

ويمكن حصر الشروط الموضوعية للتفتيش :

- أن يكون التفتيش بصدد جريمة إلكترونية واقعة بالفعل سواء كانت جناية أو جنحة.

- لا بد من اتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة الإلكترونية أو المشاركة في ارتكابها.

- لا بد من توافر دلالات وأمارات قوية أو قرائن على وجود أجهزة، أدلة معلوماتية تفيد في كشف الحقيقة لدى المتهم[1].

وتفتيش نظم الحاسب الآلي وفق الأسلوب الأمريكي يلخص فيما يلي:

- اقتحام قوة الشرطة للمكان بصورة سريعة ومن كافة منافذه في وقت واحد.

- إبعاد سائر المشتبه فيهم عن كافة أنظمة ومعدات الكمبيوتر الموجودة في المكان على الفور كي لا يتمكنوا من تدمير أي دليل، وتوضع أجهزة الكمبيوتر الموجودة بالمكان في عهدة فريق يضم اثنين من العملاء أولهما مكتشف تم تدريبه تدريبا متقدما على نظم المعلومات وهو الذي يقوم بعملية الضبط ويتولى نزع مقبس الكهرباء الخاص بسائر الأجهزة كما يقوم بالبحث عن الأقراص المرنة والصلبة والملفات وحاويات الاسطوانات، والثاني مسجل يقوم بتصوير كافة الأجهزة والمعدات بالكيفية التي تم ضبطها عليه كما يقوم بتصوير

[1] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 209-210.

كافة الغرف الأخرى الموجودة بالمنزل حتى لا يدعي المجرم أن الشركة قد سرقت منزله أثناء التفتيش[1].

2- **تحديد محل التفتيش**: قد يقع التفتيش على شخص وقد يقع على مكان، والمقصود بالشخص قد يكون من مستغلي أو مستخدمي الكمبيوتر ومن خبراء البرامج، وقد يكون من المحللين ومن مهندسي الصيانة والاتصالات أو من مديري النظم المعلوماتية، أو من أي أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية أو أجهزة حاسب آلي محمولة أو تليفونات متصلة بجهاز المودم أو مستندات[2].

والسلطة المختصة بتفتيش نظم الحاسب الآلي وفقا للقواعد الإجرائية المنصوص عليها في هذا الخصوص، بيد انه لا بد من توافر صفة المحقق بمن يقوم بالتفتيش مع الإذن بالتفتيش وإن يكون أصلا مختصا بالتحقيق في الجريمة[3]، واستثناءا فان اغلب النظم الإجرائية تجيز تفتيش الأشخاص بناءا على حالة التلبس دون الحصول على إذن من سلطات التحقيق وفي غير حالات التلبس فانه يستلزم استصدار أمر بالتفتيش من الجهة المختصة، وفقا لأحكام القانون تحت طائلة البطلان[4].

الفرع الثاني: ضبط الأدلة في الجريمة الإلكترونية

---

[1] عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجزائية، في جرائم الكمبيوتر والانترنيت، المرجع السابق، ص289-291.

[2] نفس المرجع، ص214-215.

[3] نفس المرجع ، ص215.

[4] بكري يوسف بكري ، المرجع السابق، ص117-121.

ضبط الأدلة مرحلة مهمة من مراحل التحقيق في الجرائم الإلكترونية وتعتبر من أصعب الإجراءات التي يقوم بها المحقق، لأنه توجد في الجريمة الإلكترونية أدلة رقمية يصعب التعامل معها.

أولا/ مفهوم ضبط الأدلة في الجريمة الإلكترونية

يمكن تعريف الضبط بأنه "وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها سواء كان هذا الشيء عقارا أو منقولا، وقد يرد الضبط على الأشخاص وهو ما يصطلح على تسميته بالقبض[1] ".

والضبط، بحسب الأصل لا يرد إلا على أشياء مادية فلا صعوبة بالتالي بضبط الأدلة في الجريمة الواقعة على المكونات المادية للكمبيوتر، كرفع البصمات مثلا عنها وكذلك لا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخه غير المشروع أو إتلافه بوسائل تقليدية كالكسر،الحرق. لكن تكمن الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج مثل الفيروس، وفي ضبط بيانات الكمبيوتر DATA لعدم وجود أي دليل مرئي في هذه الحالات ولسهولة تدمير الدليل في ثوان معدودة ولعدم معرفة كلمات السر أو شفرات المرور أو ترميز البيانات[2].

ثانيا/إجراءات ضبط الأدلة في الجريمة الالكترونية

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، المرجع السابق، ص 207-208.
[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية ، المرجع السابق، ص274.

تضبط الأدلة في الجريمة الإلكترونية وفق إجراءات خاصة فيما يخص ضبط المكونات المعنوية للجريمة.

أ.**ضبط المكونات المادية في الجريمة الإلكترونية**: وهذا لا يثير أي إشكال فيخضع الضبط في هذه الحالة إلى قواعد الضبط في الجريمة الالكترونية، ذلك أن معظم التشريعات أجازت ذلك ومثاله نص المادة 487 من قانون الإجراءات الجنائية الكندي، والمادة 251 من قانون الإجراءات اليوناني، كذلك ما جاء في قانون إساءة استخدام الحاسوب في انكلترا الصادر سنة 1990[1]،أما المشرع الجزائري فقد تطرق للقواعد الخاصة بالضبط من خلال نص المادة 84 التي يفهم بعد استقراءها انه يجب جرد الوثائق أو الأشياء المضبوطة ووضعها في أحراز مختومة يجوز لقاضي التحقيق وضابط الشرطة القضائية المندوب عنه الاطلاع على الوثائق والمستندات المراد حجزها ووضعها في أحراز مختومة بعد تحرير محضر بذلك، ولا يجوز فتح هذه الاحراز أو الوثائق إلا بحضور المتهم مصحوبا بمحاميه، ويمكن إصدار نسخ للوثائق التي تبقى مضبوطة[2]، إذا تم تسليم نسخ يقوم الكاتب بالتأشير عليها بمطابقتها للأصل، أما إذا اشتمل الضبط على نقود أو سبائك أو أوراق تجارية أو أوراق ذات قيمة مالية ولم يكن من الضرورة لإظهار الحقيقة الاحتفاظ بها عينا فإنه يتم إيداعها بالخزينة[3] والمادة 47 من قانون الإجراءات الجزائية ومن بين الأدلة المتحصل عليها:

[1] علي حسن محمد الطوالبة، المرجع السابق، ص 140.

[2] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، المرجع السابق، ص 98.

[3] محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، المرجع السابق، ص98.

1. **الورق**: يعتبر الورق من الأدلة التي ينبغي الاهتمام بها في البحث وتفتيش مسرح الجريمة وينقسم الورق إلى أربعة أنواع:

- أوراق تحضيرية يتم إعدادها بخط اليد كمسودة أو تصوير للعملية التي يتم برمجتها.

- أوراق تالفة تتم طباعتها للتأكد، ومن ثم إلقاءها في سلة القمامة.

- أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة[1].

2. **جهاز الكمبيوتر و ملحقاته**:

- **وحدات الإدخال** Input Unit : وتستعمل هذه الوحدات لإدخال المعلومات أو المعطيات أو البرامج المراد معالجتها من الوسط الموجودة عليه إلى ذاكرة الحاسوب، وتكون وسائل الإدخال على أنواع: وسائل تسمح بالاتصال المباشر ON-LINE بين الوسط الخارجي وبين وحدة المعالجة المركزية، وتمثل لوحة المفاتيح[2]، وتشمل وحدات الإدخال كذلك مشغل الأقراص الممغنطة، والفأرة التي عن طريقها يحرك السهم الذي يظهر على شاشة الحاسب ثم يضغط على الأمر المراد تنفيذه، ويتولى الجهاز تنفيذ ذلك الأمر[3]، كذلك تشمل الماسح الضوئي SCANNER: الذي يتم عن طريقه إدخال صورة أي مستند أو صورة لخريطة أو لإنسان أو حيوان أو أي ورقة إلى جهاز الحاسب الآلي، مشغل الأقراص CD ROOM

[1] محمد الأمين البشيري، التحقيق في الجرائم المستحدثة، جامعة نايف العربية للعلوم الأمنية، الرياض، ط1 ،2004 ص117.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة، الأردن، ط1، 2008، ص 25.

[3] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية، المرجع السابق، ص397.

DRIVER ووظيفته تشغيل الأقراص المدمجة أو قرص الليزر الذي يحوي البيانات والمعلومات التي يريدها المجرم الإلكتروني أو يرغب في تزويرها أو اختراقها لغرض إجرامي، أيا كانت صورة السلوك الإجرامي المقترف[1].

- **وحدات المعالجة المركزية** Central Processing Unit: وتعتبر بمثابة العقل المفكر و المسيطر على عمل باقي الوحدات المكونة لجهاز الحاسوب وتقوم بمعالجة البيانات حسب التعليمات الواردة في البرنامج، حيث يتم فيها جميع العمليات الحسابية أو المنطقية وتتكون بدورها من وحدة التحكم و السيطرة Control Unit ووحدة الحساب والمنطق Arithmetic Logic Unit[2].

- **وحدة الذاكرة** Memory Unit : وهي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز أو تخزين النتائج الآتية من وحدة المعالجة المركزية و تنقسم إلى[3]:

- **وحدة الذاكرة الرئيسية** Main Memory : وهي الوحدة التي تقوم بحفظ البيانات والنتائج بشكل مؤقت[4]وتشمل ذاكرة القراءة فقط ROM والذاكرة العشوائية أو ذاكرة الوصول العشوائي RAM[5].

---

[1] نفس المرجع، ص 397.

[2] نهلا عبد القادر المومني، المرجع السابق، ص 26.

[3] نفس المرجع، ص26.

[4] عبد الفتاح بيومي حجازي، المرجع السابق، ص 398.

[5] نهلا عبد القادر المومني، المرجع السابق، ص 27.

- **وحدة الذاكرة المساعدة** Auxiliary Memory: و تستخدم لتخزين كميات هائلة من البيانات وبصورة دائمة، حيث لا تفقد محتوياتها بانقطاع التيار الكهربائي، ومن أهم وسائط التخزين المستخدمة: الأقراص المرنة الصلبة، الأشرطة الممغنطة والأقراص المضغوطة[1].

- **وحدات الإخراج** Output Unit : هي الوحدات التي يمكن من خلالها تحويل المعلومات غير المقروءة وغير المرئية إلى معلومات مقروءة، أو مرئية أو هما معا، فهي وسائل استخراج نتائج الاتصال بين الأفراد والحاسب الآلي، وتشمل الشاشات بأنواعها، الطابعات على مختلف أنواعها وكذلك وحدات رسم المنحنيات البيانية والوحدات الطرفية[2].

ب.ضبط المكونات المعنوية: انقسمت التشريعات الإجرائية حول إمكانية ضبط الأشياء

المعنوية فظهر اتجاهين الأول يرى عدم إمكانية تصور إجراء الضبط على الكيان المعنوي كونه ينصب على بيانات الحاسوب التي تختلف عن الأشياء المادية المحسوسة القابلة للضبط.

ومن التشريعات التي أخذت بهذا الاتجاه: قانون الإجراءات الجنائية الألماني، حيث حصرت المادة 94 منه محل الضبط على الأشياء المادية المحسوسة أو الملموسة[3]، واتبعت اليابان نفس النهج، ويقترح إتباع هذا الاتجاه إضافة عبارة المواد المعالجة عن طريق

[1] علي جبار الحسناوي، المرجع السابق، ص24-25.

[2] محمد حماد مرهج الهيتي، جرائم الحاسوب، المرجع السابق، ص 42.

[3] علي حسن محمد الطوالبة، المرجع السابق، ص146.

الحاسوب أو بيانات الحاسوب إلى النص القانوني الذي ينص على التفتيش والضبط ليشمل التطور التكنولوجي لبيئة المعلومات [1].

أما الاتجاه الثاني فيرى بأنه لا مانع من ضبط البيانات الإلكترونية مستندين إلى أن الغاية من التفتيش هو ضبط الأدلة المادية المفيدة في كشف الحقيقة، وبالتالي يمتد هذا المفهوم ليشمل البيانات الإلكترونية بمختلف أشكالها ومن أتباع هذا الاتجاه القانون الكندي مثاله ما جاء في نص المادة 487 وكذلك الشأن بالنسبة لفرنسا وأمريكا[2]، أما المشرع الجزائري فكما سبق القول يأخذ بمبدأ جواز التفتيش والضبط لأنظمة الحاسوب[3].

ويمكن تعريف نظام الحاسوب بأنه تعليمات مكتوبة بلغة ما موجهة إلى جهاز تقني معقد يسمى بالنظام المعلوماتي بغرض الوصول إلى نتيجة معينة، أو هو مجموعة من التعليمات المتتابعة بصفة منطقية توجه إلى الكمبيوتر لأداء عمل أو أعمال معينة [4]، ويطلق على أنظمة الحاسوب اسم البرمجيات التي تعد بمثابة العمود الفقري وعصب عمل الحاسب الآلي حيث لا يمكن للفرد أن يقوم بأي عملية بدونها[5].

ومن بين المكونات المنطقية لجهاز الحاسوب التي يمكن ضبطها هي المعلومات والبيانات وبرمجيات الحاسوب: التي تشمل الوثائق، المستندات والمواد التي يطلق عليها

---

1 نفس المرجع، ص146.

2 نفس المرجع، ص147-148.

3 انظر المواد 47 و 84 من قانون الإجراءات الجزائية الجزائري.

4 احمد خليفة الملط، المرجع السابق، ص42.

5 بلال أمين زين الدين، المرجع السابق، ص23.

المواد المساندة، وهي مواد مكتوبة في صورة كتيبات أو منشورات تطبع حاليا على الوسائط الإلكترونية مثل الأقراص المرنة أو المدمجة وتنقسم إلى برمجيات النظم والبرمجيات التطبيقية[1].

المطلب الثاني: المعاينة و ندب الخبراء في الجريمة الإلكترونية

الانتقال لمكان الجريمة الإلكترونية يكن لعدة أغراض منها معاينة مسرح الجريمة وذلك لإثبات صلة الأشخاص، الأماكن والأشياء بالجريمة، إلا أن المعاينة وحدها لا تكفي لإثبات ذلك، الأمر الذي يستدعي الاستعانة بالخبرة الفنية أو التقنية في مجال الانترنت والعالم الافتراضي.

الفرع الأول: المعاينة في الجريمة الإلكترونية

قبل التطرق إلى إجراء المعاينة في الجريمة الإلكترونية ، يجب تحديد تعريف المعاينة لغة واصطلاحا وقانونا.

أولا/تعريف المعاينة في الجريمة الإلكترونية

[1] نهلا عبد القادر مومني، المرجع السابق، ص28-29.

أ.تعريف المعاينة لغة: المعاينة هي المشاهدة بالعين، عاين غيره رآه بعينه ، وجاء في الأمثال والعيان لا يحتاج إلى بيان، ويضرب لإظهار مزايا المشاهد للتصديق بالشيء دون برهان[1].

ب. تعريف المعاينة اصطلاحا: هي إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها كذلك جميع الأشياء الأخرى التي تفيد في كشف الحقيقة، واتخاذ ما يلزم من إجراءات كضبط بعض الأشياء[2].

فالهدف من المعاينة هو لغرضين اثنين: الأول جمع الأدلة الناتجة عن الجريمة " الآثار" والثاني إتاحة الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة لكي تكون لديه فكرة واضحة لا لبس فيها ولا غموض عن كيفية وقوع الجريمة[3].

ولقد أشارت قوانين الإجراءات الجنائية إلى إجراء المعاينة باعتباره إجراء من إجراءات التي تمتلكها السلطات التحقيقية بمختلف فئاتها وطوائفها[4]، وهذا ما ورد في نص المادة 79 من قانون الإجراءات الجزائية الجزائري " يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها ....."[5].

---

[1] علي بن هادية ، بلحسن البليش، الجيلاني بن الحاج، ص 642.

[2] محمد حماد مرهج الهيتي، المرجع السابق، ص255.

[3] نفس المرجع، ص 256.

[4] نفس المرجع ، ص257.

[5] الأمر 66-155 المؤرخ في 18 صفر 1386 الموافق 08 يونيو 1966 يتضمن قانون الإجراءات الجزائية المعدل والمتمم بالقانون رقم 06- 22 المؤرخ في 29 ذي القعدة عام 1386 الموافق ل 20 ديسمبر 2006، المتضمن قانون الإجراءات الجزائية .

ج. تعريف المعاينة قانونا:

المعاينة هي إثبات حالة الأماكن والأشياء والأشخاص وكل ما يعتبر في كشف الحقيقة فهي بهذا المعنى تستلزم الانتقال إلى محل الواقعة أو أي محل آخر توجد به آثار يرى المحقق أن لها صلة بالجريمة والأصل أن إجراء المعاينة متروك لتقدير المحقق لا يقوم بها إلا إذا كان هناك فائدة من ورائها، كما أن هناك حالات يوجب فيها القانون على النيابة الانتقال فورا إلى مسرح الجريمة وهي حالة إخطارها بجناية متلبس بها[1].

ثانيا/الانتقال و المعاينة في الجريمة الإلكترونية

يرى البعض أن أهمية المعاينة تتضاءل في الجريمة الإلكترونية وذلك لندرة تخلف الآثار المادية عند ارتكاب الجريمة الإلكترونية، كما أن طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار، فعند تلقي بلاغ عن وقوع إحدى الجرائم الإلكترونية وهذا بعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته[2].

ومسرح الجريمة الإلكترونية يختلف عن مسرح الجريمة التقليدية كالقتل والسرقة فالجريمة الإلكترونية قد تكون جريمة مستمرة كما في حالة الجرائم الاقتصادية – السرقة والاحتيال- وقد يكون مسرحها كالجرائم الأخرى كما في التزوير وإتلاف البرامج وتفجير المباني والمنشأت، ففي حالة الجريمة المستمرة ذات الأهداف الاقتصادية تكون المعاينة هدفها

[1] عبد الفتاح بيومي حجازي ، المرجع السابق، ص100.

[2] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، المرجع السابق، ص17.

المداهمة وضبط الأدلة على الطبيعة، وفي الحالة الثانية وبعد وقوع الجريمة فالأمر متوقف على اعترافات المتهمين متى تم القبض عليهم وكذلك شهادة الشهود والقرائن، وعند إجراء المعاينة بعد وقوع الجريمة في المجال الإلكتروني فيجب مراعاة الإجراءات التالية عند الانتقال إلى مسرح الجريمة[1]:

ضرورة وجود معلومات مسبقة عن مكان الجريمة، من حيث الأجهزة المطلوب معاينتها وشبكاتها مع وجود خريطة تبين الموقع المراد معاينته، تحديد الأجهزة المحتمل تورطها في الجريمة الإلكترونية حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة، سواء من الضبط أو التأمين أو حفظ الأوراق، كما يجب على القائمين بالمعاينة، تأمين الأجهزة والمعدات التي يتم الاستعانة بها خلال إجراء المعاينة، وبما أن الجريمة الإلكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختص في مجال التقنية الحديثة، وإخطاره مسبقا حتى يستعد من الناحية الفنية والعملية ويعد خطة مناسبة للمعاينة، وأكيد قبل كل شيء يجب مراعاة ما جاء في القوانين الجنائية حول المعاينة وذلك تحقيقا لمبدأ الشرعية[2].

الفرع الثاني: ندب الخبراء في الجريمة الإلكترونية

[1] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، المرجع السابق، ص17.

[2] عبد الفتاح بيومي حجازي ، الجوانب الإجرائية لأعمال التحقيق، دار النهضة العربية، القاهرة، ط1، 2009، ص586.

تعتبر الخبرة من أهم الإجراءات التي تتخذ للتنقيب عن الأدلة التي تساعد عن الكشف عن الجريمة الإلكترونية كون الجريمة الإلكترونية ترتكب بوسائل مستحدثة ومعقدة يصعب التعامل معها.

أولا/ تعريف الخبرة في الجريمة الإلكترونية

ولمعرفة الخبرة في الجريمة الإلكترونية يجب التطرق أولا لتعريف الخبرة لغة واصطلاحا.

أ. **تعريف الخبرة لغة**: الخبير لغة هو اسم من أسماء الله تعالى أي العالم بما كان وما سيكون.

ب. **تعريف الخبرة اصطلاحا**: الخبير في اصطلاح المحاكم هو من يعين للتدقيق في مختلف الأمور المتعلقة بشتى القضايا ويكون لرأيه فيها القول الفاصل[1].

والخبرة هي الوسيلة لتحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات، فهي في الحقيقة ليست دليلا مستقلا عن القولي أو الدليل المادي، إنما هي تقييم فني لهذا الدليل والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة، الشهادة والتفتيش.[2]

[1] على بن هادية، بن لحسن البليش الجلالي بن الحاج يحي، المرجع السابق، ص302.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص321.

وعليه يمكن تعريف الخبير انه كل شخص له إلمام بأي علم أو فن سواء كان اسمه مقيدا في جدول الخبراء على مستوى المحاكم أم لا [1].

كما عرف الخبير " بأنه كل شخص له دراية بمسالة من المسائل وقد يستدعي التحقيق فحص مسالة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها في نفسه فيمكنه أن يستشير فيها خبيرا كما هو الحال في تقرير الصفة التشريحية في جرائم القتل أو تحليل المادة المطعومة في جريمة تسمم أو فحص لخطوط الكتابة المدعى بتزويرها[2]"، ولما كان قاضي التحقيق هو المختص بالتحقيق، قد يتعرض في عمله لمسائل فنية يصعب عليه كرجل قانون البت فيها حينئذ يجوز له ندب أهل الخبرة حتى يخرج التحقيق في صورة موضوعية صادقة[3].

ثانيا/ الخبير في الجريمة الإلكترونية:

من المعلوم أن هناك حاجة دائمة إلى خبراء وفنيين عند وقوع الجريمة الإلكترونية ويمتد عملهم ليشمل المراجعة والتدقيق على العمليات الآلية للبيانات، وكذلك إعداد البرمجيات وتشغيل الحاسب الآلي وعلومه، وان نجاح الاستدلالات وأعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة وتخص هؤلاء الخبراء، وكذا يجب على المحقق الجنائي أن يحدد للخبير الإلكتروني دوره في المسالة الانتداب فيها على وجه الدقة، وبالنظر إلى أن الجريمة

[1] احمد بسيوني أبو الروس،التحقيق الجنائي و التصرف و الأدلة الجنائية،ط2 ، 2008، ص33.

[2] عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، المرجع السابق، ص24.

[3] مروك نصر الدين ، المرجع السابق، ص390.

الإلكترونية لها الخصوصية التي تتعلق بها فإن الخبير الإلكتروني قد يكون من الجناة الذين سبق لهم ارتكاب مثل هذه الجرائم وتم تذويبهم داخل المؤسسات الإلكترونية للاستفادة من قدراتهم فضلا عن تأهيلهم كمواطنين صالحين[1].

ثالثا/ أساليب عمل الخبير في الجريمة الإلكترونية

هناك أسلوبان لعمل الخبير هما :

أ. القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها كجريمة التهديد أو النصب، جرائم النسخ ..الخ، ثم يقوم الخبير بعملية تحليل رقمي لها، وذلك لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أعدت فيه، وتحديد عناصر حركتها، وكيف تم التوصل إلى معرفتها وأخيرا التوصل لمعرفة برتوكول الانترنت "IP" الذي ينسب إلى جهاز الحاسوب الذي صدرت عنه هذه المواقع[2].

ب . القيام بتجميع وتحصيل لمجموعة المواقع الذي لا تشكل موضوعها جريمة في ذاته، ولكن الجرائم تقع من جراء تتبع موضوعات هته المواقع، مثلما ما هو الحال في المواقع

[1] عبد الفتاح بيومي حجازي، المرجع السابق، ص329-330.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 301.

التي تساعد الغير على معرفة جرعات المخدرات والمؤثرات العقلية حسب وزن الإنسان، بإيهامه أنه إذا تم تتبع التعليمات الواردة فيها لن يصل إلى الشخص إلى حالة إدمان، كذلك الشأن بالنسبة لكيفية إعداد القنابل وتخزينها أو كيفية التعامل مع القنابل الزمنية ... الخ[1].

رابعا / دور الخبير التقني في حفظ الأدلة الإلكترونية

إن التحفظ على الأدلة الإلكترونية من العمليات المعقدة، حيث تحتاج أولا إلى رصد دقيق لمدى صحة البيانات التي يحتوي عليها الكمبيوتر، وكذلك صحة حركة الكمبيوتر فلو كان هناك فيروس في الجهاز لتم التشكيك في صحة الأدلة المستفادة منه، ويحفظ الدليل في العالم الافتراضي برصد موقع الانترنت أو المعلومات التي تشير إلى الجريمة، والتي تكون في مظاهر مختلفة الأشكال ونأخذ على سبيل المثال جريمة القذف في غرف الدردشة، هنا يتم اللجوء إلى ذلك ذاكرة الخادم الذي يتولى ربط هذه الغرف عبر العالم الرقمي للتوصل إلى تحديد موضوع القذف وتاريخه، ولقد لجأت العديد من المحاكم إلى ميكنة إدارتها رقميا، بحيث يتم تسليم الأدلة إلى إدارة متخصصة تتولى حفظ الأدلة الرقمية[2].

ويتعين على الخبير تضمين المسائل التالية في مهمته :

- تركيب الحاسب الآلي، وطرازه ونوعه ونظام تشغيله والأنظمة الفرعية التي يستخدمها.

[1] نفس المرجع، ص 301.

2 خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية المرجع السابق، ص 309-310.

- بيئة الحاسب أو الشبكة من حيث طبيعتها، تركيزها أو توزيعها، وكذلك نمط ووسائط الاتصالات.

- المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.

- الآثار الاقتصادية والمالية المترتبة على التحقيق في الجريمة الإلكترونية.

- كيفية عزل النظام المعلوماتي - عند الحاجة-، دون إتلاف الأدلة أو الأجهزة أو تدميرها.

- إمكانية نقل أدلة الإثبات إلى أوعية أخرى دون تلف.

- إمكانية نقل أدلة الإثبات لأوعية مادية كالأوراق على أن تكون مطابقة لما هو مسجل في الحاسب الآلي أو النظام أو الشبكة[1].

وينصرف رأي الخبير إلى الوقائع اللازم إصدار رأيه الفني بشأنها، كما يجب أن يتوقف رأيه عند المسائل الفنية دون أن يتعدى للمسائل الأخرى كالمسائل القانونية.

1 عبد الفتاح بيومي حجازي، المبادئ الإجرائية للتحقيق، المرجع السابق، ص 330-331.

الخاتمة :

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 انه 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- الجريمة الإلكترونية هي الأفعال المخالفة للقانون التي ترتكب بواسطة الكمبيوتر من خلال شبكة الانترنت .

2- مرتكب الجريمة الإلكترونية 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 الجريمة الإلكترونية من شخص لأخر، فقد تكون دوافع شخصية هدفها تحقيق مصلحة خاصة، وقد تكون خارجية بهدف الانتقام مثلا.

4- الجريمة الإلكترونية 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 الجريمة الإلكترونية والقبض على مرتكبيها ونسبتها إليهم عدة معوقات، أهمها معوقات تشريعية تكمن في عدم حصر لكل صور الجريمة الإلكترونية في القوانين الجنائية.

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

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

8- المعاينة في الجريمة الإلكترونية 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 تقيدر مدى خطورة المجرم المعلوماتي، وهذا يؤثر على الحكم عليه كان يصدر في حقه حكم غير متكافئ مع الجريمة المرتكبة.

2- عدم حصر صور الجريمة الإلكترونية في المواد القانونية وفتح المجال للمحقق في أن ينظر في جميع الجرائم المتعلقة بالجرائم الإلكترونية 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 ولان 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 الجريمة الإلكترونية لأنه موضوع غير مستهلك بالرغم من أهميته، ولأن هذه الجريمة لاقت انتشارا واسعا على الصعيد الوطني.

قائمة المراجع

أ- المراجع العامة

1.أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الجزائر،ط2006،3.

2. احمد بسيوني أبو الروس،التحقيق الجنائي و التصرف و الأدلة الجنائية،ط2 2008.

3.إلياس أبو عبيد، أصول المحاكمات الجزائية، منشورات الحلبي الحقوقية، لبنان ج1، ط1 ، 2006.

4.براء منذر عبد اللطيف، شرح قانون أصول المحاكمات الجزائية، دار الحامد للنشر،عمان، ط1 ، 2009.

5.بلعليات إبراهيم، أركان الجريمة و طرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر،ط1 ، 2006 .

6.حسن الجوخندار،التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، دار الثقافة، عمان،ط1 ،2008.

7.عبد الرحمان خليفي، محاضرات في قانون إجراءات جزائية، دار الهدى، الجزائر 2012 .

8.عبد الله اوهايبية، شرح قانون الإجراءات الجزائية الجزائري ،دار هومة ،الجزائر،ط2 2011.

9.العربي شحط عبد القادر،نبيل صقر، الإثبات في المواد الجزائية، دار الهدى الجزائر،2006.

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

11. علي فضيل البوعينين، ضمانات المتهم في مرحلة المحاكمة، دار النهضة العربية،القاهرة 2006.

12. عماد محمد احمد ربيع ،حجية الشهادة في الإثبات الجزائي، مكتبة دار الثقافة مركز غنيم، الأردن ، ط1 ، 1999.

13. عمر بن إبراهيم بن حماد العمر ، إجراءات الشهادة في مرحلتي الاستدلال و التحقيق الابتدائي في ضوء نظام الإجراءات السعودي ، مذكرة ماجستير ، جامعة نايف العربية للعلوم الأمنية ،2007 .

14. عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلتي الاستدلال و التحقيق الابتدائي.

15. غسان مدحت الخيري، الطب العدلي والتحري الجنائي، دار الراية، المملكة الأردنية ، ط1 ،2013.

16. فرج علواني هليل،التحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، الإسكندرية، 2006 .

17. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر ط2، 2009 .

18. محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري،دار هومة الجزائر ط3 ، 2008 .

19. محمد علي سالم الحلبي، الوجيز في أصول المحاكمات الجزائية، دار الثقافة عمان، ط1 ، 2005.

20. محمد علي سكيكر، آلية المسؤولية الجنائية، دار الفكر الجامعي، الإسكندرية، ط1 2008 .

21. مروك نصر الدين، محاضرات في الإثبات الجنائي، دار هومة، الجزائر، ج1 2003.

ب- المراجع المتخصصة

22. احمد خليفة الملط،، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية ، ط2 2006

23. بكري يوسف بكري،التفتيش عن المعلومات في وسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، ط1 ، 2011 .

24. بلال أمين زين الدين، جرائم نظم المعالجة الآلية للبيانات، دار الفكر الجامعي، الإسكندرية، ط1، 2008.

25. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت دار الثقافة، الأردن، ط1، 2011.

26. خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الالكترونية ، دار الفكر الجامعي الإسكندرية، ط1 ،2009 .

27. خالد ممدوح، أمن الجريمة الالكترونية، الدار الجامعية،الإسكندرية،2008 .

28. ضياء مصطفى عثمان، السرقة الالكترونية، دار النفائس،عمان، ط 1 ، 2011.

29. عبد الفتاح بيومي حجازي ،الجوانب الإجرائية لأعمال التحقيق، دار النهضة العربية، القاهرة ط1 ، 2009 .

30. عبد الفتاح بيومي حجازي، مكافحة جرائم الانترنيت ، دار الفكر الجامعي الإسكندرية ، ط1 2006 .

31. عبد الفتاح مراد،شرح جرائم الكمبيوتر والانترنيت،شركة البهاء، مصر.

32. عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، جامعة نايف العربية للعلوم الأمنية، الرياض،2007.

33. علي جبار الحسناوي ، جرائم الحاسوب و الانترنيت،دار اليازوري ، الأردن 2009، ص 147،148.

34. علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنيت،عالم الكتب الحديث،الأردن ط1 ،2004.

35. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الآلي، الدار الجامعية بيروت 1999.

36. محمد الأمين البشيري،التحقيق في الجرائم المستحدثة،جامعة نايف العربية للعلوم الأمنية، الرياض،ط1 ،2004.

37. محمد أمين الشوابكة، جرائم الحاسوب و الانترنت،دار الثقافة ، عمان، ط1 2007.

38. محمد حماد مرهج الهيتي، ،جرائم الحاسوب ، دار المناهج ،عمان، ط1 2006.

39. محمد مصطفى موسى، التحقيق في الجرائم الالكترونية، مطابع الشرطة القاهرة،2009.

40. محمد منير الجنبيهي و ممدوح محمد ، الجوانب الإجرائية لجرائم الانترنيت والحاسب الآلي ووسائل مكافحتهما، دار الفكر الجامعي،الإسكندرية، 2006.

41. نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، منشورات الحلبي الحقوقية، لبنان،ط1 ، 2005.

42. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت،دار الفكر الجامعي الإسكندرية، ط1،2007 .

43. نهلا عبد القادر المومني،الجرائم المعلوماتية ، دار الثقافة،الأردن،ط1 ، 2008.

ج-الرسائل العلمية

44. بلال بن جامع ، المشكلات الأخلاقية و القانونية المثارة حول شبكة الانترنيت ماجستير في علم المكتبات تخصص إعلام علمي ، جامعة منتوري ، قسنطينة 2006.

45. عبد الله بن سعيد أبو داسر، إثبات الدعوى الجنائية ، أطروحة دكتوراه في القانون، جامعة الإمام محمد بن سعود الإسلامية السعودية، 1443ه.

د - المقالات

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

47. الملتقى الوطني حول الجريمة الالكترونية ، جريدة الأمة العربية ، وهران 2013/02/01 .

هـــــ - القوانين

48. القانون المتعلق بالمبادلات والتجارة الإلكترونية عدد 83 لسنة 2000 المؤرخ في 9 أوت 2000 .

49. مذكرة توضيحية للقانون الجزائي العربي الموحد ،جامعة الدول العربية ، الجزء الثاني ، رقم 229 ، د 12 بتاريخ 1996/11/19 .

50. الأمر 66-155 المؤرخ في 18 صفر 1386 الموافق 08 يونيو 1966 يتضمن قانون الإجراءات الجزائية المعدل و المتمم بالقانون رقم 06- 22 المؤرخ في 29 ذي القعدة عام 1386 الموافق ل 20 ديسمبر 2006 ، المتضمن قانون الإجراءات الجزائية .

51. الأمر رقم 04-15 المؤرخ في رمضان 1425 الموافق ل:10 نوفمبر 2004 المعدل و المتمم للأمر رقم 66-156 الموافق ل 8 يونيو 1966 المتضمن قانون العقوبات.

و - المواقع الالكترونية

52. http://www.moi.gov.qa/UNCCPCJDoha/Arabic/Previous_Congress es.html - بتاريخ 2014/09/03 على الساعة 10:30

الفهـــــــــــــــــــــــــــــــرس

مقدمة..... أ-

هـــ

الفصل الأول: ماهية الجريمة الإلكترونية و التحقيق فيها..... 6-51

المبحث الأول: ماهية الجريمة الإلكترونية.....7

المطلب الأول: مفهوم الجريمة الإلكترونية.....8

الفرع الأول: تعريف الجريمة الإلكترونية.....8

أولا/ تعريف الجريمة لغة.....9

ثانيا/ تعريف الجريمة اصطلاحا.....9

ثالثا/ تعريف الجريمة الإلكترونية فقها.....9

رابعا/ تعريف الجريمة الإلكترونية قانونا.....12

الفرع الثاني: خصائص الجريمة الإلكترونية والمجرم الإلكتروني 14

أولا/ خصائص المجرم الإلكتروني.....15

ثانيا/المجني عليه في الجريمة الإلكترونية.....18

ثالثا/أنواع المجرمين الإلكترونيين و صفاتهم.....19

رابعا/خصائص الجريمة الإلكترونية.....22

الفرع الثالث : تقسيمات الجريمة الإلكترونية وأضرارها.....24

أولا / تقسيمات الجريمة الإلكترونية.....24

ثانيا/ أضرار الجريمة الإلكترونية.....28

المطلب الثاني: أركان الجريمة الإلكترونية وصورها.....29

الفرع الأول: الركن الشرعي للجريمة الإلكترونية.....30

أولا/ على مستوى الدولي.....31

ثانيا/ على المستوى الوطني.....33

الفرع الثاني:الركن المادي للجريمة الإلكترونية.....34

الفرع الثالث : الركن المعنوي للجريمة الإلكترونية.....36

المبحث الثاني: التحقيق في الجريمة الإلكترونية.....36

المطلب الأول: مفهوم التحقيق في الجرائم الإلكترونية.....37

الفرع الأول: تعريف التحقيق في الجريمة الإلكترونية.....37

أولا/ تعريف التحقيق..... 38

ثانيا/ تعريف المحقق.....39

الفرع الثاني: خصائص التحقيق في الجريمة الإلكترونية.....40

أولا/ خصائص التحقيق.....41

ثانيا/ الخصائص الفنية للمحقق في الجريمة الإلكترونية..... 42

الفرع الثالث: معوقات التحقيق الجنائي في الجرائم الإلكترونية.....45

أولا/ معوقات تشريعية.....46

ثانيا/ المعوقات المتعلقة بالجريمة و الجهات المتضررة.....46

المطلب الثاني: جهاز التحقيق الجنائي في الجريمة الإلكترونية و الصعوبات التي تواجهه.....47

الفرع الأول: جهاز التحقيق الجنائي في الجريمة الإلكترونية و أقسامه..... 48

أولا/ تعريفه جهاز التحقيق الجنائي في الجريمة الإلكترونية.....48

ثانيا/ أقسام جهاز التحقيق الجنائي في الجريمة الإلكترونية.....48

الفرع الثاني: الصعوبات تتعلق بجهات التحقيق في الجريمة الإلكترونية.....50

الفصل الثاني: إجراءات التحقيق في الجريمة الإلكترونية.....52-91

المبحث الأول: اتصال المحقق بالجريمة الإلكترونية.....53

المطلب الأول: آلية التحقيق في الجريمة الإلكترونية.....53

الفرع الأول: تلقي البلاغات والشكاوى حول الجريمة الإلكترونية.....54

أولا/ البلاغات في الجريمة الإلكترونية..... 54

ثانيا/ الشكوى في الجريمة الإلكترونية.....56

الفرع الثاني: الوسائل المساعدة التي يستخدمها المحقق في جرائم الإلكترونية.....57

أولا/الوسائل المادية.....57

ثانيا/الوسائل الإجرائية.....62

المطلب الثاني: الاستجواب وسماع الشهود في الجريمة الإلكترونية..... 63

الفرع الأول: الاستجواب في الجريمة الإلكترونية.....63

أولا/ الاستجواب عند الحضور الأول في الجريمة الإلكترونية.....64

ثانيا /الاستجواب في الموضوع في الجريمة الإلكترونية.....64

ثالثا/الاستجواب الإجمالي في الجريمة الإلكترونية.....65

الفرع الثاني: سماع الشهود في الجريمة الإلكترونية.....65

أولا/تعريف الشهادة وأنواعها.....66

ثانيا /الشهادة الإلكترونية.....68

المبحث الثاني: الانتقال إلى مسرح الجريمة الإلكترونية.....70

المطلب الأول: التفتيش و ضبط الأدلة في الجريمة الإلكترونية.....70

الفرع الأول: التفتيش في الجريمة الإلكترونية.....71

أولا/ تعريف التفتيش.....71

ثانيا/ القواعد العامة لتفتيش نظم الحاسوب والانترنيت.....72

الفرع الثاني: ضبط الأدلة في الجريمة الإلكترونية.....77

أولا/ مفهوم ضبط الأدلة في الجريمة الإلكترونية.....77

ثانيا/إجراءات ضبط الأدلة في الجريمة الإلكترونية.....78

المطلب الثاني: المعاينة و ندب الخبراء في الجريمة الإلكترونية.....83

الفرع الأول: المعاينة في الجريمة الإلكترونية.....83

أولا/تعريف المعاينة في الجريمة الإلكترونية.....84

ثانيا/الانتقال و المعاينة في الجريمة الإلكترونية.....85

الفرع الثاني: ندب الخبراء في الجريمة الإلكترونية.....86

أولا/ تعريف الخبرة في الجريمة الإلكترونية.....87

ثانيا/ الخبير في الجريمة الإلكترونية.....88

ثالثا/ أساليب عمل الخبير في الجريمة الإلكترونية.....89

رابعا / دور الخبير التقني في حفظ الأدلة الإلكترونية.....89

الخاتمة.....92 -95

تلخيص المذكرة:

الجريمة الالكترونية 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 و الشهود 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.

Résumé :

Crime électronique est une des crimes développés, enjoignant à la Commission signifie un plus high-tech à l'intelligence et l'expérience de l'auteur dans le domaine de la technologie moderne, et il mesure serait étudiée profiter de la nature de la vie privée en raison de la nature de la cybercriminalité, où il ya des pays les plus touchés, y compris l'équipement spécial pour enquêter, prendre des rapports et des plaintes via Internet par les sites web qui lui est dédié et lorsque vous recevez des communications de l'enquêteur apparition d'électronique de crime appelle les suspects et les témoins à interroger les suspects et les dépositions des témoins, témoins de la cybercriminalité sont des gens qui Fenians, les propriétaires de l'expérience et de la spécialisation en informatique et en sciences de l'informatique et l'Internet, et quand vous allez à la scène du crime est Détective recherché toutes ml convoqué pour révéler la vérité, y compris les systèmes d'information, et quand il n'y a aucune preuve, il ajuste les scores qui lui sont consacrés, mais si la preuve électronique, il s'ajuste en fonction de règles spéciales comme la chiffrement par exemple, et l'enquêteur a examiné la scène du crime de physique et numérique avec des experts.