الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي
جامعة محمد بوضياف - المسيلة

كلية الحقـــوق و العلـــوم السياسية
قسم: الحقوق
رقم: .....

ميدان: الحقـــوق و العلـــوم السياسية
فرع: الحقوق
تخصص: قانون جنائي

مذكرة مقدمة لنيل شهادة الماستر أكاديمـــي

إعداد الطالب(ة): يوسف جفال

تحت عنوان

التحقيق في الجريمة الإلكترونية

لجنة المناقشة:

أ. بلحو نسيم	جامعة: محمد بو ضياف	رئيســـا
أ. سعدي الربيع	جامعة: محمد بو ضياف	مشرفا و مقررا
أ. حططاش عمر	جامعة: محمد بو ضياف	مناقشا

السنة الجامعية:2017/2016

بسم الله الرحمن الرحيم

"وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ وَسَتُرَدُّونَ إِلَىٰ عَالِمِ
الْغَيْبِ وَالشَّهَادَةِ فَيُنَبِّئُكُم بِمَا كُنتُمْ تَعْمَلُونَ"

سورة التوبة الآية (105)

إهداء

أهدي هذا العمل الذي هو زبدة دراستي إلى من ينعقد لساني لوصفها...

إلى أمي التي أمسكت يدي وأخذتني عند نهر العلم وفارقتني عند الضفة وأخفت دموع خوفها ... أوصلتني وأركبتني وأيقظتني ووبختني هي صورة رحمة الله في الدنيا ربي احفظها لي

....إلى ليث بيتنا وسقف كوخنا إلى ساقي اسرتنا وحاميها ... إلى كل تلك القسوة والتوجيه إلى ابي الذي ليس له مثيل ... لكل إبداع وإنجاز .. لكل مربي ولد صالح يدعو له..أعانني الله أن أكون ولدك الصالح..أبي

شكر وعرفان

...الحمد لله الذي جعلني في مكاني هذا بعملي هذا

..إلى كل من ساهم في ترقيتي إلى هذا المكان .. من كل قلبي أشكركم وأحمد الله لوجودكم أصدقائي وعائلتي وكل من اعانني لست شيئا دونكم ولست شيئا بعدك...

إلى أستاذي الذي يصبب مثل النمر على طلبته بالعلم جعلك الله منيرا ونورا يهتدى به ..سعدي الربيع..

... لن تكون الحروف ولو تكن أبدا في وقت ما كافية للبوح بما يحمله القلب من امتنان .. شكرا جزيلا لكم

مـــــــقـــدمـــــة

بالرغم من المزايا التي تحققت ولا تزال تتحقق كل يوم بفضل التطور الهائل في المجال الالكتروني على جميع الأصعدة في شتى مجالات الحياة المعاصرة، لدرجة حتى أصبحت جميع القطاعات المختلفة تعتمد في أداء عملها بشكل أساسي على استخدام الأنظمة الإلكترونية، لما تتميّز به من عنصري السرعة والدقّة في تجميع المعلومات كتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدّة دول.

لكن وعلى الرغم من المزايا الهائلة التي تحققت، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية والخطيرة جراء سوء استخدام هذه التقنية، فإن بعض الأشخاص يحاولون استغلال المخترعات العملية وما تقدمه من وسائل متقدّمة في ارتكاب العديد من الجرائم التقليدية ، مستغلين الإمكانيات الهائلة لهذه المستحدثات أو استحداث صور أخرى من الإجرام يرتبط بهذه التقنيات التي تصير محلا لهذه الجرائم أو وسيلة لارتكابها، وقد تزايدت معدلات هذه الجرائم في العقدين الأخيرين بكثرة وبصورة أدّت إلى ظهور ظاهرة إجرامية جديدة تعرف بالإجرام الالكتروني.

على ضوء ذلك، فإن هذه الظاهرة الإجرامية التقنية أثارت العديد من الإشكالات في نطاق قانون الإجراءات الجزائية، الذي وضعت نصوصه لتحكم الإجراءات المتعلقة بجرائم تقليدية لا توجد صعوبات كبيرة في إثباتها أو التحقيق فيها وجمع الأدلة المرتبطة بها، وهو ما لا يمكن تصوّره في جريمة ترتكب في بيئة افتراضية تقنية لا تخلف أي أثار مادية محسوسة ولا يرتكبها إلا مجرمون يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الآلية للمعطيات والإلمام بالمهارات كالمعارف التقنية، كما أنّ هذه الجريمة تتم في الخفاء ويعمد مرتكبوها إلى إخفاء أنشطتهم الجرمية عن طريق التلاعب بالبيانات، والذي غالبا ما يتحقق في غفلة من المجني عليه، فضلا عن سهولة تدمير الدليل ومحوه من مسرح الجريمة ،مما جعل الأدلة في الجريمة الإلكترونية صعبة الإثبات.

وعليه فمن الأسباب التي دفعتني إلى تناول هذا الموضوع بالدراسة، راجع لحداثة الموضوع، والتزايد المستمر للجرائم الالكترونية، و كذا الرغبة في التعمق في البحث ومواجهة النشاط الإجرامي الالكتروني.

و من هنا و تتجلى أهمية دراسة هذا الموضوع من خلال معرفة الجرائم المرتكبة ضد الحاسوب وشبكة الانترنت وإلقاء العبء على الدولة بوضع التشريعات اللازمة لحماية المجتمع منها، بالإضافة إلى أهمية معرفة مدى خطورة جرائم الحاسوب التى تطال الحق في المعلومات، وتمس الحياة للأفراد وتهدد الأمن القومي والسيادة الوطنية، وكذلك تهديد إبداع العقل البشري ولذلك يجب الالمام بماهية جرائم الحاسوب وطبيعته وإظهار موضوعها وخصائصها ومخاطرها وحجم الخسائر الناجمة عنها ودوافع مرتكبيها، وهذا يتخذ أهمية استثنائية لسلامة التعامل مع هذى الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية.

غير أن الهدف الأساسي من وراء هذه الدراسة، نظرا لتزايد استخدام الحاسوب والانترنت ظهور ونمو التجارة الالكترونية الدولية، فان هدفها الرئيسي هو تنظيم التجارة الدولية وحمايتها من الاعمال غير المشروعة وتجنب الاحتيال والغش وسرقة المعلومات من اجل استقرار التعامل وشعور الناس بالثقة والاطمئنان، أي أن الجرائم المرتبطة بالحاسوب والانترنت تدخل في عدد الجرائم المنظمة التي لها صفة الاستمرارية، وكذلك يمكن أن ترتكب بشكل فردي، مما يوجب توفير الحماية الجنائية لها وإدراج نصوص قانونية تجرمها في قوانين العقوبات، والإجراءات القانونية الصحيحة الواجب اتباعها من قبل النيابة العامة والضوابط العدلية في كشف جريمة الحاسوب والانترنت وآلية الإثبات الجنائي على المتهم المقترف لهذه الجرائم والطرق الفنية التي تقوم بها السلطة المختصة بالتحقيق في كشف الجريمة.

و عليه فالإشكالية الرئيسة لهذه الدراسة هي:

ما مدى فاعلية الآليات القانونية في التحقيق الجنائي في الجريمة الإلكترونية؟

و حرصنا في هذه الدراسة و نزولا عند موجبات البحث العلمي، و كما هو متعارف عليه فإن طبيعة البحث في المواضيع القانونية التي تفرض علينا نوعية المنهج المتبع فلقد اخترنا منهجا يلم بدراسة الموضوع بكل جوانبه، و هو المنهج الوصفي التحليلي الذي يهدف إلى بيان إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، وذلك من خلال الرجوع الى المرجع القانوني والتخصصات والرسائل والدراسات والبحوث والاتفاقيات الدولية ذات صلة.

و من الدراسات السابقة التي تناولت موضوع التحقيق في الجريمة الالكترونية، و من خلال عملية البحث التي قمنا بها عن المراجع المتعلقة بالموضوع، و نظرا لحداثته وجدنا رسالة دكتوراه للطالب ربيع حسين المعنونة بآليات البحث والتحقيق في الجرائم المعلوماتية، و كذلك

مذكرة ماجستير للطالب سعيد علي نعيم تحت عنوان آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري.

و عليه فقد قسمت بحثي هذا إلى فصلين:

بحيث تضمن **الفصل الأول** الإطار المفاهيمي للجريمة الالكترونية والتحقيق فيها،الذي يحتوي على مبحثين، تضمن المبحث الأول ماهية الجريمة الالكترونية، أما المبحث الثاني فتضمن ماهية التحقيق الجنائي في الجريمة الالكترونية.

والفصل الثاني فخصصناه لدراسة القواعد الإجرائية في استخلاص الدليل الالكتروني والقيمة القانونية له، الذي يحتوي بدوره على مبحثين، تضمن المبحث الأول القواعد الإجرائية في استخلاص الدليل الالكتروني، والمبحث الثاني تضمن القيمة القانونية للدليل الالكتروني في مجال الإثبات الجنائي.

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية والتحقيق فيها

تعد الجرائم الإلكترونية ظاهرة إجرامية حديثة نظرا لارتباطها بالتكنولوجيا الحديثة، فقد ترتب على ذلك إحاطة هذه الظاهرة بكثير من الغموض، لأجل ذلك فقد بدا لي أنه وقبل الخوض في الإجراءات التي تنطبق على الجرائم الإلكترونية أن أنوه على جانب من القواعد الموضوعية لهذه الظاهرة الإجرامية، إذ يجب الإلمام بماهية الجرائم الإلكترونية وطبيعتها وإظهار موضوعها وخصائصها، وهذا حتما في منظورنا يتخذ أهمية استثنائية لسلامة التعامل مع هذه الظاهرة من طرف القائمين على مكافحتها.

وعلى ضوء ذلك سأقسم هذا الفصل إلى ماهية الجريمة الإلكترونية في المبحث الأول أما المبحث الثاني سيكون تحت عنوان ماهية التحقيق الجنائي في الجريمة الإلكترونية.

المبحث الأول: ماهية الجريمة الإلكترونية

أثيرت العديد من التساؤلات حول تحديد الطبيعة القانونية للجريمة الإلكترونية، ويرجع سبب ذلك إلى تعدد وجهات النظر بخصوص هذا النوع من الجرائم حيث ظهرت عدة آراء فقهية في محاولة فهم المقصود بالجريمة الإلكترونية، وتحديد تعريف لها مع تبيين طبيعتها القانونية، كما أن تعريف الجريمة الإلكترونية يستوجب الإلمام بالجانب الموضوعي والإجرائي لها، مع دراسة العوامل المختلفة التي تتداخل في تكوين الجريمة، والإحاطة بالأمور الفنية لها.

وعليه سنحاول من خلال هذا المبحث أن نتطرق إلى ماهية الجريمة الإلكترونية، حيث تضمن المطلب الأول مختلف التعريفات التي استخدمت لوصف وضبط خصائص هذا النوع من الإجرام، مع تبيين المعايير التي استند عليها الفقهاء في تعريفهم للجريمة الإلكترونية، ولا يكتمل البحث في ماهية الجريمة الإلكترونية دون البحث في خصائصها وطبيعتها وأركانها وهو ما سنتطرق إليه في المطلب الثاني

المطلب الأول: تعريف الجريمة الإلكترونية

لم يتفق الفقه على تعريف جامع للجرائم الإلكترونية، نظرا لغياب تعريف قانوني لهذا النوع من الجرائم في أغلب التشريعات، بالإضافة إلى غياب مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن استغلال غير القانوني لتقنية المعلومات واستخدامها .

وفي ظل هذا الفراغ القانوني حاول الفقه إيجاد تعريف للجرائم الإلكترونية ،وانقسمت بدورها إلى اتجاهين رئيسيين وهذا بالنظر الى الزاوية التي ينظر من خلالها لهذا النوع من الجرائم، حيث أن الاتجاه الأول مضيق لمفهوم الجريمة الإلكترونية، أما الاتجاه الثاني فقد حاول التوسع في تعريف الجريمة الإلكترونية.

الفرع الأول: المفهوم الضيق للجريمة الإلكترونية

يذهب أنصار هذا الاتجاه إلى حصر الجريمة الإلكترونية في الحالات التي تتطلب قدرا كبيرا من المعرفة التقنية، وأن الجرائم التي تفتقر إلى هذه الدرجة من المعرفة تعد جرائم عادية تتكفل بها النصوص التقليدية للقوانين العقابية.

من التعريفات التي وضعها أنصار هذا الاتجاه أيضا ما ذهب إليه الفقيه MERWE حيث يرى أن الجريمة الإلكترونية: هي الفعل غير المشروع الذي يدخل في ارتكابه الحاسب

الآلي أو هي الفعل الإجرامي الذي يستخدم في ارتكابه الحاسب الآلي كأداة رئيسية، أو هي مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الآلية للبيانات.[1]

وعرفها آخرون بأنها: "الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا هاما، أو هي كل فعل إجرامي يستخدم الحاسب الآلي في ارتكابه كأداة رئيسية".[2]

فيما ذهب الفقيه ROSBLAT على أنها: "كل نشاط غير مشروع موجه لنسخ أو تغيير أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي أو تغييرها أو حذفها او التي تحول عن طريقه".[3]

حسب الدكتورة هدى فشقوش هي: "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"، أو هي "أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبط بتقنية المعلومات".[4]

عرفها كل من CASTLE,R.TOTT و A.HARD بأنها: "تلك الجرائم التي يكون قد حدث في مراحل ارتكابها بعض العمليات الفعلية داخل الحاسوب"، وبمعنى آخر "هي التي يكون للحاسب الآلي فيها دورا إيجابيا أكثر من سلبيته".[5]

ما يؤخذ على التعريفات السابقة أنها جاءت قاصرة عن الإحاطة بأوجه ظاهرة الإجرام الإلكتروني، فالبعض من فقهاء هذا الاتجاه ركز على معيار موضوع الجريمة، والبعض الآخر ركز على وسيلة ارتكابها، والبعض الآخر على معيار النتيجة.

الفرع الثاني: المفهوم الواسع للجريمة الإلكترونية

إزاء الانتقادات التي وجهت الى الاتجاه الأول حاول الفقهاء تعريف الجريمة الإلكترونية على نحو واسع لتفادي أوجه القصور التي شابت تعريفات الاتجاه المضيق للتصدي لظاهرة الإجرام الإلكتروني.

---

[1] طارق إبراهيم الدسوقى عطية، الأمن المعلوماتي النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، مصر، 2009، ص 153.

[2] حنان ريحان مبارك المضحاكي، الجرائم المعلوماتية ، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014، ص25.

[3] طارق إبراهيم الدسوقى عطية، المرجع السابق، ص154.

[4] خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب و الانترنت، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان، 2011، ص28

[5] احمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية مصر، 2006، ص 30.

وعلى العكس من الاتجاه السابق، فان أنصار هذا الاتجاه يذهبون إلى التوسيع من مفهوم الجريمة الإلكترونية، حيث يرى الفقيهان CREDO,MICEL بأنها تشمل استخدام الحاسب كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته.

كما تمتد هذه الجريمة لتشمل الاعتداءات المادية، سواء كان هذا الاعتداء على جهاز الحاسوب ذاته، أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وانتهاك ماكينات الحسابات الآلية، بما يتضمنه من شبكات تمويل الحسابات المالية بطريقة الكترونية، وتزييف المكونات المادية والمعنوية للحاسوب، بل وسرقة الحاسوب في حد ذاته أو مكوّن من مكوناته.[1]

تناول رأي أخر من الفقه تعريف الجريمة الإلكترونية بأنها: "عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسوب وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض لها عقابا.[2]

عرفت في إطار المنظمة الأوربية للتعاون و التنمية الاقتصادية بأنها: "كل فعل أو امتناع من شأنه أن يؤدي إلى الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية".[3]

وجاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقدة في فيينا سنة 2000 تعريف الجريمة الإلكترونية كما يلي: "يقصد بالجريمة الإلكترونية أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبيه، أو داخل نظام حاسوبي، والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[4]

لاشك أن هذا الاتجاه ينطوي على توسيع كبير لمفهوم الجريمة الإلكترونية، إذ يؤخذ عليه هذا التوسع الذي من شأنه أن يسقط وصف الجريمة الإلكترونية على أفعال قد لا تكون كذلك لمجرد مشاركة الحاسوب الآلي في النشاط الإجرامي فبعض الجرائم كسرقة الحاسوب

[1] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، الإسكندرية، مصر، 2004، ص44،45.

[2] طارق إبراهيم الدسوقى عطية، المرجع السابق، ص158.

[3] حنان ريحان مبارك المضحاكي، المرجع السابق، ص26،27.

[4] خالد عياد الحلبي، المرجع السابق، ص30.

الآلي او الأقراص مثلا فلا يمكن إعطاؤها وصف الجريمة الإلكترونية على سلوك الفاعل لمجرد أن الحاسوب أو أحد مكوناته المادية كانت محلا لفعل الاختلاس.

الفرع الثالث: تعريف المشرع الجزائري للجريمة الإلكترونية

تبنى المشرع الجزائري للدلالة على الجريمة الإلكترونية، مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، حيث يمثل نظام المعالجة الآلية للمعطيات المسألة الأولية، أو الشرط الأولي الذي يلزم تحقيقه حتى يمكن البحث في توافر أو عدم توافر أركان أي جريمة من جرائم الاعتداء على هذا النظام، فإذا تخلف هذا الشرط الأولي، لا يكون هناك مجال لهذا البحث.[1]

نظام المعالجة الآلية للمعطيات تعبير فني تقني يصعب على المشتغل بالقانون إدراك حقيقته بسهولة، فضلا عن أنه تعبير يخضع للتطورات السريعة والمتلاحقة في مجال فن الحاسبات الآلية، لذلك فالمشرع الجزائري على غرار التشريع الفرنسي لم يعرف نظام المعالجة الآلية للمعطيات فأوكل بذلك مهمة تعريفه لكل من الفقه و القضاء.[2]

المطلب الثاني: خصائص وأركان الجريمة الإلكترونية

للجريمة الإلكترونية خصائص واركان تتمثل في:

الفرع الأول: خصائص الجريمة الإلكترونية

أدى ارتباط الجريمة الإلكترونية بجهاز الحاسوب وشبكة الانترنت إلى إضفاء مجموعة من الخصائص و السمات المميزة لهذه الجريمة عن الجرائم التقليدية ويمكن إجمالها في ما يلي:

أولا: الجريمة الإلكترونية عابرة للحدود الوطنية

في عصر الحاسب الآلي ومع انتشار شبكة الانترنت أمكن ربط عدد هائل لا حصر لها من الحواسيب عبر العالم بهذه الشبكة، بحيث يغدو أمر التنقل والاتصال فيما بينها أمرا سهلا، طالما حدد عنوان المرسل إليه، أو أمكن معرفة كلمة السر، وسواء تم ذلك بطرق مشروعة أو غير مشروعة في هذه البيئة، يمكن أن توصف جرائم التقنية بأنها جرائم عابرة للدول، إذ غالبا ما يكون الجاني في بلد ومجني عليه في بلد آخر، كما قد يكون الضرر المتحصل في بلد ثالث

[1] أمال قارة، الحماية الجنائية للمعلوماتية في التشريع الجزائري، الطبعة الأولى، دار هومة، 2006، ص100،101.

[2] المرجع نفسه، ص101.

في الوقت نفسه، وعليه تتخذ جرائم التقنية شكلا جديدا من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية.[1]

بهذه الخاصية التي تتميز بها الجريمة الإلكترونية كونها جريمة عابرة للحدود خلقت العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول تحديد القانون الواجب التطبيق، بالإضافة إلى إشكالية تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام.

ونتيجة لهذه الطبيعة الخاصة للجريمة الإلكترونية، ونظرا للخطورة التي تشكلها على المستوى الدولي، والخسائر التي تتسبب بها ، ظهرت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لهذه الجرائم، وتجدر الإشارة هنا إلى جهود الانتربول في هذا المجال، من خلال ضباط الارتباط المنتشرين في كافة الدول عبر العالم، والمكلفين بتوفير قاعدة بيانات ضخمة يمكن أن تشكل نقطة انطلاق للمكافحة و التصدي لهذه الجرائم.[2]

ثانيا: الجريمة الإلكترونية صعبة الاكتشاف والإثبات

نظرا للطبيعة الخاصة الذي تتميز بها الجريمة الإلكترونية فإن إثباتها يحيط به كثير من الصعوبات، والتي تتمثل في صعوبة اكتشاف هذه الجرائم، لأنها لا تترك أثرا خارجيا، فالجريمة الإلكترونية لا عنف فيها ولا أثر اقتحام لسرقة مثلا، وإنما هي أرقام وبيانات تتغير أو تمحى من السجلات المخزنة في ذاكرة الحاسوب وليس لها أي أثر خارجي مرئي، وبمعنى آخر فإن الجريمة الإلكترونية هي جرائم فنية، وهي جرائم هادئة لا تتطلب العنف، ورغم ذلك فان البعض يشبّه هذه الجرائم بجرائم العنف مثل ما ذهب إليه مكتب التحقيقات الفدرالي بالولايات المتحدة الأمريكية نظرا لتماثل دوافع المتعدين على نظم الحاسوب الآلي مع مرتكبي العنف.[3] فإذا تم اكتشاف الجريمة الإلكترونية، فلا يكون ذلك إلا بمحض الصدفة، نظرا لعدم وجود أثر مادي لما يجري خلال تنفيذها من عمليات، حيث يتم نقل المعلومات بالنبضات الإلكترونية، ولذلك يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية، إلى جانب إمكانية ارتكابها خارج الحدود الوطنية والدول والقارات وذلك باستخدام شبكات الاتصال ودون تحمل عناء الانتقال، إلى جانب

[1] أسامة احمد المناعسة، جلال محمد الزعبي، جرائم تقنية نظم المعلومات الإلكترونية، الطبعة الثالثة ، دار الثقافة للنشر و التوزيع ، عمان ،2014 ، ص93.

[2] أسامة احمد المناعسة ، جلال محمد الزعبي ، المرجع السابق ، ص96.

[3] محمد علي العريان ، المرجع السابق ، ص53.

تلك الرغبة في استقرار حركة المعاملات و محاولة إخفاء أسلوب ارتكاب الجريمة حتى لا يتم تقليدها من جانب الآخرين.[1]

ثالثا: خصوصية مرتكب الجرائم الإلكترونة

يتصف المجرم المعلوماتي بخصائص معينة تميزه عن المجرم الذي يرتكب الجرائم التقليدية، فإذا كانت الجرائم التقليدية لا تتطلب مستوى علمي معرفي للمجرم في عملية ارتكابها، فإن الأمر يختلف بالنسبة للجرائم الإلكترونية، فهي جرائم فنية تقنية في الغالب، والأشخاص الذين يقومون بارتكابها عادةً يكونون من ذوي الاختصاص في مجال تقنية المعلومات الإلكترونية، أو على الأقل شخص لديه حد أدنى من المعرفة و القدرة على استعمال جهاز الحاسوب، والتعامل مع شبكة الانترنت، كما أن الباعث إلى ارتكاب المجرم لهذا النوع من الجرائم قد تكون مختلفة عن بواعث ارتكاب الجرائم من قبل المجرم التقليدي.[2]

الفرع الثاني: أركان الجريمة الإلكترونية

تتخذ الجريمة المرتكبة عبر الانترنت من الفضاء الافتراضي مسرحا لها، مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي، فهي تشترك بوجود الفعل غير المشروع، والمجرم يقوم بهذا الفعل، من خلال هذا التشابه سوف نتطرق إلى تبيان الأركان التي تقوم عليها هذه الجريمة، وبالتالي نعمد إلى تبيان مدى انطباق مبدأ الشرعية على الجريمة الإلكترونية في الفرع الأول، و نوضح الركن المادي في الفرع الثاني، لننتهي إلى تحديد الركن المعنوي في الفرع الثالث.

أولا: الركن الشرعي

يقصد بالركن الشرعي للجريمة وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع هذا الفعل، يبنى على ذلك عدم جواز ملاحظة الشخص عن فعل ارتكبه قبل صدور نص التجريم، وعن فعل ارتكبه بعد إلغاء نص التجريم كما لا يجوز قياس افعال لم ينص المشرع على تجريمها وأفعال أخرى ورد نص التجريم عليها مهما يكن بينها من تشابه من حيث

[1] محمد علي العريان ، المرجع السابق، ص54.

[2] طارق إبراهيم الدسوقي عطية، المرجع السابق، ص176،177.

الدوافع أو الفاعلية أو النتائج أو العناصر، ذلك أنه لا يجوز أيضا التوسع في تفسير النصوص الجزائية، وعلى القضاة التقيد بمدلول النص و الالتزام بمضامينه.[1]

يترتب على إعمال قاعدة شرعية الجرائم والعقوبة نتيجة مهمة، تتمثل في عدم رجعية القاعدة الجنائية، أي بمفهوم المخالفة تنطبق القواعد الجنائية بأثر فوري ولا مجال لإعمالها بأثر رجعي، إلا إذا نص القانون على ذلك صراحة في النص القانوني أو إذا ما أعملت قاعدة تطبيق القانون الأصلح للمتهم.[2]

إن الركن الشرعي للجريمة الذي هو الصفة غير المشروعة للفعل الذي يقوم به الجاني له ركنين أساسين :

- مطابقة الفعل لنص التجريم.
- أن لا يخضع الفعل المرتكب لسبب من أسباب الإباحة.

يقصد بمطابقة الفعل لنص التجريم هو تطابق الأفعال التي يجرمها القانون مع النصوص التشريعية الموجودة، أما بالنسبة لخضوع الفعل لسبب من أسباب الإباحة فقد ذهب اجتهاد المحكمة العليا إلى أنه لتطبيق نظرية العقوبة المبررة أن يكون النص الواجب التطبيق يقرر نفس العقوبة.[3]

ثانيا: الركن المادي

يقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق، التي يكفلها الدستور و القانون وقد ذهب الدكتور رضا فرح إلى تقسيم الركن المادي في حد ذاته إلى ثلاث عناصر:[4]

- السلوك الإجرامي.

[1] أسامة احمد المناعة ،جلال محمد الزغبي ، المرجع السابق ، ص45.

[2] حنان ريحان مبارك المضحاكي ، المرجع السابق، ص57.

[3] بلعليات إبراهيم ، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري ، الطبعة الأولى ، دار الخلدونية، الجزائر،2007 ، ص 94،95.

[4] المرجع نفسه ، ص17.

- النتيجة الإجرامية.
- العلاقة السببية بين الفعل والنتيجة.

1- السلوك الإجرامي

هذا السلوك يوجد بصورتين فقد يكون بفعل إيجابي، إذ يفترض في هذه الصورة قيام الجاني بفعل إرادي بغية إحداث نتيجة معينة، كما يمكن أن يكون بفعل سلبي يأخذ وصف الامتناع عن إتيان أمر يوجبه المشرع، وفي الجريمة الإلكترونية يمكن أن نجده بنوعيه السلوك الإيجابي او السلبي. لا ننسى التطور الكبير في محتوى وطبيعة هذا السلوك الإجرامي الذي تطور بتطور الوسائل التي وجدت بين يدي الفاعل، وهذا السلوك الذي طورته أيضا عقلية الفاعل الذكية، والتي استطاعت أن تخرج من تقليدية السلوك الجرمي إلى مساحات أكثر تعقيدا أوجدت بلا شك صعوبات كثيرة.[1]

2- النتيجة الإجرامية

يقصد بالنتيجة الإجرامية الأثر المادي الذي يحدث، فالسلوك قد أحدث تغييرا ملموسا، ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج، بغض النظر عمّا يمكن أن يحدثه السلوك الإجرامي من نتائج أخرى.[2]

3- العلاقة السببية بين الفعل والنتيجة

تتمثل العلاقة السببية في الصلة التي تربط بين العقل والنتيجة، وتثبت أن ارتكاب الفعل هو الذي أدى إلى حدوث النتيجة وأهمية الرابطة السببية ترجح إلى إسناد النتيجة الى الفعل هو شرط أساسي لتقرير مسؤولية مرتكب الفعل عن النتيجة، وتحقق الرابطة السببية تلازما ماديا بين الفعل والنتيجة يؤدي إلى وقوف مسؤولية الجاني عند حد الشروع، إذ لا يعد مسؤولا عن النتيجة التي تحققت، أما إذا كانت غير عمديه فإن نفي رابطة سببية يؤدي إلى انتفاء المسؤولية كليةً عنها ذلك أنه لا شروع في الجرائم غير العمدية.[3]

[1] أسامة احمد المناعة، جلال محمد الزغبي، المرجع السابق، ص53-55.

[2] بلعلبات إبراهيم، المرجع السابق، ص18.

[3] أسامة احمد المناعة، جلال محمد الزغبي ، المرجع السابق، ص58،59.

ثالثا: الركن المعنوي

يقوم الركن المعنوي للجريمة المرتكبة عبر الانترنت على أساس مجسد في توافر الإرادة الجرمية لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرمه القانون كانتحال شخصية المزود عبر الانترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر النتيجة الجريمة المترتبة على الأفعال السابقة، فتكتسب إرادة الجاني الصفة الجرمية من العمل غير المشروع الذي يبين الشبه في ارتكابه وهو عالم بالآثار الضارة الناشئة عنه.[1]

يختلف الركن المعنوي في الجرائم المعلوماتية من جريمة إلى أخرى، فجريمة الدخول غير المصرح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة باعتبار حماية المشرع لمحل الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطا أو سهوا ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي.[2]

وفي جريمة الاحتيال الإلكتروني التي بدورها جريمة عمدية ، يتطلب المشرع قصدا جنائيا لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع.[3]

[1] خالد عياد الحلبي ، المرجع السابق ، ص 73،74.

[2] حنان ريحان مبارك المضحاكي ، المرجع السابق، ص107.

[3] احمد خليفة الملط ، المرجع السابق ، ص113-121.

المبحث الثاني: مفهوم التحقيق الجنائي في الجريمة الإلكترونية

للتحقيق أهمية في إثبات وقوع الجرائم وإقامة الدليل على مرتكبيها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل عليه اسمه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة، ومن يقوم بالتحقيق هم الضبطية القضائية وقضاة وفق إجراءات البحث و التحري المحددة وفقا لقانون الإجراءات الجزائية.

وعليه سنعالج هذا المبحث ضمن مطالبين، نتناول في المطلب الأول الأجهزة المكلفة بالبحث و التحري عن الجرائم الإلكترونية، وخصائص التحقيق و المحقق في الجرائم الإلكترونية والدليل المناسب للإثبات فيها في المطلب الثاني.

المطلب الأول: الأجهزة المكلفة بالبحث والتحري عن الجرائم الإلكترونية

يمكن القول أن المحقق هو من يتولى التحقيق من رجال الضبطية القضائية، أو من أعضاء النيابة العامة، أو قضاة التحقيق ويلحق بالمحقق الجنائي الباحث الجنائي الذي يكون غالبا من الشرطية القضائية، الذين خول لهم القانون مهمة جمع الاستدلالات عن المشتبه بهم.

وسنحاول من خلال هذا المطلب استعراض ابرز الهيئات المختصة في مجال مكافحة الجرائم الإلكترونية، وسنتناول الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بفرع أول، إضافة لتلك الوحدات التابعة لسلك الامن الوطني في فرع ثان، وكذلك تلك التابعة لقيادة الدرك الوطني في فرع ثالث.

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

نص المشرع في المادة 13 من القانون 09-04[1] على ضرورة إنشاء هيئة ذات وظيفة تنسيقية، تعمل على اتخاذ الإجراءات اللازمة للوقاية من هذه الجرائم، وتتولى تنشيط وتنسيق عملية الوقاية من الجرائم الإلكترونية، وكذلك مصاحبة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي يجريها بشأن هذه الجرائم.

[1] المرسوم رقم 09-04 مؤرخ في 8 غشت 2009، يتضمن القواعد الخاصة من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ، الجريدة الرسمية العدد 47، بتاريخ 5 غشت 2009.

أولا: التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال

تعرف حسب أحكام المواد من 01 إلى 04 من القانون 09-04 بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر العاصمة.

ثانيا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

تنص المادة 14 من نفس القانون على انه "تتولى الهيئة المذكورة في المادة 13 خصوصا المهام التالية":

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها.
- مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال بما في ذلك تجميع المعلومات.
- تبادل المعلومات مع نظيرتها في الخارج قصد جمع المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.

ثالثا: اختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

بينت الفقرة 02 من المادة 04 من المرسوم الرئاسي 15-261 [1] المهام الأساسية التي تكلف بها الهيئة وهي على سبيل الحصر، الهدف منها هو الوقاية من الجرائم الإلكترونية ومكافحة هذه الأخيرة من خلال الإسهام في أعمال البحث والتحقيق ومد يد العون لمصالح الشرطة القضائية وابرز مهام هذه الهيئة هي[2]:

- اقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

[1] المرسوم الرئاسي رقم 15-261 مؤرخ في 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، بتاريخ 8 أكتوبر 2015.

[2] المرجع نفسه، ص 16،17.

- تنشيط وتنسيق عمليات الوقاية عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.
- مساعدة السلطة القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية .
- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماسة بأمن الدولة وذلك تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.
- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.
- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.
- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.
- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

الفرع الثاني: الوحدات التابعة لسلك الأمن الوطني والدرك الوطني

توجد لدى مديرية الأمن الوطني والدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام مجموعة من الوحدات نكرها منها:

أولا: الوحدات التابعة لسلك الأمن الوطني

تضع مديرية الأمن الوطني في إطار تجسيد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم وبالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في

مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات.[1]

وقد أنشأت المديرية العامة للأمن الوطني المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة، ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي، بالإضافة إلى أنه يوجد على مستوى مراكز الأمن الولائي فرق متخصصة ومهمتها التحقيق في الجرائم الإلكترونية تعمل بالتنسيق مع هذه المخابر.[2]

ثانيا: الوحدات التابعة للدرك الوطني الجزائري

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام ومحاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية نذكر منها:[3]

- المصالح والمراكز العلمية والتقنية.
- هياكل التكوين.
- المصلحة المركزية للتحريات الجنائية.
- المعهد الوطني لعلم الإجرام.

يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، وإنجاز المقاربات الهاتفية، وتحسين التسجيلات الصوتية و الفيديو و الصورة و ذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومية للدرك الوطني وهو قيد الإنشاء.[4]

---

[1] ربيعي حسين، المرجع السابق، ص176.

[2] سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013، ص107.

[3] ربيعي حسين، المرجع السابق، ص182،183.

[4] سعيد علي نعيم، المرجع السابق، ص107.

المطلب الثاني: خصائص التحقيق والمحقق في الجرائم الإلكترونية والدليل المناسب للإثباتها

إذا كان التحقيق يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته وسرعة البديهة لديه وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا تطويرا لأساليبه وتكليف جهات مختصة لممارسته من أجل مواكبة حركة الجريمة وتطور أساليب ارتكابها في هذه البيئة

الفرع الأول: خصائص التحقيق والمحقق في الجرائم الإلكترونية

تعد مرحلة التحقيق مرحلة هامة في سبيل البحث والتحري عن الجرائم، وتبلغ هذه المرحلة أعلى مستوياتها عندما يتعلق الأمر بالجريمة الإلكترونية، لأنها تعد حجر الزاوية الذي سيتم علي أساسه مباشرة الدعوى، فما يتم جمعه من معلومات وأدلة رقمية الكترونية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبقى متاحا بعد مرور وقت قصير على ارتكابها والسبب في ذلك يعود إلى الطبيعة التقنية لهذه الجرائم.

أولا: خصائص التحقيق في الجريمة الإلكترونية

التحقيق الجنائي عموما هو علم يخضع لما يخضع له سائر أنواع العلوم الأخرى، فله قواعد ثابتة و راسخة بدونها ما كان ليتمتع التحقيق بتلك الصفة وهذه القواعد إما قانونية و إما فنية، فالأولى لها صفة الثبات التشريعي لا يملك المحقق إزاءها شيئا سوى الخضوع والامتثال أما الثانية فتتميز بالمرونة التي يضفي عليها المحقق من خبرته وفطنته ومهارته الكثير.[1]

1- تعريف التحقيق

عرف بمعناه العام أنه: اتخاذ جميع الإجراءات و الوسائل المشروعة التي توصل إلى كشف الحقيقة وإظهارها.[2]

---

[1] خالد محمود إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، مصر، 2009، ص56.

[2] عمر بن إبراهيم بن حماد العمري، إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، رسالة ماجستير جامعة نيف العربية، 2007، ص22.

وكذلك عرف التحقيق بأنه مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق، طبقا للشروط والأوضاع التي يحددها القانون، بهدف البحث عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة ارتكبت لتقدير لزوم محاكمة المدعى عليه أو عدم لزومها.[1]

أوهو دراسة مسائل أو ظواهر بالاستناد على شهادات أومعلومات.[2]

2- تعريف التحقيق في الجريمة الإلكترونية

يمكن تعريفه بأنه: عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجرائم الإلكترونية الرقمية من فاعل ودليل الكتروني رقمي لتقديمه إلى السلطات التحقيق القضائي في هذه الجرائم لإقامة العدل[3].

ثانيا: خصائص المحقق في الجريمة الإلكترونية

أمام التطور التقني والتكنولوجي الذي صاحب الجريمة المعلوماتية ،فإن المتخصصين بالتحقيق في هذا النوع من الجرائم المستحدثة يختلفون عن أولائك المختصين بضبط الجرائم التقليدية من حيث الخصائص وطريقة التكوين، ذلك أن التحقيق في هذه الجرائم لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية وإنما يعتمد على البناء العلمي والتكنولوجي وهم يتولون مهمة البحث والتحري عن الجرائم المعلوماتية وكشف النقاب عنها.

1- تعريف المحقق

هو الشخص القائم بأعمال إجراءات التحقيق الجنائي، وعرف أيضا أنه كل من عهد إليه القانون بتحري التحقيق في البلاغات و الحوادث الجنائية، ويساهم بدوره في كشف غموضها وصولا إلى معرفة حقيقة الحادث وكشف مرتكبه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة.[4]

---

[1] عمر بن إبراهيم بن حماد العمري، المرجع السابق، ص 23.

[2] Hachette, le dictionnaire pratique du français, imprimé en France, Imprimerie hérissey , Évreux (Eure) N°2896 , Collection N°25 Edition N02, 1983, p600.

[3] مصطفى محمود موسى، المرجع السابق، ص 166 .

[4] خالد محمود إبراهيم، المرجع السابق، ص 86.

وعرف أيضا بأنه: كل شخص يقوم بعمل من أعمال التحقيق، سواء بصورة أصلية أو بصورة استثنائية، يقوم بهذه الأعمال بناء على تخويل مباشر من قبل المشرع، أو بصورة غير مباشرة بناء على ندب أو تكليف من جهة لها الاختصاص الأصيل و الأساسي وفي نطاق الإجراء الذي تم تخويلهم القيام به.[1]

2- تعريف المحقق في الجرائم الإلكترونية

المحقق الجنائي في الجريمة الإلكترونية هو المكلف بالبحث عن الحقيقة في الجريمة الإلكترونية، والكشف عن مرتكبيها وتجميع أدلة الإدانة أو البراءة ضدهم لإحالتهم للقضاء، فالمحقق هو المكلف بتنفيذ إجراءات القانون المطبق، كل حسب اختصاصه.[2]

3- الخصائص الفنية للمحقق

يجب أن تتوافر بعض الأمور في المحقق ليقوم بعمله على أحسن وجه:[3]

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

- وصول الاخبارات و البلاغات عن الجرائم الواقعة على الحاسوب والانترنت من الفنيين الذين يعملون على هذه الأجهزة.

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

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

- البحث عن الأدوات المستخدمة في ارتكاب الجريمة وطرق الدخول إلى البرامج المخزنة وكيفية الحصول على الأرقام السرية والشفرات التي تمكنهم من الدخول إلى الحاسوب.

---

[1] محمود حماد مرهج الهيني، أصول البحث والتحقيق الجنائي، دار الكتاب القانونية، القاهرة، مصر، 2014، ص123.

[2] مصطفى محمود موسى، المرجع السابق، ص 253 .

[3] خالد عياد الحلبي، المرجع السابق ، ص 183،184.

– وضع خطة عمل مع جميع أعضاء فريق التحقيق، والتشاور معهم لمعرفة جميع الجوانب الفنية للجريمة التي يجري التحقيق بشأنها.

الفرع الثاني: دليل الإثبات في الجريمة الإلكترونية

يختلف الوسط الذي ترتكب فيه الجريمة المعلوماتية من وسط مادي إلى وسط معنوي (الوسط الافتراضي)، مما أدى إلى ظهور أدلة جنائية خاصة يمكن الاعتماد عليها في الإثبات، بحيث تكون من ذات الطبيعة التقنية الناجمة عن النظم الإلكتروني التي تنتج منها في حالة الاعتداء عليها، وتتفق مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهي الأدلة الرقمية أو الإلكترونية حسب ما عبرت عنها الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية.[1]

أولا: تعريف الدليل الإلكتروني

عرفته المنظمة العالمية لدليل الحاسوب في قرار لها في أكتوبر 2001 بأنه: المعلومات ذات القيمة المحملة والمخزنة أو المنقولة في صورة رقمية، وكانت قد عرفته في مارس 2000 بأنه: المعلومات المخزنة أو المنقولة والتي يمكن الاعتماد عليها أمام المحكمة.[2]

كذلك عرف الدليل الإلكتروني بأنه: الدليل الذي يجد أساسا له في العالم الافتراضي ويقود إلى الجريمة وهو كدليل بيانات يمكن إعدادها أو تخزينها بشكل إلكتروني، وعرف كذلك بأنه معلومات يقبلها العقل والمنطق ويعتمدها العلم، يتم الحصول عليها بإجراءات علمية وقانونية، بترجمة المعلومات والبيانات المخزنة في الحاسوب وملحقاته وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة.[3]

[1] سعيداني نعيم ، المرجع السابق، ص 119.

[2] مصطفى محمود موسى، المرجع السابق، ص 213.

[3] خالد عياد الحلبي، المرجع السابق، ص .230

وكذلك عرفه الفقه بأنه الدليل الذي يتم الحصول عليه بواسطة التقنية الإلكترونية من الحاسوب وشبكة الانترنت، والأجهزة الإلكترونية الملحقة والمتصلة به، وشبكات الاتصال من خلال إجراءات قانونية، لتقديمها للقضاء كدليل إلكتروني جنائي يصلح لإثبات الجريمة.[1]

ويعرف أيضا بأنه: الدليل المأخوذ من أجهزة الحاسوب ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور والأصوات والأشكال والرسوم ، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه وبشكل قانوني يمكن الأخذ به أمام أجهزة تنفيذ وتطبيق القانون.[2]

ثانيا: أشكال الدليل الإلكتروني

ليس للدليل الرقمي صورة واحدة بل يوجد له العديد من الصور والأشكال نذكر منها على سبيل المثال:

1- الصورة الرقمية:

هي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية والصورة الرقمية تمثل تكنولوجيا بديل للصورة التقليدية.[3]

2- النصوص المكتوبة:

وتشمل الأوراق التحضيرية التي يتم إعدادها بخط اليد كمسودة أو تصور العملية التي يتم برمجتها، وكذلك نصوص أساسية وقانونية محفوظة في الملفات العادية وتكون لها علاقة بالجريمة[4].

[1] المرجع نفسه، ص 231.

[2] محمود عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتاب القانونية، مصر، 2006، ص 88.

[3] سعيداني نعيم، المرجع السابق، ص 127.

[4] محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، دار الجامعة ، عمان، 2014، ص 117.

3- التسجيلات الصوتية:

وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلة الرقمية، وتشمل المحادثات الصوتية على الانترنت.[1]

ثالثا: أنواع الدليل الالكتروني

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

1- أدلة أعدت لتكون وسيلة إثبات:

وهي السجلات التي تم إنشاؤها بواسطة الجهاز تلقائيا، وتعتبر هذه السجلات من مخرجات الجهاز ولم يساهم الانسان في إنشائها، وكذلك السجلات التي تم حفظ جزء منها بالإدخال وجزء تم انشاؤه بواسطة الجهاز. [2]

2- أدلة لم تُعَد لتكون وسيلة إثبات:

هذا النوع من الأدلة الإلكترونية نشأ دون إرادة الفرد، وله أثر يتركه الجاني دون أن يكون راغبا في وجوده ويسمى بالبصمة الإلكترونية وتتجسد في الآثار التي يتركها مستخدم شبكة الانترنت بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الحاسوب أو شبكة الانترنت.[3]

[1] سعيداني نعيم ، المرجع السابق، ص 128.

[2] سعيداني نعيم ، المرجع السابق، ص 128، 129.

[3] خالد عياد الحلبي، المرجع السابق ، 235، 236.

الفصل الثاني: القواعد الإجرائية في استخلاص الدليل الالكتروني والقيمة القانونية له

إن طبيعة الجرائم الإلكترونية بعناصرها ووسائل ارتكابها، قد تدفع المشرع الجزائي إلى إعادة النظر في كثير من المسائل الجزائية، خاصة فيما يتعلق بمسألة الإثبات، ذلك أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لا بد أن يكون من طبيعة إلكترونية، وهو الأمر الذي يقودنا إلى الحديث عن مسألة قبول هذا الدليل أمام القضاء ومدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التزييف والأخطاء، وكذا مصداقيته ومشروعيته فإن الأمر لا يتوقف عند هذا الحد، بل يتجاوزه إلى مسألة تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية للسلطة التقديرية للقاضي إعمالا لمبدأ السلطة التقديرية للقاضي الجزائي الذي يشكل جوهر أي حكم، وعليه قسمنا هذا الفصل إلى مبحثين، المبحث الأول تحت عنوان القيمة القانونية للدليل الالكتروني في مجال الإثبات الجنائي، أما المبحث الثاني فيتمثل في القواعد الإجرائية في استخلاص الدليل الإلكتروني.

المبحث الأول: القواعد الإجرائية في استخلاص الدليل الإلكتروني

إن التطور التقني الذي لحق نظام المعالجة الآلية فضلا عن الطبيعة الخاصة للدليل الرقمي سيؤدي حتما إلى تغيير كثير من المفاهيم السائدة حول إجراءات وطرق الحصول عليها، وهو الأمر الذي يحتاج بالضرورة إلى إعادة تقييم منهج بعض الإجراءات التقليدية في قانون الإجراءات الجزائية، فضلا عن استحداث قواعد إجرائية أخرى تتلاءم مع طبيعة البيئة التقنية، فتطور الإثبات ووسائله أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم، وهو الأمر الذي سوف نعالجه من حيث بحث القواعد الإجرائية التقليدية، وإلى أي مدى يمكن الاستناد إليها في الحصول على الدليل الرقمي في المطلب الأول، ثم نعرج إلى القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني وصعوبات التحقيق في الجريمة الإلكترونية في المطلب الثاني.

المطلب الأول: القواعد الإجرائية التقليدية في استخلاص الدليل الالكتروني

مما لاشك فيه أن المشرع لم يجز استخلاص الدليل من غير ضوابط تحكم ذلك عن طريق قواعد إجرائية معينة أهمها التفتيش، وضبط الأشياء والخبرة، إن هذه القواعد عامة النطاق تنظم استخلاص الدليل في جميع الجرائم، تقليدية كانت أو مستحدثة إلا أنها في الثانية قد تكون بحاجة إلى تطوير لكي تتناسب مع خصوصيتها وطبيعة الدليل الذي يصلح لإثبات الجريمة الإلكترونية.

الفرع الأول: التفتيش

يمكن تعريف التفتيش بصفة عامة أنه: ذلك الإجراء الذي يدخل ضمن إجراءات التحقيق الابتدائي أو القضائي، ولا يمكن أن يقوم به سوى النيابة العامة و قاضي التحقيق، عن طريق أمر ندب أحد مأموري الضبط القضائي المختص بإجرائه، والغرض منه هو البحث عن أدلة الإثبات للجريمة المرتكبة، وكل ما يفيد للوصول إلى الحقيقة في متابعة أي شخص يشتبه أنه مرتكب الجريمة.[1]

[1] بلعليات إبراهيم ، المرجع السابق ، ص 214.

أولا: القواعد الموضوعية لتفتيش أنظمة الحاسوب

وتلخص هذه القواعد كالآتي:[1]

– وقوع جريمة إلكترونية.

– ارتكاب شخص أو أشخاص معينين لإحدى الجرائم الإلكترونية أو الاشتراك فيها.

– توافر أدلة قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية أو إلكترونية تفيد في كشف الحقيقة.

– أن يكون محل التفتيش هو الحاسوب بكل مكوناته المادية والمعنوية وشبكات الاتصال الخاصة به.

ثانيا: القواعد الشكلية لتفتيش نظام الحاسوب

وتتضمن عدة قواعد نذكرها كما يلي:[2]

– أن يتم بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة.

– أن يكون أمر التفتيش مسببا.

– تكوين فريق تفتيش يتضمن خبراء وفنيين متخصصين بالحاسوب والأنظمة الإلكترونية بالإضافة إلى رجال الشرطة المتخصصين بالحماية و الأمن.

الفرع الثاني: استخلاص الدليل في الجريمة الإلكترونية

الضبط والاستخلاص هو العثور على أدلة إثبات الجريمة التي يباشر التحقيق بشأنها والتحفظ عليها، والضبط هو الغاية من التفتيش ونتيجته المباشرة، ولذلك يتعين عند إجرائه أن تتوفر فيه نفس القواعد التي تطبق على التفتيش.[3]

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، الطبعة الأولى، دار الفكر الجامعي 2006، ص 385،386.

[2] خالد عياد الحلبي، المرجع السابق، ص154،155.

[3] مصطفى محمود موسى ، المرجع السابق ، ص208.

الضبط يعني أيضا وضع اليد على أي شيء يتصل بالجريمة التي وقعت من أجل الكشف عن الحقيقة وعن مرتكبيها، والهدف الذي تسعى إليه سلطة التحقيق من أجل القيام بالتفتيش، وهو ضبط الأدلة و الوثائق والأشياء التي تفيد في الكشف عن الجريمة، لذلك ينبغي التقيّد بالقواعد الإجرائية التي تحدد الأماكن التي يجوز تفتيشها والأشخاص الذين يجري تفتيشهم.[1]

أولا: مدى صلاحية الضبط في الجريمة الإلكترونية

محل الضبط يكون بطبيعته وبحسب تنظيمه القانوني وغايته، لا يرد إلا على الأشياء أما الأشخاص فلا يصلحون ليكونوا محلا للضبط بالمعنى الدقيق إلا في حدود الاستثناءات الإجرائية، وإذا كانت بعض القوانين تتحدث عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف تماما عن ضبط الأشياء، نظرا لكون الضبط محلا في مجال الجريمة الإلكترونية، والبيانات المعالجة الكترونيا[2] فقد ثار التساؤل هل يصلح هذا النوع من البيانات أن يكون محلا للضبط وهو وضع اليد على شيء مادي ملموس؟

انقسم الفقه إلى اتجاهين يرى البعض أن بيانات الحاسوب لا تصلح أن تكون محلا للضبط، لانتفاء الكيان المادي عنها ولا سبيل لضبطها، إلا بعد نقلها على كيان مادي ملموس ويستند هذا الرأي إلى أن النصوص التشريعية المتعلقة بالضبط يكون محل تطبيقها الأشياء المادية الملموسة، ويرى اتجاه ثاني أن البيانات المعالجة إلكترونيا ما هي إلا ذبذبات الكترونية أو موجات كهرومغناطيسية قابل للتسجيل والحفظ والتخزين على وسائط مادية وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره.[3]

ثانيا: الأشياء محل الضبط في الجريمة الإلكترونية

الأشياء التي يتم ضبطها في مجال الجرائم الإلكترونية والتي لها قيمة في الإثبات هي:[4]

- ضبط جهاز الحاسوب وملحقاته.

---

[1] خالد عياد الحلبي، المرجع السابق، ص 168.

[2] سعيداني نعيم، المرجع السابق، ص 159.

[3] خالد عياد الحلبي، المرجع السابق، ص 171.

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

– ضبط المعدات المستعملة في شبكة الانترنت.

– ضبط وسائط التخزين المتحركة كالأقراص المدمجة، والأقراص المرنة، والأشرطة المغناطيسية.

– ضبط البرمجيات

– ضبط البريد الإلكتروني والذي قد يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الرسائل الإلكترونية.

ثالثا : الصعوبات التي تواجه عملية الضبط

عملية ضبط البيانات المعالجة إلكترونيا تواجهها عدة صعوبات منها:[1]

– حجم الشبكة التي تحتوي على المعلومات المعالجة الكترونيا والمطلوب ضبطها.

– وجود بيانات في شبكات أو أجهزة تابعة لدولة أجنبية.

– يشمل التفتيش و الضبط أحيانا اعتداء على حقوق الغير، أو على حرمة حياتهم الخاصة، فيجب اتخاذ الضمانات اللازمة لحماية هذه الحقوق والحريات.

الفرع الثاني: الخبرة في إثبات الجريمة الإلكترونية

تعتبر الاستعانة بالخبراء من بين الإجراءات التي يلجا إليه القضاء وسلطات التحقيق على حد سواء ، وذلك كل ما استعصى عليهم الأمر ، ومن بين هذه المجالات التي تستدعي اللجوء إلى الخبرة نجد الجريمة الإلكترونية، حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا شخص ذو دراية وخبرة في مجال الإلكترونيات.[2]

[1] خالد عياد الحلبي، المرجع السابق، ص 172

[2] صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير ، جامعة مولود معمري ، تيزي وزو ، كلية الحقوق والعلوم السياسية ، 2013، ص 87.

أولا: أنواع الخبراء الإلكترونيون.

الخبير في الجريمة الإلكترونية: هو الفني المتخصص وصاحب الخبرة في التقنية الإلكترونية وشبكاتها، والذي يكون قد رأى أو سمع أو أدرك بحواسه معلومات هامة لازمة للدخول في نضام المعالجة الآلية الرقمية للبيانات، إذا كانت مصلحة التحقيق تقتضي البحث عن الدليل الرقمي الإلكتروني داخله ويتمثل الخبراء الإلكترونيون في مايلي:[1]

- المبرمجون.
- المحلل هو الشخص الذي يضع خطوات العمل ويقوم بتجميع بيانات نظام معين.
- مهندس الصيانة والاتصالات.
- مشغل الحاسوب الآلي وشبكاته.
- مدير النظام المعلوماتي.

ثانيا: أهمية الخبرة في البحث عن الدليل الإلكتروني

تكمن أهمية الخبرة في الأدلة التي تقدمها لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجزائية، لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة في المواد 143 الى 156 من قانون الإجراءات الجزائية، واعتبرها من إجراءات البحث عن الدليل حيث نصت المادة 143: على أنه لجهات التحقيق أو الحكم عندما تعرض لها مسالة ذات طابع فنّي أن تأمر بندب خبير إما من تلقاء نفسها أو بناء على طلب من النيابة العامة وإما بطلب من الخصوم.[2]

وتكمن أهمية الخبرة في مجال البحث عن الدليل الإلكتروني في أنها وسيلة من وسائل الإثبات التى تهدف إلى كشف بعض الدلائل، أو تحديد مدلولها بالاستعانة بالمعلومات العلمية

[1] مصطفى محمود موسى، المرجع السابق، ص172.

[2] قانون رقم 66-155 مؤرخ في 08 يونيو 1966 المعدل و المتمم لقانون الإجراءات الجزائية، الجريدة الرسمية العدد 48، المعدل و المتمم للأمر رقم 15-02 مؤرخ في 23 جويلية 2015، الجريدة الرسمية العدد 40، و المعدل و المتمم بالأمر 17-02.

وهي البحث في مسائل مادية أو فنّية يصعب على المحقق أن يبحث فيها، ويعجز عن جمع الأدلة بالوسائل الأخرى للإثبات.[1]

تبرز أهمية الاستعانة بالخبرة في مجال الجرائم الإلكترونية، في أنه عند غيبها تعجز الضبطية القضائية في كشف غموض الجريمة لنقص الكفاءة و التخصص اللازمين للتعامل مع الجوانب التقنية و التكنولوجية التي ارتكبت بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل والإهمال عند التعامل معه.[2]

ولعل هذه الأهمية للخبرة في مجال التحقيق في الجريمة الإلكترونية جعل بعض التشريعات لا تكتف بالنصوص التقليدية التي تنظم الخبرة، وعمدت إلى إدراج نصوص قانونية خاصة تنظم الخبرة في هذا المجال، ونجد أن المشرع الجزائري أشار في المادة 05 الفقرة الأخيرة من القانون رقم 09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه:"يمكن للسلطة المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدابير المتخذة لحماية المعطيات التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

المطلب الثاني: القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني وصعوبات التحقيق في الجريمة الإلكترونية

كان لتطور أساليب ارتكاب الجريمة الإلكترونية منحى تصاعدي بين الجرائم المرتكبة في الجزائر، أي فرض على المشرع الاعتماد على قواعد إجرائية خاصة في سبيل مكافحة الجريمة الإلكترونية وهو ما جاء به القانون 06-22 المؤرخ في ديسمبر 2006 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 يوليو 1966 والمتضمن لقانون الإجراءات الجزائية.

[1] صغير يوسف، المرجع السابق، ص 89.

[2] مصطفى محمود موسى، المرجع السابق، ص 222.

الفرع الأول: القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني

نـص المشرع الجزئري على إجراءات خاصة تهدف إلى ضبط الأدلة في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وبعض الجرائم الأخرى، وتتمثل هذه الإجراءات في التسرب واعتراض المراسلات وكذلك من خلال القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، استحداث إجراءين آخرين هما المراقبة الإلكترونية وحفظ المعطيات.[1]

أولا: التسرب (الاختراق) واعتراض المراسلات.

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

1- التسرب (الاختراق)

نضم المشرع الجزائري أحكام التسرب في الفصل الخامس من قانون الإجراءات الجزائية من المادة 65 مكرر 11 إلى مكرر 18 ، حيث بين كيفية القيام بعملية التسرب وكذا شروط القيام بهذا الإجراء، وكذلك الأحكام الجزائية لمن تسبب في الكشف عن هوية الضابط أو العون المتسرب، ويتم الاستماع إلى الضابط المتسرب بوصفه شاهدا عن الجرائم المرتكبة بعد انتهاء المهلة المحددة في رخصة التسرب.

أ- مفهوم التسرب:

المقصود بالتسرب: هو قيام ضابط أو عون الشرطة القضائية بمراقبة الاشخاص المشتبه في أنهم ارتكبوا الجريمة بإظهار أنه مساهم معهم أو شريك، بحيث يستعمل الضابط أو العون هوية مستعارة وذلك إذا ما ارتبط البحث والتحري واحدة من الجرائم التالية:

- جرائم المخدرات.
- الجريمة المنظمة العابرة للحدود الوطنية.
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

[1] معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري و التشريع المقارن، مذكرة ماجستير جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2011-2012، ص106.

- جرائم تبييض الأموال.
- الجرائم الموصوفة بأفعال إرهابية أو تخريبية.
- الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد.[1]

ب- طرق التسرب في مجال الجريمة المعلوماتية:

يمكن تصور عملية التسرب في نطاق الجرائم الإلكترونية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي، وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها أو اشتراكه في محادثات في غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم، والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما في ذلك أسماء أو صفات هيئات مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام المخترق للمواقع، أو كيفية ارتكاب الجرائم وحتى المشاركة معهم في ارتكابها لتجميع كل ما يمكن جمعه من الأدلة.[2]

2- اعتراض المراسلات السلكية واللاسلكية

أ- مفهوم اعتراض المراسلات

استحدث بموجب المادة 65 مكرر إلى65 مكرر10 من قانون الإجراءات الجزائية، إمكانية قاضي التحقيق أن يأمر ضابط الشرطة القضائية بترخيص كتابي وتحت إشرافه مباشرة للقيام باعتراض المراسلات التي تتم عن طريق وسائل الاتصالات السلكية واللاسلكية ، ووضع الترتيبات التقنية دون موافقة الشخص المعني من اجل القيام بالتقاط وتثبيت وتسجيل وبحث فيسرية وفي أي مكان عام أو خاص والتقاط الصور لأي شخص.

إن مقتضيات المادة ليست مطلقة بل ترد عليها بعض الاستثناءات عن طريق تشريع قواعد إجرائية، تنص على تقييد هذه الحرية من أجل الحفاظ على المصلحة العامة للمجتمع وأمنه وسلامته، وهذا لحسن سير التحريات والتحقيقات القضائية، بحيث منح حق اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع ترتيبات تقنية دون

[1] المادة 65 مكرر 12 من قانون الإجراءات الجزائية، المرجع السابق.

[2] سعيداني نعيم، المرجع السابق، ص177,

مراقبة المعنيين من أجل التقاط الصور وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن عامة أو خاصة.[1]

في المادة 619 من القانون 00-03 المؤرخ في 05 سبتمبر 2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات، اعتبر أن مادة المواصلات هي كل اتصال مجسد في شكل كتابي يتم عبر كافة الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، ولا تعتبر الكتب والجرائد والمجلات واليوميات كمادة مراسلات.[2]

إلا أنه بالرجوع إلى نص المادة 39 من الدستور الجزائري التي تنص: على أن سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة، ولذلك نصت المدة 303 من قانون العقوبات التي تعاقب كل من يفضح أو يتلف رسائل أو مراسلات موجهة للغير[3]، إذا يمكن التوصل للقول بان المراسلات الخاصة تعني كل رسالة مكتوبة بأي شكل من الأشكال سواء مادية أو إلكترونية وسواء كانت على دعامة ورقية أو رقمية، مرسلة بأي وسيلة لعدد معين ومحدد من المرسل إلى المرسل إليهم، باستثناء الكتب والمجلات والجرائد والدوريات التي لا تعتبر مراسلات خاصة.

وهذا ما جاء به القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها في المادة 2 الفقرة "و" في تعريفه للاتصالات الإلكترونية: على أنها تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور او أصوات أو معلومات مختلفة بأي وسيلة كانت.

وتجدر الإشارة في هذا الصدد إلى أن المراسلات التي يمكن اعتراضها يجب أن تتسم بالخصوصية ولكي تكون كذلك يلزم أن يتوافر فيها عنصران أساسيان هما:[4]

---

[1] قادري سارة، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماجستير ، جامعة قاصدي مرباح ، ورقلة ، كلية الحقوق والعلوم السياسية ، قسم الحقوق، 2013- 2014، ص 27.

[2] قانون رقم 00-03 مؤرخ في 5 غشت 2000 المحدد للقواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية، الجريدة الرسمية العدد 48، بتاريخ 6 غشت 2000.

[3] القانون رقم 16-01، مؤرخ في 6 مارس 2016 المتضمن الدستور الجزائري، الجريدة الرسمية العدد 63، بتاريخ مارس 2016.

[4] سعيداني نعيم ، المرجع السابق ، ص 179.

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

-عنصر شخصي والمراد به إرادة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون الرسالة.

وعند توفر هذان العنصران في الرسالة فإنها تتصف بالمراسلة الخاصة التي لها خصوصيتها وسريتها المحمية قانونا ولا أهمية لشكل الرسالة أو طريق نقلها وتوصيلها إلى المرسل إليه.

لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي.

ب- طرق اعتراض المراسلات الإلكترونية

يعتبر البريد الإلكتروني أهم وسيلة تقنية في مجال التراسل الالكتروني ومن ثمة فعملية الاعتراض تنصب عليه، ومن المعلوم أن كل رسالة إلكترونية تظهر فيها معلومات عامة مثل تاريخ إنشاء الرسالة وتاريخ تلقيها وكذا عنوان المرسل وعنوان المرسل إليه، وهذه المعلومات ليست كافية لمعرفة المرسل إذ بإمكان هذا الأخير إرسال رسائله من صناديق بريد مسجلة بأسماء وهمية، كما أن هناك وسائل تتيح للمرسل أن يرسل رسائله دون أن يظهر فيها عنوان بريده الإلكتروني الصحيح، لذلك لابد من الحصول على المزيد من المعلومات التي يمكن العثور عليها في حاشية رسائل البريد الالكتروني والتي يطلق عليها مصطلح Email Heade [1] والمعلومات التي تحتويها الحاشية هي عبارة عن معلومات تراكمية لمختلف الأجهزة الخادمة للبريد الإلكتروني التي مرت من خلالها الرسالة، ونجد أن حاشية المعلومات تتضمن أرقام IP [2] مختلفة تمثل أرقام خاصة بكل الأجهزة التي مرت بها الرسالة، وعادة ما يظهر رقمIP الخاص بمرسل الرسالة أمام عبارة x originating IP [3] ، وفي حالة عدم ظهور هذه العبارة فإن رقم IP

[1] Imail Header: صفحة تحتوي على عنوان IP لشركة البريد الالكتروني وعنوان IP الخاص ببريد الشخص مرسل الرسالة.

[2] IP هو عبارة عن رقم يمثل عنوان جهاز الحاسوب على الانترنت ويكون بهذا الشكل 192.168.1.1. وهو اختصار لكلمة Protocol Internet

[3] x originating IP صحة تحتوي على عناوينIP شركة البريد وIP الشخص مرسل الرسالة في شركة هوتمايل

الخاص لمرسل الرسالة يكون أمام آخر كلمة received [1] ، وتعد هذه المعلومات أساسية يمكن من خلالها الاستدلال على صاحب الرسالة ويصبح بعد ذلك من السهل الحصول على المزيد من المعلومات عن المرسل، وذلك بإدخال رقم IP في بعض المواقع أو البرامج التي تقوم بالكشف عن مصدر الرسالة والمكان الجغرافي التي أرسلت منه، وكذلك مزود الخدمة الذي يتعامل معه المرسل وبذلك يكون من السهل اعتراض المراسلات والإطلاع على محتواها دون علم مرسلها.[2]

ثانيا: المراقبة الإلكترونية وحفظ المعطيات

سوف نتناول بالشرح إجراءات المراقبة الإلكترونية فقط على اعتبار انه سبق الحديث عن حفظ المعطيات.

1- مفهوم الرقابة الإلكترونية للاتصالات

استحدث المشرع الجزائري إجراءات المراقبة الإلكترونية بموجب المادة 03 من القانون 09-04 الصادر بتاريخ 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها حينما أجاز تبعا لمستلزمات التحريات والتحقيقات القضائية الجارية في إظهار هذا النوع من الجرائم اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها[3]، غير أن المشرع الجزائري لم يتطرق إلى تحديد المقصود بمراقبة الاتصالات الإلكترونية واكتفى بتحديد مفهوم الاتصالات الإلكترونية وذلك في الفقرة "و"من المادة الأولى من نفس القانون.

من الواضح أن المشرع الجزائري لم يعتبر هذا الإجراء من ضمن طرق الحصول على الدليل الإلكتروني فقط بل أدرجه ضمن التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية، فإلى جانب القيام بإجراءات مراقبة الاتصالات الإلكترونية فإنه يمكن كذلك

[1] Received صحة تحتوي على عناوينIP شركة البريد وIP الشخص مرسل الرسالة في شركة ياهو

[2] سعيداني نعيم، المرجع السابق، ص 181 ، 182.

[3] المادة 03 من القانون09-04 :"مع مراعات الاحكام القانونية التي تضمن سرية المراسلات والاتصالات. يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات او التحقيقات القضائية الجارية ، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون ، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية."

تطوير هذه التقنية، لكي تعمل في بيئة الرقابة لغرض الوقاية من احتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة وهو ما أقرته المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

2- شروط المراقبة التقنية للاتصالات

اعتبر المشرع الجزائري المراقبة التقنية للاتصالات وسيلة إجرائية للحصول على الدليل في مجال الجريمة الإلكترونية بمجموعة من الشروط أهمها:[1]

- أن يتم تنفيذ هذا الإجراء تحت سلطة القضاء وبإذن منه، وهو ما أكدته المادة 04 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها بنصها على أنه:" لا يجوز إجراء عملية المراقبة إلا بإذن من السلطة القضائية المختصة".

- أن تكون هناك ضرورة تتطلب هذا الإجراء، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري والتحقيق دون اللجوء الى المراقبة الإلكترونية، وهو ما أكد عليه المشرع في المادة 4 الفقرة "ج" من القانون 09-04 المتضمن القواعد الخاصة للوقاية من جرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

الفرع الثاني: معوقات و صعوبات التحقيق في الجريمة الإلكترونية

يتسم التحقيق في الجريمة الإلكترونية بالعديد من المعوقات والصعوبات التي تؤثر على عملية التحقيق التي تؤدي بها إلى الخروج بنتائج تنعكس على نفسية المحقق، بفقدانه الثقة في نفسه وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها أيضا على المجرم نفسه، حيث يشعر أن الجهات القضائية غير قادرة على اكتشاف أمره وأن خبرة القائمين على المكافحة والتحقيق، لا تجاري خبرته وعلمه الأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من الجرائم التي قد تكون أكثر فداحة وأشد ضررا على المجتمع.

[1] سعيداني نعيم ، المرجع السابق ، ص 185.

أولا: المعوقات المتعلقة بجهات التحقيق

توجد معوقات للتحقيق في الجريمة الإلكترونية تتعلق بالسلطة القائمة بالتحقيق وتجمع لعدة أسباب نذكرها كالآتي:

1- قلة خبرة القائمين بالتحقيق في هذه الجرائم

لقلة المهارات الفنية المطلوبة للتحقيق في هذا النوع من الجرائم ونقص المهارات في استخدام جهاز الحاسوب والانترنت، وعدم توافر المعرفة بأساليب ارتكاب الجرائم الإلكترونية، وقلة الخبرة في مجال التحقيق في جرائم الحاسوب والانترنت وقلة المعرفة باللغة الأجنبية لا سيما أن للعاملين في مجال الحاسوب مصطلحات عملية خاصة أصبحت تشكل الطابع المميز لمحادثاتهم وأساليب التفاهم بينهم، وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات.[1]

2- الصعوبات التقنية لاستخدام بروتوكول TCP / IP في الإثبات.

هناك تحديات عند استخدام المحقق بروتوكول **TCP/ IP** [2] كدليل الكتروني للإثبات وهي:[3]

- بروتوكول IP وحدة معلوماتية تحتوي على معلومات عن الحاسوب وليس عن الأشخاص، لذلك فمن الصعوبة إثبات أن شخصا محددا أحدث الفعل غير المشروع، ومع ذلك يمكن أن يستخدم كقرينة قضائية ضد مالك الجهاز إلى أن يثبت العكس.

- الجاني يعمد إلى استخدام عناوين ومعلومات غير صحيحة أو غير قانونية باستخدام حاسوبه الشخصي في ملف خدمات عامة لتجنب التعرف عليه، ويستخدم عنوان IP له مستخدمين كثر ويمكنهم استخدام نفس العنوان، وبعد مرور فترة زمنية يقوم بغلق الاتصال، وبعد فترة يعاود الاتصال مما يجعل النشاط الإجرامي غالبا مزعا على عدة عناوين.

---

[1] خالد ممدوح ابراهيم، المرجع السابق، ص 69.

[2] هو اختصار لكلمة Transmission Control Protocol بروتوكول التحكم في نقل البيلنات وكلمة Internet protocol بروتوكول TCP/IP هو العصب المحرك للانترنت يضم مجموعة بروتوكولات مطورة كطريق للتواصل بين مختلف أنواع الحواسيب.

[3] خالد عياد الحلبي ، المرجع السابق، ص 226.

– تكون المعلومات المحملة لمصدر عنوان IP غير حقيقية أو زائفة وهذا ممكن باستخدام مصدر زائف لمصدر عنوان IP بحيث يظهر بأن المعلومات جاءت من حاسوب محدد وفي الحقيقة جاءت من حاسوب آخر.

3– ارتفاع تكاليف جمع الأدلة

إن التحقيق في هذه الجرائم يحتاج إلى خبراء متخصصين وهؤلاء يحتاجون إلى دورات مستمرة متزامنة مع تطور التقنية الإلكترونية، وهذا الأمر مرتبط بتكاليف باهظة، وكذلك التفتيش عن الأدلة يحتاج إلى فحص آلاف الصفحات خصوصا عندما لا تثبت تلك الصفحات شيئا.

ثانيا: عوائق تتعلق بالجريمة والجهة المتضررة منها

المعوقات المتعلقة بالجريمة الإلكترونية تتمثل في:[1]

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

الجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في زمن قصير جدا بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعمل بها فإنه يستهدف بالمحو السريع عدم استطاعة السلطات إقامة الدليل ضده، وبالتالي تملصه من مسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسوب الآلي أو الشبكة أو في الأجهزة.

أما المعوقات المتعلقة بالجهات المتضررة من جرائم الحاسوب والانترنت، وهي عدم إدراك خطورة جرائم الحاسوب والانترنت من قبل المسئولين بالمؤسسات المجني عليها التي تعد من معوقات التحقيق، وكذلك إغفال الجانب الإرشادي للمستخدمين إلى خطورة الجرائم المتعلقة بالانترنت، وتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، وهذا يؤدي إلى الإحجام عن الإبلاغ عن الجريمة، التي تعتبر من أهم وأخطر الإشكالات التي تتعلق بعملية الإبلاغ عن

[1] خالد ممدوح ابراهيم ، المرجع السابق ،ص 65.

الجريمة الإلكترونية، حيث يحجم البعض عن إبلاغ السلطات المختصة بالجرائم التي ارتكبت بحقهم خاصة إذا تعلق الأمر بالمؤسسات المالية أو ما شابهها.[1]

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

البحث الثاني : القيمة القانونية للدليل الإلكتروني في مجال الإثبات الجنائي

لقد أثارت مسألة الدليل الرقمي الكثير من التساؤلات حول تعبيره أو عدم تعبيره عن الحقيقة، نظرا لما يمكن أن تخضع له طرق الحصول عليه من التزييف والتحريف والعبث، وهو ما يثير مسألة مشروعية الأخذ به، إذ يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا من حيث وجوده ومن حيث الحصول عليه.

إن مجرد وجود دليل يثبت وقوع الجريمة ونسبيتها إلى شخص معين لا يكفي أن يكون دليل إثبات، إذ يجب أن تكون لهذه الأدلة قيمة قانونية وقيمة الدليل الجنائي تتوقف على مسألتين رئيسيتين الأولى مشروعية الدليل والثانية هي حجية الدليل على المراد إثباته.

المطلب الأول : مشروعية الدليل الإلكتروني

تعرف المشروعية بأنها التوافق والتقيد بأحكام القانون في إطاره ومضمونها العام، فهي تهدف إلى تقرير ضمانة أساسية وجدية للأفراد لحماية حريتهم وحقوقهم الشخصية ضد تعسف السلطة ومن التطاول عليها في غير الحالات التي رخص فيها القانون بذلك من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته.[1]

لذلك فإنه لصحة الإجراءات التي تقوم بها جهة التحقيق أن لا تخل بمبدأ المشروعية من أجل أن الحصول على دليل صحيح وسليم يستند عليه القضاء في أحكامه والحقيقة أن مشروعية الدليل الإلكتروني هي مشروعية الوجود ومشروعية الحصول.

الفرع الأول: مشروعية وجود الدليل الإلكتروني

تقتضي مشروعية وجود الدليل الإلكتروني أن يكون المشرع قد قبل هذا الدليل ضمن أدلة الإثبات الجنائي.

يقصد بمشروعية الوجود أن يكون الدليل معترفا به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إليه والاستدلال به لتكوين عقيدته وقناعته للحكم بالإدانة أو البراءة، ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول

[1] هلال عبد الله محمد، حجية مخرجات الكمبيوتر في المواد الجنائية، الطبعة الثانية، دار النهضة العربية ، مصر، 2008 ص104.

الدليل الإلكترونية، تتمثل في طبيعة نظام الإثبات السائد في الدولة إذ يختلف النظام القانوني في موقفها من حيث الأدلة التي يمكن قبولها في الإثبات،[1]وهناك اتجاهان رئيسيان الاتجاه الأول هو نظام الأدلة القانونية، أما الاتجاه الثاني فهو نظام الإثبات الحر.

أولا: أنظمة الإثبات المقيد

فيه يقوم المشرع بتحديد أدلة الإثبات حصرا، وكذا القوة الثبوتية لكل دليل من أدلة الإثبات بناء على قناعته، وهو ما يعرف بنظام الأدلة القانونية، إذ لا يكون لقناعة القاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، إذ تحدد للقاضي الأدلة التي يجوز له قبولها واللجوء اليها في الإثبات ولا سبيل لإنشاء أي دليل لم ينص عليه القانون صراحة ضمن أدلة الإثبات.[2]

ثانيا: نظام الإثبات الحر

وفقا لهذا النظام يتمتع القاضي الجنائي بحرية مطلقة في شأن إثبات الوقائع المعروضة عليه، فلا يلزمه القانون بأدلة للاستناد إليها في تكوين قناعته، فله أن يبني هذه القناعة على أي دليل وإن لم يكن منصوصا عليه، وكل الأدلة تتساوى قيمتها في الإثبات في نظر المشرع، والقاضي هو الذي يختار من بين ما يطرح عليه ما يراه صالحا للوصول إلى الحقيقة، وهو في ذلك يتمتع بمطلق الحرية لقبول الدليل أو رفضه إذا لم يقتنع به، فالمشرع لا يتدخل في تحديد القيمة الإقناعية للدليل، فعلى الرغم من توفر شرط الصحة في الدليل إلا أن القاضي يملك أن يرده تحت مبرر عدم الاقتناع، ولذلك فالقاضي في مثل هذا النظام يتمتع بدور إيجابي في هذا النظام.

الفرع الثاني: مشروعية الحصول على الدليل الالكتروني

من الضروري أن يتم رسم ضوابط و أطر معينة، يتعين أن تمارس في نطاقها عملية البحث عن الأدلة وتحصيلها والتحقيق فيها، بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع

[1] خالد عياد الحلبي ، المرجع السابق، ص 235، 236.

[2] شيماء عبد الغني، محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2007، ص 435، 436.

من ورائه، وهو الوصول الى الحقيقة الفعلية في الدعوى وهي الهدف الاسمى لقانون الإجراءات الجزائية.

ويعني مبدأ مشروعية الحصول على الدليل الإلكتروني بما يتضمنه من مفاهيم الكترونية، ضرورة اتفاق الإجراءات مع القواعد القانونية والأنظمة المتبعة في وحدات المجتمع المتحضر، أي أن قاعدة مشروعية الدليل الجنائي لا تقتصر فقط على مجرد المطابقة مع القواعد القانونية، بل يجب أن تراعي المبادئ السامية لحقوق الانسان وقواعد النظام وحسن الآداب في المجتمع[1] .

ويشترط في الدليل الجنائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة، وذلك يقضي أن تكون الجهة المختصة بجمع الدليل قد التزمت بالشروط التي يحددها القانون في هذا الشأن ونحن هنا نبحث عن مشروعية الدليل الإلكتروني، فإننا نقتصر على ما يثير جمع هذا الدليل من إشكالات قانونية بالنظر إلى طبيعته الخاصة، ولذا يمكننا القول ان ما يثيره الدليل الالكتروني من حيث مشروعية الحصول عليه يتركز بشكل اساسي في اجراءات التفتيش للبحث عن هذا الدليل وذلك يتم بنقطتين رئيستين:[2]

- صفة القائم بالتفتيش .
- مدى مشروعية التفتيش عن الدليل الالكتروني وفي ضبطه في الوسط الافتراضي.

من المقرر أن الإدانة في أي جريمة لا بد ان تكون مبنية على أدلة مشروعية في الحصول عليها وفق قواعد الأخلاق والنزاهة، واحترام القانون من طرف الجهة المتخصصة بجمع الدليل الجزائي بما يتضمنه من لأدلة مستخرجة من وسائل الكترونية.

ولا يكون إلا إذا أجرى التفتيش عنه أو الحصول عليه أو كانت عملية تقديمه إلى القضاء و إقامته أمامه بالطرق التي رسمها القانون، فمتى ما تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد بقيمته مهما كانت دلالته الحقيقية وذلك لعدم مشروعيته، وعلى هذا الأساس فإن إجراءات جمع الأدلة الإلكترونية المتحصلة من الوسائل الإلكترونية إذا خالفت

[1] حسين ربيعي ، المرجع السابق ، ص 265.

[2] خالد عياد الحلبي ، المرجع السابق ، ص 239.

القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة، وبالتالي بطلان الدليل المستمد منها ولا تصلح لان تكون أدلة تبنى عليها الإدانة في المواد الجنائية.[1]

المطلب الثاني : حجية الدليل الإلكتروني في الإثبات الجنائي وموقف المشرع الجزائري منه

إن مجرد الحصول على الدليل الإلكتروني وتقديمه للقضاء لا يكفي لاعتماده كدليل للإدانة، إذ أن الطبيعة الفنية الخاصة بالدليل الالكتروني تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة الشخص غير المتخصص إدراك ذلك العبث، فضلا عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإبلاغ عن الحقيقة فتبدو عادية في مثل هذا النوع من الأدلة، لذلك تثور فكرة الشك في مصداقيتها كأدلة للإثبات الجنائي.[2]

الفرع الأول: حجية الدليل الإلكتروني في الإثبات الجنائي

إن مسألة تقييم الدليل الجنائي في إثبات الوقائع الجرمية مسألة موضوعية محضة للقاضي أن يمارس سلطته التقديرية فيها.

أولا: تقييم الدليل الإلكتروني من حيث سلامته من التزوير

يمكن التأكد من سلامة الدليل الالكتروني من العبث به بعدة طرق نذكر منها : [3]

– فكرة التحليل التناظري الرقمي والتي من خلالها يتم مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثم يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا، ويستعان في ذلك استخدام جهاز الحاسوب الذي يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون الدليل الرقمي، وهذا العلم يستعان به أيضا في كشف مدى تلاعب بمضمون هذا الدليل.

– استخدام عمليات حسابية خاصة تسمى الخوارزميات ويلحق إلى هذه التقنية في حالة عدم الحصول النسخة الأصلية للدليل الرقمي، وفي حالة العبث قد وقع على النسخة الأصلية

[1] سعيداني نعيم ، المرجع السابق ، ص 210.

[2] خالد عياد الحلبي ، المرجع السابق ، ص 246.

[3] سعيداني نعيم ، المرجع السابق ، ص217.

بالإمكان التأكد من سلامة الدليل الرقمي من التحريف والتغيير باستعمال هذه العمليات الحسابية .

– استعمال الدليل المحايد وهو نوع من الأدلة الرقمية المخزون في البيئة الافتراضية لا علاقة له بموضوع الجريمة، ولكنه يساعد في التأكد من مدى سلامة الدليل الرقمي المقصود من حيث عدم حصول أي تعديل عليه في نظام الحاسوب[1] .

ولا شك أن الخبرة التقنية تمثل في هذه الحالة دورا مهما في التثبت من سلامة الدليل الرقمي، فإذا كان للخبرة التقنية أهمية كبرى في مجال استخلاص الدليل الرقمي، فإن لها ذات الدور في بحث مصداقية وتقييمه من حيث عدم حصول أي عبث عليه، فنقص الثقافة المعلوماتية للقاضي الجزائي قد يحتم عليه كواجب قضائي أن يستعين في هذه المسائل بوسائل الخبرة كنهج، ليس من اجل استيفاء الدليل فحسب بل لبحث مصداقيته في مجال معالجة الآلية للمعلومات وتحقيق اليقينية لهذا الدليل.

ثانيا: تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المتبعة في الحصول عليه

سبق الحديث على أن الدليل الرقمي يتم الحصول عليه بإتباع جملة من الإجراءات الفنية، والتي من الممكن أن يعتريها خطأ قد يشكك في سلامه نتائجها، الأمر الذي يحتم إخضاعها إلى اختبارات كوسيلة للتأكد من سلامة هذا الإجراءات من حيث إنتاجها لدليل تتوافر فيه المصداقية لقبوله كدليل إثبات ويتبع في ذلك مجموعة من الخطوات :

– إخضاع الأدلة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج ويكون ذلك بإتباع اختبارين أساسيين يتم التأكد من خلالهما أن الأداة المستخدمة عرضت كل المعطيات المتعلقة بالدليل الرقمي، وفي ذات الوقت لن تضف إليها أي بيانات جديدة وهو ما قد يعطي النتائج المقدمة مصداقية في التدليل على الوقائع، أو يمثل هذان الاختباران في:[2] اختبار السلبيات الزائفة ومفاده أن تخضع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الرقمي، وأنه لم يتم إغفال معطيات مهمة عنه، أما الاختبار الثاني والذي يجري باختبار الايجابيات الزائفة مفاده إخضاع الأداة

[1] خالد عياد الحلبي ، المرجع السابق ، ص 249.

[2] سعيداني نعيم ، المرجع السابق ، ص 218.

المستخدمة في الحصول على الدليل الرقمي للاختبار يمكن من التأكد من أن هذه الأداة لاتعرض معطيات إضافية جديدة.[1]

– الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم نتائج أفضل، إذ تبين الدراسات العلمية والبحوث المنشورة في مجال تقنية المعلومات بالطرق السليمة التي يجب إتباعها في الحصول على الدليل الرقمي، وفي المقابل بينت تلك الدراسات أيضا الأدوات المشكوك في كفائتها وهو ما يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات.[2]

من خلال ما تقدم يمكن الوقوف على سلامة الدليل الإلكتروني، فإذا توافرت في الدليل الالكتروني الشروط العامة لما يمكن أن يمثل أساسا لتأكيد الثقة فيه، فإنه يبدو ومن غير المعقول أن يعيد القاضي تقييم هذا الدليل وطرحه من جديد على البحث، فإن الدليل الإلكتروني بوصفه دليلا علميا فإن دلالته قاطعة شأن الواقعة المستشهد به منها، فإذا سلمنا سابقا بإمكانية التشكيك في سلامة الدليل الالكتروني بسبب قابليته للعبث ونسبة الخطأ في إجراءات الحصول عليه، فتلك مسألة فنية لا يمكن للقاضي أن يقطع في شأنها برأي حاسم وإن لم يقطع به أهل الاختصاص.

إذا توافرت في الدليل الالكتروني الشروط السابقة بخصوص سلامته من العبث والخطأ، فإن هذا الدليل لا يمكن رده استنادا لسلطة القاضي التقديرية إذا سلطة القاضي في رد الدليل استنادا لفكرة الشك، يلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك في الدليل، وهو ما لا يستطيع القاضي الجزم به متى توافرت في هذا الدليل شروط السلامة، بحيث يقتصر دور القاضي على بحث صلة الدليل بالجريمة، ولا شك أن الخبرة تحتل في هذه الحالة دورا مهما في التأكد من صلاحية هذا الدليل كأساس لتكوين عقيدة القاضي، فبحث مصداقية الدليل هي من صميم فن الخبرة لا القاضي.[3]

[1] خالد عياد الحلبي ، المرجع السابق ، ص 251.

[2] سعيداني نعيم ، المرجع السابق ، ص 218.

[3] هلالي عبد الله احمد ، المرجع السابق ، ص 95.

الفرع الثاني: موقف المشرع الجزائري من الدليل الالكتروني في مجال الإثبات الجنائي

إن من واجب القاضي الجنائي سواء كان قاضي التحقيق أو غرفة الاتهام أو المحكمة الجزائية، أن تقيم الدليل على المتهم، ولا يجوز أن يحاكم المتهم و يدان بمجرد وجود قرائن بل لا بد أن تكون هذه الدلائل مكملة لبقية الأدلة المادية الأخرى كما يجب أن تتسم إجراءات جمع الأدلة بالمشروعية وذلك احتراما للحرية الشخصية للمتهم باعتباره بريئا إلى أن تثبت إدانته بحكم بات.[1]

إن الإثبات الجنائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل ووجود الدليل على ذلك، ويعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة وكشف الجريمة ونسبتها إلى المتهم، وقد ذهب الفقه الإجرائي إلى وضع نظامين إجرائيين في مجال الإثبات الجنائي يختلفان فيما بينهما من حيث الأسس التي يقوم عليها كل واحد منها وقد سبق الإشارة إليهما.

تنتمي الجزائر إلى مجموعة الدول التي تتبنى نظام الإثبات الحر في مجال الإثبات الجنائي، فهي تساير النظم اللاتينية كفرنسا وبلجيكا والأردن وسوريا، وهو الأمر الذي كرسته المادة 212 من قانون الإجراءات الجزائية التي جاء في نصها على أن: "يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص بها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص، ولا يجوز للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه."

إن إقرار المشرع الجزائري للحرية في تقديم الأدلة وتركها للقانعة الشخصية لقاضي الموضوع هو لتعزيز إثبات قرينة البراءة، وتعزيز لممارسة حقوق الدفاع الفردية ، غير أن هذا الإطلاق بدون تحديد وتخصيص يعد قصورا تشريعيا واضحا فلا نجد ضمن قانون الإجراءات الجزائية ما يدل على أن الدليل الالكتروني، هو دليل من نوع خاص شانه شان الجرائم الإلكترونية ، فغياب أدنى نص قانوني في هذا الشأن يؤدي إلى ظهور إشكالات متعلقة بطبيعة الأدلة المقدمة أمام الجهات القضائية، بحيث يمكن لهذه الأخيرة وفي حال عدم إلمامها بتقنية

[1] بلعليات ابراهيم . المرجع السابق ، ص 139.

المعلوماتية دحض هذا الدليل وعدم الاعتداد به ، ولو كان حائزا على القوة الثبوتية، وتتوفر فيه كافه شروط الصحة وكذلك العكس صحيح.

أما بالنسبة لسلطة القاضي الجزائري في تقدير الدليل الالكتروني، فإن المادة العلمية للدليل الالكتروني جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي، إن هناك من يرى أن الدليل العلمي ومنه الدليل الالكتروني له قوته الثبوتية الملزمة حتى للقاضي، مستندين في رائيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين، وهناك من يرى بأن مبدأ حرية القاضي في الاقتناع، يجب أن يبسط سلطاته على كل الأدلة دون استثناء حتى على الدليل الرقمي، معتبرين أن إعطاء الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى مذهب الإثبات القانوني المقيد، والمشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأية طريقة من طرق الإثبات ما عدا الجرائم التي قد يتطلب إثباتها دليلا معينا، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين اقتناعه من أي دليل يطمئن عليه.[1]

[1] سعيداني نعيم ، المرجع السابق ، ص229.

الخـــــاتـــــمـــة

بعد استعراضنا بالبحث و الدراسة لموضوع آليات البحث و التحقيق في الجرائم الالكترونية، اتضح لنا جليا مدى التحول الذي مس مجلات البحث في مجال العلوم الجنائية، فقد تأثرت هذه الأخيرة بالتطور التكنولوجي و بالخصوص بتطبيقات التقنيات الإلكترونية، فقد حاولنا من خلال كل ما استعرضناه إضفاء الطابع الفني و التقني بالقدر المستطاع إلى الطابع القانوني للبحث، وذلك من خلال الاعتماد على مزيج من المصطلحات القانونية و العلمية الالكترونية، و كل ذلك بغرض إبراز مدى تقدم البحوث في المجال القانوني الجنائي و بالخصوص في مجال الإجراءات الجنائية المتعلقة بأعمال البحث و التحقيق، و التي طالما تميزت بالطابع التقليدي المادي، غير أن تأثر الجريمة بتطور نمط الحياة في ظل عصر تكنولوجيا المعلومات، عجل باستحداث مفاهيم و إجراءات قانونية حديثة تهدف إلى تطوير أعمال البحث و التحقيق في مجال الجرائم الإلكترونية ، بهدف ملاحقة جرائم و مجرمي الجرائم الالكترونية، ضمانا لعدم فقدان السيطرة على استعمالات تقنية المعلوماتية و عدم حيادها عن أهدافها الرئيسية المتمثلة في خدمة المصالح المعرفية للمجتمعات و الشعوب، و يمكن لنا أن نوجز ما تضمنه بحثنا من نتائج منبثقة عن الإشكالية المطروحة في مجال التحقيق في الجريمة الالكترونية فيما يلي:

1- يستحيل القضاء على ظاهرة الإجرام الالكتروني بشكل نهائي، و ذلك لاتصالها المباشر بالتقنية الالكترونية، ففكرة التخلي عن هذه التقنية هي الحل الوحيد لمشروع القضاء على الجريمة الالكترونية، و ذلك بالرغم من درجة التطور التي آلت إليها المنظومة القانونية العقابية منها و الإجرائية في مجال مكافحة الجريمة الالكترونية.

2- على المستوى القانوني و التشريعي فإننا لاحظنا مدى الاهتمام الذي توليه الدول و الحكومات لهذا المجال من خلال التحديثات المستمرة و المتوالية للنصوص العقابية والإجرائية، بشكل متناسق مع تطور الأساليب الإجرامية، و هي الجهود التي لاحظنا قلتها في التشريع الجزائري الذي أصبح يميزه الجمود و القدم مقارنة بما آلت إليه الجريمة الالكترونية، و كل ذلك بدعوى عدم تأثر المجتمع الجزائري بالظاهرة الإجرام الالكتروني بالشكل الذي يستوجب سن و تعديل النصوص على وجه الاستعجال، و هي المعطيات و الحجج التي من شانها تشجيع المجرمين على التصعيد من نشاطهم و تهديد المصالح العامة و الخاصة، خصوصا و أن هذه التقنية الالكترونية أصبحت من التقنيات الأكثر شيوعا في الجزائر.

3- إن إجراءات البحث و التحقيق المعلوماتي هي إجراءات من نوع خاص يشترط لمباشرتها التقييد بمجموعة من الشروط أهمها شرط التقييد بالنص الإجرائي الملائم، لما قد تنطوي عليه هذه الإجراءات من مساس بالحريات الفردية و إطلاع على مستودع سر الأفراد، كالتصنت الإلكتروني و اعتراض البريد الإلكتروني، و حجز للمعطيات و البيانات الشخصية، و كل ذلك حفاظا على سلامة الإجراءات من طائلة البطلان و كذلك حفاظا على حريات الأفراد و كرامتهم.

4- تخضع إجراءات البحث و التحقيق المعلوماتي لاختصاص جهات متخصصة في التعامل مع الجرائم الالكترونية، تعتمد في تكوينها على مجموعة من المختصين في مجال المعلوماتية و كذلك في مجال التحقيق الجنائي، مما يجعل منهم أفضل الأشخاص الذين يستطيعون التكفل بمهام البحث و التحقيق في الجرائم الإلكترونية، نظرا لتقديرهم العلمي و المعرفي بالأساليب الإجرامية الالكترونية، و كذلك القواعد القانونية للتعامل بالشكل الشرعي مع الجريمة المعلوماتية، إضافة إلى مراعاتهم لجملة من القواعد العملية الاحتياطية منها و الأصلية عند مباشرة الإجراءات التي تهدف إلى جمع الأدلة، بشكل يكون الهدف منه ضمان حسن سير الإجراءات و الحفاظ على سلامتها من طائلة البطلان، و كذا سلامة الأدلة من مخاطر التلف و الفقدان.

5- تعتمد إجراءات البحث و التحقيق في مجال الجرائم المعلوماتية على القواعد الفنية العملية أكثر منه على القواعد الإجرائية القانونية.

6- يقترن نجاح إجراءات البحث و التحقيق في الجرائم الالكترونية بمدى براعة و فعالية و جاهزية الجهات المختصة بمباشرة الإجراءات لتتبع الأدلة الإلكترونية، و تحصيلها و حفظها بغرض عرضها على الجهات المختصة بتقديرها.

و من خلال الملاحظات السابقة الذكر ارتأينا ، وبناء على كل ما استعرضناه جاز لنا وضع تنويه مجموعة من التوصيات التي تساهم في حل الإشكاليات و العوائق التي صادفتنا في مجال البحث و لتكون إسهاما علميا واضح، و التي تتمثل فيما يلي:

1- العمل على التحسس بخطورة الجريمة الالكترونية على الأمن العام، و أمن الأفراد من خلال إدراج مفهوم الجريمة المعلوماتية ضمن المقررات الدراسية.

2- ضرورة العمل على تحسس ضحايا الجرائم الالكترونية بضرورة التبليغ عن أي جريمة الكترونية قد يقعون ضحايا لها.

3- يجب و على وجه الاستعجال استحداث نصوص قانونية متلائمة و مستوى التطور الذي آلت إليه تقنية الإلكترونية و درجة خطورة الجرائم الالكترونية.

4- تعديل قانون الإجراءات الجزائية على وجه الاستعجال من خلال إدراج قسم خاص بأعمال البحث و التحقيق في الجرائم الالكترونية.

هذه جملة من المقترحات التي يرى الباحث ضرورة تبنيها و تجسيدها على ارض الواقع من اجل الوصول إلى ضمان فعالية قصوى في عمل الجهات المختصة بالبحث و التحقيق في الجرائم الالكترونية، وبالتالي تجسيد السياسة الهادفة على تامين الفضاء الإلكتروني، و مكافحة الجرائم الالكترونية.

قـائـمـة المـراجـــع

أولا: باللغة العربية

1- النصوص القانونية

- **القوانين:**

1. القانون رقم 16- 01، المؤرخ في 6 مارس 2016، المتضمن الدستور الجزائري، جريدة الرسمية، رقم 63، بتاريخ مارس 2016.

- **الأوامر**

1. الأمر رقم (66-155)، المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم، بالأمر رقم(17-07)، المؤرخ في 27 مارس 2017، جريدة الرسمية، رقم 20 بتاريخ 29 مارس 2017.

2. الأمر رقم (66-156)، المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم، بالقانون رقم(14-01)، المؤرخ في 4 فبراير 2014، جريدة رسمية، رقم 7، بتاريخ 16 فبراير 2014.

- **المراسيم**

1. المرسوم رقم (09-04)، المؤرخ في 16 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجيردة الرسمية، العدد 47 بتاريخ 05غشت 2009.

2. المرسوم الرئاسي، رقم (15-261)،المؤرخ في 08 اكتوبر 2015 ويحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 53، بتاريخ 08 اكتوبر 2015.

2- الكتب:

1. أحمد خليفة الملط، **الجرئم المعلوماتية**، الطبعة الثانية، دار الفكر الجامعي، الاسكندرية، 2006.

2. أسامة أحمد المناعسة، جلال محمد الزعبي **جرائم تقنية نظم المعلومات الالكترونية**، الطبعة الثاثة، دار الثقافة للنشر و التوزيع، عمان،2014 .
3. أمال قارة، **الحماية الجنائية للمعلوماتية في التشريع الجزائري**، الطبعة الاولى، دار هومة، 2006.
4. بلعليات ابراهيم، **أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري**, الطبعة الاولى، دار الخلدونية، الجزائر.
5. حنان ريحان مبارك المضحاكي، **الجرائم المعلوماتية**، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2014.
6. خالد عياد الحلبي، **اجراءات التحري والتحقيق في جرائم الحاسوب و الأنترنت**، الطبعة الاولى، دار الثقفة للنشر و التوزيع، عمان.
7. خالد محمود إبراهيم **فن التحقيق الجنائي في الجرائم الإلكترونية**، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2009.
8. شيماء عبد الغني محمد عطا الله، **الحماية الجنائية للتعاملات الالكترونية**، دار الجامعة الجديدة، الاسكندرية، 2007.
9. طارق ابراهيم الدسوقى عطية، **الأمن المعلوماتي النظام القانوني للحماية المعلوماتية**، دار الجامعة الجديدة، الاسكندرية، 2009.
10. عبد الفتاح بيومي حجازي ، **مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والانترنت**، الطبعة الاولى ،دار الفكر الجامعي ،2006 .
11. حمد الأمين البشري، **التحقيق في الجرائم المستحدثة**، الطبعة الاولى، دار الجامعة، عمان، 2014.
12. محمد علي العريان، **الجرائم المعلوماتية**، دار الجامعة الجديدة، الاسكندرية، 2004.
13. محمود حماد مرهج الهيني، **أصول البحث والتحقيق الجنائي**، دار الكتاب القانونية، القاهرة، 2014.
14. محمود عبد الحميد عبد المطلب، **البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والانترنت**، دار الكتاب القانونية، مصر، 2006.

15. مصطفى محمد موسى، **التحقيق الجنائي في الجرائم الالكترونية**، الطبعة الاولى، مطابع الشرطة، القاهرة، 2009.
16. هلال عبد الله محمد، **حجية مخرجات الكمبيوتر في المواد الجنائية**، الطبعة الثانية، دار النهضة العربية ،2008 .

3- المذكرات الجامعية

1. معتق عبد اللطيف، الإطار القانوني لمكافحةجرائم المعلوماتية في التشريع الجزائري والتشريع المقارن،مذكرة ماجستير، جامعة العقيد الحاج لخضر، باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق،2011-2012.
2. ربيع حسين، آليات البحث والتحقيق في الجرائم المعلوماتية، رسالة دكتوراه، جامعة باتنة 1، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2015-2016.
3. سعيد علي نعيم، آليات البحث والتحري من الجرائم المعلوماتية في القانون الجزائري، مذكرة ماجستير، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، قسم الحقوق، 2012-2013
4. صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة ماجستير ، جامعة مولود معمري تيزي وزو ، كلية الحقوق والعلوم السياسية ، 2013.
5. عمر بن ابراهيم بن حماد العمري، إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الاجراءات السعودي ،مذكرة ماجستير جامعة نيف العربية 2007.
6. قادري سارة، أساليب التحري الخاصة في قانون الاجراءات الجزائية، مذكرة ماجستير جامعة قاصدي مرباح ، ورقلة ، كلية الحقوق والعلوم السياسية ، قسم الحقوق 2014.

ثانيا: باللغة الاجنبية

1. Hachette, le dictionnaire pratique du français, imprimé en France, Imprimerie hérissey , Évreux (Eure) N°2896 , Collection N°25 Edition N02, 1983.

فهرس المحتويات

مقدمة.....04

الفصل الأول: الإطار المفاهيمي للجريمة الالكترونية والتحقيق فيها.....07

المبحث الأول: ماهية الجريمة الالكترونية 09

المطلب الأول: تعريف الجريمة الالكترونية 09

الفرع الأول: المفهوم الضيق للجريمة الإلكترونية.....09

الفرع الثاني: المفهوم الواسع للجريمة الإلكتروني.....10

الفرع الثالث: تعريف المشرع الجزائري للجريمة الإلكترونية.....12

المطلب الثاني: خصائص وأركان الجريمة الإلكترونية 12

الفرع الأول: خصائص الجريمة الإلكترونية.....12

أولا: الجريمة الإلكترونية عابرة للحدود الوطنية.....12

ثانيا: الجريمة الإلكترونية صعبة الاكتشاف والإثبات 13

ثالثا: خصوصية مرتكب الجرائم الإلكترونية 14

الفرع الثاني: أركان الجريمة الإلكترونية.....14

أولا: الركن الشرعي 14

ثانيا: الركن المادي 15

ثالثا: الركن المعنوي 17

المبحث الثاني: مفهوم التحقيق الجنائي في الجريمة الالكترونية 18

المطلب الأول: الاجهزة المكلفة بالبحث و التحري عن الجرائم الالكترونية 18

الفرع الأول: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال....18

أولا: التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال.....19

ثانيا: مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.....19

ثالثا: اختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.....19

الفرع الثاني: الوحدات التابعة لسلك الأمن الوطني والدرك الوطني.....20

أولا:الوحدات التابعة لسلك الأمن الوطني.....20

ثانيا: الوحدات التابعة للدرك الوطني الجزائري.....21

المطلب الثاني: خصائص التحقيق والمحقق في الجرائم الإلكترونية والدليل المناسب للإثباتها.....22

الفرع الأول: خصائص التحقيق والمحقق في الجرائم الإلكترونية.....22

أولا: خصائص التحقيق في الجريمة الإلكترونية.....22

ثانيا: خصائص المحقق في الجريمة الإلكترونية.....23

الفرع الثاني: دليل الإثبات في الجريمة الإلكترونية 25

أولا: تعريف الدليل الإلكتروني.....25

ثانيا: أشكال الدليل الإلكتروني.....26

ثالثا: أنواع الدليل الالكتروني.....27

الفصل الثاني: القواعد الاجرائية في استخلاص الدليل الالكتروني والقيمة القانونية له.....28

المبحث الأول: القواعد الاجرائية في االستخلاص الدليل الالكتررواني 30

المطلب الاول: القواعد الاجرائية التقليدية في االستخلاص الدليل الالكتروني.....30
الفرع الأول: التفتيش.....30
أولا: القواعد الموضوعية لتفتيش أنظمة الحاسوب.....31
ثانيا: القواعد الشكلية لتفتيش نظام الحاسوب.....31
الفرع الثاني: استخلاص الدليل في الجريمة الإلكترونية.....31
أولا: مدى صلاحية الضبط في الجريمة الإلكترونية.....32
ثانيا: الأشياء محل الضبط في الجريمة الإلكترونية.....32
ثالثا : الصعوبات التي تواجه عملية الضبط.....33
الفرع الثاني: الخبرة في إثبات الجريمة الإلكترونية.....33
أولا: أنواع الخبراء الإلكترونيون.....34
ثانيا: أهمية الخبرة في البحث عن الدليل الإلكتروني.....34
المطلب الثاني: القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني وصعوبات التحقيق في الجريمة الإلكترونية.....35
الفرع الأول: القواعد الإجرائية الحديثة في استخلاص الدليل الالكتروني.....36
أولا: التسرب (الإختراق) واعتراض المراسلات.....36
ثانيا: المراقبة الإلكترونية وحفظ المعطيات.....40
الفرع الثاني: معوقات و صعوبات التحقيق في الجريمة الإلكترونية.....41
أولا: المعوقات المتعلقة بجهات التحقيق.....41
ثانيا: عوائق تتعلق بالجريمة والجهة المتضررة منها.....43

المبحث الثاني : القيمة القانونية للدليل الالكتروني في مجال الاثبات الجنائي.....45

المطلب الأول: مشروعية الدليل الالكتروني.....45

الفرع الأول: مشروعية الدليل الإلكتروني.....45

أولا: أنظمة الإثبات المقيد.....46

ثانيا: نظام الإثبات الحر.....46

الفرع الثاني: مشروعية الحصول على الدليل الالكتروني.....46

المطلب الثاني : حجية الدليل الإلكتروني في الإثبات الجنائي وموقف المشرع الجزائري منه.....48

الفرع الأول: حجية الدليل الإلكتروني في الإثبات الجنائي.....48

أولا: تقييم الدليل الإلكتروني من حيث سلامة التزوير.....48

ثانيا: تقييم الدليل الإلكتروني من حيث السلامة الفنية للإجراءات المتبعة في الحصول عليه.....49

الفرع الثاني: موقف المشرع الجزائري من الدليل الالكتروني في مجال الإثبات الجنائي.....51

الخاتمة:.....53

قائمة المراجع.....57

فهرس المحتويات:.....61

ملخص الدراسة.....65

ملخص الدراسة

ملخص:

لقد عرفت حياة الإنسان في هذه السنوات الاخيرة تطورا لم يسبق له مثيل ، و ذلك بفعل التطور المذهل لتقنية الإلكترونية و إنتشارها اللامحدود ، كما تنامت إلى جانب ذلك التهديدات أكثر بفعل إنتشار نوع جديد من الجرائم يضاف إلى قائمة الجرائم التي كانت معروفة مسبقا وهي الجرائم الإلكترونية.

لقد تضمنت الدراسة في هذا المجال معطيات قانونية و أخرى فنية و تقنية نظرا لطبيعة الموضوع الذي يعتبر نقطة تقاطع بين علوم الحاسوب و النظم المعلوماتية و العلوم القانونية الإجرائية، ولذلك فقد عالجنا في إطار فصلين مختلف الجوانب المتصلة بالموضوع من أجل الوصول إلى مفاهيم قانونية حديثة تتماشى و طبيعة الجرائم الإلكترونية، فعالجنا في إطار الفصل الأول مفهوم تقنية المعلوماتية بإعتبارها الوعاء المنطقي للجريمة الإلكترونية والإجراءات الخاصة بالبحث و التحقيق بشأنها ، كما تناولنا بالتعريف الجريمة الإلكترونية ذاتها من كافة النواحي الفقهية منها والقانونية، أما موضوع دراستنا في إطار الفصل الثاني فقد تمحور حول دراسة مدى إنقسام الفقه و القانون حول مدى إعتبار الفضاء الإلكتروني والجرائم الإلكترونية محلا لإجراءات البحث و التحقيق الجنائي، ومدى تأقلم القانون مع هذا التوجه المستحدث للنصوص الإجرائية ، من خلال استعراض مختلف الهيئات الخاصة المكلفة بإجراءات البحث والتحقيق بشأن الجرائم الإلكترونية وقد ركزنا دراستنا في هذا المجال حول الهيئات المكلفة بالبحث و التحقيق المنتمية إلى مختلف الهيئات سواء الأمنية كمصالح الشرطة والدرك خصوصا في ظل المتغيرات الأخيرة و التي التي شهدت تنصيب الهيئة الوطنية المكلفة بالوقاية و مكافحة الجرائم الإلكترونية بتاريخ ال 8 أكتوبر 2015

لنختتم بحثنا بخاتمة حاولنا من خلالها الخروج بأكبر قدر ممكن من النتائج التي تفيد في الإجابة عن الإشكالية الأساسية و الإشكاليات الفرعية، مع تحصيل مجموعة من التوصيات القانونية التي من شانها دعم آليات البحث و التحقيق في الجرائم الإلكترونية.

Résumé:

La vie humaine que je connais dans ces années, le développement récent est sans précédent, et ainsi par le développement étonnant de la technologie électronique et leur diffusion illimitée, et a grandi avec elle plus de menaces par la propagation d'un nouveau type de crime est ajouté à la liste des crimes qui ont été connus à l'avance, un cyber-crime.

L'étude a inclus dans ces données sur le terrain juridique et d'autres techniques et de la technologie en raison de la nature du sujet qui est le point d'intersection entre les systèmes scientifiques de la procédure de l'informatique et d'information et juridique, a donc traité avec sous deux aspects différents pertinents pour l'accès aux concepts de moderne juridique en ligne et la nature des crimes électroniques, Fgana dans le premier chapitre, le concept de la technologie en tant que cadre logique navire d'information et des procédures pour la recherche sur la criminalité électronique et enquête sur eux, comme nous avons eu affaire à la même définition du crime électronique à tous les égards, y compris la jurisprudence et juridique, Le sujet de notre étude dans le chapitre II cadre a mis l'accent sur l'étude de l'étendue de la fragmentation de la jurisprudence et du droit sur l'étendue de l'examen du cyberespace et la cybercriminalité soumis à des procédures de recherche et les enquêtes criminelles, et la mesure d'adapter la loi à cette tendance des textes nouvellement créés procédure, par un examen des différents organes propres procédures coûteuses de recherche et d'enquête sur les crimes électroniques que nous avons concentré notre étude dans ce domaine autour des organismes chargés de recherche et d'enquête appartenant à divers organismes, à la fois sécurité de la police Kmassalh et de la gendarmerie, en particulier à la lumière des variables récentes et qui a vu l'inauguration de l'Autorité nationale chargée de la Ba Prévention et lutte contre le courrier électronique en date du 8 Octobre 2015 crimes

Pour conclure notre recherche à travers laquelle nous avons essayé de sceller autant que possible à partir des résultats qui aident à répondre au problème de base et sous-problèmes, avec la collection d'une série de recommandations juridiques qui soutiendraient les mécanismes de recherche et d'investigation des crimes cybernétiques