وزارة التعليـم العالـي والبحث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة عبد الحميد بن باديس مستغانم

كلية الحقوق والعلوم السياسية

قسم : الحقوق

المرجع: .....

مذكرة نهاية الدراسة لنيل شهادة الماستر

تحديات الإثبات الجنائي في الجرائم الإلكترونية

ميدان الحقوق والعلوم السياسية

الشعبة: الحقوق

التخصص: قانون قضائي

من إعداد الطالب:

رحوزهرة

تحت إشراف الأستاذ:

بنورسعاد

أعضاء لجنة المناقشة

الأستاذ:	عوايل عبد الصمد	رئيسا
الأستاذ:	بنور سعاد	مشرفا مقررا
الأستاذ:	عوايل عبد الصمد	مناقشا

السنة الجامعية: 2023/2022

تاريخ المناقشة: 2023/06/26

الإهداء

اللهم لك الحمد قبل أن ترضى و لك الحمد اذا رضيت و لك الحمد بعد الرضا

نحمد الله عز وجل أنه وفقنا على إنجاز هذا العمل المتواضع

إلى قرة عيني، إلى نبع الحنان...إلى من وهبتني الحياة ...

أمي العزيزة حفظها الله

إلى من يزيدني إنتسابي له و ذكره فخرا و إعتزازا

أبي العزيز

إلى إخوتي الأحباء

و إلى كل من جمعتني معهم حدائق الدراسة.

شكر وتقدير

اعترافا بالفضل لأهله و عملا بقول الرسول صلى الله عليه وسلم:

((من صنع اليكم معروفا فكافئوه فإن لم تجدوا ما تكافئونه به فادعوا له حتى تروا أن قد كافئتموه)).

أتقدم بخالص الشكر والإمتنان والعرفان إلى الأستاذة الطيبة

بنورسعاد

التي كان لي عظيم الحظ في نيل شرف إشرافها ومرافقتها في المذكرة وطوال المسار الدراسي

كما أشكر كل الأساتذة الذين درسوني طوال مسار دراستي

وأشكر كل طاقم الإدارة وكل موظفي كلية الحقوق صلامندر

قائمة المختصرات

أولا: باللغة العربية:

ج : الجزء

ج.ر :الجريدة الرسمية

ص : صفحة

ص.ص : من الصفحة إلى الصفحة

ط : الطبعة

ف : الفقرة

ق.إ.ج : قانون الإجراءات الجزائية

ق.إ.م.إ : قانون الإجراءات المدنية والإدارية

ق.إ.م.ف : قانون الإجراءات المدنية الفرنسي

ق.ع : قانون العقوبات

م : المادة

م.ق : المجلة القضائية

ثانيا: باللغة الفرنسية:

Art : Article

Ed : Edition

In : Dans

Op.cit : (Opère-citato), Référence précédemment citée

P : Page

PP : De la page a la page

مقدمة

لاشك أن التطور التكنولوجي الذي شهده العصر الحديث في مجال التقنية والمعلوماتية حقق للبشرية الرقي والتقدم في شتي مجالات الحياة لا سيما في مجال الاتصالات السلكية واللاسلكية حتى أصبح يطلق عليه تسمية العصر المعلوماتي أو عصر ثورة المعلومات.

إن تدفق التقنية وانتشار التكنولوجيا ساعد علي تحقيق الرفاهية وتسهيل ربط الاتصالات وإجراء المعاملات مع اختزال الوقت والتكلفة حتي أصبح العالم وكأنه قرية صغيرة،لا تخفي فيها خافية.

لكنه الي جانب المزايا التي جلبتها التكنولوجيا والتقنية من خلال الوسائل المتاحة للجمهور أو لطائفة معينة علي غرار الانترنيت أو الانترانات، ترتبت عدة سلبيات علي سوء استخدام تلك الوسائل.

فقد أدى سوء استخدام التكنولوجيا الي تسهيل ارتكاب الكثير من الجرائم التقليدية علي نطاق واسع علي غرار جرائم السرقة وجرائم التجسس وانتهاك حرمة الحياة الخاصة وحرمة المراسلات والجرائم المخلة بالآداب العامة، بالإظافة الى بروز نوع جديد من الجرائم ذو طبيعة خاصة، تدعي الجريمة المعلوماتية أو الجريمة الالكترونية. لا تقل في خطورتها وحجم الأضرار التي قد تلحقها عن خطورة أهم واشد الجرائم التقليدية فتكا.

ورغم أهمية الجرائم المعلوماتية وخطورتها وتوسع الأضرار التي قد تلحقها بالدول التي سارعت الي إدخال التقنية المعلوماتية في أنظمتها الأمنية، الاجتماعية والاقتصادية غير أن تلك الدول تخلفت عن تكريس الإطار القانوني الذي يحمي تلك المنظومات من الاعتداء عليها أو سوء استغلالها، خاصة الأفعال الضارة والتي ترقي الي وصف الجرائم. والأخطر من ذلك فأن تلك الدول أهملت وضع ايطار قانوني للبحث عن تلك الجرائم وتقصيها وتقديم مرتكبيها أمام العدالة الجنائية، من خلال وضع الأليات والترتيبات اللازمة لذلك ومن خلال تعزيز مبدأ الإثبات بتكريس الدليل الالكتروني وتقنينه.

إن المشرع الجزائري لم يشذ عن هذه القاعدة، فهو لم يتبني تجريم أفعال الاعتداء علي الانظمة المعلوماتية الا من خلال تعديل قانون العقوبات بموجب القانون رقم: 04/15 المؤرخ في:2004/11/10 وهو إن فعل ذلك، فانه لم يوضح الاطار القانوني لإثبات الجريمة المعلوماتية.[1]

ومدى القبول بالدليل الالكتروني، رغم التعديل الذي مس قانون الاجراءات الجزائية بموجب الأمر رقم: 06/22 المؤرخ في: 20 /12/ 2006، والذي أدى الى ادخال وتقنين أساليب جديدة في البحث والتحري لمواجهة بعض الجرائم الخاصة.[2]

[1] القانون رقم: 04/15 المؤرخ في:2004/11/10 المعدل للأمر رقم 66-156 المؤرخ في 8 يونيو سنة 1966 المتضمن قانون العقوبات
[2] الأمر رقم: 06/22 المؤرخ في: 20 /12/ 2006 المعدل للأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

إن توجه الدول إلي اعتماد مفهوم الادارة الالكترونية أو الحكومة الالكترونية يحتاج الي أنظمة معلوماتية أمنة ومحصنة ضد أي اعتداء أو سوء استغلال. ويتطلب ذلك إيجاد برامج حماية وقائية وهي غير كافية من الناحية الواقعية. كما يتطلب الأمر إيجاد وسائل حماية ردعية، تتمثل أساسا في ألية التجريم والعقاب. أي تحديد الأفعال التي تهدد أمن وسلامة الانظمة المعلوماتية تحديدا كافيا نافيا للجهالة وتجريمها. ثم ضبط وايقاف مرتكبيها وإحالتهم إلى الجهات القضائية المختصة لمحاكمتهم محاكمة عادلة، وتسليط العقوبات المقررة عليهم في حالة إدانتهم، حتي يرتدعوا ويكونوا عبرة لغيرهم.

إن تفعيل آلية التجريم والعقاب لا يكون الا من خلال ايجاد سبل قانونية كفلية بضمان الحريات والحقوق الاساسية للمواطن وتكريس قرينة البراءة. وذلك بالنص علي طرق

وإجراءات البحث والتحري عن الجرائم الماسة بالأنظمة المعلوماتية واثباتها، بحيث يكون الدليل المقدم الي الجهات القضائية دليل مقبول ومشروع يستند الي المنطق وما يستوعبه العقل البشري.

إن خصوصية الجرائم الالكترونية من حيث أنها جرائم ترتكب بسرعة كبيرة، خفية لا تثير أي ضجة، ذات أثار واسعة النطاق قد تمتد الي عدة دول وترتكب من طرف أشخاص أذكياء ضالعين في التكنولوجيا لا يخلفون ورائهم أدلة مادية، تجعل من الطرق التقليدية لإثبات الجرائم العادية عاجزة عن مواجهة هذا النوع من الجرائم، وذلك ما ستحاول هذه

الدراسة ابرازه من خلال حصر العقبات الاجرائية التي تعترض اثبات الجرائم الالكترونية، والتطرق الي السبل الكفيلة لإزالة تلك العقبات والتطرق كذلك إلي مفهوم الدليل الالكتروني المستمد من الانظمة المعلوماتية محل الاعتداء والذي يعد دليلا حاسما لإدانة مرتكبي تلك الجرائم ومعاقبتهم.

منهج الموضوع:

– المنهج التاريخي: ويعد من المناهج القانونية المشهورة والمعروفة، حيث قمنا بالبحث حول الجرائم الإلكترونية في القوانين والتشريعات السابقة ، ودراسة التعديلات التي لحقت هذه القوانين، ومقارنتها.

– المنهج التحليلي:

يعتبر المنهج التحليلي في العلوم القانونية من المناهج الرائدة وواسعة الاستخدام في مجال البحث العلمي في العلوم القانونية ، حيث قمنا بتقسيم الجرائم الإلكترونية بحسب القوانين والتشريعات التي تدخل في حكمها ، والعمل على كل قسم قانوني.

من هنا نطرح الإشكالية التالية:

ما هي الإجراءات القانونية التي كرسها المشرع الجزائري لمتابعة وإثبات الجرائم الإلكترونية ؟.

وللإجابة على هذه الإشكالية ضمن أسلوب منهجي نقترح الخطة التالية:

الفصل الأول: الإطار النظري للجرائم الإلكترونية

المبحث الأول: مفهوم الجرائم الإلكترونية

المبحث الثاني: مفهوم الأدلة الجنائية في الجرائم الإلكترونية

الفصل الثاني: الوسائل الإجرائية للإثبات في الجرائم الإلكترونية

المبحث الأول: إجراءات التحقيق في الجرائم الإلكترونية

المبحث الثاني: معوقات الإثبات في الجرائم الإلكترونية

الفصل الأول

تمهيد

إن التطور التكنولوجي الهائل الذي شهده عالم التكنولوجيا خاصة في الآونة الأخيرة وذلك توافقا مع انتقال المجتمعات إلى المجتمع الرقمي أي من الواقع الفعلي إلى الواقع الافتراضي في ظل الانفتاح العالمي وارتباط الأسواق الدولية ببعضها البعض.

ومن هنا يمكننا القول بأن التطور السريع والمستمر في استخدام الحاسوب صاحبته ظاهرة تعد خطيرة للغاية وهي الجرائم الإلكترونية وهي ظاهرة تعتبر من الجرائم المستحدثة والخطيرة التي لم يكن المجتمع البشري يتوقعها، حيث أصبحت هذه الظاهرة الإجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم خطورتها أنها تطال الحياة الخاصة للأشخاص وتستهدف المعلومات التي تهدد وتنتهك الأفراد في ممتلكاتهم وخصوصياتهم والمؤسسات في كيانها المادي والاقتصادي وحتى المعلومات في أمنها وسيادتها خاصة أنها جرائم ذكية تنشأ في بيئة إلكترونية رقمية.

فالحاسوب قد يكون هدفا للجريمة أو أداة لها وبيئة لها وإما أداة للكشف عنها ومجابهتها لهذا وجب الإلمام بالجريمة الإلكترونية من حيث تحديد مفهومها ومحدداتها.

حيث سنتطرق في هذا الفصل الي تحديد الطبيعة الخاصة للجرائم الإلكترونية من خلال المبحث الأول مفهوم الجرائم الإلكترونية ثم سنتطرق في المبحث الثاني الى مفهوم الأدلة الجنائية في الجرائم الإلكترونية

المبحث الأول: مفهوم الجرائم الإلكترونية

لقد عرف رواج الانترنت كوسيلة للاتصالات واستعمالها في جل المعاملات اليومية ظهور سلبيات عديدة، خاصة بعد استغلال الكثير من المجرمين هذا التغير في نمط المعاملات مما أدي إلى ظهور جرائم لم يكن يعرفها القانون من قبل ك الجريمة الإلكترونية بحيث أخذت هذه الظاهرة الإجرامية حيزا كبيرا من الدراسات من أجل تحديد مفهومها، ولهذا قسمنا هذا المبحث إلى مطلبين: سنتطرق إلى مفهوم الجرائم الإلكترونية في المطلب الأول ثم محددات الجريمة الإلكترونية في المطلب الثاني.

المطلب الأول: تعريف الجرائم الإلكترونية

يقصد بالجريمة الالكترونية تلك المتصلة بتكنولوجيات الإعلام والاتصال مما يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات أو الاستخدام غير المشروع للبيانات المخزنة في أنظمة الحاسوب والتلاعب بها أو تدميرها فهي ترتكب عن طريق الحاسوب الألي والانترنت، ولقد بذلت جهود كبيرة من أجل الوصول إلى وضع تعريف مناسب وملائم للجريمة المعلوماتية بغية تطويقها وضمان تعاون دولي لمحاربتها.

قبل التطرق إلى تعريف الجريمة الالكترونية او المعلوماتية نشير إلى توضيح بعض المصطلحات في مجال المعلوماتية، فهذه الكلمة كما يبدو مشتقة من معلومة والمعلومات يستخدمها البعض كألفاظ مترادفة للبيانات، بينما يرى مختصون بأن هذه الأخيرة مجموعة من الحقائق أو المشاهدات أو القياسات التي تكون عادة في شكل حروف أو أرقام أو اشكال خاصة توصف أو تمثل فكرة، وتمثل هذه البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات.[1]

[1] جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الاحكام الموضوعية للجرائم المتعلقة بالانترنت، ط1، دار النهضة، العربية، مصر، 2001، ص 03.

وقد أصبحت المعلومات تشكل قيمة اقتصادية هائلة نظرا لضخامة حجمها وقيمتها وتوصف بكونها تشكل في الوقت الراهن سلعة تباع وتشترى، وبذلك أضحت محل اهتمام عالمي تحظى بالحماية.[1]

الفرع الأول: المصطلحات الدالة على الجريمة

إن التعريف بالجريمة محل الدراسة، يعني بناء تصور ذهني عام ومجرد لإدراكها والإلمام بكامل جوانبها بحيث لا تلتبس بغيرها.

وأنه من شأن إطلاق التسمية المناسبة علي الجريمة محل الدراسة، أن يساعد في التعريف بها وتمييزها عن غيرها.

لقد تنوعت المصطلحات التي أطلقت للتعبير علي الجريمة، وتعددت بتعدد التعاريف التي أعطيت لها.

إن المصطلحات التي أطلقت علي الجريمة محل الدراسة عبر تطورها التاريخي عديدة ومتنوعة، وهي مصطلحات حاولت الجمع بين البعدين القانوني والتقني للظاهرة بنسب متفاوتة، وربما يرجع السبب في ذلك الي التطور الذي تمر به وتنوع واختلاف وسائل ارتكابها وظهور أشكال جديدة مستحدثة بالإضافة الي اختلاف الزاوية التي ينظر من خلالها واضع التعريف[2]، ومن أقدم تلك المصطلحات، مصطلحيCOMPUTER ABUSE وCOMPUTER MISUSE واللذين يعنيان إساءة الاستعمال أو الاستخدام التعسفي لجهاز الكومبيوتر وهما مصطلحين متشابهين من الناحية الظاهرية، لكن الفرق بينهما يتمثل في الدور الذي تلعبه المعلومات، فالمصطلح الأول يستعمل إذا كانت المعلومات هي الهدف من الجريمة أي في حالة إلحاق الضرر بالمعلومات. أما الثاني فيستخدم فيما إذا كانت المعلومات هي الوسيلة كما في حالما إذا تم إلحاق الضرر بواسطة المعلومات، ومن الواضح

[1] كوثر مازوني، الشبكة الرقمية وعلاقتها بالملكية الفكرية، دار هومة للطباعة والنشر، الجزائر، 2008، ص 115.
[2] عبابنة محمود احمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للتوزيع والنشر، عمان، 2009، ص 14.

أن المصطلحين السالفي الذكر لا يميزان بين ما هو سلوك إجرامي وبين ما هو سلوك غير أخلاقي. وبالتالي فهما مصطلحين لا يعبران حتما عن الجريمة محل الدراسة.[1]

كما أطلق للتعبير عن الجريمة، مصطلحي الغش المعلوماتي والاختلاس المعلوماتي ومن الواضح أنهما يمثلان جزءا من الظاهرة الإجرامية محل الدراسة أو فعلين من الأفعال التي فيها إساءة استخدام للحاسوب، وبالتالي لا ينبغي استخدامهما للتعبير عن عموم الظاهرة الاجرامية وعلي إطلاقها.[2]

وقد عبر بعض الباحثين المتخصصين في مجال التقنية وفي مكافحة الجرائم التي لها صلة بالحاسوب عن الظاهرة الإجرامية، بمصطلح جرائم التقنية العالية، ويعاب علي هذا المصطلح أنه يربط بين الجريمة وبين استخدام التقنية العالية، رغم أن مصطلح التقنية العالية في حد ذاته، مصطلح غير محدد واسع وغير دقيق، وهو يدخل في معناه مبتكرات كثيرة غير الحاسوب.[3]

كما أطلق علي الظاهرة مصطلح الجرائم الإلكترونية[4]، ويعاب علي هذا المصطلح ربطه للجريمة بالإلكترونيات وهي ذات مجال واسع يتجاوز الحواسيب إلى غيرها من الأجهزة ذات الطابع الإلكتروني علي غرار الهواتف الذكية وأجهزة البث والأقمار الاصطناعية.

وقد اعتمد رجال الفقه القانوني اللاتيني، مصطلح الجرائم الإلكترونية وهي ترجمة للمصطلح الفرنسي INFORMATIQUE الذي أوجده الفرنسي فيليب دريفس عام 1962 نتيجة قيامه بتجميع المقطع الأول من كلمة معلومات INFORMATION مع المقطع الأخير من كلمة اتوماتيك AUTOMATIQUE لوصف المعالجة الآلية للمعلومات[5]، وقد

---

[1] البعلبكي منير، قاموس المورد: إنكليزي-عربي، دار العلم للملايين، بيروت، 1990.

[2] الشوا محمد، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحوث المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، جمهورية مصر العربية 1993، ص 513.

[3] محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنيت، رسالة ماجستير، جامعة نايف العربية، 2004، ص 29.

[4] يوسف أمير فرج، الجرائم المعلوماتية علي شبكة الانترنيت، دار المطبوعات الجامعية، الطبعة الأولى، الاسكندرية، 2008، ص 107.

5 رستم هشام، قانون العقوبات ومخاطر التقنية، مكتبة الآلات الحديثة، أسيوط، 1992، ص 16.

انتشر استعمال هذا المصطلح، عندما تبنته الأكاديمية الفرنسية للمعلومات في شهر أفريل 1968م وعرفته بأنه علم التعامل العقلاني، الذي يتم على الأخص بواسطة آلات أوتوماتيكية مع المعلومات بحسبانها دعامة للمعارف الإنسانية والاتصالات في شتى مجالات التقنية والاقتصاد والاجتماع [1]، وهناك من يعتبر أن هذا المصطلح غير مناسب، على اعتبار أن الإلكترونية أصبحت الآن فرعا مستقلا بين فروع المعرفة وعلومها، وأن استخدام كلمة الإلكترونية كترجمة عربية للمصطلح الفرنسي INFORMATIQUE ترجمة غير صحيحة، فكلمة الإلكترونية لا تعبر عن عملية المعالجة الآلية التي يفترض أن تتعرض لها المعلومات بحسب المصطلح الفرنسي.[2]

وهذا يؤدي إلى مصطلحين متشابهين هما جرائم تقنية المعلومات INFORMATION TECHNOLOGY CRIME ومصطلح جرائم نظم المعلومات INFORMATION SYSTEMS CRIME، الذين يبدوان أكثر وضوحا من سابقهما في التعبير عن الجرائم التي تقع علي أنظمة أو تقنيات المعالجة الآلية للمعلومات، لكنهما مصطلحين يستندان لفهمهما إلي مصطلح المعلومات وهو من أكثر المصطلحات إثارة للجدل بين الباحثين.[3]

وهناك أيضا مصطلحين شائعين هما جرائم الحاسوب والجرائم ذات الصلة بالحاسوب اللذان انتشر استخدامهما لدي العديد من الباحثين[4]، كما أستعمل في الدليل الخاص بمنع ومكافحة الجرائم المتصلة بالحاسوب الذي أصدرته هيئة الأمم المتحدة في العام 1994 م، وأعتبر هذان المصطلحان دقيقان في التعبير عن الظاهرة، غير أن ظهور الانترنيت وانتشارها وما ترتب عن ذلك من ظهور أنماط جديدة من جرائم الحاسوب تستغل هذه الوسيلة العصرية

1 شتا محمد، الحماية الجنائية لبرامج الحاسوب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001، ص 33.
[2] محمد بن نصير محمد السرحاني، المرجع السابق، ص 30.
[3] رستم هشام، المرجع السابق، ص 23.
[4] PARKER ،DONN ،Fighting Computer Crime: A New Framework For Protecting Information. Hoboken ،New Jersey: John Wiley And Sons.1998

للاتصال، أضاف بعدا جديدا للظاهرة، فظهر مصطلح جديد يعبر عن الأنماط الجديدة من الجرائم وهو جرائم الإنترنت.[1]

وقد اتجه بعض الباحثين إلى الاعتماد علي مصطلح جرائم الحاسوب باعتبار أن جرائم الانترنيت ما هي إلا جزء من جرائم الحاسوب فلا بد من استعمال الحاسوب لارتكاب جرائم الانترنيت، غير أن البعض الأخر ميز بين المصطلحين وأخذ بهما معا فصار يطلق علي الظاهرة، جرائم الحاسوب والانترنت.[2]

كما ظهر في أمريكا مصطلح CYBERCRIME الذي يتكون من كلمتين : CRIME وCYBER، وهي كلمة مشتقة من مصطلحCYBERNETICS، الذي تم تداوله منذ أربعينيات القرن العشرين، للدلالة على دراسة آلية السيطرة والتوجيه في الإنسان والآلة وقد أستخدم مصطلح CYBER في محاولة لتصوير ذلك المكان الافتراضي غير المحسوس حيث تتواجد وتنتقل البيانات الإلكترونية من خلال الحواسيب والشبكات.[3]

وقد حاول بعض الباحثين العرب تعريب مصطلح CYBERCRIME إلى الجريمة التخيلية[4]، لكنها محاولة لم تكن موفقة باعتبار أن ترجمة كلمة تخيلي إلي اللغة الانجليزية تعطي كلمة IMAGINABLE وليس وكلمة CYBER، وهو ما دفع بعض الباحثين إلي تحويل كلمة CYBER تحويلا حرفيا إلي اللغة العربية وأصبحوا يطلقون علي الظاهرة مصطلح الجريمة السيبرانية أو الجريمة السيبيرية تشبيها للفضاء الافتراضي بشساعة المناطق السيبرية، ومن ذلك قيام الدكتور عبد الحي السيد بمناسبة إعداد مشروع تنسيق التشريعات السيبرانية لتحفيز مجتمع المعرفة في المنطقة العربية لفائدة اللجنة الاقتصادية والاجتماعية لغربي آسيا« الإسكوا » باعتماد تسمية الجريمة السيبرانية علي الظاهرة.

---

[1] محمد بن نصير محمد السرحاني، المرجع السابق، ص 30.

[2] محمد بن نصير محمد السرحاني، المرجع نفسه، ص 30.

[3] RIEMER ANDREA K ،An inventory of Preventive Multilateral Activities in the Fields of Computer-related crime and Cyberthreats in Europe. 2001http://www.isn.ethz.ch/crn/intorg/ cyberthreads.pdf.

[4] البشرى محمد الامين، الأدلة الجنائية الرقمية ودورها في الإثبات، المجلة العربية للدراسات الامنية والتدريب، جامعة نايف العربية للعلوم الامينة، الرياض، 2003، عدد 33.

إن المصطلح الأقرب لتوصيف الظاهرة محل الدراسة هو مصطلح جرائم المعالجة الألية للمعطيات أو البيانات، ذلك لأن ربط الجريمة بالمعالجة الألية للمعطيات أو البيانات أمر ضروري وهام لتحديد نطاق التجريم وحصره، وهو يتفق تماما مع مبدأ الشرعية وكذا التفسير الضيق للنصوص الجنائية، ويؤدي ذلك الي نتيجة هامة مفادها اقصاء كل الجرائم التي لا تنصب علي المعالجة الألية للمعطيات أو البيانات من نطاق التجريم، وتفادي عملية التجريم المزدوج، لبعض الوقائع التي قد تقع أصلا في نطاق الجرائم العادية، علي غرار جرائم النصب والاحتيال حتي ولو ارتكبت باستعمال الحاسوب وشبكة الانترنيت، كما أن الجريمة الواحدة قد ترتكب باستعمال عدة طرق ووسائل، فالوسيلة التي ترتكب بها الجريمة ليست معيارا علي طبيعة الجريمة وليس لها أي اثرا علي تصنيفها.

كما أنه لكل جريمة مصلحة تحميها، فاذا تعرضت تلك المصلحة للضرر أو الانتهاك قامت الجريمة واستوجبت العقاب، فالمصلحة التي تحميها الجرائم محل الدراسة هي المعالجة الألية للمعطيات أو البيانات، فكلما تم الحاق الضرر بتلك البيانات والمعطيات التي تم معالجتها أليا بأي طريقة واقترن ذلك بوجود نية جنائية، قامت الجريمة واستوجبت العقاب.

الفرع الثاني: تعريف الجرائم الإلكترونية.

إن البحث في تعريف الجريمة محل الدراسة، يؤدي الي الاصطدام بالكثير من التعاريف الفقهية المختلفة، وهو ما دفع بعض الفقهاء إلي القول أن هذه الجريمة تقاوم التعريف[1]، ورغم الجهود التي بذلتها عدة هيئات دولية في محاولة فهم هذه الظاهرة، غير أن تلك الهيئات وغيرها من الفقهاء عجزوا عن وضع تعريف واحد متفق عليه.[2]

[1] رستم هشام، الجرائم المعلوماتية: أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، بحوث مؤتمر القانون والكمبيوتر والإنترنت، دولة الإمارات العربية المتحدة، 2000، ص6.

[2] الحيسناوي علي جبار، جرائم الحاسوب والانترنيت، دار اليازوري العلمية للنشر والتوزيع، الاسكندرية، 2009، ص 33.

ونظرا لطبيعة الخاصة للجرائم الإلكترونية، أختلف الفقه في وضع تعريف جامع لها لذلك بذل الفقهاء جهودا ما أجل محاولة وضع تعريف لها حيث ظهر اتجاهان: الاتجاه الأول يعرف بالاتجاه التقليدي المحصور في تعريفه، ويعرف الاتجاه الثاني بالاتجاه الموسع لها.

1- المنظور التقليدي للجرائم الإلكترونية:

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وربطها بعناصر عديدة كالحاسوب أو مستخدمه أو بموضوع الجريمة حيث عرفها الفقيه ماروي على أنها: الفعل غير مشروع الذي يستخدم في ارتكابه الحاسب الآلي، وهناك من عرفها على أنها: فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه، وفي تعريف أخر هي: الأفعال غير القانونية المرتكبة بواسطة العمليات الإلكترونية والتي تمس بالنظام المعلوماتي أو بالمعطيات التي يحتويها ومهما كانت الغاية من ذلك.[1]

كما عرفت أيضا أنها: مجموعة الأفعال غير القانونية التي تتم عبر شبكة الانترنت أو تبث عبر محتوياتها.[2]

كما عرفها الفقيه تديمان بأنها: كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي.[3]

كما عرفها الفقيه روزنبلات بأنها: نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه.[4]

---

[1] يزيد أبو حليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري في ضوء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات - قانون العقوبات - قانون الإجراءات الجزائية - قوانين خاصة، دار الجامعة الجديدة للنشر، الإسكندرية، 2019، ص 48.

[2] هروال هبة نبيلة، جرائم الانترنت دراسة مقارنة، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة أبو بكر بالقايد، تلمسان، 2014، ص 2.

[3] غانم مرضي الشمري، الجرائم المعلوماتية، ماهيتها خصائصها وكيفية التصدي لها قانونا، ط1، دار العلمية الدولية للنشر والتوزيع، عمان، 2016، ص 25.

[4] حسن الطوالبة، الجرائم الإلكترونية، ط1، جامعة العلوم التطبيقية، مملكة البحرين، 2008، ص 48.

والتعريف الذي جاء به الأستاذ توم فورستر بأنها: فعل إجرامي يستخدم الكومبيوتر في ارتكابه كأداة رئيسية.[1]

وتعريف تاديمان بأنها: كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب.[2]

ويعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف الحاسب بأنها: الجرائم التي تلعب فيها البيانات الكومبيوترية والبرامج المعلوماتية دورا رئيسيا.[3]

وعليه يربط أنصار هذا الاتجاه تعريفهم لهذه الجرائم بضرورة وجود الحاسب الذي قد يكون أداة للجريمة أو هدفا لها ناهيك عن وجود معارف مسبقة بتكنولوجيا الكومبيوتر ليس فقط من المجرم المعلوماتي، وإنما أيضا من القائمين على ملاحقة هذا النوع من الجرائم، وهذا يضيق على نحو كبير من الجريمة الإلكترونية التي هي في اتساع يوما بعد يوم تبعا لتطور تكنولوجيا المعلوماتية.[4]

2- التعريف الموسع للجرائم الإلكترونية

على عكس الاتجاه السابق يذهب فريق من الفقهاء لضرورة التوسيع من مفهوم الجريمة الإلكترونية أو المعلوماتية وعدم حصرها في الحاسوب وحده أو في موضوع الجريمة أو في شخص مستخدمه وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية.[5]

1 TOM FORESTER ،Essential Proplems To Hig-Tech Society First Mit Pres Edition ، Cambridge ،Massachusetts ،1989 ،P: 104 .

2 TIEDEMANN ،Fraude Et Autres Delits D'affaires Commis A L'aide D'ordinateurs Electroniques. R.D.P.C 1984. N°7; P:61.

3 أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة للنشر، الإسكندرية، 2015، ص 93.

4 يزيد أبو حليط، المرجع السايق، ص 49.

5 يزيد أبو حليط، المرجع السابق، ص 50.

فعرفت على أنها: كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال أو الأشياء المعنوية.[1]

كما عرفها الأساتذة ليستانك و فيفانت أنها: مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب.. كما أن الخبير الأمريكي باركر تبني مفهوما واسعا للجريمة المعلوماتية على أنها: كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل.[2]

كما عرفتها منظمة التعاون الاقتصادي والتنمية بأنها: كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية، كما تعرف أيضا: تلك الجرائم المرتكبة ضد الأملاك باستعمال الثقنية أو المعلوماتية.

كما أورد الدكتور الشوا محمد، في مؤلف له تحت عنوان الغش المعلوماتي كظاهرة إجرامية مستحدثة تعريفا مشابها للتعريف السابق، حيث عرف الغش المعلوماتي بأنه: كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلومات، ويهدف إلى الاعتداء على الأموال المادية والمعنوية.[3]

وتعرف الجرائم الإلكترونية بأنها الجرائم الواقعة على الحاسوب الآلي تعّرف بأنها أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب. والجريمة تلك تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية 4، وذلك نظرا للبيئة التي تتم فيها، أي البيئة الإلكترونية، وهي تشمل الجرائم المنصبة على استغلال

[1] بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري (دراسة مقارنة)، مذكرة مكملة من مقتضيات نيل شهادة الماستر، كلية الحقوق جامعة محمد خيضر، بسكرة، 2016، ص 10.
[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 1، دار الثقافة للنشر وتوزيع، عمان، 2008 ص 49.
[3] الشوا محمد، مرجع سابق، ص8.
[4] أسامة أحمد المناعسة، جلال محمد الزغبي وصايل فاضل الهواوشة، جرائم الحاسب الآلي والأنترنت، ط الأولى، دار وائل للنشر والتوزيع، عمان الأردن، 2001 . ص 78

البيانات المخزنة على الكومبيوتر بشكل غير مشروع، الجرائم التي يتم من خلالها اختراق الكومبيوتر لتدمير البرامج والبيانات الموجودة في الملفات المخزنة، الجرائم التي يكون جهاز الكومبيوتر محلا أو وسيلة لارتكاب الجريمة أو التخطيط لها، وأخيرا الجرائم التي يتم فيها إساءة استخدام الكومبيوتر أو استعماله بشكل غير قانوني من قبل الأشخاص المرخص لهم باستعماله.[1]

وعرفتها هدي قشقوش بأنها: كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات.[2]

كما عرفها الفقيهان TOTTY وARDCASTLE بأنها: تلك الجرائم التي يكون قد وقع في مراح ارتكابها بعض العمليات الفعلية داخل نظام الحاسوب، وبعبارة أخرى هي تلك الجرائم التي يكون دور الحاسوب فيها إيجابيا أكثر منه سلبيا.[3]

ويعرفها الأستاذان ROBERT J.LINDQUIST ،JACK BOLOGNA بأنها: جريمة يستخدم فيها الحاسوب كوسيلة أو أداة لارتكابها أو يمثل إغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها.[4]

إن هذه التعريفات واسعة تتيح الإحاطة الشاملة قد الإمكان بظاهرة جرائم التقنية، كما أنها تعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية.

[1] زيبحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011 . ص 44.

[2] هدي قشقوش، جرائم الحاسوب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، 1999، ص 20.

[3] TOTY AND HARDCASTLE: Computer Related Crime In Information Technology and the law U .K.1986 ;P26 .

[4] TOTY AND HARDCASTLE ،Ouvrage Precedent ،P26.

وتعريف PARKER لجريمة الحاسوب بأنها: كل سلوك سيئ متعمد يتطلب معرفة بنظم المعلومات وينتج عنه على وجه التأكيد أو الاحتمال، إما معاناة الضحية أو حصول الجاني على مكسب غير مستحق.[1]

وهو نفس التعريف الذي قال به الدكتور حسن داود بقوله: أن جريمة الحاسوب هي السلوك السيئ المتعمد الذي يستخدم نظم المعلومات لإتلاف المعلومات أو إساءة استخدامها، مما يتسبب أو يحاول التسبب، إما في إلحاق الضرر بالضحية أو حصول الجاني على فوائد لا يستحقها.[2]

يلاحظ علي هذين التعريفين أنها يربطان قيام الجريمة بتحقيق النتيجة الإجرامية وهي أن يلحق ضرارا بالضحية أو أن يحصل الجاني علي مكاسب غير مستحقة. وهما بذلك لا يشملان العديد من الجرائم الإلكترونية التي لا يلحق فيها بالضحية أي ضرر ولا يحقق من ورائها الجاني أي مكاسب، كما هو الشأن في بعض جرائم اختراق الشبكات والأنظمة الإلكترونية.

ويعرفها خبراء منظمة التعاون الاقتصادي والتنمية في عام 1983 على أنها: كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها، إذ يعتمد هذا التعريف على معيارين: أولهما وصف السلوك، وثانيهما اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها، كما يجمع الفقه الفرنسي بصفة عامة على القول بأن فكرة الغش المعلوماتي التي تعادل جرائم الحاسب الآلي تشمل العديد من الأفعال المتنوعة، حيث عرف كل من الفقيه ميشال والفقيه ريدو الجريمة المعلوماتية بأنها: سوء استخدام الحاسب ويشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، وكذا الاستخدام غير المشروع لبطاقات الائتمان وانتهاك ماكينات الحاسب الألية بما تتضمنه من

[1] PARKER DONN B ،Ouvrage Precedent ،P ; 57-58.

[2] داود حسن، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، : 2000، ص 32.

شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب وسرقة الحاسب الآلي في حذ ذاته أو أي مكون من مكوناته.[1]

وبذلك تمثل هذه التعاريف المفهوم الموسع للجرائم الإلكترونية، والتي تتم بالحاسوب سواء كان هدفا لها أو وسيلة لارتكابها، أو عن طريق شبكة الإنترنت أو بأي وسيلة إلكترونية أخري تظهر مستقبلا كوسائل الاتصال الحديثة مثل الهاتف النقال وجهاز الفاكس وغيرها.[2]

3- تعريف الجريمة الإلكترونية في التشريع الجزائري

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب أحكام المادة 2 من القانون رقم 04-09 على أنها: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، أو أية جريمة أخري ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية.[3]

ويلاحظ من هذا التعريف ما يلي:[4]

أولا: أن المشرع الجزائري اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكترونية، وثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

[1] يزيد أبو حليط، المرجع السابق، ص 50.
[2] يزيد أبو حليط، المرجع السابق، ص 51.
[3] المادة 02 من القانون رقم 04-09 المؤرخ في 14 شعبان عام 1430، الموافق ل 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47.
[4] إسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد11، سبتمبر، مسيلة، 2018، ص 353.

ثانيا: كما حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الإلكترونية في القانون الجزائري.

المطلب الثاني: محددات الجرائم الإلكترونية

تتحدد الجرائم الإلكترونية بطبيعة خاصة، تميزها عن الجرائم التقليدية، فهي جرائم ترتبط أساسا بالتقنية الإلكترونية وبالأنترنيت، وهي جرائم خفية لا تحدث ضجة ويمكن ارتكابها عن بعد كما انها لها اثار مدمرة وعابرة للحدود الوطنية.

الفرع الأول: المحددات المرتبطة بالجريمة في حد ذاتها.

تعتبر الجريمة الإلكترونية من الجرائم الأكثر انتشارا واتساعا فهي جريمة لا تعترف بالحدود الجغرافية، كما أنها من الجرائم الخطرة بل الأكثر خطورة، وفي نفس الوقت الأكثر صعوبة في الاكتشاف والاثبات.

1) <u>الجرائم الإلكترونية عابرة للحدود:</u>

يمكن القول أن من أهم محددات الجريمة الإلكترونية هي تخطيها للحدود الجغرافية، أو كما يطلق عليها أنها جرائم ذات طبيعة متعددة الحدود، فبعد ظهور شبكة الانترنيت واتساعها لتشمل كل دول العالم، لم تعد الحدود عائقا تقف أمام نقل وتدفق المعلومات عبر الدول مهما تباعدت، فالقدرة التي تتمتع بها الحواسيب في نقل وتبادل كم هائل من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مفادها أن أماكن متعددة من دول مختلفة قد تتأثر بالجريمة الإلكترونية الواحدة في آن واحد فالجريمة الإلكترونية تتميز بالسرعة في التنفيذ وكبر حجم المعلومات والأموال المستهدفة، والمسافة الكبيرة التي تفصل الجاني عن تلك المعلومات والأموال.

فاتساع نطاق الجريمة الإلكترونية جعلها صعبة المتابعة والاثبات، فقد يرتكب الجاني سلوكه الجرمي في الدولة ما وتتحقق النتيجة في الدولة أخرى، فهي علي هذا الصعيد تطرح العديد من الاشكاليات، تتعلق بالاختصاص القضائي في متابعة مرتكب الجريمة، لا سيما مع عدم تناسق التشريعات العقابية في هذا المجال خاصة مع إختلاف التشريع المعتمد في الدول، ناهيك عن الاشكاليات الأخرى المتعلقة بغياب التعاون القضائي الدولي في مجال البحث والتحري والتحقيق وتسليم المجرمين وقلة الخبرة والتكوين.

بمعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا إذ إن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي تم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد أخر وهو بهذا السلوك قد يضر شخص أخر موجود في بلد ثالث.[1]

2) خطورة الجرائم الإلكترونية:

لقد دفعت المزايا التي توفرها تقنية الإلكترونية من سرعة ودقة وتطور مستمر إلي انتشار استخدامها علي نطاق واسع وفي شتي مجالات الحياة الخاصة والعامة. بل إن استخدم الإلكترونية أصبح أمرا حتميا لدي المؤسسات المالية والبنكية كما أضحي لدي الدول المتطورة وسيلة لا غني عنها في نتظيم مختلف نواحي الحياة العامة، بعدما تبنت مفهوم الحكومة الكترونية. وهو الأمر الذي زاد في خطورة الجرائم الإلكترونية، كون أن أنشطة

[1] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2013، ص 31.

الاعتداء علي تلك الأنظمة والشبكات الإلكترونية قد تخلف خسائر مالية معتبرة وأضرار لا تلحقها أخطر الجرائم التقليدية.[1]

إن خطورة الجريمة الإلكترونية تبرز على مستويين:

أ- على مستوى الفرد:

فلقد أصبح الفرد في عالمنا اليوم أكثر ارتباطا مما سبق باستخدام التقنية الإلكترونية في قضاء بعض مصالحه، بل أصبح في بعض الدول المتطورة ينجز تعاملاته ويدير أعماله وبحوثه ويتواصل مع العالم الخارجي عن طريق استخدام الانترنت. وهو ما يجعله هدفا سهلا للجرائم الإلكترونية التي قد تستهدف، انتهاك حرمة حياته الخاصة وخصوصيته وقرصنة هويته الشخصية وأرقام بطاقاته الائتمانية وابتزازه وتهديده والاحتيال عليه وسرقة مؤلفاته أو إبتكاراته أو ملفات خاصة به علي غرار الصور العائلية والأفلام.... الخ.

ب- على مستوى المؤسسات والهيئات العامة والخاصة:

إن الاتجاه الغالب لدي المؤسسات والهيئات العامة والخاصة، القيام بتسيير شؤونها وإدراة نشاطها وتقديم خدماتها عن بعد وعلي مدار الساعة واليوم، بالاستعانة بالشبكات الإلكترونية لا سيما شبكة الانترنيت التي تمكن من أداء الخدمة بسرعة ودقة وجودة. لكن ورغم تلك المزايا فإن تزايد حجم أنشطة الاعتداء علي تلك المؤسسات والهيئات، في إطار الجرائم الإلكترونية قد تلحق بها أضرار جسيمة قد تتصل الي حد الاطلاع على معلومات سرية لصفقة أو مناقصة أو أمور تسويقية خاصة والاستفادة منها والعبث بمخازن المعلومات الخاصة بالشركة بحذفه أو تعديلها أو تعطيل الوصول إليها وسرقة الأموال وتحويل الحسابات المصرفية الخاصة بالشركة والغش في المعاملات الالكترونية كالتغيير في المبيعات، السطو الإلكتروني، تعطيل الأنظمة الإلكترونية... الخ.

[1] أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الأولي، دار الفكر العربي، الاسكندرية، 2005، ص 107.

3) صعوبة الاكتشاف والإثبات:

تتميز الجريمة الالكترونية بصعوبة اكتشافها وإثباتها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادةء حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء صعوبة في اكتشاف الجريمة الالكترونية وإثباتها إلى عدة عوامل منها.[1]

أولا: أن الجريمة الالكترونية لا تترك أثار مادية، فهي جريمة تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية ولا توجد مستندات ورقية، فهذه الجريمة عبارة عن أرقام تتغير في السجلات فالجريمة الالكترونية لا تترك شهودا يمكن استجوابهم ولا أدلة يمكن فحصها.

ثانيا: صعوبة الاحتفاظ بدليل الجريمة الالكترونية، إذ يستطيع المجرم في أقل من ثانية أن يمحو أو يحرف أو يغير المعلومات الموجودة في الكمبيوتر.[2]

ثالثا: تحتاج الجريمة الالكترونية لاكتشافها إلى خبرة فنية، حيث تتطلب جريمة الكمبيوتر إلمام ومعلومات واسعة سواء لارتكابها أو التحقيق فيها، كما أن رجال الضبطية القضائية يجدون صعوبة للتعامل مع الدليل الالكتروني، فقد يتسبب المحقق دون قصد في إتلاف الدليل الالكتروني أو تدميره كما في حالة محو البيانات الموجودة على الأسطوانة الصلبة أو قد لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو الطابعة أو الماسح الضوئيء لذلك أصبح من الضروري في وقتنا إجراء دورات تدريبية لرجال الضبطية القضائية ورجال القضاء والخبراء والفنين للتعاون فيما بينهم وصولا إلى أحسن الطرق لمكافحة الجريمة الالكترونية.

---

[1] ثنيان ناصر آل ثنيان، إثبات الجريمة الالكترونية دراسة تأصيلية تطبيقية، رسالة ماجستير، كلية الدراسات العليا قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص 24.

[2] حسين فريجة، الجرائم الالكترونية والانترنت، مجلة المعلوماتية، العدد 36، أكتوبر، 2011، ص 3.

رابعا: تعتمد الجريمة الالكترونية على الخداع والذكاء في التعرف على مرتكبيها، إن الذي يساعد على عدم التعرف على مرتكبي الجرائم الالكترونية هو إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم تجنبا للإساءة إلى سمعتها وهز ثقة العملاء بها، وإخفاء أسلوب ارتكاب الجريمة خوفا من قيام الأخريين بتقليد هذا الأسلوب، وهو ما يدفع المجني عليه إلى الإحجام عن إبلاغ السلطات المختصة بها، كما أن الجريمة المعلوماتية تعتمد على الذكاء وهي جريمة فردية تعتمد على مهارات عالية وإلمام بتكنولوجيا النظم المعلوماتية.[1]

كما أن صعوبة إكتشاف الجريمة الإلكترونية، أو اكتشافها بعد زمن طويل، يجعل من مسألة الإثبات في بعض الأحيان شبه مستحيلة، فلطالما كان إثبات الجرائم التقليدية يتستند الي قرائن وأدلة مادية ملموسة، وهو الأمر الذي قد لا يتوفر في جرائم الإلكترونية التي يقع مجال ارتكابها في الكيان المنطقي واللامحسوس ضمن شبكة الانترنيت أو الأنظمة الإلكترونية وأنظمة المعالجة الألية للمعلومات. إضافة الي أن المجرم المعلوماتي هو مجرم يتمتع بالذكاء والمهارة والمعرفة باستعمال التقنية الإلكترونية، وهو غالبا ما يلجأ بعد تنفيذ جريمته الي محو الأدلة التي تسمع بتقفي اثره بسرعة فائقة[2]، لذلك فإن هذا النوع من الجرائم لا يترك أثرا ملموسا ولا يخلف ورائه دليلا ماديا.

وتثار مسألة صعوبة الاثبات كذلك علي المستوي التشريعي، فان كانت بعض الدول قد قامت بتجريم بعض الأفعال والنشاطات الإجرامية علي اعتبار أنها جرائم معلوماتية، غير أنها لم تحيين النصوص القانونية المتعلقة بالإثبات ولم تعترف بالدليل الرقمي الذي يعد أهم وسيلة في إثبات الجرائم الإلكترونية.

[1] حسين فريجة، المرجع السابق، ص 3.
[2] نائلة عادل محمد فريد، جرائم الحاسوب الألي الاقتصادية، الطبعة الاولي، دار النهضة العربية، القاهرة، ص 49.

كما أن مسألة الإثبات تثار علي صعيد أخر وهو صعيد التعاون الدولي في مكافحة الجرائم الإلكترونية، وكما تطرقنا سابقا الي أن الجريمة الإلكترونية لا تعترف بالحدود الجغرافية، فأن مسالة إثباتها قد تتسع الي أكثر من نطاق جغرافي واحد. ويتطلب الأمر تكاثف الجهود والتعاون الدولي في مسائل البحث والتحري عن الجرائم وإثباتها وتسليم المجرمين ومحاكمتهم.

4) السرعة في التنفيذ

مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف؛ أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة.[1]

تتميز جرائم الانترنت بأنها جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوي تقني يوظف في ارتكاب الأفعال غير المشروعة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو الغرير بالقاصرين، فمن هذا المنطلق تعد الجريمة المرتكبة عبر الانترنت من الجرائم النظيفة فلا أثار فيها لأية عنف أو دماء وإنما مجرد أرقام وبيانات يتم تغيرها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي.

[1] يوسف الصغير، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون الخاص، كلية الحقوق، جامعة مولود معمري تيزي وزو، 2013، ص 16.

الفرع الثاني: المحددات المرتبطة بالمجرم المعلوماتي

جرى الاعتقاد بوجود علاقة وثيقة بين الفقر، المستويات الاجتماعية الدنيا، كالجهل وغير ذلك من الآفات الاجتماعية من جهة وبين الجريمة من جهة ثانية، غير أن ذلك الاعتقاد لم يعد صحيحا مع ظهور الأشكال الجديدة من الاجرام، كالجرائم الإلكترونية، التي أصبح يطلق عليها إعلاميا عبارة جرائم النخبة أو جرائم "أصحاب الياقات البيضاء"، مع ما للتعبيرين من وحي إيجابي، فمصطلح النخبة أو لها دلالة على الخطورة والتفوق، وهي الصفات التي قلما يمكن تتصورها في المجرم التقليدي. وهو في هذا الشأن بخلاف المجرم المعلوماتي الذي يظهر في المجتمع بصفة المتميز ذو المكانة الاجتماعية المرموقة، الذي يجد مبرارات لارتكاب جرائمه ويرى أن هناك أهدافا نبيلة تحركه خاصة اذا كان نشاطه موجها ضد مؤسسة أو هيئة أو جماعة لها انتماء ما.

لقد تطرق العديد من الكتاب الي السمات والخصائص التي يتميز بها المجرم المعلوماتي عن غيره من المجرمين، ولعل أكثر تلك المميزات، هي تلك التي أشار اليها الأستاذ PARKER بكلمة **S.K.R.A.M** وهي تعني: المهارة **S**KILLS، المعرفة **K**NOWLEDGE، الوسيلة **R**ESOURCES، السلطة **A**UTHORITY، والباعث **M**OTIVES[1].

فالمهارة: هي أبرز سمة يتمتع بها المجرم المعلوماتي، ويقصد بها المهارة في إستعمال أجهزة الحاسوب ومختلف البرامج المتعلقة به والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال، أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات، أو بمجرد التفاعل الاجتماعي مع الآخرين، إلا أن ذلك لا يعني ضرورة أن يكون المجرم المعلوماتي على قدر كبير من العلم في هذا المجال. بل إن الواقع العملي قد أثبت أن بعض

[1] Parker Donn B ،Ouvrage Precedent ،P ;114

أنجح مجرمي الإلكترونية لم يتلقوا المهارة اللازمة لارتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال.

أما المعرفة: فيقصد بها أدراك المجرم المعلوماتي لماهية الحاسوب ومكوناته ومفهوم النظام المعلوماتي وأساسيات عمل شبكات الحاسوب ومصطلحاتها، وكيفيات اختراق الشبكات والحواسيب واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويل مسارها، والبرامج المعدة لذلك الغرض، كما تتوفر لدي المجرم المعلوماتي غالبا المعرفة بالظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، إذ أنه باستطاعة المجرم المعلوماتي أن يكون تصورا كاملا لجريمته.

أما الوسيلة: فيقصد بها مختلف المعدات والتجهيزات والبرامج التي يتزود بها المجرم لارتكاب جريمته أو لإخفاء أثرها، علي غرار أجهزة الحاسوب والبرامج وهي في الغالب تجهيزات وبرامج غير مكلفة بالنظر الي الأضرار أو الخطورة التي تتميز بها الجريمة في حد ذاتها، ومن بين الوسائل التي يعتمد عليها المجرم المعلوماتي في تنفيذ جريمته نذكر، الشفرات الخبيثة، وهي برمجيات صممت لتنتقل من حاسوب إلى آخر ومن شبكة إلى أخرى بهدف إجراء تعديلات في أنظمة الحاسوب عمدا وبدون موافقة مالكي أو مشغلي هذه الأنظمة، مثل الفيروسات.[1]

أما السلطة: فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم المعلوماتي والتي تمكنه من ارتكاب جريمته، قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات والتي تعطي الفاعل مزايا متعددة كفتح الملفات ومحو أو تعديل المعلومات التي تحتويها أو مجرد قراءتها أو كتابتها، وقد تتمثل هذه السلطة في الحق في

[1] الفيروس Virus: هو نوع من أنواع البرمجيات التخريبية الخارجية، صنعت عمدا بغرض تغيير خصائص ملفات النظام. تتكاثر الفيروسات عن طريق توليد نفسها بنسخ شفرتها المصدرية وإعادة توليدها، أو عن طريق إصابة برنامج حاسوبي بتعديل خصائصه، إصابة البرامج الحاسوبية يتضمن، ملفات البيانات، أو قطاع في القرص الصلب.

استعمال الحاسوب الآلي أو إجراء بعض التعاملات. وقد تكون هذه السلطة غير حقيقية كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.

ويقصد بالباعث: الدافع أو الهدف المتوخي وراء ارتكاب الجريمة، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة الإلكترونية غير أن البعض يرى أن أغلب مجرمي الإلكترونية ليس لديهم أطماع مادية بقدر ما يحاولون حل مشكلات مادية تواجههم لا يستطيعون حلها باللجوء إلى الجرائم الأخرى[1]، ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسوب وتخطي حواجز الحماية المضروبة حوله، وأخيرا الانتقام من رب العمل أو أحد الزملاء، حيث يفرق مرتكبي هذه الجرائم بين الأضرار بالأشخاص، الأمر الذي يعدونه غاية لا أخلاقية، وبين الإضرار بمؤسسة أو جهة في استطاعتها اقتصاديا تحمل نتائج تلاعبهم.[2]

وقد قامت بعض الدراسات الي تصنيف مجرمي الإلكترونية إلى سبعة مجموعات مختلفة، تتمثل فيما يلي[3] :

المجموعة الأولى: وهم الأشخاص الذين يرتكبون جرائم الإلكترونية بغرض التسلية والمزاح مع الآخرين، بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم.

المجموعة الثانية : وهي تضم الأشخاص الذين يهدفون إلى الدخول إلى أنظمة الحاسوب غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة، أو بدوافع الفضول أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

---

[1] PARKER DONN B ،Ouvrage Precedent ،P ;142

2 هشام محمد فريد رستم، الجوانب الاجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، مصر، 1994، ص 38.

3 نائلة عادل محمد فريد، مرجع سابق، ص 48.

المجموعة الثالثة: وتضم الأشخاص الذين يرغبون في الحاق خسائر بالمجني عليهم دون أن يكون الحصول على مكاسب مالية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثيرون من مخترقي فيروسات الحواسيب وموزعيها.

المجموعة الرابعة: وهم الطائفة الأكثر شيوعا بين مجرمي الإلكترونية، فهم يقومون بارتكاب جرائم الإلكترونية التي تلحق بالمجني عليهم خسائر ولا يستطيع حلها بالوسائل الأخرى بما فيها اللجوء إلى الجريمة التقليدية.

المجموعة الخامسة: وهم مجرمي الإلكترونية الذين يبتغون تحقيق الربح المادي بطريقة غير مشروعة، ويقترب المجرم المعلوماتي المنتمي إلى هذه الطائفة في سماته من المجرم التقليدي.[1]

المجموعة السادسة: وتضم المنظمات الاجرامية كالجماعات الإرهابية وأفراد الجريمة المنظمة، وغيرها من المجموعات التي تربط بين أفرادها معتقدات وأفكار اجتماعية أو سياسية أو دينية وتسعي إلي فرضها باللجوء إلى النشاط الإجرامي لاسيما عبر شبكات الانترنيت وذلك بالإتيان بسلوكات مخالفة للقانون ومجرمة كالترويج للأفعال الإرهابية أو التخريبية، للفت الأنظار إلى ما يدعون إليه، وان اعتماد المؤسسات المختلفة داخل الدول على أنظمة الحواسيب في إنجاز أعمالها والأهمية القصوى للمعلومات التي تحتويها في أغلب الحالات قد جعل من هذه الأنظمة هدفا جذابا لهذه الجماعات، ومن الأمثلة الشهيرة في هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة في أوربا باسم THE RED BRIGADES بتدمير ما يزيد عن 60 مركزا للحواسيب خلال الثمانينات لتلفت النظر إلى أفكارها ومعتقداتها.[2]

المجموعة السابعة وتضم مجرمي الإلكترونية المعنيين بإساءة استخدام الحواسيب، والإهمال الذي يترتب عليه نتائج خطيرة قد تصل إلى الحاق أضرار مالية بليغة او ازهاق الأرواح.

---

[1] PARKER DONN B ،Ouvrage Precedent . P144-146.

[2] نائلة عادل محمد فريد، مرجع سابق، ص 63.

المبحث الثاني: مفهوم الأدلة الجنائية في الجرائم الإلكترونية

من المعلوم أن إثبات الجريمة يكتسي أهمية بالغة إذا أن الغاية في الإثبات هي الوصول إلى الحقيقة، فالجريمة واقعة من الماضي وليس بالإمكان معاينتها والتعرف على حقيقتها واسنادها للمتهم والقضاء بشأنها لا يتم إلا بالاستعانة بوسائل تجسد صورتها كما حدثت وهذه الوسائل هي ما يسمى بأدلة الإثبات فالاهتمام يبدأ في صورة الشك والقاضي يمحص هذا الشك بأدلة الإثبات فيصل بالشك إلى اليقين.

والملاحظ أن الإتبات يختلف بين أحكام القانون المدني والجنائي كلية ففي الجانب المدني عرفه الدكتور عبد الرزاق السنهوري في كتابة الوسيط في شرح القانون المدني بقوله: الإثبات بمعناه القانوني هو على مبدأ البيّنة على من ادعى أنّ الاثبات الجنائي سيقع على عاتق النيابة التي حركت الدعوى.[1]

هذا فضلا على أن أوجه الاختلاف بين الإثبات الجنائي و المدني أن مبدأ الحياد للقاضي المدني دون أن يتدخل في توجيه الأطراف على عكس القاضي الجزائي الذي هو ملزم بالبحث والتحري للوصول إلى الحقيقة، يقتضي منا فهم ماهية وصورة الأدلة المتحصلة من الوسائل الإلكترونية، فهم معني الادلة بوجه عام، ثم التطرق الى ماهية الأدلة المتحصلة من الوسائل الالكترونية.

[1] عبد الرزاق السنهوري، الوسيط في شرح القانوني المدني، الجزء الثاني، دار احياء التراث العربي، بيروت، لبنان، 1952، ص 67.

المطلب الأول: تعريف الأدلة الجنائية

أطلقت على الإثبات الجنائي تعاريف عديدة منها ما أوردها الدكتور هلالي عبد اللاه أحمد بأن: الإثبات هو التنقيب على الدليل وتقديمه وتقديره لاستخلاص السند القانوني للفصل في الدعوى وأضاف بأن الإثبات أعم وأشمل من كلمة دليل.[1]

وتعد الأدلة بصفة عامة من المسائل الهامة في القانون والفقه، لطالما حظيت باهتمام الكثير من الدراسات الفقهية والقانونية، ذلك لأن الحق من دون دليل كالعدم، فالدليل وحده هو الذي يظهر الحق ويثبته، والإثبات هو جوهر الحق وأساسه.

وتعد الأدلة الجنائية من أهم أنواع الأدلة علي الإطلاق لما لها من أهمية بالغة في إثبات الجرائم ومعاقبة مرتكبيها، وحماية المصلحة العامة والدماء والأموال والممتلكات والحرمات من الانتهاك، وفي نفس الوقت ضمان حقوق الانسان وحرياته من الضياع، أي أن للأدلة الجنائية أهمية كبيرة في الموازنة بين المصلحة العامة وحمايتها وبين المصلحة الخاصة للأفراد، وهي الوسيلة الوحيدة لدحض قرينة البراءة التي يتمتع بها كل فرد في المجتمع.

فالدليل كل وسيلة مرخص بها أو جائزة قانونا لإثبات أو نفي الواقعة المرتكبة، أو هو الوسيلة التي يستعين بها القاضي للوصول إلى اليقين القضائي الذي يقيم عليه حكمه في ثبوت الاتهام المعروض عليه، أو هو ببساطة كل ما يؤدي إلى كشف الحقيقة المبحوث عنها في جريمة معينة[2]، وهناك شروط من الواجب أن تتوفر في الدليل الجنائي وأولها

[1] عبد اللاه أحمد هلالي، النظرية العامة للإثبات في المواد الجنائية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 1987، ص 340.

[2] عمار عباس الحسيني، التحقيق الجذ الحديثة في كشف الجريمة، الطبعة الأولى، منشورات دار الحلبي، لبنان، 2015، ص 146.

المشروعية بمعنى أن يكون الحصول عليه وفقا للإجراءات القانونية وأن يكون له أصلا في الدعوى ولا يشوبه غموض.[1]

إن مفهوم الأدلة الجنائية قد يختلط في نفس الوقت مع بعض المفاهيم المتقاربة له علي غرار مفهوم الاثبات الجنائي، ومفهوم الاستدلال الجنائي ومفهوم الدلالة، مما يوجب توضيح الأدلة الجنائية وأنواعها وما هو الفرق بينها وبين المفاهيم المشابهة لها.

الفرع الأول: تعريف الأدلة الجنائية وتمييزها عن المفاهيم المشابهة لها.

أولا: تعريف الادلة الجنائية:

أ- **الأدلة اللغة:** الأدلة جمع دليل، والدليل هو ما يستدل به، والدليل الدال أيضا، وهو المرشد والكاشف، من ذلك دللت علي الشيئ ودللت اليه، وقد دله علي الطريق، يدله بالضم، دلالة بفتح الدال وكسرها وهو اسم، والمصدر دلولة وهو ما يقتضيه اللفظ علي إطلاقه، ومنه الامارة، أي العلامة حيث لم يفرق الفقهاء بين الأمارة وبين الدليل، وهي عند الأصوليين الدليل الظني، ومنه البرهان، أي الحجة والدلالة، ويطلق علي ما يقتضي الصدق لا محالة، ومنه الحجة: وهو ما تثبت به الدعوي من حيث الغلبة علي الخصم.[2]

ب- الأدلة الجنائية اصطلاحا:

يعرف فقهاء القانون الوضعي، فقد أوردوا لها العديد من التعاريف، منها: أنها الواقعة التي يستمد منها القاضي البرهان علي إثبات اقتناعه بالحكم الذي ينتهي اليه.[3]

ومنها: أنها الوسيلة الاثباتية المستخدمة في تحقيق اليقين لدي القاضي أو في ترجيح موقف الشك لديه.[1]

[1] عبد الله أوهايبية، شرح الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومة، الجزائر، 2008، ص 279.
[2] محمد كمال عواد، الضوابط الشرعية والقانونية للأدلة الجنائية، دار ريم للنشر والتوزيع، 2011، ص 26.
[3] مأمون سلامة، قانون الاجراءات الجنائية، الطبعة الاولي، دار الفكر، 1980، ص 764.

ومنها: أنها الوسيلة المبحوث عنها في التحقيقات بغرض إثبات صحة واقعة تهم الجريمة أو ظرف من ظروفها المادية أو الشخصية.[2]

إن التعاريف السابقة وإن اختلفت صيغها، غير أنها تصب في مفهوم واحد، وهو أن الأدلة الجنائية هي الوسيلة أو الأداة التي يتم عبرها إثبات أو نفي صحة واقعة ما وإسنادها لشخص معين، فالأدلة الجنائية هي الوسائل التي يستعان بها في مراحل الدعوى الجنائية لكشف الحقيقة التي تؤدي الى اقتناع القاضي.

ثانيا : التمييز بين الأدلة الجنائية وبين المفاهيم المشابهة لها.

1-التمييز بين الأدلة الجنائية وبين الاثبات الجنائي:

لقد استعمل الفقهاء لفظي الدليل والإثبات كمترادفين، رغم أنه قد يكون لهما مدلولين مختلفين، فمعني الإثبات كألية يختلف عن معني الإثبات كنتيجة فالإثبات الجنائي كألية، يعني إقامة الدليل لدي الجهات المختصة علي حقيقة واقعة ذات أهمية قانونية بالطرق والقواعد التي يحددها القانون. فالإثبات الجنائي بذلك يكون أوسع مدلولا من مفهوم الدليل، بل إن الدليل الجنائي في هذه الحالة هو خلاصة عملية الاثبات الجنائي التي تمر بعدة مراحل، التي تنطلق بعملية البحث والتحري ثم التحقيق الجنائي وصولا الي المحاكمة الجنائية وهي المرحلة الاخيرة التي يكون فيها القاضي قناعته بما توصلت اليه عملية الاثبات الجنائي وما تمخضت عنه من أدلة إثبات أو نفي. أما الاثبات الجنائي كنتيجة فهو يعني النتيجة التي إنتهت إليها عملية الاثبات وهي اقامة الدليل علي صحة واقعة جنائية معينة واسنادها لمرتكبها. وهنا يكون الإثبات مرادفا للدليل.

[1] أحمد ضياء الدين محمد خليل، رسالة دكتوراه: مشروعية الدليل في المواد الجنائية، جامعة عين شمس، 1982، ص 366.

[2] حمدي الجاسم، أصول المحاكمات الجزائية، مطبعة عبد العالي 1962، ص 237.

2-التمييز بين الأدلة الجنائية وبين الاستدلال الجنائي:

يقصد بالاستدلال الجنائي، القيام بجمع المعلومات بشأن واقعة جنائية معينة قصد معاونة سلطة التحقيق علي اتخاذ قرارها بتحرك الدعوي العمومية أو حفظها. [1] فعملية الاستدلال الجنائي إذن، هي عملية سابقة عن عملية التحقيق القضائي، وهي بذلك لا ينتج عنها أي دليل، لأن الدليل لا ينشأ الا في ظل الضوابط والضمانات التي يقررها القانون. فمثلا لا يمكن اعتبار التصريحات التي يدلي بها المشتبه فيه أمام عناصر الضبطية القضائية بارتكابه لجريمة ما اعترافا جنائيا، لأنها لم تنشأ في ظل الضوابط والضمانات القانونية التي يجب أن ينشأ فيها الدليل الجنائي علي غرار حقوق الدفاع، وضمانات الحياد... الخ، وبذلك فان تلك التصريحات لا ترقي الي مرتبة الدليل الجنائي، ولا يؤخذ بها الا علي سبيل الاستدلال. ومما سبق نستنتج أن عملية الاستدلال تكون سابقة لعملية الاثبات الجنائي أو عملية الحصول علي الدليل الجنائي.

3-التمييز بين الأدلة الجنائية وبين الدلالة:

الدلالة، الجمع دلائل، وهي عملية الاستنتاج العقلي الذي يمارسه القاضي لإيجاد الصلة بين واقعتين، بهدف التوصل الي معرفة حكم الواقعة المعلومة أو الثابتة بالنسبة له[2]. وهي بهذا المعني تشبه القرينة إلا أنها أقل درجة في الاثبات منها. فالقرينة هي ما يستنبطه المشرِّعُ أو القاضي من أمر معلوم على أمر مجهول أو هي استنتاج شيء معيّن إذا توافرت الوقائعُ التي يعتبرها القانون أساسا لهذا الاستنتاج بدلا من الاعتماد على الوقائع والظروف المحتملة. في حين أن الدلالة تحتمل صور شتي من التأويل والاحتمال. وهي بذلك تصلح أساسا لتوجيه الاتهام أو أساسا لبداية الإثبات، ولا تصلح لأن تكون أساسا للإدانة لأن مبناها

[1] أبو العلاء علي النمر، دراسة تحليلية، الاثبات الجنائي، دار النهضة العربية، الطبعة الثانية، ص 05.
[2] كمال محمد عواد، الضوابط الشرعية والقانونية للأدلة الجنائية، دار ريم للنشر والتوزيع، 2011، ص 41.

غير يقيني ولا تبني الادانة الا علي اليقين. وبذلك تختلف الدلالة عن الدليل في درجة الاثبات ودرجة اليقين.

4-التمييز بين الأدلة الجنائية ووسيلة الحصول عليها:

قد يلتبس الأمر لدي البعض، بخصوص التمييز بين الأدلة الجنائية وبين الوسائل الإجرائية التي قررها القانون للحصول عليها، فيعتقد أن تلك الوسائل الاجرائية أدلة جنائية، والحقيقة خلاف ذلك، ذلك لأن الوسائل الإجرائية ما هي الا شكليات قررها القانون وحدد لها ضوابط وأحاطها ببعض الضمانات الغرض منها البحث عن الأدلة الجنائية خلال مباشرة عملية التحقيق القضائي. وبمعني أخر، فإن الوسائل الاجرائية هي الايطار الشكلي للأدلة الجنائية، فيها وفي إطارها يتم استخلاص الدليل الجنائي الذي يعتمد عليه القاضي في تكوين اقتناعه. فأعمال الخبرة أو التفتيش أو المعاينة والاستجواب وما الي غير ذلك من وسائل اجرائية لا تعتبر أدلة جنائية، وإنما ما يتمخض عن تلك الإجراءات من نتائج إيجابية هو ما يمكن إعتباره كدليل جنائي.[1]

الفرع الثالث: أقسام الأدلة الجنائية.

إن الأحكام ينبغي أن تبنى على الجزم واليقين لا على الظن والاحتمال فينبغي على القاضي دائما أن يؤسس اقتناعه بالإدانة على أدلة قوية وقاطعة لا يشوبها الغموض والإبهام ولا يعتريها التناقض فيما بينها[2]، ولقد انقسم الفقه بشأن مسألة إطلاق أو تقييد الأدلة الجنائية إلي ثلاثة اتجاهات رئيسية، اتجاه يري عدم جواز تقييد حرية الاثبات في المسائل الجنائية. واتجاه ثاني يري بعدم جواز اطلاق الاثبات في المسائل الجنائية، واتجاه ثالث توافقي بين الاتجاهين السالفي الذكر.

[1] كمال محمد عواد، المرجع السابق، ص 44.
[2] مزين خلف، محاضرات في القانون الجنائي-المحاضرة الثامنة، كلية القانون، جامعة المستنصرية، العراق، 2017، ص 2.

فالاتجاه الاول: الذي يطلق عليه المذهب الحر أو المطلق[1] والقائل بحرية الاثبات في المسائل الجنائية، يري أن تقييد حرية الاثبات في المسائل الجنائية قد يؤدي الي اهدار الكثير من الحقوق والاضرار بمصلحة المجتمع في مواجهة الجريمة. ذلك أنه لا يمكن توقع مكان وزمان وقوع الجريمة أو الظروف التي سترتكب فيها، حتي يتم تصور ووضع الايطار القانوني اللازم لإثباتها. وبذلك فان حصر الأدلة الجنائية في نصوص قانونية وتقييد حرية القاضي في تكوين اعتقاده بناءا علي ما تم حصره، قد يؤدي الي ترجيح كفة المجرم علي حساب المجتمع والضحية، خاصة ما إذا كان المجرم ملما بالقانون ومدركا لماهية الأدلة الجنائية التي قد تدينه، وبالتالي فانه يسعي الي التخطيط المحكم لارتكاب جريمته وتنفيذها دون أن يخلف وراءه اي دليل، بل إن بإمكانه حتي أن يصطنع لنفسه أدلة لتبرئة ساحته في حالة اتهامه. في حين تجد جهات التحقيق والضحية نفسها عاجزة عن الاتيان بدليل واحد في القضية.

وما يؤيد هذا الرأي، هو أن اطلاق حرية الاثبات في المسائل الجنائية من شأنه أن يؤدي الي تحقيق العدالة، وموازنة الكفة بين ما يتمتع به المجرم من ظروف وملابسات وغموض قد تساعده في ارتكاب الجريمة والافلات من العقاب وبين حق المجتمع والضحية في اثبات الجريمة وبالتالي تحقيق العدالة من خلال الادانة والعقاب. كما أنه من جهة أخري فان تقييد مسائل الاثبات الجنائي من شأنه أن يقصي الكثير من الأدلة التي قد يفرزها التقدم العلمي لا سيما تلك اللازمة والضرورية لإثبات بعض الجرائم المستجدة علي غرار الجرائم الإلكترونية.

ويري أصحاب هذا الرأي، أن حرية الإثبات في المسائل الجنائية وإن كانت تعني حرية القاضي في تكوين اقتناعه بناءا علي الأدلة الجنائية التي تقدم اليه، لكن ذلك لا يعني أنه حر في إتباع أهوائه وميولاته الشخصية، بل يجب أن يكون الاقتناع أو اليقين الذي

[1] كمال محمد عواد، المرجع السابق، ص 46.

يتوصل إليه القاضي مؤسسا علي مقتضيات المنطق والعقل. وأن مسالة الاقتناع مرتبطة بجملة من المبادي القانونية الهامة، كمبدأ عدم جواز الحكم بمقتضي العلم الشخصي، ومبدأ وجاهية الدليل الجنائي ومناقشته حتي يصلح أساسا للاقتناع، ومبدأ شرعية الدليل الجنائي وهو أن يكون قد تم الحصول عليه في ايطار الضوابط والأطر التي حددها القانون.

أما الاتجاه الثاني: ويطلق عليه اسم المذهب المقيد[1]، فيري أصحابه بضرورة تقييد حرية الاثبات في المسائل الجنائية، وذلك بالنص علي طرق محددة في الاثبات يتقيد بها خصوم الدعوي الجنائية والقاضي علي حد السواء، بحيث لا يمكن اثبات الجريمة واسنادها لمرتكبها ولا يمكن للقاضي الوصول الي الادانة الا من خلال تلك الوسائل التي قررها القانون فلا مجال لإعمال السلطة التقديرية للقاضي ولا مجال للأخذ باقتناعه الشخصي.

ويري أصحاب هذا الرأي أن تقييد حرية الاثبات من شأنه أن يوفر ضمانات أكبر للمتهم بحيث لا تبني الادانة الا علي اسباب يقينية موضوعية وليس علي أسباب شخصية ذلك ان تحديد مسألة الاقتناع من شأنه أن يثير الكثير من اللبس لاستحالة التأكد من عدم اقترانها بالعوامل النفسية والشخصية للقاضي، كما أن تحقيق العدل يقتضي ان يتم النظر الي الواقعة الاجرامية من خلال الوسائل والأدلة التي يحددها القانون. فاذا كان القانون هو الذي يحدد عناصر الواقعة الاجرامية فمن الأجدر أن يقوم بتحديد أدلة وطرق اثبات تلك العناصر، فالقانون لا يعترف بالحقيقة الواقعية الا اذا تم اثباتها بالطرق التي حددها وتصير بذلك عبارة عن حقيقة قضائية[2].

أما الاتجاه الثالث: فيطلق عليه تسمية النظام المختلط [3]، لأخذه بالاتجاهين السابقين معا فهو يأخذ بنظام الاثبات المقيد في اثبات بعض الجرائم، وفي نفس الوقت يأخذ بنظام الاثبات الحر في البعض الاخر من الجرائم. فنجد أن بعض الجرائم يحدد لها القانون طرق ووسائل اثبات محددة بحيث لا يجوز اثباتها بخلاف الأدلة التي يتطلبها القانون فالقاضي مقيد في

[1] كمال محمد عواد، المرجع السابق، ص 77.
[2] محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، الطبيعة الثالثة، 1997، ص 407.
[3] كمال محمد عواد، المرجع السابق، ص 46.

تكوين اقتناعه بالأدلة المنصوص عليها قانونا كما هو الحال بالنسبة لا ثبات جريمة الزنا. وفي جرائم أخري لا يخول للقاضي السلطة التقديرية في تقييم الدليل بل عليه الأخذ به كما نص عليه في القانون إلا في حالة الطعن بالتزوير، كما هو الشأن في بعض المحاضر التي تحرر لإثبات بعض الجرائم علي غرار الجرائم الجمركية فالقانون يصبغ علي المحاضر التي يحررها أعوان الجمارك وفقا لشروط معينة قوة اثباتية مطلقة، ولا يمكن دحض ما جاء في تلك المحاضر بأدلة أخري ما عدا بالطعن فيها بالتزوير. كما نجد في جرائم أخري، تقدير مسألة القبول بدليل الإدانة متروكة للسلطة التقديرية للقاضي، الذي له أن يبني قناعته علي أي دليل يقدم إليه، شرط تسبيب حكمه وتبيان الأسباب التي أدت به إلي التوصل إلي الإدانة.

لقد حاول الفقه تقسيم الأدلة الجنائية، وخرج بالعديد من التقسيمات نوردها فيما يلي:

أ- تقسيم الأدلة من حيث مصدرها:

تنقسم الأدلة الجنائية من حيث مصدرها إلي أربعة أقسام هي:

1. **الأدلة المادية:** وهي تلك الأدلة التي يمكن لمسها أو رؤيتها كوجود الشيء المسروق في حيازة الجاني أو ضبط الجاني حاملا سلاحا استعمل في تنفيذ الجريمة أو آثار أقدام أو بصمات الأصابع التي يعثر عليها في محل الحادثة، فهي تنبعث من عناصر مادية ناطقة بنفسها وتؤثر في اقتناع القاضي بطريق مباشر ويطلق عليها بالأدلة الفعلية لأنها تنتج عن وجود الآثار المادية ذات الارتباط بالجريمة.[1]

ونظرا لما للأدلة المادية من أهمية في الإثبات وذلك لتأثيرها على وجدان القاضي وإحساسه وجب على المحقق أن يسرع في الحصول عليها وتثبيتها بعد ارتكاب الجريمة مباشرة حتى لا تضيع معالمها أو يعتريها النقض أو التلف أو التغيير، ويمكن الحصول على

[1] مزين خلف، المرجع السابق، ص 6.

هذه الأدلة بواسطة الكشف على محل ارتكاب الجريمة او التفتيش او الاستعانة بالخبراء من أطباء عدليين وغيرهم من ذوي الاختصاص.

2. **الأدلة القولية:** وهي الأدلة التي تنبعث من عناصر شخصية والتي تصل إلى المحقق على لسان الغير وهي تؤثر في اقتناع القاضي بطريق غير مباشر ويسميها فقهاء القانون بالأدلة المعنوية لأنها تستنبط من واقع الإعترافات والأقوال التي يدلي بها الجناة والمشتبه بهم او في الأقوال التي ترد على لسان شخص ما كالمجنى عليه او الشهود وهي في مجموعها تعد أدلة مجردة لا تستمد من أمور حسية او مادية وإنما يتوصل إليها من أمور معنوية او غير مادية وقد تحتمل الكثير من التأويل وقد لا تتفق مع الحقائق المادية الثابتة كاعتراف المتهم وشهادات شهود النفي أو الإثبات.[1]

3. **الأدلة الفنية:** وهي الأدلة الناتجة عن الخبرة، وتتضمن رأي خبير بشأن وقائع معينة. فالأدلة الفنية مناطها الخبرة والتجربة وهي بذلك تختلف عن الشهادة، لأن الشهادة هي سرد للوقائع كما تم إدراكها من قبل الحواس.

4. **الأدلة القانونية:** وهي الأدلة التي حددها المشرع حصرا وعين قوتها في الإثبات ومن ثم لا يمكن للقاضي أن يعطي أي دليل منها قوة اكبر مما أعطاها المشرع، ويعد هذا النوع من الأدلة الأصل في المسائل المدنية، في حين لا نجد تحديدا للأدلة في المسائل الجنائية ذلك إن القاضي له الحرية في تكوين قناعته من أي دليل في الدعوى الجزائية.

غير أن الأمر ليس بهذا الإطلاق ففي بعض الحالات يورد القانون استثناءات معينة على حرية القاضي في الإثبات والاقتناع فيمنعه من الأخذ بدليل معين او يمنعه من الحكم بالإدانة إلا إذا توافر لديه دليل محدد.

ب- تقسيم الأدلة من حيث علاقتها بالواقعة المراد إثباتها.

تنقسم الأدلة من حيث علاقتها بالواقعة المراد إثباتها، إلي أدلة مباشرة وأدلة غير مباشرة.

[1] مزين خلف، المرجع السابق، ص 5.

1. **الأدلة المباشرة:** هي أدلة قاطعة في إثبات الجريمة، والوقائع المرتكبة من طرف الجاني، فالقاضي يكون اقتناعه في إثبات الوقائع ولا يحتاج إلى أدلة أخرى، وهذه الأدلة تنقسم بدورها إلى عدة أقسام التي منها: الاعتراف، الشهادة. وبالتالي فهي دليل إثبات سهل ومؤكد، وهذا لأنه لا يحتاج إلى مناقشة أو تعليق، فوجود الأموال المسروقة في حيازة المتهم يعد من الأدلة المادية المباشرة، أما شهادات الشهود الذين أدركوا وقوع الجريمة بإحدى حواسهم الخمسة فتعد من الأدلة المعنوية المباشرة.[1]
2. **الأدلة غير المباشرة:** سُميت بالأدلة غير المباشرة، وهذا لأنها لا تنصب على الواقعة المراد إثباتها بصورة مباشرة، وإنما بصورة غير مباشرة، أي بمعنى أنها تنصب على واقعة أخرى ذات صلة منطقية وثيقة بها، وعلى المحقق أن يحكم عقله فيستنبط من الواقعة التي انصب الدليل عليها الواقعة الأخرى التي يراد إثباتها، فمثلا لو أراد المحقق أن يثبت وجود الجاني في مسرح الجريمة، فإن إثبات واقعة وجود بصمة أصابعه من خلال إعمال قواعد المنطق يدل بصورة غير مباشرة على أن وجود هذه البصمات دليل على وجوده في مسرح الجريمة، حيث أنّ وجود بصماته يُعد دليلا غير مباشرا على وجوده، وهذا لأن الإثبات انصب على واقعة منها ثم الاستدلال على واقعة أخرى.

إن أهمية الأدلة المباشرة سواء كانت مادية أو معنوية في الإثبات الجنائي أقوى من الأدلة غير المباشرة وذلك لأنها تؤخذ مباشرة من وقائع الجريمة أما الأدلة غير المباشرة فإنها تستنتج من الظروف المحيطة بوقائع الجريمة وهذا من شأنه أن يدعوا للقيام بعملية استنتاج قد تؤدي إلى الخطأ او الصواب.[2]

[1] مزين خلف، المرجع السابق، ص 7.
[2] مزين خلف، المرجع السابق، ص 8.

ت- تقسيم الأدلة من حيث الأثر المترتب عليها.

تنقسم الأدلة من حيث الأثر المترتب عليها إلي ثلاثة أقسام، هي: أدلة الاتهام، أدلة النفي وأدلة الحكم.

1. **أدلة الاتهام:** وهي الأدلة التي تسمح بتقديم المتهم للمحاكمة، غير أنها لا تصلح لأن تكون أساسا للإدانة لعدم كفايتها، وهي بذلك تكون بحاجة إلي أدلة أخري.[1]
2. **أدلة النفي:** وهي الأدلة التي تسمح بتبرئة ساحة المتهم أو تخفيف مسؤوليته.[2]
3. **أدلة الحكم:** وهي الأدلة التي تصلح لأن تكون في حد ذاتها أساسا للحكم بالإدانة، فهي أدلة تتوفر فيها كافة الشروط والضوابط القانونية ولا تحتاج إلي أدلة أو قرائن أخري تعززها.[3]

المطلب الثاني: مفهوم الأدلة ذات الطابع الإلكتروني

يقوم مبدأ الإثبات الجنائي علي قاعدة هامة مفادها أن القاضي لا يقضي بعلمه الشخصي وأن إحاطته بوقائع الدعوى يجب أن يتم من خلال ما يُطرح عليه من أدلة يتم مناقشتها أمامه، فالدليل هو الوسيلة التي ينظر من خلالها القاضي للواقعة موضوع الدعوى، وعلى أساسه يبني قناعته، لذلك اهتمت مختلف الأنظمة القانونية علي اختلاف الأسس التي تقوم عليها، بتنظيم الأدلة الجنائية وتحديد شروط مشروعيتها واجراءات الحصول عليها وتقدير قوتها الاثباتية وحجيتها، وأن استحداث أي نوع من الأدلة يجب أن يخضع للضوابط والشروط التي يحددها النظام القانوني الذي يقوم في ظله هذا الدليل.

إن تطور المعاملات عن طريق استعمال الحاسوب في البيع والشراء بظهور التجارة الالكترونية، وتداول حركة رؤوس الأموال وما صاحب ذلك من جرائم تستخدم الشبكة المعلوماتية كوسيلة لها أو تلك التي يكون الحاسوب مجالا لها فقد صاحب ذلك ظهور أدلة

[1] حسين محمود ابراهيم، الوسائل العلمية الحديثة في الإثبات، دار النهضة العربية، 1981، ص45.
[2] حسين محمود ابراهيم، المرجع السابق، ص 45.
[3] أمال عبد الرحيم عثمان، شرح قانون الإجراءات الجنائية، 1989، ص 400.

إثبات أخرى قد تصلح في الإثبات الالكتروني أمام القضاء المدني مثل الشبكات الالكترونية والمحفظة الالكترونية، استعمال بطاقات الائتمان الالكترونية والممغنطة يضاف لها الكتابة الالكترونية والتوقيع الالكتروني والبريد الالكتروني وعلى العموم فإن الإثبات الالكتروني يتم عن طريق جمع وحفظ وتحليل الأدلة الإلكترونية من أية دعامة للتخزين تعمل بواسطة الإعلام الآلي لعرضها أمام القضاء قصد إثبات التهمة أو نفيها عن شخص ما.[1]

فقد كانت الأدلة التي تعترف بها مختلف الأنظمة القانونية، من طبيعة محسوسة، فهي إما أدلة مادية علي غرار وسائل ارتكاب الجريمة، أو أدلة سمعية كشهادة الشهود والاعتراف، أو أدلة مرئية علي غرار الصور وأشرطة المراقبة لكنه ونتيجة للتطور التكنولوجي وانتشار استعمال التقنيات الإكترونية في التعاملات اليومية وما ترتب عن ذلك من استخدامها كوسيلة لارتكاب الجرائم، وكموضوع للجريمة في حد ذاتها، اختلف الوسط الذي ترتكب فيه الجريمة، من وسط مادي إلى وسط افتراضي واستحال علي الأدلة الجنائية التقليدية مواكبة هذا الانتقال، لاختلاف طبيعة العالمين المادي والافتراضي، فلكل منهما طبيعته وخصائصه، فكان لزاما أن يظهر نوع جديد من الأدلة يتفق مع طبيعة وخصائص العالم الافتراضي، أطلق عليها تسمية الأدلة الإلكترونية، وسميت بالأدلة الإلكترونية نظرا لأن التقنية الإلكترونية تقوم علي نظام التشفير الرقمي، بحيث تأخذ البيانات سواء كانت صورا أو تسجيلات أو نصوص داخل هذا النظام، شكل شفيرات مكونة من أرقام، أما تسمية الأدلة الالكترونية فمردها الي أن هذا النوع من الأدلة يتكون أساسا من مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية الالكترونية.

لقد أثارت الأدلة الإلكترونية الكثير من التساؤلات، المتعلقة بماهية تلك الأدلة وبطبيعتها القانونية، والسبب في ذلك يرجع الي أنها أدلة حديث النشأة، أوجدتها التقنية الإلكترونية وهي من طبيعة خاصة من حيث تكوينها ومن حيث الوسط الذي تنشأ فيه، وهذا

[1] فراح مناني، أدلة الاثبات الحديثة في القانون، دار الهدى، الجزائر، 2008، ص 262.

يثير التساؤل حول ماهيتها ومشروعيته وقيمتها القانونية، فالدليل الجنائي بوجه عام، يجب أن يكون معلوما ومقبولا من الناحية القانونية أي مشروعا من حيث وجوده وطريقة الحصول عليه، فمشروعية الوجود تقتضي أن يكون الدليل قد قبله المشرع ضمن أدلة الإثبات الجنائي.

الفرع الأول: تعريف الدليل المتحصل من الوسائل الإلكترونية

يأخذ الإثبات الالكتروني مفهوما مختلف عن سابقه باختلاف طبيعة كل منهما فالأدلة الالكترونية إما أن تكون مخرجات ورقية يتم انتاجها عن طريق الطابعات أو الرسم، وإما أن تكون مخرجات غير ورقية مثل الأشرطة، الاقراص المضغوط، اسطوانات الفيديو[1]، وهي عبارة عن دعائم أو وسائط لحفظ المعلومات بمعنى أن البيانات قد تم تخزينها في الأشرطة أو على القرص الصلب أو القرص المضغوط أو أي أجهزة التخزين الرقمية.[2]

وقد صدر في فرنسا القانون رقم 230 لسنة 2000 في 13 مارس 2000 والذي عدل نص المادة 1316 من القانون المدني ليتم الأخذ بالسندات الالكترونية والتوقيع الالكتروني، و وردت العديد من التعاريف في الأدلة الإلكترونية، فهناك من عرفها بأنها: بيانات يمكن إعدادها وتراسلها وتخزينها رقميا، بحيث تمكن الحاسوب من تأدية مهمة ما [3]، إن هذا التعريف يربط بين البيانات المخزنة وبين جهاز الحاسوب، وفي ذلك تضييق وحصر شديد لمعني الأدلة الإلكترونية، فهو يربط البيانات بالحاسوب، ويكون قد أقصي من التعريف، طيفا واسعا من الأدلة المتحصلة من أجهزة اخري غير الحاسوب علي غرار الهواتف النقالة الذكية والتي يمكن من خلالها الولوج الي شبكة الانترنيت والقيام بعدة عمليات اتصال معقدة، وكذلك الات التصوير الرقمية المتطورة...الخ.

[1] عبد اللاه أحمد هلالي، حجية المخرجات الالكترونية، الطبعة الأولى، دار النهضة العربية، القاهرة، مصر، 1997، ص 22.

[2] فراح مناني، أدلة الاثبات الحديثة في القانون، دار الهدى، الجزائر، 2008، ص 262.

3 وهو التعريف الذي أخذ به التقرير الأمريكي المقدم الى ندوة الانتربول العلمية حول الدليل الرقمي 2001، ص 05.

كما عرفت بأنها: الدليل الذي يجد له أساسا في العالم الافتراضي ويقود الي الواقعة غير المشروعة ومرتكبها[1]، وهو تعريف يستند الي عنصرين، هما منشأ الدليل الرقمي ومحيطه وهو العالم الافتراضي، والهدف أو الغاية من وجوده وهي الواقعة غير المشروعة ومرتكبها. أن التعريف باستعمال المنشأ والغاية أو الهدف، وإن كان يؤدي الي معني ينطبق علي مفهوم الأدلة الإلكترونية، إلا أنه تعريف يبقي قاصرا عن الإحاطة بالمعني الكامل لها، ما دام أنه لم يتطرق الي تحديد مكونات الأدلة الإلكترونية، ما دامت تلك المكونات معلومة وبإمكانها اضفاء ووضوح أكثر علي التعريف.

وعليه فإنه هناك من عرف الدليل الرقمي بأنه: الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهى مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون.[2]

وعرفت بأنها: مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية.[3]

فالبيانات أو المعطيات المخزنة في ذاكرة الحاسوب إما أن تكون مرصودة ومثبتة على دعامة أو حامل كالأقراص أو اشرطة ممغنطة فهذه الأخيرة تعد من حكم الأشياء المادية يجوز ضبطها بسهولة أما البيانات الالكترونية فإنه لا يمكن ضبطها لانتفاء الكيان

1 عمر بن محمد يونس، الجرائم الناشئة عن استخدام الانترنت، الطبعة الاولى، دار النهضة العربية القاهرة، 2004، ص 4.
2 خالد ممدوح إبراهيم، الدليل الالكتروني في جرائم المعلوماتية، بحث منشور على الانترنت الرابط:- http://www.f-law.net، ص 02.
3 طارق محمد الجملي، الدليل الرقمي في مجال الاثبات الجنائي، بحث منشور علي الانترنيت.

المادي إلا بعد نقلها على كيان مادي ملموس عن طريق التصوير الفوتوغرافي، كما ذهب إلى ذلك المشرع الجزائري بإمكانية حجز المعلومات إذ ورد في المادة 06 من القانون 04-09.بأنه يمكن حجز المنظومة المعلوماتية برمتها إذا كان ضروريا لمصلحة التحقيق وذلك بعد نسخها على دعامة مادية.[1]

فهذا التعريف يعطي صورة أدق وأوضع للدليل الرقمي، فهو علي خلاف التعريفات السابقة، يبرز مكونات الأدلة الإلكترونية ويشير الي أنها، المجالات أو النبضات المغناطسية أو الكهربائية، كما أنه لا يربط تلك المجالات او النبضات المغناطسية أو الكهربائية، بأداة تقنية معينة كالحاسوب أو الهواتف الذكية أو غير ذلك، مما يجعل التعريف مرنا قابل للتكييف مع التطور التقني ما يتوصل اليه العلم من مخترعات أو انماط جديدة من الاستغلال، لكنه في رأينا يظل ناقصا، لأنه لا يمكن اعتبار جميع النبضات المغناطسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية، أدلة رقمية، إلا إذا كانت تدل علي واقعة غير مشروعة يعتبرها القانون جريمة وعلي مرتكبها.

ويمكن تعريف الأدلة الإلكترونية على أنها: مجموعة البيانات التي تتخذ شكلا إلكترونيا أو رقميا كالنبضات المغناطسية أو الكهربائية أو غير ذلك من الأشكال والتي تكون محفوظة ويمكن استغلالها وتجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية و/أو مرئية، والتي تتخذ شكلا الكترونيا أو رقميا أو غير ذلك من الأشكال التي قد تظهر وتتجسد مع التطور التقني وتتلائم مع العالم الافتراضي الذي توجد فيه.

[1] زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، الطبعة الاولى، مطبعة دار الهدى، الجزائر، 2011، ص 150.

وحتي تصنف البيانات ضمن خانة الأدلة الإلكترونية يجب أن تكون مخزنة ومحمية من كل ما يمكن أن يفسدها أو يتلف نوعيتها أو حالتها الراهنة، ويتطلب ذلك أن تكون هناك جهة مسؤولة عن حفظ تلك البيانات.[1]

الفرع الثاني : محددات الدليل المتحصل من الوسائل الإلكترونية.

ينشأ الدليل الرقمي في البيئة الافتراضية، وتحدده أربع عناصر رئيسية، تتمثل في:

1-الدليل الرقمي دليل علمي:

كما جاء في تعريف الدليل الرقمي، فانه يرتكز أساسا علي بيانات تتخذ شكلا الكترونيا غير مشاهد وغير محسوس، فهو دليل أفرزه التطور العلمي في مجال التقنية، فهو يتمتع بالصبغة العلمية، التي يترتب عنها أربعة نتائج:

الاولى: أنه لا يمكن الحصول على الدليل الرقمي أو الاطلاع على محتواه سوى باستخدام الأساليب والأدوات العلمية.

الثانية: أنه لا يمكن البحث والاستدلال عن الدليل الرقمي الا باستعمال التقنية الإلكترونية أو الوسائل العلمية.

الثالثة: هي أن الأدلة الإلكترونية تهدف الي إثبات الحقيقة المطلقة، وفقا للقاعدة القائلة بأن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة، وبذلك تتميز الأدلة الإلكترونية عن الأدلة التقليدية في أن الأولي لا تتأثر بالعوامل الشخصية فهي تثبت الحقيقة المطلقة خالية من الشوائب، أما الثانية فغالبا ما تتأثر بالعوامل المحيطة بها كالزمن والمكان وتكون قدرتها علي الاتيان بالحقيقة كما وقعت نسبية، علي غرار الشهادة أو الاعتراف... الخ.

الرابعة: هي أن التعامل مع الأدلة الإلكترونية علي غرار الأدلة العلمية الأخرى، يتطلب خبرة وتخصصا، فالبحث عن الأدلة الإلكترونية يجب أن يتم من طرف أشخاص

1 اتفاقية جرائم الكومبيوتر التقرير التفسيري الفقرة 162.

مؤهلين ملمين بالتقنية الإلكترونية وبماهية الأدلة الإلكترونية وأماكن البحث عنها وطرق استخلاصها وحفظها، بل إن التعامل مع الأدلة الإلكترونية من طرف أشخاص غير مختصين قد يؤدي في غالب الاحيان الي تلفها وضياعها، وبالتالي الى محو أثار الجريمة وإفلات مرتكبها من العدالة. وغالبا ما تلجا الجهات المختصة بتعقب الجرائم الإلكترونية والتحقيق فيها باللجوء الي الخبرة العلمية التي توفرها جهات متخصصة، تمتلك أدوات وأجهزة متطورة من أجل البحث عن الأدلة الإلكترونية ومعاينتها وضبطها وحفظها في وسائط مادية.

2-الدليل الرقمي دليل تقني:

كما سبق الذكر أن الأدلة الإلكترونية هي وليدة انتشار استعمال التقنية، فهي أدلة تقنية لا مادية، يتطلب إدراكها والتعامل معها استعمال أجهزة ووسائل تقنية كالحاسوب والبرامج مع التحكم والالمام بالمعرفة التقنية، فالدليل الرقمي بحكم أنه ينشأ في العالم الافتراضي علي شكل أرقام متسلسلة، وفقا لترتيب معين لتؤدي نتيجة أو أمر معينا أو من حيث أنه يتخذ شكل نبضات كهربائية أو مغناطسية غير مرئية، يتطلب وسائل وأجهزة لها القدرة علي استيعاب وفهم تلك الأدلة وترجمتها الي اللغة التي يفهمها الانسان، فلا مجال لمقارنة الأدلة الإلكترونية مع الأدلة العادية في هذه النقطة. وهناك من يري أن الطابع التقني للأدلة الرقمية يدعو الي فصل اجراءات البحث والاستدلال عن اجراءات الخبرة. كون أن ضبط الأدلة الإلكترونية لا يكون حتما باللجوء الي الخبرة العلمية، ويضرب مثلا عن ذلك، أن سلطات التحقيق الجنائي في العديد من الدول وعلى رأسها الولايات المتحدة الأمريكية لديها مقومات الاستدلال والتحقيق التقنية الكاملة، وذلك نتيجة لما تحظى به مؤسساتهم من هيكلة تقنية كبيرة، ويري أصحاب هذا الرأي أن مؤسسات الضبط القضائي وسلطات التحقيق

في الولايات المتحدة الأمريكية وألمانيا ساهمت بشكل كبير في تطوير تكنولوجيا المعلومات من خلال البحث المستمر فيها[1].

3-الدليل الرقمي دليل متنوع ومتطور:

باعتبار أن الأدلة الإلكترونية، هي أدلة علمية وتقنية، فإن ذلك حتما يجعل منها أدلة متنوعة ومتطورة، فمع تقدم الاكتشافات العلمية وتطور التقنية، تبرز أشكالا جديدة من الجرائم الإلكترونية، وتتبعها أشكالا جديدة من الأدلة الإلكترونية لم تكن معروفة من قبل. وتقسيم الأدلة الإلكترونية الي نوعين رئيسين:

- أدلة أعدت لتكون وسيلة إثبات: وهذا النوع من الأدلة الإلكترونية يمكن إجماله فيما يلي:
  - السجلات التي تم أنشاؤها بواسطة الآلة تلقائيا، وتعتبر هذه السجلات من مخرجات الآلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسوب الآلي.
  - السجلات التي جزء منها تم حفظه بالإدخال وجزء تم انشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة وتتمُّ معالجتها من خلال برنامج خاص، كإجراء العمليات الحسابية على تلك البيانات.
- أدلة لم تعد لتكون وسيلة إثبات: وهذا النوع من الأدلة الإلكترونية نشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغبا في وجوده.

ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهى ما يمكن تسميه أيضا بالآثار الإلكترونية الرقمية، وهى تتجسد في الآثار التي يتركها مستخدم الشبكة الإلكترونية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافه الاتصالات التي تمت من خلال الآلة أو شبكة الانترنيت. والواقع أن هذا النوع من الأدلة لم يُعد أساسا للحفظ من قبل من صدر عنه، غير أن الوسائل الفنية الخاصة تمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من

1 عمر محمد بن يونس، مقال بعنوان الدليل الرقمي، 2006، ص 8.

نشوئها، فالاتصالات التي تجرى عبر الانترنت والمراسلات الصادر عن الشخص أو التي يتلقاها، كلها يمكن ضبطها بواسطة تقنية خاصة بذلك تمكن من من ضبط تحركات مستخدم الشبكة عن طريق تحديد الجهاز الذي يستعمله[1]، كما تتخذ الأدلة الإلكترونية ثلاثة أشكال رئيسة هي: الصور الرقمية، التسجيلات والنصوص المكتوبة. ومن الأدلة الإلكترونية المعروفة نجد عنوان برتوكول الانترنيت، وهو عنوان فريد لكل حاسوب يدخل الي شبكة الانترنيت ولا يمكن ان يدخل الشبكة جهازان بنفس العنوان في أي مكان.

ويعد الوصول الي عنوان برتوكول الانترنيت أحد الأدلة الإلكترونية الهامة جدا ولها معاني لا تقبل الشك لدي الخبير، ويستخدم الخبير الروابط كأدلة لمعرفة صفحات المواقع التي تصفحها المجرم.

4-الدليل الرقمي يصعب التخلص منه:

إذا كانت الأدلة الإلكترونية غير ملموسة وسهلة الازالة والاخفاء غير أنها تميز في نفس الوقت بانها صعبة التخلص منها، فالتخلص من البيانات أو الأدلة الإلكترونية وحذفها لا يحول دون استرجاع تلك البيانات أو الأدلة، اذا تتوفر تكنولوجيا المعلومات علي برامج بإمكانها استرداد كل الملفات التي تم الغاؤها أو محوها من الحاسوب، فالدليل الورقي يمكن التخلص منه بتمزيق الورقة التي تحمله في حين إن الدليل الإلكتروني يمكن إعادته إلى الوجود، حتى وإن كان قد تعرض للإزالة.[2]

لقد اتجه بعض الكتاب الي القول أن محاولة التخلص من الأدلة الإلكترونية باستعمال خصائص المحو والازالة أو باستعمال برامج مخصصة لذلك، في حال ما إذا ثبت وقوعها، تعد في حد ذاتها جريمة يعاقب عليها القانون، كما أن إستعمال خصائص الالغاء

1 عبد الفتاح بيومي حجازي، الدليل الرقمي والتزوير في جرائم الكمبيوتر والانترنت، دراسة معمقة في جرائم الحاسوب الآلي والانترنت، بهجت للطباعة والتجليد، مصر، 2009، ص 64.
2 عمر محمد بن يونس، مرجع سابق، ص 10.

والحذف للأدلة الإلكترونية لا يعني إزالتها بشكل نهائي، وإنما هو في الحقيقة مجرد إخفاء لها وبالتالي يمكن إعادة استرجاعها واستعمالها من جديد.

5- الدليل الرقمي دليل غير ملموس:

أي أنه ليس دليلا ماديا، فهو عبارة عن المجالات مغناطيسية أو كهربائية، ومن ثم فإن ترجمة الدليل الرقمي وإخراجه في شكل مادي ملموس لا يعني أن هذا التجمع يعتبر هو الدليل، بل أن هذه العملية لا تعدو كونها عمليه نقل لتلك المجالات من طبيعتها الرقمية إلى الهيأة التي يمكن الاستدلال بها على معلومة معينة.

خلاصة

إن أهمية المعلومة والبيانات التي تعد المادة الخام التي يتم تجهيزها ومعالجتها لتتحول إلى معلومة فتصبح ذات قيمة اقتصادية بمثابة سلعة تباع وتشرى باتت تحظى بحماية قانونية.

فالتطور الحالي الذي لحق ثورة الاتصالات عن بعد وما أفرزته هذه الثورة من وسائل الكترونية متقدمة ومتعددة قد انعكس أثره على الجرائم التي تمخضت عن ذلك بحيث تميزت هذه الجرائم بطبيعة خاصة من حيث الوسائل التي ترتكب بها، ومن حيث المحل الذي تقع عليه ومن حيث الجناة الذين يرتكبونها، بحيث يمكن القول أن الأساس في خطر هذه الجرائم يكمن في أنها في طبيعتها تجمع بين الذكاء الاصطناعي والذكاء البشري، مما يجعل إثباتها جنائيا قد يكون في منتهى الصعوبة، خاصة مع مبدأ المشروعية أو مبدأ سيادة القانون، فلا جريمة ولا عقوبة دون نص ولا عقوبة دون حكم قضائي صادر من محكمة مختصة وفقا للقانون، إذ أنه من غير الممكن أن يؤسس حكما قانونيا على دليل غير مادي أو غير

مكيف أو متحصل عليه بطرق غير مشروعة، وفي ذلك يبرز موقف المشرع الجزائري من خلال النصوص التشريعية التي بادر بها لمواكبة مختلف التشريعات العالمية بغية مواجهة ظاهرة الجرائم الالكترونية.

الفصل الثاني

تمهيد

يتضمن قانون الإجراءات الجزائية قواعد المتعلقة بالاختصاص والإثبات لتتوافق مع الحالات التي تنص عليها إجرائيا، ولتطبيقها في مجال البحث والتحري عن الجرائم التي كانت سائدة أثناء بداية سريانها، فالجرائم العادية تختلف عن الجرائم الإلكترونية في طبيعتها وخصائصها وفي وسائل ارتكابها وفي أبعادها ونتائجها، ولا لذا تختلف كذلك في طرق ووسائل إثباتها، فمشروعية الإثبات تستلزم قبول الدليل من طرف المشرع والنص عليه ضمن أدلة الإثبات الجنائي، أما مشروعية الحصول عليه، فتقتضي أن يتم تحصيل الدليل الجنائي وفقا للإجراءات والوسائل التي حددها القانون، كالمعاينة والتفتيش، والخبرة واعتراض المراسلات وغير ذلك، مع مرعاة إمكانية القيام بإجراءات جمع وتحصيل الأدلة الجنائية في التحقيق حول الإجرام الإلكتروني وما يعترضها من تحديات.

المبحث الأول: إجراءات التحقيق في الجرائم الإلكترونية

يعد مسرح الجريمة بمثابة سجل لأحداث الجريمة ووقائعها، ويمكن أن يقدم الكثير من المعلومات حول ظروف الجريمة وملابسات ارتكابها وهوية منفذها، ولعل أن أي معاينة لمسرح الجريمة تبدأ بالتفتيش عن الأدلة الجنائية من أجل ضبطها وحجزها، ثم تحليلها ودراستها من قبل المختصين، وإن كان الدليل المتحصل عليه بحاجة الي قراءة علمية أو فنية، فإنه يخضع لأعمال الخبرة من طرف أشخاص مؤهلين أو باستخدام أجهزة علمية.

كما أنه يمكن تحصيل الأدلة الجنائية الإلكترونية عن طريق اعتراض المراسلات والإتصالات الرقمية، وهي وسيلة عملية مستحدثة، تم إعتمادها في مجال الإثبات الجنائي الحديث.

المطلب الأول: التفتيش والخبرة

التفتيش كإجراء للبحث عن الأدلة الجنائية يختلف مفهومه في الجرائم التقليدية عنه في الجرائم الإلكترونية، وتعتبر الخبرة احدي وسائل البحث عن الأدلة الجنائية ذات الطابع الفني وتقديرها من طرف اشخاص متخصصين تتوفر لديهم الخبرة والمعرفة الكافية في مجالات محددة من العلم والمعرفة. وهي بذلك وسيلة من وسائل التحقيق القديمة لكنها فعالة في التحقيق في الجرائم الإلكترونية بحكم أن الادلة الرقمية هي أدلة علمية وتقنية.[1]

الفرع الأول: التفتيش

التفتيش لغة هو: الاستقصاء في البحث الطلب، أما اصطلاحا فهو: البحث عن أدلة الجريمة وكل ما يفيد في كشف الحقيق من أجل إثباتها أو إسنادها للمتهم سواء كان محله

[1] علي محمود علي حموده، الادلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث القي في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، رقم العدد1، دبي، الامارات العربية المتحدة، سنة 2003، ص 29.

شيئا أو مكانا أو شخصا، فهو اجراء من اجراءات التحقيق تقوم به سلطة حددها القانون يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق أو ترجح وقوعها فى محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبة، تغليبا للمصلحة العامة على مصالح الافراد الخاصة.[1]

وعرف بأنه: إجراء من إجراءات التحقيق تقوم به سلطة مختصة لأجل الدخول إلى نظم المعالجة الآلية للبيانات بما تشمله من مدخلات وتخزين ومخرجات لأجل البحث فيها عن أفعال غير مشروعة تكون مرتكبة وتشكل جناية أو جنحة والتوصل من خلال ذلك إلى أدلة تفيد في إثبات الجريمة ونسبها إلى المتهم بارتكابها.[2]

ويعد التفتيش اجراء هام من اجراءات التحقيق، وهو استثناء علي القاعدة العامة التي تقضي بحرمة حياة المواطن الخاصة وحرمة شرفه وحرمة مسكنه.[3]

أولا: شروط القيام بإجراء التفتيش

لا يجوز اللجوء إلى القيام بإجراء التفتيش، الا في الحالات التي أباحها القانون ووفقا للشروط والقيود التي نص عليها في قانون الإجراءات الجزائية، ويمكن تصنيف تلك الشروط أو القيود الي ثلاثة أصناف، منها ما يتعلق بالمكان، ومنها ما يتعلق بالزمن ومنها ما يتعلق بالأشخاص.

1- الشروط الزمينة:

[1] علي محمود علي حموده، المرجع السابق، ص 30.

[2] هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، ط1، دار النهضة العربية، القاهرة، سنة 1997، ص 73.

[3] وهذا ما نصت عليه المادة 39 من الدستور 2020 بنصها: تضمن الدولة عدم انتهاك حرمة المسكن والمادة 48 فلا تفتيش إلا بمقتضى القانون، وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة.

لقد قيد القانون اجراءات التفتيش بحدود زمنية، فلا يجوز اتخاذ اجراءات التفتيش الا في الوقت الذي حددته تبعا لطبيعة أو خطورة الجريمة المرتكبة، فلا يجوز التفتيش خارج الايطار الزمني الذي حدده القانون. وأن أي مخالفة لذلك، تؤدي إلي بطلان إجراءات التفتيش.[1]

2- الشروط المكانية:

فاذا كان التفتيش هو استثناء علي القاعدة القائلة بحرمة المساكن، فذلك يعني أنه يجب أن يقع التفتيش علي مسكن[2]، أو علي محل يحظي بالحماية القانونية، حتي تتمتع هذه الأخيرة من القيود التي فرضها القانون، وبمفهوم المخالفة، فان جميع الاماكن غير المعدة للسكن، والتي لا تحظي بحماية قانونية خاصة لا يمكن أن تستفيد من القيود التي ضربها القانون علي اجراءات التفتيش، كالأماكن العمومية والأماكن المعدة لاستقبال الجمهور.[3]

وإن كان يجوز تفتيش المساكن فإنه يشترط أن يكون صاحبه من الاشخاص الذين ساهموا في ارتكاب الجريمة أو من الأشخاص الذين يشتبه في أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة، علي أن تقدير المساكن القابلة للتفتيش، تبقي مسألة موضوعية متروكة لتقدير السلطة القضائية المشرفة علي التفتيش.

3- شروط سلطة التفتيش:

نظرا لأهمية التفتيش وخطورته، فقد أخضعته التشريعات الجنائية لإشراف السلطة القضائية[4]، كما أناطته ببعض الضمانات المتمثلة في حضور صاحب المسكن أو من يمثله أو شخصين أخرين غير تابعين لسلطة القائم بالتفتيش.[1]

[1] المادة 47 من قانون الاجراءات الجزائية الجزائري.
[2] المادة 355 من قانون العقوبات الجزائري.
[3] المادة 80 من قانون المحاماة الجزائري.
[4] المادة 44 من قانون الاجراءات الجزائية الجزائري.

ثانيا: التفتيش في الجرائم الإلكترونية.

إن الجريمة الإلكترونية جريمة غير مادية فهي في الغالب لا تترك أثار مادية ملموسة، كما أنها جريمة يمكن ارتكابها عن بعد، وبسرعة كبيرة، ويمكن محو أثارها وازالتها أو اخفاء الأدلة الرقمية الناتجة عنها بسرعة كبيرة وهو الأمر الذي قد يجعل اجراءات التفتيش غير فعالة في مواجهتها.

لقد اتجه بعض الفقهاء في تحليلهم لمسرح الجريمة الإلكترونية الي أنه يتكون من جزئين:

مسرح تقليدي: ويقع خارج بيئة الحاسوب، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون الى مسرح أية جريمة تقليدية قد يترك فيها الجاني آثار عدة، كالبصمات وغيرها وربما ترك متعلقات شخصية أو وسائط تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه.

مسرح افتراضي: ويقع داخل بيئة الحاسوب، ويتكون من البيانات الرقمية التي تتواجد وتتنقل داخل بيئة الحاسوب وشبكاته، في ذاكرته وفي الأقراص الصلبة الموجودة بداخله، والتعامل مع الأدلة الموجودة في هذا المسرح يجب أن لا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع.[2]

إن مكونات هذا المسرح مادية وملموسة يمكن معاينتها بالحواس لا يشكل عائقا في اتخاذ إجراء التفتيش بشأنه، فالتفتيش في هذه الحالة يرد على المكونات المادية للحاسوب وملحقاته، بما في ذلك البيانات المخزنة في أوعية أو وسائل مادية كالأشرطة الممغنطة

[1] المادتين 44 و47 من قانون الاجراءات الجزائية الجزائري.
[2] محمد بن نصير محمد السرحاني، مرجع سابق، ص 77.

والأقراص والضوئية، وذلك تبعاً للمكان أو الحيز الموجودة فيه، ولو أنه من الصعوبة بما كان أن يتم تحديد موقع هذا المسرح المادي خاصة في حالة ارتكاب الجريمة عن بعد باستعمال شبكة الانترنت، وحتي في حالة تحديد الموقع فقد يتصادم ذلك مع كونه يقع خارج حدود الدولة التي تحققت بها اثار الجريمة.[1]

إن عملية البحث عن الأدلة الرقمية في جهاز الحاسوب أو في شبكة معلوماتية أو في شبكة الانترنت لا يتطلب حضور صاحب المسكن أو المشتبه فيه أو المتهم، ذلك لأن عملية التفتيش ترتكز علي خبرة المحقق وعلي إلمامه بالتقنية الإلكترونية، وأن حضور صاحب المسكن أو المشتبه فيه أو المتهم خلال عملية التفتيش أمر لا جدوي منه، خاصة واذا كان ذلك الشخص ليست لديه المعرفة اللازمة بجهاز الحاسوب وبخباياه، وقد تدارك المشرع الجزائري ذلك في النصوص المنظمة لإجراءات التفتيش، حيث نص صراحة علي اعفاء التفتيش المتخذ في التحقيق في الجرائم الماسة بأنظمة المعالجة للمعطيات من القيود التي لا تتلائم مع طبيعته، كما نص المشرع الجزائري في المادة 05 من القانون رقم: 09-04 المؤرخ في 14 شعبان 1430 الموفق ل 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه: يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول، بغرض التفتيش، ولو عن بعد، إلى:

- منظومة إلكترونية أو جزء منها وكذا المعطيات الإلكترونية المخزنة فيها.
- منظومة تخزين إلكترونية.

[1] أسامة أحمد المناعسة، جرائم الحاسوب الآلي والأنترنت، دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر، عمان، الأردن، 2000، ص 56.

في الحالة المنصوص عليها في الفقرة "أ" من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة إلكترونية أخرى، وأن هذه المعطيات يمكن الدخول إليها، انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

إن تفتيش المكونات المنطقية للحاسوب أثار خلافا كبيرا في الفقه بشأن جواز تفتيشها فذهب رأي إلى جواز ضبط البيانات الالكترونية بمختلف أشكالها، ويستند هذا الرأي في ذلك على إلى أن القوانين الإجرائية عندما تنص على إصدار الإذن بضبط أي شيء فإن ذلك يجب تفسيره بحيث يشمل بيانات الحاسوب المحسوسة وغير محسوسة، كما أن الضبط يجب أن يقع عليها متي إذا اتخذت شكلا ماديا. [1]

وذهب المشرع الجزائري إلى تفتيش مساكن أشخاص يظهر أنهم يحوزون على أشياء لها علاقة بالأفعال الجنائية الإلكترونية، فالتفتيش يرد على الكيانات المعنوية في الحاسوب، بحسب أن هذه الكيانات المعنوية وإن كانت غير مادية إلا أنها تدخل في نطاق الأشياء المادية.[2]

فلقد تطورت طرق التفتيش بحيث أنها أصبحت لا تقف، عند ضبط الأدوات المادية المستخدمة في ارتكاب الجريمة أو ضبط جسم الجريمة الذي يحقق نموذجها القانوني وإنما يمكن لهذه الطرق كذلك أن تتعامل مع الجرائم التي ترتكب بالوسائل الالكترونية كالحاسوب، أو تقع عليه. فيمكن تبعا لذلك تسجيل البيانات المعالجة آليا بعد تحويلها من نبضات أو

[1] حسين بن سعيد بن سيف الغفاري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، بحث منشور علي الرابط http://www.minshawi.com، ص20.

[2] د. هلالي عبد الله أحمد، مرجع سابق، ص 89.

ذبذبات أو إشارات أو موجات كهرومغناطيسية إلى أشياء محسوسة تسجل وتخزن على وسائل معينة، وعلى هذه الوسائل يرد التفتيش أو الضبط.[1]

ويترتب على ذلك أنه يمكن تفتيش نظام معلومات الحاسوب ووسائط أو أوعية حفظ وتخزين البيانات المعالجة آليا كالأسطوانات والأقراص والأشرطة الممغنطة ومخرجات الحاسوب، ويدخل في هذا التفتيش أيضا المحتويات المخزنة في الوحدة المركزية للنظام والتي يمكن عزلها ككيان قائم بذاته.[2]

ثالثا: ضوابط التفتيش على الأدلة الإلكترونية

إذا كان التفتيش كوسيلة إجرائية يهدف الي الحصول على دليل يساعد في إثبات الجريمة فان حكمه يرتبط بطبيعة المكان المراد تفتيشه، هل هو من الأماكن العامة أو من الأماكن الخاصة، حيث أن لصفة المكان وطبيعته أهمية قصوى في مجال التفتيش، فإذا كانت المكونات المادية للحاسوب موجودة في مكان خاص كمسكن المتهم أو ملحقاته كان لها حكمه، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المسكن وبنفس الضمانات والإجراءات القانونية، واذا كانت تلك المكونات المادية متصلة بحواسيب أخرى موجودة في مساكن أو أماكن أخري غير مسكن المتهم، تعين مراعات تسبيب الأمر بتفتيش هذه الأماكن[3]، أما إذا حاز المتهم للمكونات وعثر عليه في مكان ما من الأماكن العامة، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال، وقد نصت بعض التشريعات على أن التفتيش يتم حتي بالنسبة لأنظمة الحاسوب، مثل ذلك، قانون إساءة استخدام الحاسوب في انجلترا

[1] JEAN P ،SPREUTELS ،Les Crimes Informatiques Et D'autres Crimes Dans Les Domaines De La Technologie Informatique En Belgique – Rev – Inter De- Dr Pen 1993 – P170

[2] هشام رستم، المرجع السابق، ص69.

[3] عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسوب الآلي، مرجع سابق، ص 37

الصادر في سنة 1990 حيث نص أن إجراءات التفتيش تشمل بما في ذلك أنظمة الحاسوب.[1]

إن التفتيش الوارد علي الكيان المنطقي لأجهزة الحاسوب والأنظمة الإلكترونية يخضع لبعض القيود يجب مراعاتها تحت طائلة البطلان. منها ما نصت عليه المادة 44 من قانون الإجراءات الجزائية بعد تعديله بالقانون رقم 06 – 22، على عدم جواز إجراء التفتيش من قبل ضابط الشرطة القضائية إلا بإذن مكتوب من وكيل الجمهورية أو قاضي التحقيق مع وجوب استظهار هذا الأمر قبل الدخول إلى المنزل والشروع في التفتيش.

ثم تنص المادة 45 من قانون الإجراءات الجزائية على القيود التي يتعين على ضابط الشرطة القضائية احترامها أثناء فترة التفتيش بصفة عامة لكن أضاف التعديل وتمم نص المادة 45 بأن رفع القيود الواردة فيها فيما يتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، إلا ما تعلق منها بالحفاظ على السر المهني وكذا جرد الأشياء وحجز المستندات.

كما تنص المادة 47 من قانون الإجراءات الجزائية علي إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل دون احترام الأوقات المذكورة في الفقرة الأولى في المادة 47 من قانون الإجراءات الجزائية، إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات غير أنه يشترط أن يكون مصحوبا بإذن مسبق من وكيل الجمهورية المختص أو قاضي التحقيق.

فالمشرع الجزائري عندما نص في المادة 05 من القانون رقم: 09-04 المؤرخ في 14 شعبان 1430 الموفق ل 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها علي جواز تفتيش أي منظومة معلوماتية

[1] WASIK (MARTIN) ،Computer Crimes And Other Crimes Against Information Technology In The United Kingdom- Rev ،Inter ،De ،Dr ،Panal 1993 ،P:640.

أو جزء منها وكذا المعطيات الإلكترونية المخزنة فيها أو أي منظومة تخزين معلوماتية، فإنه حسب رأيينا أن المشرع قصد الأنظمة الإلكترونية التي تقع داخل الدولة وحتى لو اتصلت مع بعضها البعض عن طريق شبكة محلية.

ففي حالة وقوع جريمة في نظم الحاسوب داخل الدولة الجزائرية فيجوز هنا لوكيل الجمهورية أو قاضي التحقيق إصدار الإذن بالتفتيش، لكن هذا الإذن بالتفتيش لا ينفذ إلا على الحاسوب الذي صدر من أجله، ويترتب على ذلك أنه إذا كان الحاسوب المراد تفتيشه يتصل بحاسوب أخر لم يصدر بالنسبة له إذن بالتفتيش لا يمكن أن يمتد إليه التفتيش حتى لو كان يحتوي على أدلة الجريمة، إلا إذا أمر قاضي التحقيق هنا في إذنه بالتفتيش أن يمتد على مستوى التراب الوطني بكامله حسب الفقرة الأخيرة من نص المادة 47 من قانون الإجراءات الجزائية.

رابعا: تفتيش الانظمة الإلكترونية عن بعد.

إن طبيعة التكنولوجيا وتطور أشكال الاتصالات وتعقيداتها، وضعت الكثير من التحديات أمام التحقيقات المتعلقة بالجرائم الإلكترونية، لا سيما أمام أعمال التفتيش والضبط بالنسبة للجرائم الإلكترونية العابرة للحدود الوطنية[1]، فالبيانات التي تحتوي على أدلة جنائية، قد تتوزع عبر شبكة حواسيب في أماكن مجهولة بعيدة تماما عن الموقع الذي يجري فيه التفتيش، وإن كان من الممكن الوصول إلي تلك البيانات من خلال حواسيب تقع في الموقع الجاري تفتيشه، غير أن تلك البيانات قد تكون موجودة فعليا، داخل اختصاص قضائي أخر أو حتى في بلد أخر. وهو ما يثير مسألتين هامتين هما مسألة الاختصاص القضائي ومسألة التعاون الدولي.

[1] KASPERSEN(W.K.HENRIK) ،Computer Crime And Other Crime Against Information Technology In Netherland ،R.I.D.P.1993 ،P 479

ونجد مبررات هذا الرأي في المادة 88 من قانون تحقيق الجنايات البلجيكي التي تنص على: إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فان هذا البحث يمكن أن يمتد إلى نظام معلوماتي أخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الامتداد وفقا لضابطين:

أ – إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث

ب – إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظرا لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث.[1]

وأجازت المادة 32 من الاتفاقية الأوروبية بشان الجرائم الإلكترونية والتي أعدها المجلس الأوروبي وتم التوقيع عليها في بودابست في 2001/11/23، إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين : الأولى إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، والثانية إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.

ويجيز القانون الفرنسي الصادر في 1991/08/10 اعتراض الاتصالات عن بعد بما في ذلك التي تتم عن طريق شبكات تبادل المعلومات. وفي هولندا أجاز المشرع، لقاضي التحقيق، أن يأمر بالتنصت على شبكات الاتصالات إذا كانت هناك جرائم خطيرة ضالع فيها المتهم وتشمل هذه الشبكة التلكس والفاكس ونقل البيانات.

[1] محمد أبو العلاء عقيدة، التحقيق وجمع الأدلة في الجرائم الإلكترونية، ورقة بحث القي في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، اكادمية شرطة دبي، مركز البحوث والدراسات، دبي، الامارات العربية المتحدة، 26 - 28 أفريل 2003، ص34.

الفرع الثاني: الخبرة

الخبرة لغة تعني تعريف الشيئ على حقيقته، وخبر الشيء، علمه عن تجربة، أما في الفقه فإن الخبرة القضائية هي وسيلة من وسائل الإثبات يتم اللجوء إليها إذا اقتضى الأمر كشف دليل أو تعزيز أدلة قائمة، كما أنها استشارة فنية يستعين بها القاضي أو المحقق في مجال الإثبات لمساعدته في تقدير المسائل الفنية التي يحتاج تقديرها إلى دراية علمية لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته[1]، كما يمكن تعريفها على أنها المهمة الموكولة من قبل المحكمة أو الهيئة القضائية إلى شخص أو إلى عدة أشخاص أصحاب اختصاص أو مهارة أو تجربة في مهنة ما أو علم لتحصل منهم على معلومات أو آراء أو دلائل إثبات لا يمكن لها أن تؤمنها بنفسها وتعتبرها ضرورية لتكوين قناعتها للفصل في نزاع معين.[2]

كما أنها طلب رأي أهل الخبرة في شأن كشف بعض جوانب الوقائع المادية التي يستعصى على قاضي الموضوع إدراكها بنفسه من مجرد مطالعة الأوراق، والتي لا يجوز للقاضي أن يقضي في شأنها استنادا لمعلوماته الشخصية وليس في أوراق الدعوى وأدلتها ما يعين القاضي على فهمها، والتي يكون استيضاحها جوهريا في تكوين قناعته في شأن موضوع النزاع.[3]

والخبرة هي الوسيلة لتحديد التفسير الفني للأدلة بالاستعانة بالمعلومات العلمية فهي في حقيقتها ليست دليلا مستقلا عن الدليل المادي، وإنما هي تقييم علمي لهذا الدليل، ويطلق لفظ خبير على كل شخص توافرت لديه معرفة عملية وفنية لتخصصه في مادة معينة

[1] عبد الحميد الشواربي، التزوير والتزييف مدنيا وجزائيا في ضوء الفقه والقضاء، منشأة، مصر1996، ص 552.
[2] أميل أنطوان ديراني، الخبرة القضائية، المنشورات الحقوقية الصادرة سنة 1977، طبعة1، بيروت، ص 17.
[3] همام محمد محمود زهران، الوجيز في إثبات المواد المدنية والتجارية، الدار الجامعية الجديدة للنشر، مصر، 2003، ص 357.

وتستعين به السلطة القضائية وجهات التحقيق في تقدير المسائل الفنية استكمالا لنقص معلومات القاضي في هذه النواحي.[1]

فالخبرة تهدف إلى التعرف على وقائع مجهولة من خلال الواقع المعلوم، فهي وسيلة تضيف إلى الدعوى دليلا، حيث يتطلب هذا الإثبات معرفة أو دراية لا تتوافر لدى رجال القضاء نظرا إلى طبيعة ثقافتهم وخبراتهم العلمية كما قد يتطلب الأمر إجراء أبحاث خاصة أو تجارب علمية تستلزم وقتا لا يتسع له عمل القاضي، فالخبرة تقتصر على المسائل الفنية دون المسائل القانونية لأن المحكمة مفروض فيها العلم بالقانون علما كافيا.

أولا: أهمية الخبرة في التحقيق في الجرائم الإلكترونية.

تلعب الخبرة دورا كبيرا في التحقيقات الجنائية في الجرائم الإلكترونية، ففي معظم دول العالم لا يزال جهاز الحاسوب أو الشبكات الإلكترونية والأدلة المستخرجة منها من اختصاص الخبراء.

وقد أجاز المشرع الجزائري، للمحقق الاستعانة بخبير متخصص في المسألة موضوع الخبرة، فقد نصت المادة 143 قانون الإجراءات الجزائية في فقرتها الأولى على أنه: يجوز لكل جهة قضائية تتولى التحقيق أو تجلس للحكم إذا تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناءا على طلب النيابة أو التحقيق أو الخصوم أو من تلقاء أنفسهم.

وبالنظر إلى الطبيعة الخاصة بالجرائم الإلكترونية فإن كشفها يحتاج إلى خبرة فنية منذ بدء مرحلة التحري، ثم تستمر هذه الحاجة في مرحلة التحقيق والمحاكمة نظرا للطابع الخاص بأساليب ارتكابها.[2]

[1] محمد فاروق عبد الحميد كامل، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، 1999، ص286.

[2] هشام محمد فريد رستم، قانون العقوبات ومخاطر التقنية المعلومات، مكتبة الآلات الحديثة، مصر، 1992، ص 137.

و إذا كانت الاستعانة بخبير أمر جوازي للمحقق أو لجهة التحقيق، إلا أنه في المسائل الفنية لا يمكن للقاضي أن يفصل فيها دون استطلاع رأي أهل الخبرة، في هذه الحالة يجب عليه أن يستعين بالخبير، فإذا قام القاضي بالفصل فيها دون مراجعة رأي الخبير كان حكمه معيبا قابلا للنقض.[1]

وبالعودة إلى نص المادة 146 نجد أن المشرع يفرض على الجهة القضائية الأمرة بندب خبير، تحديد مهمته بدقة. وهذا يعود بنا إلى ضرورة تأهيل سلطات التحقيق أو الحكم في الجرائم الإلكترونية لنجاح الهدف المتوخى من التحقيق في هذا النوع المستجد من الجرائم.

كما تجدر الإشارة الي أنه يجب على القاضي اختيار الخبراء ذوي الإمكانيات العلمية والمقدرة الفنية الحالية فلا يكفي مجرد الحصول على شهادة علمية، إذ يجب مراعاة الخبرة العلمية، فالوسائل الالكترونية متعددة وفي تطور مستمر وشبكات الاتصال بينها متنوعة فطبيعتها الفنية تجعلها موزعة على تخصصات فنية وعلمية دقيقة.[2]

وتقتضي فاعلية الخبرة ضرورة الجمع بين التعمق في كل من الدراسة العلمية والنظرية والممارسة العملية للتخصص العلمي والنظري، وكذا متابعة مستمرة للتطورات التي تلحق بفروع التخصص، غير أن ذلك ليس شرطا لازما في بعض الأحيان فقد يقتصر الخبير على مجرد الخبرة العملية في فرع التخصص دون أن يكون هناك رصيد من الدراسة العلمية والنظرية وهو الأمر الذي نلاحظه في مجالات الخبرة في الفروع المهنية المختلفة.[3]

والخبير لا يشترط فيه الكفاءة العلمية العالية في مجال التخصص فحسب بل يجب عليه أن يضاف إليها سنوات من أعمال الخبرة في المجال الذي تميز فيه، وعلى وجه

[1] محمد أبو العلاء عقيدة، المرجع السابق، ص 05.
[2] هشام محمد فريد رستم، المرجع السابق، ص 140 و141.
[3] محمد فاروق عبد الحميد كامل، المرجع السابق، ص 286.

الخصوص الجرائم ذات الصلة بالحاسوب، فقد يتعلق الأمر بتزوير المستندات أو التلاعب في البيانات أو الغش أثناء نقل أو بث البيانات أو جريمة من الجرائم الأموال أو الاعتداء على حرمة الحياة الخاصة، وتستوجب طبيعة الجرائم الإلكترونية توافر شروط خاصة في الخبير الذي ينتدب لبحث مسائل فنية وعلمية متعلقة بها، وهي:[1]

- الإلمام بتركيب الحاسوب وصناعته، طرازه، نوعه، نظم تشغيله الرئيسية والفرعية

الأجهزة الطرفية الملحقة به، وكلمات المرور أو السر وأنماط التشفير.

- طبيعة البيئة التي يعمل في ظلها الحاسوب أو الشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

- المكان المحتمل لأدلة الإثبات وشكلها وهيئتها.

- قدرة الخبير على إتقان المهام المسندة اليه، دون أن يترتب على ذلك أعطاب أو تدمير الأدلة المحصلة من الوسائل الإلكترونية.

- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بدون أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على الحاسوب أو النظام أو الشبكة.[2]

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص 138.

[2] عبد الفتاح بيومي حجازي، المرجع السابق، ص 149.

المطلب الثاني: اعتراض المراسلات

يعتبر اعتراض المراسلات والاتصالات الالكترونية من الطرق الاجرائية الحديثة التي تعتمد علي التقنية والتجهيزات الالكترونية والتي تم ابتكارها لمواجهة الجرائم الخطيرة التي تهدد الأمن والسلامة العامة علي غرار الجرائم الارهابية، الجرائم الإلكترونية.

ونظرا لأهمية هذه الوسيلة الاجرائية في استخلاص الأدلة الجنائية الرقمية لمواجهة الجريمة الإلكترونية، ارتأينا ان نتطرق الي تبيان مفهومها وطبيعتها القانونية والقيود التي فرضها المشرع عليها باعتبار أنها استثناء علي القاعدة العامة.

أولا: مفهوم اعتراض المراسلات والاتصالات والمراقبة الالكترونية.

تنص المادتن 39 و 47 من دستور 2020 علي أنه: لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، يحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

لكنه ولما كانت المصلحة العامة في مواجهة بعض أنواع الجرائم الخطيرة، تقتضي أن يتم المساس بسرية المراسلات والاتصالات الخاصة، فقد أجاز القانون القيام باعتراض تلك المراسلات والاتصالات الخاصة وبالمراقبة الالكترونية ضمن شروط وقيود حددها مسبقا وأوكل مهمة الإشراف عليها للسلطة القضائية.

فلقد جاء في نص المادة: 03 من القانون رقم 09 – 04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أنه مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، وحسب متطلبات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، ووفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، يتم

وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية.

ولم ينص المشرع الجزائري على تعريف محدد لاعتراض المراسلات أو الاتصالات الإلكترونية، لكنه أشار ضمنيا إلى أنها تتم بوضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها.

فإذا كانت شبكات الحاسوب تستخدم خطوط الهاتف وتستعين بجهاز معدل الموجات والذي يستطيع تحويل الإشارات الرقمية المستخدمة بواسطة الحاسوب إلى موجات تناظرية تنقل مع الموجات الصوتية خلال خطوط الهاتف وبذلك فانه يتبين وجود علاقة بين المراسلات التي تتم بالطرق التقليدية وتلك التي تتم بالرسائل الالكترونية، بحيث يمكن القول أن هناك تنصتا ومراقبة الكترونية تتم على شبكات الحاسوب.[1]

ومن ثم لا يجوز التصنت عليها أو الاطلاع على الأسرار التي تحتويها إلا بذات الطرق التي ينص عليها قانون الإجراءات الجزائية، فلا يستطيع الشخص اختراق صندوق البريد الالكتروني، أو الدخول الي أنظمة الحاسوب المخزنة به الرسائل البريدية الالكترونية وضبطها إلا عن طريق إتباع إجراءات قانونية محددة في القانون ومن قبل أشخاص مخولين قانونا بذلك.[2]

إن التفتيش واعتراض المراسلات إجراءان مختلفان، ولكل منهما طبيعته وشروطه ومبرراته، فالتفتيش هو استثناء علي المبدأ الدستوري الذي يقضي بحرمة المسكن والحياة الخاصة، واعتراض المراسلات هو استثناء علي المبدأ الدستوري الذي يقضي بحرمة المراسلات والاتصالات الخاصة وسريتها. كما أن اجراءات التفتيش تتخذ بعد وقوع الجريمة،

[1] هلالي عبد الله أحمد، مرجع سابق، ص 221.

[2] رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجبل للطباعة، الطبعة السادسة عشر، 1985، ص 358.

اما اجراءات اعتراض المراسلات والاتصالات فإنها تكون فورية أي خلال عملية ارسال البيانات أي قبل وقوع الجريمة وتمامها.[1]

ثانيا: ضوابط اعتراض المراسلات والاتصالات الالكترونية.

لما كان اعتراض المراسلات والاتصالات الالكترونية استثناء علي القاعدة الدستورية التي تقضي بسرية المراسلات والاتصالات الخاصة، فقد أحاط المشرع هذه الوسيلة الاجرائية بمجموعة من الضوابط تتمثل في أن تتم في حالات معينة وتحت اشراف السلطة القضائية.

و قد تطرق المشرع الجزائري في تعديله الأخير لقانون الإجراءات الجزائية بالقانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 في نص المادة 140 المتممة للباب الثاني من الكتاب الأول من الأمر رقم 66-155 بفصل الرابع تحت عنوان " اعتراض المراسلات وتسجيل الأصوات والتقاط الصور" والمواد 65 مكرر 5 إلى المادة 65 مكرر 10 لإجراء اعتراض المراسلات، كما تطرق في القانون رقم 09 - 04 المؤرّخ في 5 أوت سنة 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الي الحالات التي يسمح فيها باللجوء الي المراقبة الالكترونية.

خاصة إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم محددة على سبيل الحصر في نص المادة 65 مكرر 5 ومن بين هذه الجرائم، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، فيسمح الإذن بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المنصوص عليها في المادة 47 من قانون الإجراءات الجزائية بغير رضا أو حتى علم الأشخاص الذين لهم حق تلك الأماكن، وتنفيذ عمليات المراقبة هنا تكون تحت المراقبة المباشرة لوكيل الجمهورية أو لقاضي التحقيق.[2]

[1] حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل اجازة المدرسة العليا للقضاء، 2008، ص 55.
[2] حاجب هيام، المرجع السابق، ص57.

و الإذن بالمراقبة أو التصنت أو اعتراض المراسلات محددة ب 4 أشهر كحد أقصى قابلة للتجديد طبقا لنص المادة 65 مكرر 7 من قانون الاجراءات الجزائية، كما المشرع خول لقاضي التحقيق الإذن أيضا بوضع هذه الترتيبات في حالة فتح تحقيق قضائي وتتم العمليات تحت مراقبته المباشرة،

وقد أجاز المشرع في نص المادة 65 مكرر 8 تسخير كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات السابقة الذكر في نص المادة 65 مكرر 5.

وعلى ضباط الشرطة القضائية تحرير محضر عن أي عملية اعتراض أو تسجيل، أو وضع ترتيبات تقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، ويذكر تاريخ بداية هذه العمليات والانتهاء منها، كما يودع أي تسجيل أو اعتراض أو نسخ تم أثناء عملية المراقبة ويتم إيداعها بالملف.

المبحث الثاني: معوقات الإثبات في الجرائم الإلكترونية

إن الإثبات هو إقامة الدليل علي وقوع الجريمة ونسبتها إلى المتهم وذلك وفق طرق مشروعة ومحددة قانونا، حيث يعد موضوع الإثبات في الجريمة الالكترونية الأساس الذي تبني عليه أي سياسة جنائية لمكافحة هذا النوع من الجرائم . وتثير مسألة الإثبات صعوبات في مواجهة الجرائم الالكترونية، التي تقع علي العمليات الالكترونية بالوسائل الالكترونية، لكون هذه الجرائم تقنية تنشأ في الخفاء في بيئة رقمية، ينتج عنها مايسمى بالأدلة الإلكترونية التي تعتبر إحدى الأثار المهمة في الكشف عن هذه الجريمة و الربط بينها وبين مرتكبيها.

فإثبات الجرائم التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية سيتأثر بطبيعة هذه الجرائم، وبالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم اكتشاف العديد من الجرائم في زمن ارتكابها، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم، أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالأفراد وبالمجتمع.

المطلب الأول: معوقات التحقيق والمتابعة الإلكترونية

إن الجرائم التي ترتكب على العمليات الإلكترونية التي تعتمد في موضوعها على التشفير والأكواد السرية والنبضات والأرقام والتخزين الإلكتروني يصعب أن تخلف وراءها آثارا مرئية قد تكشف عنها أو يستدل من خلالها على الجناة. وكمثال لذلك نجد أن السرقة الإلكترونية بنسخ الملفات وسرقة وقت الآلة يصعب على الشركات التي تكون الضحية لمثل هذه الأفعال اكتشاف أمرها وملاحقة الجناة عنها . ولعل هذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الإلكترونية تلقى بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية حيث تصعب قدرتهم على فحص واختبار البيانات محل الاشتباه

خاصة في حالات التلاعب في برامج الحاسبات، ومن ثم فقد يستحيل عليهم الوصول إلى الجناة. فمن المعلوم أن جهات التحري والتحقيق اعتادت على الاعتماد في جمع الدليل على الوسائل التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة ولكن في محيط الإلكترونيات فالأمر مختلف، فالمتحري أو المحقق لا يستطيع أي منهما تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية

الفرع الأول: المعوقات التقنية في التحقيق والمتابعة الإلكترونية

يمكن تقسيم التحديات التقنية في التحقيق والمتابعة الإلكترونية إلي معوقات مرتبطة بصعوبة اكتشاف الجريمة، ومعوقات متعلقة بصعوبة اثبات الجريمة.

أولا: المعوقات المرتبطة بصعوبة اكتشاف الجريمة.

من بين هذه المعوقات:

1-إنعدام الأثر المادي للجريمة: تبقي أغلب الجرائم الإلكترونية مجهولة، ما لم يتم التبليغ عنها للجهات المعنية، فالجرائم الإلكترونية لا تصل إلى علم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية لا تخلف أثار مادية كتلك التي تخلفها الجريمة العادية مثل الكسر في جريمة السرقة[1]، فالعديد من الجرائم الالكترونية تتم دون أن يشعر بها القائمون على تشغيل الأجهزة الإلكترونية، كجرائم التجسس التي تتم عن طريق اعتراض النبضات الالكترونية، وعن طريق زرع برامج تجسس خاصة في أجهزة الحاسوب، وجرائم اختلاس التي تتم عبر تعديل البرامج والتلاعب بالأنظمة الإلكترونية. ويرجع السبب في افتقاد الآثار التقليدية للجريمة المرتكبة عبر الانترنت إلى ما ذكره بعض الفقهاء من أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسوب دون أن يتوقف

[1] عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت، دراسة متعمقة في جرائم الحاسوب الالي والأنترنت، بهجات للطباعة والتجليد، مصر، 2009، ص41.

ذلك على وجود وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معدا ومخزنا على جهاز الحاسوب.[1]

كما أن الوسائل التي ترتكب بها الجرائم الإلكترونية تتخذ شكل قالب غير تقليدي فهي ترتكب عادة عن طريق نقل المعلومات على شكل نبضات الكترونية غير مرئية تنساب عبر أجزاء الحاسوب، وشبكة الاتصالات العالمية بصورة آلية، كما تنساب الكهرباء عبر الأسلاك.[2] وتأتي مشكلة ضبط هذه المعطيات وإحرازها في شكل الكتروني ووضعها في قالب قانوني لاستغلالها في البحث وإذا كانت بعض التجهيزات والتقنيات تسمح للباحثين بالوصول إلى هذه المعطيات التي تبقى في ذاكرة الحاسوب المستعمل، إلا أنها تتطلب خبرة عالية وإمكانيات قد لا تتوافر عادة لدى مصالح الشرطة القضائية المكلفة بالبحث وحتى في حالة حجز المعطيات الرقمية، فان البيانات أو المعلومات التي تشتمل عليها لا تتضمن آثار أو بصمات يمكن الاستدلال من خلالها على صاحبها، بل يحتاج الوصول إلى هذا الهدف إلى عمليات بحث وتحري أخرى للوصول على نسق من القرائن المادية التي يمكن الاستدلال من خلالها على المجرم، بل يحتاج الوصول إلى هذا الهدف إلى عمليات بحث وتحري أخرى التي يمكن أن تعزز دلالتها وقيمتها في الإثبات.

2- الطبيعة الدولية للجريمة الإلكترونية: اذا تطلب ارتكاب جريمة تقليدية علي غرار القيام بسرقة مصرف ما، تنقل المجرم الي موقع ذلك المصرف والدخول اليه ومن ثمة السطو علي الاموال الموجودة فيه، مع ما قد يترتب عن ذلك من نتائج وأدلة هامة، نتيجة تواجد المجرم بمسرح الجريمة فقد يتم التعرف عليه من بعض الشهود وقد يتم التقاط صور له باستعمال اجهزة المراقبة، وقد يتم اكتشاف هويته من خلال البصمات التي يتركها خلفه،

[1] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، مرجع سابق، ص 83.

[2] محمد حماد مرهج الهيتي، جرائم الحاسوب- ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، الطبعة الاولى، دار المناهج للنشر والتوزيع، عمان، 2006، ص99.

لكن الامر يختلف بالنسبة للجرائم الإلكترونية لا سيما تلك المرتكبة عبر الانترنت، فغالبا ما ترتكب تلك الجرائم عن بعد، أي انها جرائم لا تشترط وجود المجرم في الموقع الذي تتحقق فيه النتيجة الاجرامية، فبإمكان المجرم الإلكتروني ان يتسلل الي انظمة مصرف ما قد يقع داخل دولته او خارج حدودها الاقليمية ويقوم بعمليات تحويل مصرفية لأموال ضخمة من حسابات المصرف او من حسابات زبائنه الي حسابات سرية، دون ان يخلف دليلا واحدا ضده. وقد يتسلل المجرم الإلكتروني الي شبكة معلوماتية داخلية أو الي جهاز حاسوب مرتبط بشبكة الانترنت ويقوم بنسخ ما يشاءا من ملفات وصور وافلام خاصة، دون ان يدرك الضحية ذلك.

ثانيا: المعوقات المتعلقة بصعوبة اثبات الجريمة.

نجد من بين تلك المعوقات:

1-فرض الجناة لتدابير أمنية: يعمد المجرمون عبر الانترنت عادة إلى إخفاء جرائمهم أو تمويهها علي أنها أعطال أو اخطاء في أنظمة التشغيل، أو إزالة أثار الجريمة عن طريق التلاعب بقواعد البيانات والقوائم في جهاز الحاسوب والبرامج، لا سيما أن التخزين الالكتروني غير مرئي والبيانات كثيرة وهي مكتوبة بلغة رقمية لا تفهمها إلا الآلة ما لم تعرض على شاشة الكمبيوتر، ليتمكن الإنسان من قراءتها وفهمها، وهذا يشكل عقبة أمام إقامة الدليل على الجريمة المرتكبة عبر الانترنت وإثباتها[1]، فلا مرية أن المجرمين الذين يرتكبون جرائم بالوسائل الالكترونية الحديثة من فئة الأذكياء الذين يخفون أفعالهم غير مشروعة قبل ارتكابها لكي لا يتم كشفهم، مما يزيد من صعوبة إجراءات التي يتوقع الحدوثها للكشف عن الأدلة التي قد تدينهم باستخدام كلمات السر التي لا تمكن غيرهم من الوصول إلى البيانات المخزنة الكترونيا أو المنقولة عبر شبكات الاتصال، وقد يلجأ هؤلاء

[1] فريد منعم جبور، حماية المستهلك عبر الإنترنت ومكافحة الجرائم الالكترونية (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010، ص 209.

المجرمون أيضا إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة لها بحيث قد يستحيل على غيرهم الاطلاع عليها ويتعذر على جهات التحري والضبط الوصول إلى كشف أفعالهم غير مشروعة.

بالإضافة إلى ذلك يقوم المجرمون عبر الانترنت بإخفاء هويتهم أو انتحال شخصية أخرى حتى لا يمكن التعرف عليهم في حالة اكتشاف الجريمة، وقيام المحققين بالتحري عنها، حيث توجد الكثير من البرامج التي تمكن المستخدم من إخفاء شخصيته، سواء أثناء إرسال البريد أو أثناء تصفح المواقع، فهم يسعون من خلالها إلى إخفاء شخصيتهم والفرار من مسائلة نظامية.[1]

2-الطبيعة غير المادية للأدلة الالكترونية: يكون دليل الإثبات في الجريمة التقليدية ماديا كالأسلحة أو الأدوات المستعملة في القتل أو الضرب، وكذلك المزاد السامة التي تستعمل في القتل، أو المحرر المزور، أو النقود التي زيفت وأدوات تزييفها، وفي كل هذه الأمثلة يستطيع رجل الضبط أو التحقيق الجنائي رؤية الدليل المادي وملامسته بإحدى حواسه.[2]

لكن في الجرائم الإلكترونية خاصة التي تقع عبر شبكة الانترنت، كالتي تقع على عمليات التجارة الالكترونية أو العمليات الالكترونية المصرفية، أو على أعمال الحكومة، يكون محلها جوانب تتعلق بالمعالجة الآلية للبيانات، فإذا وقعت جرائم معينة على هذه الجوانب غير المادية، فإنه يصعب إقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذي وقعت عليه الجريمة.

فلا يوجد شك في إثبات الأمور التي تترك أثار مادية، بعكس إثبات الأمور غير المرئية، فإنه يكون في منتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أي أثار قد تدل عليه

[1] محمد بن عبد الله بن علي المنشاوي، جرائم الانترنت في المجتمع السعودي، رسالة مقدمة إلى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية تخصص قيادة أمنية، أكاديمية نايف العربية للعلوم الأمنية، الرياض، السعودية، 2003، ص 54.

[2] عبد الفتاح بيومي الحجازي، مرجع سابق، ص 36

أو تكشف عنه بحسبان أن أغلب المعلومات والبيانات التي تتداول عبر أجهزة الحاسوب والتي من خلالها تتم العمليات الالكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة.[1]

3-صعوبة الوصول إلى الدليل: إن الطبيعة غير المرئية للأدلة المتحصل عليها من الوسائل الالكترونية تعد أحد ابرز المشكلات في التعامل مع الجرائم الإلكترونية، وتجعل من الكشف عن هذا النوع من الادلة وتجميعه لإثبات وقوع الجريمة والتعرف على مرتكبها عملية صعبة ومعقدة، خاصة إذا تمت إحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول المواقع والتي تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة محاولات الوصول إليها والاطلاع عليها أو نسخها.

4- سهولة محو الأدلة الإلكترونية: إن الأدلة الرقمية بما أنها بيانات معبر عنها بلغة الارقام، يمكن التلاعب بها واخفائها بسهولة، وبالتالي يعتبر ذلك من بين الصعوبات التي يمكن أن تعترض العملية الإثباتية في مجال الجرائم الإلكترونية، بحيث يقوم الجاني بمحو أو تدمير أدلة الإدانة في زمن قصير جدا، فضلا عن سهولة تنصله من هذا العمل بإرجاعه حسبما تشهد على ذلك وقائع عديدة، على خطأ في نظام الحاسوب أو الشبكة أو في الأجهزة[2]، كما أن هناك بعض الأفعال غير المشروعة التي يرتكبها جناة الانترنت ويكون أمرها حكرا عليهم كالتجسس عل الملفات الخاصة، والوقوف على ما بها من أسرار، وقد يخربون الأنظمة تخريبا منطقيا بحيث يمكن تمويهه بأنه خطأ في البرامج أو الأجهزة أو نظام التشغيل.

[1] غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004، ص 539.

[2] - من أمثلة على ذلك قيام احد مهربي الأسلحة في النمسا بإدخال تعديلات على الأوامر العادية لنظام التشغيل جهاز الحاسوب الآلي الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذا الحاسوب من خلال لوحة المفاتيح محو وتدمير كافة البيانات كاملة. لمزيد من التفاصيل انظر هشام محمد فريد رستم، الجرائم المعلوماتية" أصول التحقيق الجنائي الفني" المرجع السابق ص 430.

ومما يزيد من خطورة إمكانية وسهولة إخفاء الأدلة المتحصل من الوسائل الالكترونية، أنه يمكن محو الدليل في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها، وفي الحالة التي قد تعلم بها فأنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده[1].

5-إتساع البيانات الواجب فحصها: تعرف قواعد البيانات بأنها عبارة عن مجموع بطاقات تشمل بيانات معدلة ومنظمة تسمح باقتطاع البيانات حسب مشيئة المستعمل، تعتبر قاعدة البيانات بأنها نظام فعال يستعمل لترتيب الملفات التي تحتوي على معلومات معينة، وتعتبر قواعد البيانات كوسيط لتخزين المعلومات ومعالجتها أي تنظيمها وترتيبها.

ويشكل الكم الهائل من البيانات التي يجري تداولها عبر الانترنت أحد مظاهر الصعوبات التقنية التي تعيق التحقيق في الجرائم التي تقع عليها أو بواسطتها، وكمثال علي ذلك فإن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات التي قد لا تثبت كلها تقريبا شيئا على الإطلاق[2]، قد تكون النتيجة سلبية بحيث لا يمكنها كشف الدليل المراد ضبطه أو تحصيله، وهذا مراده في المقام الأول عدم وجود آلية للفرز الذاتي للملفات المخزنة، حتى يمكن الوقوف على الملفات غير مشروعة وضبطها، ما يجعل القضاء لا يكترث بالدليل الرقمي، ولا يعول عليه كثيرا لافتقاره الى المصداقية التي تجعله جديرا بالثقة، لذلك وفي ظل إمكانية خروجها عن نطاق الدولة والبعد الجغرافي بين مرتكب الجريمة والضحية.[3]

[1] حسين بن سعيد بن سيف الغفاري، مرجع سابق، ص 19.
[2] هشام محمد فريد رستم، المرجع السابق، ص 430.
[3] سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض2003، ص98.

الفرع الثاني: المعوقات البشرية في التحقيق والمتابعة الإلكترونية

يمكن تقسيم التحديات البشرية في التحقيق والمتابعة الإلكترونية إلي معوقات متصلة بالمجني عليهم، ومعوقات مرتبطة بالجهات التي تتولي التحقيق في الجرائم الإلكترونية.

أولا: المعوقات المتصلة بالمجني عليهم.

من بين تلك المعوقات نجد:

1-عدم الابلاغ عن الجرائم الإلكترونية: إن تكتم المجني عليهم وإحجامهم في الابلاغ عن الجرائم الإلكترونية يؤدي الي صعوبة اكتشاف الجريمة واثباتها، ذلك لأن المجني عليه غالبا ما يكون شخصا معنويا كالبنوك أو المؤسسات المالية، ويتم التكتم في مثل هذه الجرائم في حال التعرض لها، ولا يتم تبليغ السلطات المختصة في مكافحة هذه الجريمة لعدة أسباب، كتفادي اطلاع الأجهزة الأمنية على المعلومات ذات الطابع السري، أو تجنب الخسائر التي يتوقع تحققها نتيجة هذا الإبلاغ بسبب نقص ثقة العملاء في هذه المؤسسات.[1]

إن أسباب الاحجام عن الابلاغ عن الجرائم الإلكترونية متعددة، منها:

- جهل الأفراد العاديين أو المسؤولين أن مثل هذه الأفعال والهجمات تعتبر جرائم تقع تحت طائلة العقاب.

- خوف المجني عليهم، خاصة المؤسسات والشركات المالية أو الامنية من أن يؤدي انتشار خبر الحادث على سمعتها ومصداقيتها وظهورها بمظهر مشين أمام الآخرين، لأن تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعا بإهمالها أو قلة خبرتها أو عدم وعيها الأمني،

[1] محمد حماد مرهج الهيتي، مرجع سابق، ص 217.

ولم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها، الأمر الذي ينعكس سلبا على أرباحها وقيمة أسهمها.

- رغبة المؤسسات والشركات التجارية في تفادي أعمال التحقيق التي قد تؤدي إلى احتجاز حواسيبها أو تعطيل شبكاتها لفترة طويلة، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق، اضافة الي الاضرار التي طالتها من جراء الجريمة في حد ذاتها.

- انعدام ثقة المجني عليهم في قدرة الجهات المكلفة بالبحث والتقصي عن الجرائم الإلكترونية والتحقيق الجنائي عن توقيف المجرمين وتقديمهم للمحاكمة. [1]

2- إهمال الشركات والمؤسسات للجانب الأمني: تتسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، على سبيل المثال نجد مستخدمو شبكة الانترنت عبر مزودي الخدمة أو بطاقات الانترنت المدفوعة ليسوا مطالبين بتحديد هويتهم عند الاشتراك في خدمة الانترنت، أي أن مزود الخدمة لا يعرف هوية مستخدم الخدمة.

3-عدم إدراك خطورة الجرائم الإلكترونية: تعد إحدى معوقات التحقيق، ذلك لان عدم ادراك خطورة الجرائم الإلكترونية من قبل الأشخاص تجعلهم يتهاونون ولا يتخذون احتياطاتهم لتفادي وقوعهم ضحايا لتلك الجرائم كتأمين شبكاتهم أو أجهزتهم التي يستعملونها، ويتركونها عرضة للاختراق ولسرقة البيانات منها حتي دون ان يدركوا ذلك.

ثانيا: معوقات مرتبطة بالجهات التي تتولي التحقيق في الجرائم الإلكترونية.

ومن بين تلك المعوقات:

[1] محمد حماد مرهج الهيتي، مرجع سابق، ص 218.

1-نقص خبرة جهات البحث والتحري: وهي تندرج ضمن صعوبات تتعلق بجهة التحقيق، حيث تفرض متطلبات العدالة الجنائية على الحكومة بشكل عام، والأجهزة المسئولة عن تتبع الجرائم وضبطها والتحقيق فيها بشكل خاص أن تتحمل مسؤوليتها في مكافحة الجريمة واكتشاف المجرمين وإيقافهم ومحاكمتهم، ومثل هذا الأمر يقتضي توفير الإمكانات التقنية اللازمة سواء في عملية التحقيق أو الكشف والاستدلال عن الجرائم.

وتواجه عملية استخلاص الدليل في الجريمة المرتكبة عبر الانترنت صعوبة نقص الخبرة لدى رجال الضبط القضائي، أو أجهزة الأمن بصفة عامة، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي.

وقد توجه فقه الجنائي إلى أن البحث والتحقيق في جرائم الحاسوب هي مسالة في غاية الأهمية والصعوبة، لاسيما بالنظر لاعتبارات التكوين العلمي والتدريبي، والخبرات المكتسبة لرجال الضبط القضائي وسلطات التحقيق الجنائي والحكم، ذلك لأن حداثة الجرائم وتقنياتها العالية تتطلب دراية من القائمين على البحث الجنائي والتحقيق، فلا يكفي أن يكون لهم الخلفية القانونية أو أركان العمل الشرطي فقط، ولكن لابد من الإلمام بخبرة فنية في مجال الجريمة المرتكبة عبر الانترنت.[1]

إلا أن المشكلة تكمن في نقص المهارة والخبرة المطلوبة للتحقيق في هذا النوع من الجرائم، ونقص المهارة في استخدام الحاسوب والانترنت، وعدم المعرفة بأساليب ارتكاب جرائم الحاسوب والانترنت، وقلة الخبرة في مجال التحقيق في جرائم الحاسوب والانترنت والمعرفة باللغة البرمجية[2]، لاسيما وأن للعاملين في مجال الحاسوب مختصرات علمية خاصة تشكل طابع لمحادثاتهم وأساليب التحاور فيما بينهم، وليس هذا فحسب بل اختصر

[1] عبد الفتاح بيومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، مرجع سابق، ص122.
[2] سليمان بن مهجع العنزي، المرجع السابق، ص 119.

العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات وهي لغة متطورة ومتجددة.

ومن أجل التحقيق في هذه الجرائم فانه لا بد من إيجاد أسلوب خاص يجمع بين الخبرة الفنية والكفاءة المهنية ومن الممكن حيال ذلك إتباع الخطوات التالية:[1]

أ – تبادل المعلومات بين المحقق وخبير الحاسوب قبل الشروع في التحقيق وأخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهمين، بحيث يشرح المحقق للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم، ومن جهة أخرى يقوم الخبير بشرح النقاط الفنية التي ينبغي استجلائها من الأشخاص، وكافة المصطلحات الحاسوبية التي يمكن استخدامها مع بيان معانيها ليتم الاستفادة منها عند الضرورة.[2]

ب –حصر النقاط المطلوبة استجلائها من قبل الخبير والمحقق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب تلك النقاط.

ج – أخذ أقوال الشهود واستجواب المتهمين من قبل المحقق وبحضور الخبير الذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب وفق الكيفية التي تتم الاتفاق عليها مسبقا قبل بدء التحقيق.

د – التنسيق بين المحقق والخبير في الحصول على البيانات المخزنة في الحاسوب الآلي وملحقاته الخاصة بالشاهد أو المتهم الذي يم التحقيق معه، مع مراعاة أن هذا الأخير لا يجوز إجباره على تقديم دليل يدينه.

---

[1] البشرى محمد الأمين، التحقيق في جرائم الحاسوب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 2004، ص 173.

[2] United Nation Manual On The Prevention And Control Of Computer ،Related Crime ، Vienna 1999.

و لضمان نجاح التحقيق في الجرائم الإلكترونية فهناك بعض القواعد التي ينبغي مراعاتها أهمها: [1]

أ – تفادي ضياع الوقت في التحقيق حول جرائم لا يمكن اكتشفها خاصة وأن الأدلة اللازمة لاكتشافها وإثبات التهمة قد قضي عليها.

ب – مراعاة وجود نوع من التعامل بين المحققين وخبراء الحاسوب العاملين في المؤسسة المجني عليها.

ج – مراعاة القوانين السارية بشأن الحقوق الفردية وسرية البريد الالكتروني وغيرها من الحقوق.

د – العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط أجهزة الحاسوب الآلي وملحقاتها وبرامجها.

هـ – مراعاة حفظ الأدلة الجنائية بالطرق المناسبة كل حالة على حدى، وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبطت عليها.

و – الاستعانة بالتقنيات المتطورة في المجال الإلكتروني في مواجهة الجرائم الإلكترونية، سيما وأن هذه التقنيات أثبتت جدارتها ونجاحها في جمع الأدلة الجنائية وصناعة البنية الاتهامية وتحليل القرائن واستنتاج الحقائق.

المطلب الثاني: المعوقات التشريعية والتنظيمية

تصطدم مسألة اثبات الجرائم الإلكترونية بالعديد من التحديات والمسائل الهامة علي الصعيد القضائي، تتمثل أساسا في انعدام وجود آليات مرنة للتعاون الدولي القضائي في المجال الجنائي لمواجهة الجرائم الإلكترونية، بحكم أنها جرائم من طبيعة خاصة تتطلب

[1] البشرى محمد الأمين، المرجع السابق، ص 178.

عملية مواجهتها تكاثف الجهود وتنسيقها علي المستوي الدولي، لا سيما عندما تصطدم أغلبية إجراءات التحقيق المتبعة في هذه الجرائم علي غرار التفتيش بعقبات قانونية علي غرار مسألة الاختصاص والقانون الواجب التطبيق.

الفرع الأول: قصور التعاون الدولي في مكافحة الجرائم الإلكترونية.

باعتبار أن الجرائم الإلكترونية، جرائم لا تعترف بالحدود الاقليمية لكل دولة، يمكن ارتكابها عن بعد، ويمكن بذلك أن تقع تحت طائلة عدة انظمة قانونية، فإن مسالة التعاون الدولي في مكافحة هذا النوع من الجرائم واثباتها، تعد مسالة هامة وحاسمة. ولكنها في نفس الوقت مسالة معقدة، لاسباب عدة منها:

أولا: صعوبة توحيد المفاهيم:

إن مفهوم الجريمة الإلكترونية في حد ذاته محل اختلاف بين مختلف الانظمة القانونية، كما أن عالم الاجرام الإلكتروني ينطوي علي الكثير من المصطلحات التقنية غير المستقرة بسبب تغير مفاهيمها وتجددها مع التطور التكنولوجي، وبذلك فانه من الصعوبة علي تلك الانظمة القانونية أن تستوعب معا تلك التغيرات وتضع مفاهيم موحدة لتلك المصطلحات خاصة مع التباين الكبير الموجود بين الدول التي تنتمي اليها تلك الأنظمة القانونية فيما يخص مدي تقدمها العلمي واستيعابها للتكنلوجيا.

إن اختلاف المفاهيم المرتبطة بالجرائم الإلكترونية بين نظام قانوني واخر يضعف من منظومة القانون الدولي في ضبط تلك الجرائم، وبالتالي يسهل علي الجناة الافلات من المسائلة الجنائية[1]. لأن عدم الاتفاق علي ماهية النمط او السلوك الاجرامي المحدد للجرائم الإلكترونية من شانه أن يؤدي الي افلات الكثير من الانشطة الاجرامية من مسالة التعاون

[1] ايهاب ماهر السنباطي، الجرائم الالكترونية -الجرائم السيبرانية -قضية جديدة أم فئة مختلفة، التناغم القانوني هو السبيل الوحيد، االندوة الاقليمية حول الجرائم المتصلة بالكومبيوتر، المملكة المغربية، جويلية 2007، ص15- 36.

الدولي، فالتباين والاختلاف الموجود بين مفهوم الجريمة الإلكترونية بين الدول يؤدي ببعضها الي تجريم افعال وسلوكات لا تعبرها دول اخري جرائم وبالتالي فإنها لا تعتبرها من مسائل التعاون الدولي.[1]

ثانيا: تنوع واختلاف الانظمة الاجرائية.

لا يقتصر التعاون الدولي علي المسائل الموضوعية فقط، لا سيما في المجال الجنائي، بل إن التعاون في المسائل الاجرائية لا يقل عنه أهمية عنه في المسائل الموضوعية، ذلك أن التعاون في حد ذاته يتطلب ايجاد وسائل اجرائية واليات يتم من خلالها، وأنه من شأن الاختلاف الموجود بين الانظمة الاجرائية للدول أن تصعب من مسالة التعاون.

إن التعاون في المسائل الاجرائية من المسائل الهامة في مكافحة الجرائم الإلكترونية خاصة وأن هذه الجرائم وبسبب طبيعتها وسرعة ارتكابها أو سهولة اخفاء الادلة الناتجة عنها، تتطلب من مختلف الانظمة القانونية الاجرائية أن تكييف الاجراءات التقليدية المتبعة من طرفها في التحقيق والمحاكمة بما يتوافق مع تلك الطبيعة والسرعة، كما أن مسالة التعاون الاجرائي، تتطلب ازاحة الكثير من العراقيل المتعلقة بتحديد طرق واليات التفتيش والضبط والحفظ والمصادرة وكيفياتها، خاصة مع امكانية اجراء التفتيش لأي منظومة معلوماتية عن بعد.

فعادة ما تختلف طرق واجراءات التحري والتحقيق في دولة ما عنها في دولة اخري وهي إجراءات وإن كانت تثبت فاعليتها في دولة ما، قد لا تكون كذلك في دولة أخري، وهي إن كانت مشروعة في دولة ما، قد لا تكون كذلك في دولة اخري، وقد لا تكون مرخص بها أصلا، كما هو الحال بالنسبة للمراقبة الالكترونية، والتسليم المراقب، والعمليات المستترة،

[1] فريد منعم جبور، مرجع سابق، ص 215.

وبالتالي فان التعاون في هذه المسائل لديه اهمية كبيرة خاصة في تقدير مشروعية وحجية الأدلة التي تستنبط في ظلها.[1]

كما تتعلق مسائل التعاون الاجرائي بالقانون الواجب التطبيق وامتداد الاختصاص القضائي، وتسليم المجرمين، وهي عادة مسائل مستعصية، غالبا ما تصطدم بمسائل اخري تحول دون الاتفاق عليها، علي غرار مسالة السيادة، ومسالة المعاملة بالمثل.

الفرع الثاني: اشكالية الاختصاص القضائي والقانون الواجب التطبيق.

قد تصل إنعكاسات الجرائم الإلكترونية إلى أكثر من نظامين قانونيين، وهذا يطرح مسألة هامة في مكافحة الجرائم الإلكترونية تتعلق بإشكالية الاختصاص القضائي والقانون الواجب التطبيق، ومدي فاعلية المبادئ القانونية المعتمدة في هذا المجال، كمبدأ الإقليمية ومبدأ الشخصية ومبدأ العينية، وكذا المعايير والضوابط المحددة للاختصاص، كمعيار الاختصاص المكاني، معيار القانون الاكثر ملائمة، ومعيار الضرر المرتقب، في حل مشكلة القانون الواجب التطبيق ومشكلة تنازع الاختصاص بنوعيه الايجابي والسلبي.

أولا: اشكالية القانون الواجب التطبيق.

إن المبادئ التقليدية السالفة الذكر وإن كانت تتفق مع طبيعة الجرائم التقليدية، غير أنها لا قد لا تجد مكان لتطبيقها في الجرائم الإلكترونية، التي تتسم بكونها جرائم لا موطن لها فغالبية تلك الجرائم ترتكب عبر شبكة الانترنت التي تتميز بانها شبكة عالمية لا مقر لها في دولة معينة، تخضع لرقابتها او سيطرتها، ونظرا لعدم وجود قانون جنائي موحد يحكم هذه الشبكة، فان القوانين الجنائية التي تطبق عليها تتعدد بتعدد الدول المرتبطة بها باعتبار أن القانون الجنائي يتعلق بسيادة الدولة. فالأصل في القوانين هو اقليمية القانون الجنائي، وبذلك

[1] براء منذر كمال عبد اللطيف، ناظر احمد منديل، « القانون القضائي الدولي في مواجهة جرائم الانترنيت » المؤتمر العلمي لتحولات القانون العام في مطلع الالفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009، ص11.

فان الدول عادة لا تهتم الا بالجرائم الإلكترونية التي ارتكبت في اراضيها أو تحققت النتائج الاجرامية بها، غير أن ذلك قد لا يتفق مع حماية مصالح الدولة، بالنظر الي البعد الدولي للجرائم الإلكترونية المرتكبة بواسطة شبكة الانترنت، حيث تضع هذه الشبكة دول مختلفة في حالة اتصال دائم، كما أن المعلومات والبيانات التي يتم ادخالها وتحميلها علي الشبكة تنتشر في ثوان معدودة في كل الدول المرتبطة بها، بحيث تكون متاحة لأي مستخدم بها.[1]

إن الاخذ بمبدأ الشخصية أو مبدأ العينية كمبدأين مكملين لمبدأ اقليمة النص الجنائي، في تحديد القانون الواجب التطبيق علي الجرائم الإلكترونية لا سيما تلك المرتكبة عبر الانترنت، محل انتقاد باعتبار أن تحديد جنسية المجرم في الجرائم الإلكترونية، عادة ما لا يتأتى الا بعد القيام بالتحقيقات اللازمة. وأن هذه التحقيقات لا بد أن تقع في ظل نظام قانوني اجرائي معين، أي أن مسالة تحديد القانون الاجرائي الواجب التطبيق تكون سابقة لمعرفة جنسية المجرم وليست لاحقة. مما يتعذر معه الأخذ بمبد الشخصية. شأنه في ذلك شان مبدأ العينية الذي يصطدم بمبدأ السيادة خاصة إذا وقعت الجريمة في دولة غير دولة المجني عليه.

ثانيا: اشكالية الاختصاص القضائي.

تثور اشكالية الاختصاص القضائي، لأن الاثار المترتبة عن الجرائم الإلكترونية المرتكبة عبر شبكة الانترنت لها امتداد واسع النطاق تشمل أكثر من نظام قانوني واحد وبذلك يحتمل أن تتنازع تلك الانظمة إيجابيا وسليبا في بسط اختصاصها القضائي للتحقيق في تلك الجرائم ومحاكمة مرتكبيها.

[1] محمد عبد الكريم سلامة، جرائم غسيل الأموال الكترونيا في ظل النظام العالمي الجديد، مؤتمر الاعمال المصرفية الالكترونية بين الشريعة والقانون، المنعقد بجامعة الامارات العربية المتحدة، كلية الشريعة والقانون، 10 الي 12 ماي 2003، المجلد الرابع، ص28.

وإن كانت هناك معايير أو ضوابط علي الصعيد الوطني لكل دولة تحكم مسألة تنازع الاختصاص هذه، غير أن الامر يختلف علي المستوي الدولي لعدم وجود نظرة موحدة أو اتفاقية دولية تحكم تنازع الاختصاص أو تنظمه.

فقد تثور مسائل التنازع الايجابي للاختصاص القضائي في حالة ما اذا تمسكت كل دولة تضررت من الجريمة الإلكترونية المرتكبة عبر الانترنت، كما قد تثور مسألة تنازع الاختصاص السلبي في حالة ما اذا كانت الانظمة القانونية التي تم ارتكاب السلوك الإجرامي أو تحققت النتيجة الإجرامية في ظلها غير مختصة بالتحقيق في الجريمة أو محاكمة مرتكبها، بسبب عدم اعترافها بأن ذلك السلوك يشكل جريمة. وبذلك يفلت المجرم من العقاب رغم أن نفس السلوك الضار الذي أتي به قد يشكل جريمة في ظل انظمة قانونية اخري، وهو الأمر الذي دفع ببعض مجرمي الانترنت علي غرار من يقومون بأنشاء مواقع خلاعية وإباحية عبر شبكات الانترنت الي انشاء تلك المواقع وادراتها في دول لا تجرم او تعاقب علي مثل تلك الافعال.

إن الاختصاص القضائي أو المحكمة المختصة بالبث في الجرائم الإلكترونية، تحكمه ثلاث معايير تتمثل في معيار الاختصاص المكاني، معيار القانون الاكثر ملائمة، ومعيار الضرر المرتقب.

فمعيار الاختصاص المكاني يقوم علي ثلاث ضوابط تتمثل في: مكان ووقوع الجريمة محل إقامة المتهم أو مكان القاء القبض عليه، وفي حالة اجتماع اكثر من ضابط، تكون المحكمة المختصة هي المحكمة التي ترفع اليها الدعوي اولا[1]. غير ان ذلك قد لا يتفق مع حسن سير اعمال الاستدلال والتحقيقات القضائية اذا ما تم استناد الاختصاص علي اساس محكمة مكان القاء القبض علي المتهم أو مكان اقامته. فالضابط الأصلح لحسن سير

[1] غازي عبد الرحمان هينان الرشيد، مرجع سابق، ص 518.

التحقيقات واتخاذ الاجراءات لا سيما اعمال المعاينة والتفتيش والضبط هو ضابط مكان ارتكاب الوقائع ومكان وجود مسرح الجريمة.[1]

ويري أصحاب معيار القانون الاكثر ملائمة أن الاستناد الي المعيار المكاني في اسناد الاختصاص القضائي فيه اجحاف في حق الدول التي تضررت من الجريمة، ذلك ان نسبة الضرر الناتج عن الجرائم الإلكترونية المرتكبة عبر الانترنت قد تتفاوت بين دولة واخري، ومن العدل والانصاف أن ينعقد الاختصاص القضائي للدولة التي تضررت اكثر من الجريمة.[2]

أما معيار الضرر المرتقب فهو يقوم علي أساس أن الضرر الذي قد تسببه الجرائم الإلكترونية المرتكبة عبر شبكة الانترنت، يمكن أن يحدث في أي دولة متصلة بهذه الشبكة.[3]

وقد يقوم المجرم بارتكاب الأفعال المكونة للجريمة الإلكترونية في دولة ما، غير أنه يستهدف ضحاياه في دول اخري، كان يقوم المجرم ببث صور أو افلام ذات طابع اباحي في اقليم دولة ما ويتم الاطلاع عليها في دول اخري، فهما نكون أمام اختصاص قضائي ايجابي متعدد لكل الدول التي تضررت من الجريمة.[4]

[1] عبد الفتاح بيومي حجازي، مبادي الإجراءات الجنائية في جرائم الكومبيوتر والانترنيت، مرجع سابق، ص 52.
[2] فريد منعم جبور، مرجع سابق، ص 207.
[3] غازي عبد الرحمان هينان الرشيد، المرجع السابق، ص 254.
[4] عبد الله عبد الكريم عبد الله، كتاب عن جرائم المعلوماتية والانترنيت (الجرائم الالكترونية)، الطبعة الاولي، منشورات الحلبي الحقوقية، بيروت، 2007، ص 47- 48.

خلاصة الفصل الثاني

يتعلق الإثبات في الجرائم الإلكترونية بالصعوبات التي تواجهها الجهات القانونية في تحصيل الأدلة اللازمة لإثبات ارتكاب جريمة إلكترونية، ويرجع ذلك للطبيعة الرقمية للجرائم الإلكترونية، وقد تنشأ تحديات فريدة تتطلب تقنيات ومهارات متخصصة، كالتعقيد التقني إذ تتطلب جرائم الإنترنت فهما عميقا للتكنولوجيا والشبكات الرقمية، وقد تكون هناك صعوبة في تحديد المكان الفعلي للمتهم أو تتبع أصول الهجمات الإلكترونية.

كما يمكن أن يكون من الصعب جمع الأدلة الرقمية المتاحة في جرائم الإنترن، وقد تحتاج الجهات القانونية إلى الحصول على معلومات من مقدمي خدمات الإنترنت أو الشركات التكنولوجية، والتعامل مع مشاكل التحفظ على البيانات وتأمينها لاستخدامها كأدلة في المحاكم، كما يمكن للجناة في الجرائم الإلكترونية استخدام التقنيات الرقمية لتزييف أو تغيير الأدلة.

ويمكن للجرائم الإلكترونية أن تتجاوز الحدود الوطنية، وهذا يزيد من التعقيدات القانونية والتقنية في جمع الأدلة وتقديمها للمحاكمة، مما يستدعي ضرورة التعاون الإقليمي والدولي والتعاون مع على المستوى التشريعي والإجرائي للوصول إلى المتهمين وجمع الأدلة.

الخاتمة

إن التطور في عالم الاتصال والتكنولوجيا أثرت كثيرا علي مختلف جوانب الحياة الاقتصادية، الاجتماعية، الثقافية والعلمية، فكانت لها أثار ايجابية علي غرار استخدام تلك التكنلوجيا في تحسين الخدمة و تحقيق الرفاهية، تخفيض التكاليف واختزال الوقت، لكنها خلفت كذلك أثار سلبية ناتجة أساسا عن الاستخدام السئ لها.

إن سوء استخدام التكنولوجيا وتسخيرها في ارتكاب الجرائم، بل حتي استحداث جرائم انصبت علي تلك التقنية في حد ذاتها، كان له أثر بالغ علي مختلف المنظومات القانونية، التي تعتبر الايطار القانوني لمعالجة أي ظاهرة اجرامية. فكان لزاما علي تلك الانظمة أن تساير ذلك التطور وتتكيف معه.

لكن ما حدث أن تطور تلك المنظومات القانونية سواءا كانت موضوعية أو اجرائية، لم يكن بنفس سرعة التطور التكنولوجي، وانتشار استخدام التقنية المعلوماتية التي اوجدت عالما افتراضيا تختلف خصائصه ومكوناته عن عالمنا الحقيقي، بل إنها لم تساير الأنماط الاجرامية التقليدية التي صارت تستخدم التقنية المعلوماتية في تنفيذها، كما أنه لم تستطع مسايرة الأنماط الإجرامية الجديدة . واصبحت بذلك عاجزة عن أداء دورها الردعي، في تحقيق الجرائم واثباتها وايقاف مرتكبيها وتقديمهم للمحاكمة وتسليط العقاب عليهم.

وهو ما دفع بالفقه الي محاولة التوسع في تفسير النصوص الجنائية التي تحكم القواعد التقليدية، في محاولة لسد ذلك القصور، من خلال التوسع في مفهوم الشيئ وتعديل

خصائصه وبسطه علي الأشياء غير المرئية وغير الملموسة كالبيانات والحقول، أو النبضات الكهرومغناطسية وغير ذلك من الأشياء غير الملموسة التي تجد لها أساسا في العالم الافتراضي الذي اوجدته التقنية المعلوماتية.

إن المحاولات الفقهية التي قادها العديد من فقهاء القانون الجنائي، كان لها أثرا هاما في إثراء المنظومات القانونية الموضوعية والاجرائية الوطنية بالدول المتقدمة خصوصا بالنصوص القانونية التي تمكن من مواجهة الاجرام المعلوماتي بكافة اشكاله. لكن تلك المحاولات لم تكن كافية بالنظر الي كبر حجم الظاهرة الاجرامية التي أصبحت ظاهرة دولية لارتباطها بالشبكة العنكبوتية، فالأنترنيت أصبحت مجالا خصبا للإجرام المعلوماتي العابر للحدود. وهو اجرام تتطلب مواجهته تكاثف الجهود وتنسيقها علي المستوي الدولي.

ورغم أهمية ألية التعاون الدولي في مواجهة الجرائم المعلوماتية العابرة للحدود، غير أنها لا تزال قاصرة عن أداء الدور المنوط بها، لاصطدامها بعدة معوقات واعتبارات، راجعة اساسا الي ضعف أغلب التشريعات الجنائية الوطنية سواءا الموضوعية أو الاجرائية عن مواكبة ظاهرة الاجرام المعلوماتي، ولعدم تحكم دول تلك التشريعات في التقنية المعلوماتية بحكم أنها مظهر من مظاهر التطور التكنولوجي، وغياب الثقافة المعلوماتية فيها. كما يرجع ذلك الي اعتبارات السيادة التي تحتج بها كل دولة في مواجهة الدول الأخرى ، وما ينتج عنها من تحفظ علي مسائل الاختصاص القضائي و التفتيش و تسليم المجرمين. وغير ذلك من المعوقات التي تحول دون التوصل الي اتفاق دولي يكرس أليات فعالة للتعاون بين

مختلف الأنظمة القانونية علي الصعيدين الموضوعي و الاجرائي لمواجهة تنامي ظاهرة الإجرام المعلوماتي.

ومن ثمة فانه للنهوض بألية التعاون الدولي وجب التفكير بداية، في تذليل العقبات التي تعترض التوصل الي اتفاق دولي لمواجهة ظاهرة الاجرام المعلوماتي، ولعل أولي تلك العقبات واكثرها أهمية هي عدم ادراك اغلبية دول المجتمع الدولي لا سيما تلك المتخلفة لمخاطر الاجرام المعلوماتي وعدم تحكمها في تكنولوجيا المعلومات والاتصالات

ولإزاحة هذه العقبة، تعين القيام بالتوعية بمخاطر هذه الظاهرة الإجرامية علي مستوي كل الدول المتصلة بالشبكة العنكبوتية، ومساعدة تلك الدول لا سيما تلك المتخلفة، في التحكم في تقنيات المعلومات والاتصالات، وسن تشريعات وطنية، موضوعية واجرائية تنظمها، وتجرم انشطة الاعتداء علي المعلوماتية، وتحدد القنوات الاجرائية لمواجهتها. ثم انشاء وسائل وسن اجراءات للتعاون علي المستوي الدولي، تتلائم مع اعتبارات السيادة ومع ما تقتضيه المواجهة من خصائص تتفق مع خصائص الاجرام المعلوماتي علي غرار السرعة، المرونة والنجاعة.

قائمة المراجع

أولا المراجع باللغة العربية

أ- التشريعات والقوانين

1. الدستور الجزائري 2020، الصادر الجريدة الرسمية رقم 82 المؤرخة في 30 ديسمبر 2020.
2. القانون 09 - 04 مؤرّخ 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
3. القانون 04/91 المؤرخ في 08 يناير 1991 المتضمن تنظيم مهنة المحاماة المعدل والمتمم
4. الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات المعدل والمتمم.
5. الأمر 66-155 المؤرخ 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

أ- الكتب والمؤلفات

1. عبابنة محمود احمد، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للتوزيع والنشر، عمان 2009.
2. البعلبكي منير، قاموس المورد إنكليزي-عربي، دار العلم للملايين، بيروت، 1990.
3. الشوا محمد، الغش المعلوماتي كظاهرة إجرامية مستحدثة، بحوث المؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، جمهورية مصر العربية 1993.
4. يوسف أمير فرج، الجرائم المعلوماتية علي شبكة الانترنيت، دار المطبوعات الجامعية، الطبعة الاولي، الاسكندرية، 2008.
5. رستم هشام، قانون العقوبات ومخاطر التقنية، مكتبة الآلات الحديثة، أسيوط، 1992.

6. شتا محمد، الحماية الجنائية لبرامج الحاسوب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2001.
7. الحيسناوي علي جبار، جرائم الحاسوب والانترنيت، دار اليازوري العلمية للنشر والتوزيع، الاسكندرية، 2009.
8. هدي قشقوش، جرائم الحاسوب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، 1999.
9. أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الأولي، دار الفكر العربي، الاسكندرية، 2005.
10. نائلة عادل محمد فريد، جرائم الحاسوب الألي الاقتصادية، الطبعة الاولي، دار النهضة العربية، القاهرة.
11. هشام محمد فريد رستم، الجوانب الاجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، اسيوط، 1994.
12. هشام محمد فريد رستم، قانون العقوبات و مخاطر التقنية المعلومات، مكتبة الآلات الحديثة، مصر، 1992.
13. محمد كمال عواد، الضوابط الشرعية والقانونية للأدلة الجنائية، دار ريم للنشر والتوزيع، مصر، 2011.
14. مأمون سلامة، قانون الاجراءات الجنائية، الطبعة الاولي، دار الفكر، مصر، 1980.
15. حمدي الجاسم، أصول المحاكمات الجزائية ، مطبعة عبد العالي، مصر، 1962 .
16. أبو العلاء علي النمر، دراسة تحليلية، الاثبات الجنائي، دار النهضة العربية، الطبعة الثانية.
17. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبيعة الثالثة، دار النهضة العربية، مصر، 1997.
18. حسين محمود ابراهيم، الوسائل العلمية الحديثة في الإثبات، دار النهضة العربية، 1981.
19. أمال عبد الرحيم عثمان ، شرح قانون الإجراءات الجنائية ، 1989.
20. عمر بن محمد يونس، الجرائم الناشئة عن استخدام الانترنت، الطبعة الاولى، دار النهضة العربية القاهرة، 2004.
21. هلالي عبد الله أحمد، تفتيش نظم الحاسوب الآلي وضمانات المتهم المعلوماتي، ط1، دار النهضة العربية، القاهرة، 1997.
22. أسامة أحمد المناعسة، جرائم الحاسوب الآلي و الأنترنت، دراسة تحليلية مقارنة، الطبعة الأولى، دار وائل للنشر ،عمان، الأردن، 2000.
23. أميل أنطوان ديراني، الخبرة القضائية، المنشورات الحقوقية، طبعة1، بيروت، 1977.

24. همام محمد محمود زهران، الوجيز في إثبات المواد المدنية والتجارية ، الدار الجامعية الجديدة للنشر، مصر، 2003.
25. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006.
26. عبد الفتاح بيومي حجازي، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت، للطباعة و التجليد، مصر، 2009.
27. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجبل للطباعة، الطبعة السادسة عشر، 1985.
28. محمد حماد مرهج الهيتي، جرائم الحاسوب– ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، دراسة تحليلية لواقع الاعتداءات التي يتعرض لها الحاسوب وموقف التشريعات الجنائية منها، الطبعة الاولى، دار المناهج للنشر و التوزيع، عمان، 2006.
29. فريد منعم جبور، حماية المستهلك عبر الإنترنت و مكافحة الجرائم الالكترونية (دراسة مقارنة)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2010.
30. عبد الله عبد الكريم عبد الله، كتاب عن جرائم المعلوماتية والانترنيت (الجرائم الالكترونية)، الطبعة الاولي، منشورات الحلبي الحقوقية، بيروت، 2007.
31. محمد فاروق عبد الحميد كامل، القواعد الفنية الشرطية للتحقيق و البحث الجنائي، ، أكاديمية نايف للعلوم الأمنية، الرياض ، الطبعة الاولي، 1999.

ب– الرسائل الجامعية والمذكرات

1. أحمد ضياء الدين محمد خليل، رسالة دكتوراه مشروعية الدليل في المواد الجنائية، جامعة عين شمس، 1982.
2. غازي عبد الرحمان هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة أعدت لنيل درجة الدكتوراه في القانون، الجامعة الإسلامية في لبنان، كلية الحقوق، 2004.
3. محمد بن نصير محمد السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب والانترنيت، رسالة ماجستير، جامعة نايف العربية، 2004 .
4. سميرة معاشي، مجلة المنتدى القانوني، ماهية الجريمة المعلوماتية، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، 2011.
5. عبد الرحمان محمد بحر، معوقات التحقيق في الجرائم، دراسة مسحية على ضباط الشرطة بدولة البحرين، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 1999.

6. محمد بن عبد الله بن علي المنشاوي، جرائم الانترنت في المجتمع السعودي، رسالة مقدمة إلى كلية الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية تخصص قيادة أمنية، أكاديمية نايف العربية للعلوم الأمنية ، الرياض، 2003.
7. سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظام المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003.
8. حاجب هيام، الجريمة المعلوماتية، مذكرة التخرج لنيل اجازة المدرسة العليا للقضاء، 2008.

ج- المقالات والاوراق البحثية

1. البشرى محمد الأمين، الأدلة الجنائية الرقمية ودورها في الإثبات، المجلة العربية للدراسات الامنية والتدريب ، جامعة نايف العربية للعلوم الامينة، الرياض، عدد 33 ، 2003.
2. هشام محمد فريد رستم، الجرائم المعلوماتية أصول التحقيق الجنائي الفني واقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي، بحوث مؤتمر القانون والكمبيوتر والإنترنت، دولة الإمارات العربية المتحدة، 2000.
3. حسن طاهر داود، جرائم نظم المعلومات، أكاديمية نايف العربية للعلوم الأمنية، الرياض، 2000.
4. خالد ممدوح إبراهيم، الدليل الالكتروني في جرائم المعلوماتية، بحث منشور على الانترنت الرابط http //www.f-law.net .
5. طارق محمد الجملي، الدليل الرقمي في مجال الاثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الاول حول المعلوماتي و القانون المنعقد في الفترة الممتدة من 28 الي 29 اكتوبر 2009، بطرابلس بليبيا، بحث منشور علي الانترنيت علي الرابط http //www.droit-dz.com/forum/showthread.
6. عمر محمد بن يونس، مقال بعنوان الدليل الرقمي، 2006.
7. علي محمود علي حموده، الادلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، بحث القي في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، مركز البحوث والدراسات، رقم العدد1، دبي، الامارات العربية المتحدة، 2003.
8. حسين بن سعيد بن سيف الغفاري، التحقيق و جمع الأدلة في الجرائم المتعلقة بشبكة الانترنت، بحث منشور علي الرابط http //www.minshawi.com.
9. محمد أبو العلاء عقيدة، التحقيق و جمع الأدلة في الجرائم الإلكترونية، ورقة بحث القي في المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، اكادمية شرطة دبي، مركز البحوث والدراسات تاريخ الانعقاد 26 – 28 نيسان 2003، دبي – الامارات العربية المتحدة.

10. البشرى محمد الأمين، التحقيق في جرائم الحاسوب الآلي، بحث مقدم لمؤتمر القانون و الكمبيوتر و الإنترنت، الطبعة الثالثة، كلية الشريعة و القانون، جامعة الإمارات العربية المتحدة، 2004.

11. ايهاب ماهر السنباطي، «الجرائم الالكترونية (الجرائم السيبرية) قضية جديدة أم فئة مختلفة؟ التناغم القانوني هو السبيل الوحيد»، االندوة الاقليمية حول الجرائم المتصلة بالكومبيوتر، المملكة المغربية، جويلية 2007.

12. براء منذر كمال عبد اللطيف، ناظر احمد منديل، « القانون القضائي الدولي في مواجهة جرائم الانترنيت » المؤتمر العلمي لتحولات القانون العام في مطلع الالفية الثالثة، كلية القانون، جامعة تكريت، العراق، 2009.

13. محمد عبد الكريم سلامة، جرائم غسيل الأموال الكترونيا في ظل النظام العالمي الجديد، مؤتمر الاعمال المصرفية الالكترونية بين الشريعة والقانون، المنعقد بجامعة الامارات العربية المتحدة، كلية الشريعة والقانون، المجلد الرابع، 10 الي 12 ماي 2003.

ثانيا المراجع باللغات الاجنبية

1. PARKER، DONN ، Fighting Computer Crime A New Framework For Protecting Information. Hoboken، New Jersey John Wiley And Sons.1998
2. RIEMER ANDREA K، An Inventory Of Preventive Multilateral Activities In The Fields Of Computer-Related Crime And Cyberthreats In Europe .2001 .Http //Www.Isn.Ethz.Ch/Crn/Intorg/ Cyberthreads.Pdf.
3. SIEBER ULRICH، Legal Aspects Of Computer-Related Crime In The Information Society.1998
Http//Europa.Eu.Int/ISPO/Legal/En/Comcrime/Sieber
4. Tom ForesterEssential Proplems To Hig-Tech Society First Mit Pres Edition، Cambridge، Massachusetts.1989.
5. TIEDEMANNFraude Et Autres Delits D'affaires Commis A L'aide D'ordinateurs Electroniques. R.D.P.C. N°7.1984.
6. TOTY AND HARDCASTLE Computer Related Crime In Information Technology And The Law U .K. 1989.

7. GOODMAN Mark، Making Computer Crime Count، Fbi Law Enforcement Bulletin 70 (8)، 10-17.2001.
Http//Www.Fbi.Gov/Publications/Leb/2001/Aug011eb .
8. SAGROS "PIERRE" ET MASSE "MICHEL Le Droit Penal Et L'informatique Journnée D'étude Du 15 Novombre Publication A L'institue De Science Criminelle De Le Faculte IV. 1982.
9. GAUTAL (JEAN – LOUIS) ، La Protection Pénale Des Logiciel " Le Droit Criminel Face Aux Technologie Nouvelles De La Communication" .
10. JEAN P، SPREUTELS Les Crimes Informatiques Et D'autres Crimes Dans Les Domaines De La Technologie Informatique En Belgique – Rev – Inter De- Dr Pen.1992.
11. WASIK (MARTIN) ، Computer Crimes And Other Crimes Against Information Technology In The United Kingdom- Rev، Inter، De، Dr، Panal.1993.
12. MOHRENSCHLAGER ،Http //Www.Nauss.Edu.Sa
13. KASPERSEN(W.K.HENRIK) ،Computer Crime And Other Crime Against Information Technology In Netherland،R.I.D.P.1993.
14. ROBERT TAYLOR. Computer. «Un Criminal Investigation Edited » By Charles Swanson Chamelin And Territto Hill . Inc .5 Edtion 1992 .
15. VOIRCHEF MEUMIER (2000)(C) La Loi De28 Novembre 2000 Relative A La Criminalité Information Rev –Art ، Pem . Crim 2002.
16. FRANCILLON (JACQUES) rimes Et D'autres Crimes Dans Le Domaine De La Technologie Informatique En France – Rev.Inter. De. Dr. P En 1993.
17. United Nation Manual On The Prevention And Control Of Computer، Related Crime، Vienna 1999.
18. Www.Startimes.Com/F.Aspx.

فهرس المحتويات

الفهرس

مـلخص مذكرة الـماستر

إن الجرائم الالكترونية حالها حال جرائم اخرى في التعدي على حقوق الاخرين لاسيما في ظل التطور التكنولوجي في كل المجالات، الا ان للجرائم الإلكترونية ميزة الاخرى كونها جرائم غير ملموسة لكن اثارها كبيرة لهذا فان الإلمام بسلوك الجاني والتعامل مع الجريمة تعد تحديا امام السلطات التحقيقية ولاسيما الإثبات، ومن هنا يتجلى دور سلطات التحقيق في كشف ملابسات ومعالم الجريمة، وذلك ما يتطلب وجود خبراء وفنيين في مجال الكشف السريع عنها حيث يتعمد مرتكبها الى اخفاء اثارها في وقت قصير قبل إكتشافها، ويمتلك القاضي بشكل عام سلطة تقديرية واسعة في تقدير الادلة الرقمية المتحصلة من مسرح الجريمة ومن الاوراق التحقيقية عند تحقيق فيها وقبل احالتها الى محكمة المختصة والوقوف على قيمة الدليل مع توافر ادلة الداعمة الى اصدار الحكم فيها.

الكلمات المفتاحية:

التحقيق، الجرائم الإلكترونية، الأدلة الإلكترونية، الإثبات، إعتراض المراسلات، التفتيش والخبرة.

Abstract of Master's Thesis

Electronic crimes are the same as other crimes in violating the rights of others, especially in light of the technological development in all fields, but electronic crimes have the advantage of being intangible crimes, but their effects are great. Therefore, knowing the behavior of the offender and dealing with the crime is a challenge for the investigative authorities, especially evidence. Hence, the role of the investigation authorities is evident in revealing the circumstances and features of the crime, which requires the presence of experts and technicians in the field of rapid detection, as the perpetrator intends to hide its traces in a short time before they are discovered, and the judge generally has wide discretion in assessing the digital evidence obtained from the crime scene. And among the investigative papers when investigating them and before referring them to the competent court and standing on the value of the evidence with the availability of supporting evidence to issue a judgment in it

Keywords:

Investigation, electronic crimes, electronic evidence, evidence, interception of correspondence, inspection and expertise.