وزارة التعليم العالي والبحث العلمي
Ministry of High Education and Scientific Research
جامعة محمد البشير الابراهيمي برج بوعريريج
University of Mohamed el Bachir el Ibrahimi-Bba
كلية الحقوق والعلوم السياسية
Faculty of Law and Political Sciences

مذكرة مقدمة لاستكمال متطلبات نيل شهادة الماستر أكاديمي في الحقوق

تخصص: إعلام آلي

الموسومة بـ:

إثبات الجريمة الإلكترونية

إعداد الطالب:
– سماتي مداني

إشراف: الدكتور
د. بن النوي خالد

لجنة المناقشة:

الاسم واللقب	الرتبة	الصفة
رفاف لخضر	أستاذ محاضر – أ–	رئيسا
بن النوي خالد	أستاذ محاضر – أ–	مشرفا ومقررا
بوقرة عيسى	أستاذ محاضر – ب–	ممتحنا

السنة الجامعية: 2025/2024


بسم الله الرحمن الرحيم
MRTsoft

شكر وعرفان

بسم الله الرحمان الرحيم

﴿ رَبِّ أَوْزِعْنِي أَنْ أَشْكُرَ نِعْمَتَكَ الَّتِي أَنْعَمْتَ عَلَيَّ وَعَلَى وَالِدَيَّ وَأَنْ أَعْمَلَ صَالِحًا تَرْضَاهُ وَأَدْخِلْنِي بِرَحْمَتِكَ فِي عِبَادِكَ الصَّالِحِينَ﴾

سورة النمل الآية 19

الشكر لله عزوجل على نعمه

أتقدم بالشكر الجزيل إلى أستاذي الفاضل: "بن النوي خالد" على نصائحه وتوجيهاته التي أنارت دربي والتي لم يبخل علي بمعلوماته القيمة.

كما أتوجه بالشكر إلى كل الزملاء والأصدقاء وكل الشكر إلى كل من ساهم في انجاز عملي هذا سواءًا بمعلومة أو نصيحة أو كلمة طيبة

إهداء

بسم الله الرحمان الرحيم

أهدي هذا العمل المتواضع إلى كل من قال الحق تعال فيهما:

(وَقُلْ رَبِّي ارْحَمْهُمَا كَمَا رَبَّيَانِي صَغِيرًا)

أمي وأبي الغاليين

أهدي إلى كل من كان له الفضل في مسيرتي هاته ولم يدخر جهدا في مساعدتي.

إلى كل من دعمني وشجعني في حياتي وأعطاني دفعة نحو الامام

سماتي مداني

مقدّمة

مقدمة

قدم الحاسب الآلي والانترنت للبشرية الرقي في جميع مناحي الحياة، إلا أن هذا التقدم المذهل واكبه من جهة اخرى تطور الفكر والعقل البشري الإجرامي، مما أدى إلى إفراز أنواعا جديدة من السلوك الإجرامي تمثلت في ظهور الجريمة المعلوماتية او الإلكترونية، التي أدت إلى حدوث خسائر فادحة غير مسبقة لمستخدمي هذه الحواسيب ولصناع برمجياتها، وكذا الإعتداء على مصالح الأشخاص سواء كانت طبيعية أو إعتبارية .

وعمدت عدة دول في سبيل مواجهة الجرائم الإلكترونية إلى وضع سياسات جنائية تتنوع بين الوقاية والمواجهة من خلال سن مجموعة من القوانين من اجل وضع حد للإنقلابات في مجال الجرائم المعلوماتية، هذه الاخيرة احدثت انقلابا هاما في النظريات التقليدية بما فيها نظرية الإثبات الجنائي، من منطلق أن أهم خاصية تتميز الجريمة الالكترونية هي صعوبة إثباتها بإتفاق الفقهاء والدارسين في مجال المعلوماتية، وما نعكس سلبا على العملية الاثباتية للجرائم المعلوماتية هو عدم تناسب النصوص المنظمة لطرق الاثبات التقليدية مع طبيعة الجريمة المعلوماتية وتطورها، بسبب سرعة اخفائها وطمس معالمها في زمن قياسي ومن أي مكان في العالم، ما استلزم على المشرعيين تبني انواع جديدة من الادلة تسمى بالأدلة الرقمية مع حرصهم على توفير الغطاء التشريعي لها .

ونظرا إلى أن الجريمة الإلكترونية من الموضوعات التي تتميز بندرة التطبيقات القضائية فيها، فإنه برز للوجود مسألة حجية الدليل الرقمي الذي يعد آلية إثبات في مجال جرائم المعلوماتية، فالقواعد العامة أصبحت قاصرة عن مواجهة خصوصية هذه الجرائم، خاصة بعد أن أصبح المجتمع المعلوماتي حقيقة لا يمكن الإستغناء عنها، وأصبحت المجتمعات المعاصرة تعتمد على البيئة الرقمية وازداد التوجه نحو التخلي عن الوثيقة في

المعاملات المختلفة بما فيها عملية الإثبات، مما أدى إلى إستحداث أشكال جديدة من الأدلة في الإثبات الجنائي، إستوجب توفرها على شروط معينة لإعتبارها دليلا كاملا يمكن من خلالها دحض قرينة البراءة وإثبات عكسها عندما يصل إقتناع القاضي إلى حد الجزم واليقين.

الإشكالية :

من خلال ما سبق ونظرا لاهمية الموضوع وتشعبه وحداثته، فإن محاولة دراسته تتطلب الخوض في الإشكالية الآتية :

- هل يخضع إثبات الجريمة الإلكترونية بصفتها جريمة مستحدثة لنفس معايير التي يخضع لها اثبات الجريمة التقليدية أم هناك إختلاف يميز بينهما ؟

والإجابة على هذه الإشكالية تستلزم طرح بعض التساؤلات الفرعية والتي نوردها على النحو التالي :

1- ما المقصود بالجريمة الإلكترونية والدليل الرقمي ؟
2- ماهي طرق إثبات الجريمة الإلكترونية ؟
3- هل يعتبر الدليل الرقمي دليلا كاملا للإثبات الجنائي ؟

أهمية الموضوع :

تكمن أهمية هذه الدراسة في التعرف على الجريمة الإلكترونية لا سيما من حيث ضبطها واثباتها، لأنه لا يختلف إثنان في أن أساس توقيع العقوبة على المتهم يكمن في إثبات إدانته وذلك بإقامة الأدلة عليه، لذا فإن الإثبات يعتبر موضوعا في غاية الأهمية، علما ان اهمية التحقيق الجنائي تتجلى في تحديد إجراءات التحقيق في الجرائم الإلكترونية، بالإضافة إلى التعريف بالبرامج والأنظمة الخاصة التي تساعد في إثبات مثل

هذه الجرائم، والتي ينبغي على رجال الضبطية القضائية من جهة والقضاء من جهة اخرى معرفتها لإثبات وقوع هذه الجرائم .

كما ان الإثبات الجنائي بالدليل الالكتروني له أهمية بالغة تتضح من خلال صلته بطائفة جديدة من الجرائم اصطلح عليها تسمية الجرائم الالكترونية، هذه الأخيرة إنتشرت في الوقت الحالي بشكل يستدعي التوقف عندها، بإعتبار انها من المواضيع التي أثارت العديد من المشاكل في نطاق الإثبات الجنائي، وهذا ما ستوجب الإعتماد على الدليل الإلكتروني أو الرقمي نظرا لتلاؤمه مع طبيعة هذه الجرائم التي تحتاج لأدلة ذات طبيعة فنية وعلمية .

أهداف الدراسة :

إزاء ما تقدم ذكره، ورغبة في تسليط الضوء على هذه الجريمة، فإن الغرض من هذه الدراسة هو معرفة مدى مواكبة القانون للتطور التكنولوجي، وكيفية تعامله مع الادلة الرقمية وكذا الكشف عن مدى حجية الدليل الالكتروني في مجال الإثبات الجنائي .

أسباب إختيار الموضوع :

تتمثل أسباب إختيار الموضوع في ما يلي :

أسباب ذاتية :

نظرا لما أحدثته الجريمة الالكترونية من ضجة كبيرة في العالم، وما للموضوع من أهمية بالغة، اخترنا الخوض في هذا الموضوع أملا منا أن نثري المكتبة القانونية بعمل ولو بسيط .

أسباب موضوعية :

نظرا لتفشي ظاهرة الاجرام الالكتروني بشكل سريع، وتطور الوسائل المستخدمة في ارتكاب الجريمة الالكترونية، مما أدى إلى خلق عدة صعوبات في إثبات هذا النوع من الجرائم، كان لزاما أن نتطرق إلى طرق إثبات هذه الجريمة المستحدثة ومعرفة قيمة الدليل الذي تثبت به أمام القضاء .

المنهج المتبع :

إعتمدنا في دراستنا على المنهج الوصفي من حيث معرفة مواصفات الدليل الإلكتروني والتي جعلته يتميز عن باقي الأدلة، إلى جانب استخدام المنهج التحليلي وهذا بغرض تحليل الموضوع من الناحية القانونية الإجرائية .

صعوبات الدراسة :

لحسن حضنا ونحن بصدد هذه الدراسة لم نواجه صعوبات كبيرة، وهذا راجع لوفرة المراجع في مجال الجريمة الالكترونية بصفة عامة واثباتها بصفة خاصة، ماعدا في التشريع الجزائري، حيث أنه لم يولي اهتمام كبيرا لموضوع إثبات الجريمة الالكترونية بالطرق الحديثة أو ما ما يسمى بالدليل الالكتروني، حيث لم نجد نصوص قانونية صريحة تعني بالدليل الرقمي في هذا الموضوع .

الدراسات السابقة :

معظم الدراسات السابقة التي إطلعنا على محتواها ونحن بصدد إنجاز مذكرتنا هذه، جاءت بمعظم الافكار التي يجب التطرق إليها في هذا الموضوع .

إلا أننا وفي دراستنا هذه تناولنا موقف المشرع الجزائري من الجريمة الإلكترونية، وكذا حجية الدليل الرقمي أمام القضاء الجزائي الجزائري .

ولمعالجة الإشكالية المطروحة والإجابة على التساؤلات الفرعية التابعة لها، قسمنا موضوعنا إلى فصلين إثنين هما :

- الفصل الأول : الإطار المفاهيمي للجريمة الإلكترونية .
- الفصل الثاني : طرق ووسائل إثبات الجريمة الإلكترونية

الفصل الأول

الإطار المفاهيمي للجريمة الإلكترونية

المبحث الاول: مفهوم الجريمة الإلكترونية المبحث الثاني: صور الجريمة الإلكترونية

الفصل الأول : الإطار المفاهيمي للجريمة الإلكتروني

لقد تطور العالم في الآونة الأخيرة في مجال التقنية مما نتج عنه استعمال الحاسب الآلي وشبكة الانترنت في جميع الميادين، لكن قد يتم إستخدام هذه الوسائل بطرق غير مشروعة الأمر الذي قد ينجر عنه ارت[1]كاب جرائم لها علاقة بهذا المجال وهو ما يعرف بالجريمة الإلكترونية ونظرا لحداثة هذه الجريمة، فقد إختلف الفقهاء في وضع تعريف موحد لها، كما إتسمت بمجموعة من الخصائص، كما لها أركان وأنواع وسأحاول التطرق في هذا الفصل إلى مفهوم الجريمة الإلكترونية و خصائصها أما في المبحث الثاني سنتطرق إلى صور الجريمة الإلكترونية .

[1] – حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، رسالة شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة، 2012/2011، ص13,

المبحث الأول: مفهوم الجريمة الإلكترونية:

لقد إخترع الحاسب الألي الأفاق امام الفكر الإنساني وأدى إلى إحداث الثورة التي يعيشها العالم اليوم .

إن المعلوماتية أو ما يسمى أيضا بعلم المعلومات، هو ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بأصل المعلومات وتجميعها وتنظيمها وتخزينها وإسترجاعها وتغيرها وكذا تحويلها وإستخدامها، كما يهتم هذا العلم بدراسة اساليب معالجة المعلومات كالأنظمة المعلوماتية ونظم المبرمجة، وبهذا المفهوم تعتبر المعلوماتية علما متصلا بالعديد من العلوم الأخرى .

من خلال هذا المبحث سأحاول التعرض إلى التعاريف المختلفة للجريمة الإلكترونية وكذا الأركان التي ترتكز عليها وخصائصها وذلك من خلال المطلبين المواليين:

المطلب الأول: تعريف الجريمة الإلكترونية:

لقد اختلف الفقهاء حول وضع تعريف موحد للجريمة الإلكترونية ويعود ذلك للإختلاف حول تحدي نطاق هذه الجريمة، فالبعض من الفقهاء ينظر إليها بمفهوم ضيق والبعض الآخر ينظر إليها بمفهوم موسع .

الفرع الأول: الإتجاه المضيق من تعريف الجريمة الإلكترونية:

يعرف أنصار هذا الإتجاه الجريمة الإلكترونية بأنها كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازم لإرتكابه من ناحية، لملاحقته وتدقيقه من ناحية أخرى[1].

حسب هذا التعريف يجب أن تتوافر معرفة كبيرة بتقنيات الحاسوب ليس فقط لإرتكاب الجريمة بل كذلك لملاحقتها والتحقيق فيها، وهذا التعريف يضيق بدرجة كبيرة من

[1]- حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي مرجع سابق، ص 22 .

الجريمة الإلكترونية، بمعنى يجب أن تتوافر قدر كبير من العلم بهذه التكنولوجيا لدى الجناة، والمختصين بملاحقتها من قضاة وضباط الشرطة وغيرهم، وهناك من يعرفها على أنها "الفعل غير المشروع الذي يتورط في ارتكابه الحاسب، أو هي الفعل الإجرامي الذي يستخدم في إقترافه الحاسوب باعتباره أداة رئيسية". كما يرى الأستاذ tredmann أن الجريمة المعلوماتية تشمل أي جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات[1].

ويرى الأستاذ rosenblatt بأن الجريمة الإلكترونية هي "نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه"[2].

حسب هذا التعريف فإن الأفعال غير المشروعة التي يستخدم فيها الحاسب الآلي كأداة لارتكابها تخرج من نطاق التجريم. ويرى الأستاذ "باركار" أن الجريمة الإلكترونية هي كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل[3].

الفرع الثاني: الإتجاه الموسع من تعريف الجريمة الإلكترونية:

على عكس الاتجاه السابق، يرى فريق آخر من الفقهاء ضرورة التوسيع من مفهوم هذه الجريمة، وبالتالي هي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك باستخدام شبكات الانترنت من خلال غرف الدردشة، واختراق البريد الإلكتروني ومختلف وسائل التواصل الاجتماعية، بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد وحتى لدولة من الدول تكون ضمن برنامج الاستهداف الحربي أو الإقتصادي أو الإضرار

---

[1]- حمزة بن عقون، الرسالة السابقة الذكر، ص14، نقلا ة عن أحمد هلالي عبد الله، ص13.

[2]- حمزة بن عقون، نفس الرسالة، ص14، نقلا عن يونس عرب، دليل أمن المعلومات والخصوصية، ص 213.

[3]- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن، 2004، الطبعة 1، ص8.

بسمعتها أو العكس ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب[1].

وفي تقرير الجرائم المتعلقة بالحاسوب أقر المجلس الأوروبي بقيام المخالفة (الجريمة) في كل حالة يتم فيها تغيير معطيات أو بيانات أو برامج أو محوها أو كتابتها، أو أي تدخل آخر في مجال إنجاز البيانات أو معالجتها وتبعا لذلك تسببت في ضرر إقتصادي، أو فقد حيازة ملكية شخص أو بقصد الحصول على كسب إقتصادي غير مشروع له أو لشخص آخر[2].

ودائما حسب أنصار هذا الإتجاه يرى البعض أن الجريمة الإلكترونية هي كل فعل ضار يستخدم الفاعل الذي يفترض أن لديه معرفة بتقنية الحاسوب نظاما حاسوبيا أو شبكة حاسوبية للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة[3].

أما البعض من الفقهاء يعرفوها بأنها كل نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسوب الآلي الرقمي وشبكة الانترنت) بطريقة مباشرة أو غير مباشرة، كوسيلة لتنفيذ الفعل الإجرامي المستهدف[4].

1- سميرة بيطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث، مقال منشور على الموقع:www.alukah.net https:/

2- مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، مجلة علمية، ص09. نقلا عن الطاهر روابنية، المسائلة، مقال، العدد 01، 1991، ص15.

3- كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب، 23/21 تشرين الأول، 2000، بدون صفحة.

4- صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013/3/6، ص 09.

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وعرفها بموجب أحكام المادة 02 من القانون رقم 09-09[1] على أنها:

"جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية."

وحسب المشرع الجزائري فإنه قد تحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الإتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الإتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية[2].

المطلب الثاني: خصائص الجريمة الإلكترونية وأركانها :

لما كانت الجريمة الإلكترونية هي نتاج التطور العلمي والتكنولوجي، وبالتالي فهي تختلف عن الجريمة التقليدية التي ترتكب في الواقع المادي الملموس، لذا نجد لها مجموعة من الخصائص، أو السمات تجعلها منفردة عن غيرها من الجرائم سواء من حيث الجريمة ذاتها، أو من حيث مرتكب الجريمة، وهذا ما يتم بيانه من خلال ما يلي:

---

[1]- القانون رقم 09-04 الصادر في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، العدد47.

[2]- سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، 2010-2011، ص16،15،14.

الفرع الأول : خصائص الجريمة الإكترونية

لمعرفة خصائص الجريمة الإلكترونية يجب التطرق إلى ما يلي :

أولا : السمات الخاصة بالجريمة الإلكترونية:

نظرا للطبيعة المميزة للجريمة الإلكترونية بإعتبارها تمس المعلومات هذا ما جعلها تتميز عن نظيرتها التقليدية بمجموعة من الخصائص أو السمات، إذ أن التعرف أكثر على خصائص هذه الجريمة يساعد في إيجاد الحلول لمكافحتها، وتتلخص هذه السمات فيما يلي:

– خفاء الجريمة وسرعة التطور في إرتكابها، حيث تتسم بأنها خفية ومستترة في أغلبها لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على شبكة الإتصالات، لأن الجانب يتضح بقدرات فنية تمكنه من إرتكاب جريمة بدقة، مثلا عند إرسال فيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وسرقة المكالمات وغيرها من الجرائم[1]، وقد تتم في ثانية أو جزء من الثانية في بعض الجرائم.

– ترتكب في بيئة رقمية معلوماتية قوامها النظم المعلوماتية الحاسوبية، وأجهزة ومعدات وتجهيزات الحاسب الآلي، بمعنى تتم بواسطة المكونات المادية للحاسوب ومكوناته البرمجيات.

– يقوم بها مجرم ذو طبيعة خاصة وإمكانات خاصة (علمية معلوماتية)، يستخدم في إرتكاب جريمته الموارد المعرفية والأساليب الإحترافية.

---

[1]– صغير يوسف، المرجع السابق، ص14،15.

– صعوبة الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على الدليل المتوفر[1].

ولعل صعوبة كشف الدليل تزداد بصورة خاصة متى ارتكبت هذه الجريمة في مجال العمل من قبل العاملين ضد المؤسسات التابعين لها، فبحكم الثقة في هؤلاء يسهل عليهم اقتراف جرائمهم دون أن يتركوا آثار تدل عليهم[2].

– الجريمة الإلكترونية تستلزم طرفا خاصة مستحدثة لإثبات قوامها التعليم والتدريب المتخصص المستمر لعلوم الحاسب الآلي، لذا فإنها تقتضي وجود رجل شرطة إلكتروني ومحقق إلكتروني، وقاضي إلكتروني، فضلا عن الخبير الإلكتروني حتى يتم كشف الجريمة وتعقب الجناة فيها ومحاكمتهم، وعليه فإن الإستعانة بالخبراء تصبح حتمية لكشف وتحليل وتفسير الدليل الجنائي، الذي يثبت البراءة أو الإدانة.

– هذه الجريمة لا يحدها مكان، فهي عالمية إذ يمكن عن طريق الحاسب الآلي أو حتى هاتف نقال لشخص في الصين مثلا أن يرتكب جريمة تزوير أو سرقة معلومات أو نقود ضد شخص طبيعي أو معنوي في الو.م.أ، والعكس.

– تدني نسبة الإبلاغ عن الجريمة من طرف المجني عليه خاصة في حالة شركات أو مؤسسات لتجنب الإساءة للسمعة والرغبة في عدم زعزعة ثقة العملاء، ففي إحدى الوقائع تعرض أحد البنوك وهو بنك في بريطانيا لسرقة ثمانية مليون جنيه إسترليني من إحدى أرصدته إلى رقم في سويسرا، وتم ضبط الفاعل متلبسا يسحب المبلغ المسروق وبدلا من محاكمته، قام البنك بدفع مليون جنيه له، بشرط التزام الفاعل بعدم الإعلام عن

---

[1]– عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحية القانونية والفنية (دراسة مقارنة)، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطلب الشرعي، الرياض، 2007، ص10.

[2]– موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقاذ ون الذي تنظمه أكاديمية الدراسات العليا، طرابلس، 2009، ص03.

جريمته، وإعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي.

– غالبا ما تكون الخسائر الناجمة عنها فادحة للمجني عليه[1].

– ذاتية الجريمة الإلكترونية تبرز بوضوح في أسلوب إرتكابها وطريقتها، فإن كانت الجريمة التقليدية تتطلب نوعا من الأسلوب العضلي الذي قد يكون في صورة الخلع أو الكسر، وتقليد المفاتيح كما هو الحال في جريمة السرقة وتحتاج كذلك إلى وجود شبكة المعلومات الدولية الانترنيت مع وجود مجرم يوظف خبراته وقدراته على التعامل مع الشبكة، للقيام بجرائم مختلفة كما يتجسس أو إختراق خصوصيات الغير أو التغرير بالقاصرين، كل ذلك دون الحاجة لسفك الدماء.

– الجريمة الإلكترونية تتم عادة بتعاون أكثر من شخص على ارتكابها إضرارا بالمجني عليه، وغالبا ما يشترك في إخراج الجريمة إلى حيز الوجود شخص متخصص في تقنيات الحاسوب والأنترنيت يقوم بالجانب الفني من المشروع الإجرامي، وشخص آخر من محيط أو من خارج المؤسسة المجني عليها، لتغطية عملية التلاعب وتحويل المكاسب[2].

ثانيا: السمات الخاصة بالمجرم الإلكتروني:

– المعرفة والمهارة والذكاء: بمعنى التعرف على كافة الظروف التي تحيط بالجريمة وتنفيذها وإمكانية نجاحها، وإحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائمهم بالتعرف على كافة الظروف المحيطة بهم، لتجنب الأمور غير المتوقعة التي من شأنها ضبط أفعالهم والكشف عنهم. كما أن المجرم الإلكتروني يستطيع أن يكون تصورا كاملا

1– عبد الناصر محمد محمود فرغلي، محمد عبيد سعيد المسماري، المرجع السابق، ص10–11.

2– سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2013–2014، ص18.

لجريمته، بالإضافة إلى أنه يتمتع بقدر لا يستهان به من المهارة في مجال تقنية الحاسوب والأنترنيت، فتنفيذ جريمة يتطلب قدرا من المهارة لدى الجانب التي قد يكتسبها عن طريق الخبرة في مجال تكنولوجيا المعلومات. الجريمة الإلكترونية يسعى إلى معرفة طرق جديدة ومبتكرة لا يعرفها أحد سواه، من أجل إختراق الحواجز الأمنية في البيئة الإلكترونية ثم نيل مبتغاه[1].

– المجرم الإلكتروني يبرر ارتكاب جريمته، إذ يوجد شعور لدى كل مرتكب فعل إجرامي أن ما يقوم به لا يدخل في قائمة الجرائم، خاصة في الحالات التي يقف فيها السلوك عند قهر نظام الحاسوب وتخطي الحماية المفروضة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الذي يعدونه غاية في اللأخلاقية، وبين الإضرار بمؤسسة أو جهة في إستطاعتها اقتصادية تحمل نتائج تلاعبهم. ويبدو أن الإستخدام المتزايد لأنظمة المعلوماتية قد أنشأ مناخا نفسيا ملائما لتصور استبعاد فكرة الخير والشر قد ساعد على عدم وجود احتكاك مباشر بالأشخاص، هذا التباعد في العلاقة الثنائية بين الفاعل والمجني عليه يسهل المرور إلى الفعل غير المشروع، ويساعد على إيجاد نوع من الإقرار الشرعي الذاتي بمشروعية هذا الفعل.

– المجرم الإلكتروني يتصف بالخوف من كشف جريمته، وبالرغم من أن هذه الخشية تصاحب المجرم على اختلاف أنماطه، إلا أنها تميز المجرم الإلكتروني بصفة خاصة، لما يترتب على كشف أمره من ارتباك مالي وفقد المركز الوظيفي في كثير من الأحيان، كما أن طبيعة الأنظمة المعلوماتية نفسها تساعد الجانب على الحفاظ على سرية أفعاله، ذلك أن كثير ما يعرض المجرم إلى إكتشاف أمره، هو أن يطرأ أثناء تنفيذ جريمته عوامل غير متوقعة.

1– سمية مزغيش، المرجع السابق، ص20.

- المجرم الإلكتروني يميل إلى التقليد، حيث يبلغ هذه الأخير أقصاه حينما يوجد الفرد وسط جماعة، إذ يكون عندئذ أسهل وأسرع انسياقا لتأثير الغير عليه، ويظهر ذلك من خلال محاولة الفرد تقليد غيره بالمهارات الفنية، مما يؤدي به الأمر إلى ارتكاب الجريمة، وذلك لعدم الإستواء في شخصية الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة التفاعل مع الوسط، المحيط، وينتهي به الأمر إلى التقليد وارتكاب الجريمة[1].

- القيام بالتخطيط والتنظيم، ففي عالم الشبكات الإلكترونية، كما هو الحال في العالم الحقيقي، يقوم بمعظم الأعمال الإجرامية أفراد أو مجموعات صغيرة حيث ترتكب أغلب الجرائم من مجموعة متكونة من عدة أشخاص يحدد لكل شخص دور معين، ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فغالبا ما يكون متخصصا فيها متخصص في الحاسب الآلي يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط أو من خارج المؤسسة المجني عليها لتغطية التلاعب ولتحويل المكاسب إليه.

- التكيف الإجتماعي، فالمجرم الإلكتروني يقوم بواجباته ويمارس حقوقه الإجتماعية والسياسية دون أي عاتق في حياته اليومية[2]، إذ تعتبر هذه الخاصية إمتداد لسمة التخطيط والتنظيم، حيث أن التكيف الإجتماعي ينشأ بين مجموعة لها صفات مشتركة، فمثلا جماعة صغار نوابع المعلوماتية أن يتكيفون في أفكارهم فيما بينهم، وتنشأ بالتالي بينهم روابط تساعدهم على ارتكاب جرائمهم، وتتعدى تلك الروابط النطاق المحلي بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في إستثمار تلك المعرفة والتقدم العلمي، وإقامة المؤتمرات الدولية بين هذه المجموعات خير دليل على تلك الصلات

1- سمية مرغيش، المرجع السابق ، ص20-21.

2- مليكة عطوي، المرجع السابق، ص12.

والروابط الدولية بينهما. بالإضافة إلى أن المجرم الإلكتروني هو عادة إنسان إجتماعي[1] بطبعه حيث يحي وسط المجتمع، ويمارس عمله في المجال المعلوماتي أو غيره من المجالات، وبناء عليه فإن كثير من الجرائم ترتكب بدافع الكبرياء (موظف طرد من عمله)، أو بدافع النصب أو الحسد أو اللهو وإظهار قدراته[2].

– التطور في السلوك الإجرامي، حيث يساهم وجود المجرم الإلكتروني في جماعة إجرامية إلى سرعة اكتسابه المهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة، وبناءا على ما تقدم يمكن تقسيم المجرم الإلكتروني إلى عدة طوائف مختلفة:

المخترقون أو المتطفلون: يتحد في هذا الإطار نوعين من المجرمين:

– الهاكرز: هو الشخص الذي يقوم بإنشاء أو تعديل البرمجيات والعتاد الحاسوبي، ويقصد بهم الشباب البالغ المقترن بالمعلوماتية والحاسبات الآلية والباعث الأساسي لدى الهاكرز هو الإستمتاع باللعب والمزاح باستخدام هذه التقنية لإثبات قدراتهم، بإكتشاف مواطن الضعف في الأنظمة ا لمعلوماتية دون إلحاق ضرر بها، لديهم الرغبة في المغامرة والتحري والإستكشاف[3]. الهاكرز ذو القبعة البيضاء (الهاكرز الأخلاقي).

والهاكر ذو القبعة السوداء هو الهاكر المفسد وأخير هناك الهاكر ذو القبعة الرمادية وهو بين الإصلاح والعبث[4].

–الكراكز: وهو المقتحم، وهذه الطائفة هي طائفة المجرمين البالغين أو المخربين المهنيين وأعمارهم تتراوح بين 25–45 عاما. ومن أبرز سمات هذه الطائفة أنهم ذوي

---

[1]– سمية مزغيش، المرجع السابق ، ص 22

[2]– محمد علي العربان، الجزائر المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص 62.

[3]– سمية مزغيش، المرجع السابق ، ص23.

[4]– موقع ويكيبيديا، الموسوعة الحرة، التاريخ 2022/05/14، 13:48. http//ar .wkiped.org/wiki/

مكانة في المجتمع، ويتمتعون بمهارات فنية في مجال الأنظمة الإلكترونية، تمكنهم من الهيمنة الكاملة في بيئة المعالجة الآلية للمعلومات[1].

- مجرموا الحاسب الآلي المحترفون: هذا النوع من المجرمين يعرف كيف يصل إلى أهدافه بإستخدام ما لديه من علم يطورونه بإستمرار، وهدفهم المصاريف وسحب الأموال من الأرصدة ونيتهم إحداث التخريب[2]، تتميز هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية.

- الحاقدون: هذه الطائفة يحرك أنشطتهم الرغبة في الإنتقام من صاحب العمل أو متصرف المنشأة المعينة معهم عندما لا يكونوا موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوصفهم موظفين أو مشتركين بالنظام محل الجريمة، حيث يستخدمون تقنيات الفيروسات والبرامج وتعطيل النظام أو الموقع المستهدف إن كان من مواقع الأنترنيت، وهم الطائفة الأسهل من حيث كشف أنشطتهم لتوفر ظروف وعوامل تساعد على ذلك[3].

- **صغار السن:** يسمون بصغار توابغ المعلوماتية، وهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآلية، ومن بينهم فئة لم تزل دون سن الأهلية مولعين بالحوسبة والإتصال، وقد تعددت أوصافهم في الدراسات الإستطلاعية، وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بالمتعثلمين، ويثير مجرموا الحوسبة من هذه الطائفة جدلا واسعا، ففي الوقت الذي كثر الحديث فيه عن مخاطر هذه الفئة، ظهرت مؤلفات ودراسات تخرج هذه الفئة من دائرة الإجرام إلى دائرة العبث وأحيانا البطولة من هذه المؤلفات[4].

---

[1]– سمية مزغيش، المرجع السابق ، ص22-23.

[2]– مليكة عطوي، المرجع السابق، ص 13.

[3]– سمية مزغيش، المرجع السابق ، ص 23-24.

[4]– المرجع نفسه، ص24-25.

- **مجرمون ذوي دوافع سياسية:** وهم أشخاص لهم ميول ودوافع سياسية معينة، تدفعهم لإختراق نظم الحاسب الآلي غير مصرح بالدخول إليها، والتي تحتوي على معلومات وبيانات غاية في السرية تتعلق بالدفاع والأمن، ويمثل المساس بها مخاطر كارثية[1].

والمجرم الإلكتروني هو إجرام الذكاء دونما الحاجة إلى إستخدام القوة والعنف وهذا الذكاء هو مفتاح المجرم الإلكتروني، لإكتشاف الثغرات وإختراق البرامج المحصنة. ويمكن إجمال القواسم المشتركة بين هؤلاء المجرمين في عدة صفات وهي:

- عادة ما تتراوح أعمارهم ما بين 18 و45 عاما.
- المهارة والإلمام الكامل والقدرة الهائلة في مجال نظم المعلوماتية.
- الثقة الزائدة بالنفس.
- الإلمام التام بمسرح الجريمة، وبما يجنيه.
- فجائية المواقف التي قد تؤدي إلى إفشال مخططه وافتضاح أمره[2].

الفرع الثاني: أركان الجريمة الإلكترونية

حتى يتسنى معاقبة الجاني على اتيان فعل ما ونكون اما تصرف يعاقب عليه القانون ،لابد من توفر الأركان الأساسية للجريمة، وهي تلك العناصر التي لا وجود للجريمة بدونها، حيث تدور الجريمة معها وجودا وعدما، وتتمثل في الركن المادي للجـ ريمة، والركن المعنوي الذي يقوم على القصد الجنائي وإتجاه إرادة الشخص نحو ارتكاب الفعل، والركن الشرعي وهو النص الذي يحوي النموذج القانوني للفعل أو الامتناع

---

[1]- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، المرجع السابق، ص09.

[2]- محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، الجزء الأول، ص30.

المجرم وهذه الأركان متوفرة سواء كانت الجريمة تقليدية أو في شكلها الإلكتروني. وعليه سنتناول هذه الأركان بالتفصيل في الفروع التالية:

اولا : الركن الشرعي

تعتبر الجريمة عمل غير مشروع يجرمه القانون ويعاقب عليه وذلك بالنظر لما يقرره القانون الجنائي والقوانين المكلمة له من أوامر ونواهي تجرم وتعاقب على كل سلوك أو فعل ترى فيه السلطة المختصة بالتشريع أنه يرقى لدرجة التجريم بما يشكله من مساس بمصالح الجماعة بعريضها بوجه عام للخطر[1] .

ويقوم الركن الشرعي على النص التشريعي المجرم للسلوك والمحدد للعقوبة المقررة له، تطبيقا لنص المادة الأولى من قانون العقوبات بقول: لا جريمة ولا عقوبة أو تدبير أمن بغير قانون وما يتماشى مع المادة 167 من دستور 2020 التي تنص على أن: تخضع العقوبات الجزائية لمبدأي الشرعية والشخصية.

وقد خص المشرع الجزائري الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بقسم خاص ضمن قانون العقوبات وهو القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان ،المساس بأنظمة المعالجة الآلية للمعطيات، ويشتمل على ثمانية مواد تضمنت كل أنواع الاعتداءات على الأنظمة المعلوماتية.

كما أنه ومن أجل الحد من هذه الجريمة، أصدر قانون خاص يعمل على وضع قواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها طبقا لقانون 04/09 الصادر بتاريخ 2009/08/05، وهذا تطبيقا لمبدأ الشرعية وعدم جواز متابعة الشخص بأفعال غير مجرمة قانونا.

---

[1] – بوخبزة عائشة ، الحماية الجزائية من الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماجستير في القانون الجنائي كلية الحقوق ، جامعة وهران ، 2012 – 2013 ص 62 .

ثانيا: الركن المادي

يسبق الفعل الإجرامي أعمال تحضيرية من شانها تفعيل الركن المادي في هذه الجريمة، كامتلاك حاسب آلي واتصاله بشبكة الانترنيت، وامتلاكه برنامج للاختراق ذوا بقوم هو باستحداث هذا البرنامج، وغيرها من هذه السمات رغم ان هذه التقنيات مشروعة بحسب الأصل مالم تستعمل في أفعال مجرمة، لذلك يشترط في الركن المادي مباشرة التصرف التقني وا ن تكون لهذا الفاعل دراية كافية وتحكم في هذه الوسائل[1].

وهذا ما أورده المشرع الجزائري في المادة الثانية من قانون 04/09 السابق الذكر جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية .

كما تناولت المادة 394 مكرر من قانون العقوبات الأعمال المادية لهذه الجريمة كالدخول أو البقاء بطريقة غير مشروعة في كل أو جزء من المنظومة للمعالجة الآلية المعلوماتية أو يحاول ذلك فمجرد محاولة تعتبر جريمة يعاقب عليها القانون، وتشدد العقوبة على هذا الفعل، كما تضاعف العقوبة في حالة المساس بهذه المعطيات سواء كان ذلك بالحذف، أوتغيير فالفعل المادي قد يتحقق بالنتيجة كدخول وتخريب أو زيادة أو محو، أو بدون نتيجة كمحاولة واكتشاف المرتكب ومتابعته من خلال المنظومة الأمنية لأي دولة .

ثالثا: الركن المعنوي

الجريمة المعلوماتية مثلها مثل الجريمة التقليدية، تقوم على عنصرين: الأول، العلم بأن الفعل مجرم، والثاني الإرادة التي تتجه إلى تحقيق نتيجة يعاقب عليها القانون.

[1] –حوالف عبد الصمد، الآليات القانونية لتلافي الجريمة المعلوماتية والحد من غنتشارها وفقا للتشريع الجزائري ، مجلة الفكر القانوني والسياسي، العدد الرابع .

ويتخذ القصد الجنائي عدة صور منها القصد الخاص والقصد العام، فهذا الأخير هو الهدف الفوري والمباشر للسلوك الإجرامي وينحصر في حدود تحقيق الفرض من الجريمة أيلا يمتد لما بعدها. أما القصد الجنائي الخاص هو ما يتطلب توافره في بعض الجرائم فلا يفي مجرد تحقيق الغرض من الجريمة بل هو أبعد من ذللك أي أنه يبحث في نوايا المجرم فما هو القصد الذي يجب توافره في الجريمة المعلوماتية .

إن المجرم المعلوماتي يتوجه من أجل ارتكاب فعل غير مشروع أو غير مسموح مع علم هذا المجرم بأركان الجريمة وبالرغم من أن بعض المحترفين يبررون افعالهم بأنهم مجرد فضوليون وأنهم قد تسللوا صدفة فلا انتقاء للعلم كركن للقصد الجنائي وكان يجب عليهم أن يتراجعوا بمجرد دخولهم ولا يستمروا في الاطلاع على أسرار الأفراد والمؤسسات لأن جميع المجرمين والأشخاص الذيم يرتكبون هذه الافعال يتمتعون بمهارات عقلية كبيرة تصل في كثير من الأحيان الى حد العبقرية . [1]

فالقصد الجنائي متوافر في جميع الجرائم المعلوماتية دون أي استثناء ولكن هذا لا يمنع أن هناك بعض الجرائم المعلوماتية تتطلب أن يتوافر فيها القصد الجنائي الخاص مثل جرائم نشويه السمعة عبر الأنترنت، أما جرائم نشر الفيروسات عبر الشبكة فهي نتوفر على القصد الجنائي الخاص، فالمجرم يهدف إلى تعطيل عمل الشبكة وفي جميع الظروف المشرع هو من يختص بتحديد الحالات التي يشترط فيها توافر القصد الجنائي الخاص[2] .

وبذلك تحققت الأركان السالف ذكرها، نكون أمام جريمة معلوماتية سخر لها المشرع كل الآليات القانونية من اجل الحد منها.

[1] – حوالف عبد الصمد ، الآليات القانونية لتلافي الجريمة المعلوماتية والحد من غنتشارها وفقا للتشريع الجزائري ، مجلة الفكر القانوني والسياسي ، العدد الرابع .

[2] – ونوغي نبيل ، الجريمة المعلوماتية في التشريع الجزائري ، مجلة العلوم القانونية والإجتماعية ، المجلد الرابع ، العدد الثالث ، جامعة زيان عاشور بالجلفة ، الجزائر 2019 ص 130 .

المبحث الثاني: صور الجريمة الإلكترونية

يشتمل هذا التصنيف اهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي في هذه الطائفة من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها .

ويهدف الجاني عادة من وراء إرتكاب هذه الجرائم تحقيق ربح مادي بطريقة غير مشروعة، إذ تهدف هذه الاجرائم الاعتداء على اموال الغير، فيستخدم المجرم المعلوماتي النظام المعلوماتي ذاته أو برامجه أو نظمه كوسيلة لتنفيذ الجريمة، ومنه لا يكون النظام المعلوماتي بعضها ذكرها المشرع الجزائري، في حين أن البعض الآخر رأى الفقه إمكانية تطبيق القواعد القانونية القائمة في قانون العقوبات عليها، نتعرض لهذه الأفكار بشكل من التفصيل من خلال ما يلي :

المطلب الأول : جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتي

للمعلومة المعالجة آليا أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتي و لما لها من قيمة إقتصادية، وبهذا تعد هدفا للجرائم المعلوماتية من خلال التلاعب فيها أو عن طريق إتلافها و هذا ما سنتناوله فيما يأتي:

الفرع الاول : الجريمة الالكترونية الواقعة على النظام المعلوماتي

وهي الجرائم الواقعة على النظام المعلوماتي التي قد تستهدف سواء المكونات المادية لنظام المعلومات أو برامج النظام المعلوماتي، أو المعلومات المدرجة بالنظام المعلوماتي على النحو التالي:

أولا: التلاعب في المعلومات

يتم التلاعب في المعلومات الموجودة داخل النظام المعلوماتي بطريق مباشر أو غير مباشر.

فأما التلاعب المباشر يتم عن طريق إدخال معلومات بمعرفة المسؤول عن القسم المعلوماتي، و يأخذ هذا التلاعب عدة صور كضم مستخدمين غير موجودين بالعمل لاسيما في المنشآت التي تضم عددا كبيرا من العاملين المؤقتين و دائمي التعيير بهدف الحصول على مرتباتهم، أو بالإبقاء على ملفات مستخدمين تركوا العمل للحصول على مبالغ مالية شهرية أو عن طرق عمل تحويلات لمبالغ وهمية لدى العاملين بالبنوك باستخدام النظام المعلوماتي بالبنك و تسجيلها و إعادة ترحيلها و إرسالها لحساب آخر في بنك آخر بهدف اختلاس تلك النقود .[1]

في حين التلاعب غير المباشر يتم عن طرق التدخل غير المباشر لدى المعلومات المسجلة بالنظام المعلوماتي باستخدام أحد وسائط التخزين أو بواسطة التلاعب عن بعد باستخدام أدوات معينة ومعرفة أرقام وشفرات الحسابات، و يتخذ ذلك عدة صور من بينها التلاعب في الشرائط الممغنطة وقد قام في هذا الصدد أحد الموظفين بأحد فروع الشركة الفرنسية ISOVERST GOBAIN بإرسال شريط ممغنط يحتوي على 139 إذن دفع وعند معالجته بالبنك بالقسم المعلوماتي تم رفض نسخه لعيب في طول الشريط، وقد حاول الخبراء أنه لو نجحت هذه العملية لتم النصب بحوالي 21 مليون فرنك فرنسي .

كما قد يتحقق التلاعب غير المباشر في المعلومات عن طريق التلاعب عن بعد باستخدام الجاني كلمة السر أو مفتاح الشفرة أو أداة ربط بالمركز المعلوماتي لأي جهة، و تكمن خطورة هذه الصورة في إمكانية تسلل الجاني إلى المعلومات المخزنة بالنظام المعلوماتي و الحصول على المنفعة المالية التي يريدها من مسافات بعيدة.

---

[1] – سوير سفيان، جرائم المعلوماتية ،مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، 2010 –2011 ص 43 .

ثانيا: إتلاف المعلومات:

و المقصود هنا هو الإتلاف المنطقي أي إتلاف معلومات الحاسوب و بياناته باستخدام الطرق المنطقية و المعلوماتية و تنوع أساليب الاعتداء على المعلومات بحسب الهدف الذي يرمي الجاني إلي تحقيقه و من ابرز هذه الاعتداءات : الفيروس المعلوماتي الدودة المعلوماتية، القنابل المنطقية.

أ- الفيروسات المعلوماتية

وهو برنامج معلوماتي أعطي تسمية فيروس لتشابهه الكبير مع الفيروس البيولوجي من حيث الانتقال والتكاثر و وظائفه التدميرية للأنظمة المعلوماتية والقدرة على تعديل البرامج الأخرى التي يرتبط بها، كما يستطيع الفيروسات التمييز بين البرامج السليمة و لبرامج التي سبق و أن أصيبت بالفيروس و لعل أهم العوامل التي ساعدت على الانتشار السريع للفيروسات داخل الأنظمة المعلوماتية هي القرصنة المعلوماتية و توافق الأجهزة و كذلك الانتشار الواسع لشبكة الانترنيت.

و بالرغم من إنتاج العديد من البرامج المضادة للفيروسات تبقى هذه الأخيرة قادرة على اختراق النظم المعلوماتية وتدعيم البيانات مهما كانت الموانع و الحصون.[1]

ب- القنبلة المعلوماتية و تنقسم إلى قسمين:

1- القنبلة المنطقية

و يهدف هذا الفيروس إلى تدمير المعلومات عند حدوث ظرف معين مثل تدمير نظام تسيير الموارد البشرية لمؤسسة معينة عند شطب اسم أحد الموظفين من القائمة.

---

[1] – قارة أمال ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، الطبعة الثانية 2007 ، دار هومة للطباعة والنشر والتوزيع الجزائر 2007 ص 127-128 .

2- القنبلة الزمنية:

يعمل هذا الفيروس في ساعة محددة من يوم معني و من ابرز الأمثلة عن ذلك فيروسMichaelanglo مايكل انجلوا وفيروسMacmag و فيروس شرنوبيل shernobel و يتميز هذا الأخير بأنه فيروس الأول الذي يصيب المكونات المادية بالخراب و التلف إلى جانب المكونات المعنوية (المعلومات) حيث اكتشف هذا الفيروس سنة 1998[1] .

ج–الدودة المعلوماتية (ver informatique)

هي عبارة عن نظام معلوماتي يمتاز بقدرته على التنقل عبر شبكات نقل المعلومات بهدف إعاقة عملها، و التشويش عليها عبر شل قدرتها على التبادل .. الخ و أهم ما تتميز به هذه الفيورسات، الانتشار، عبر الشبكات عن طريق توليد نفسها و من أشهرها الدودة التي أطلقها الطالب الأمريكي في جامعة كورنال Cornell university ، روبيرت موريس سنة 1988 عبر شبكات الجامعات و الشبكات العسكرية في الولايات المتحدة بتدمير الآلاف من الحواسيب و تعطيل الشبكات و كان هدفه من هذا هو إظهار ضعف مقاييس امن الشبكات قائلا : أردت أن أعرف إذا كان بإمكاني كتابة برنامج يستطيع قدر الإمكان الانتشار بشكل واسع على شبكة الانترنيت ..." و قد حكم على روبرت سنة 1995، عملا بأحكام المادة 1030 /5/a من قانون إساءة استخدام الحاسوب الصادر سنة 1986 بالمراقبة لمدة ثلاثة سنوات و بالعمل بالخدمة الاجتماعية لمدة 400 ساعة .[2]

ولقد أصبح مجرموا المعلوماتية يتفاخرون باستخدامها كوسيلة لاختراق الأنظمة و من الأمثلة الواقعية على ذلك ما حدث في صفحة إدارة الدفاع الأمريكية DOD الخاصة

[1] – عامر بزرا فايز " فيروسات الكمبيوتر دار ضنين للنشر، عمان الطبعة الأولى ،1994 .

[2] – راجع أنور الحربي ، لمزيد من المعلومات حول مخاطر الفيروس القنبلة الالكترونية ، "مجلة آفاق الانترنت، السنة الثانية العدد 14، 1999، ص 37.

بالقوات الجوية الأمريكية التي تعرضت واجهتها المرحبة بزوار الموقع إلى اعتداء أجبر المسؤولين على إغلاق المواقع التي تملكها إدارة الدفاع الأمريكية، ليتم تريب برنامج وقاية اشد أمنا.

لا تختلف جريمة إتلاف المعلومات عن بقية الجرائم الواقعة على الأموال من حيث انطوائها على اعتداء غير مشروع على حق الملكية و أمام تأييد الغالبية العظمى من الفقه و من مختلف النظم لفكرة عدم انطباق النصوص الخاصة بجرائم الهدم أو الإتلاف على إتلاف أو تعديل أو إلغاء المعلومات فقد تدخل المشرع في العديد من الدول ليشمل بالحماية الجنائية كل صور الاعتداء كما فعل المشرع الأمريكي في العديد من الولايات أو بالنص على كل جريمة على حدى كما فعل المشرع الفرنسي.

ففي الولايات المتحدة الأمريكية ينظر إلى المال بوصفه أي شيء ينطوي على قيمة وهو مفهوم يشمل الأموال المعنوية أي المعلومات البيانات حيث تعاقب قوانين كل من ولايات اريزونا و كاليفورنيا و فلوريدا و جورجيا و ميسوري، و أتاوا طبقا لهذا المفهوم، على الإتلاف القصدي للبيانات و المعلومات أو البرامج.

و تأخذ جريمة إتلاف المعلومات إحدى الصور الثلاثة:

أ – الإدخال:

و يقصد به عملية لإدخال إضافة معطيات جديدة على المعلومات الموجودة داخل النظام، و يتحقق هذا الفعل في الفرض الذي يتم فيه إدخال أي فيروس معلوماتي في النظام. حتى و لو لم يحدث أي ضرر فمجرد إدخال هذا الفيروس، يحقق الركن المادي لهذه الجريمة.

ب- **المحو أو الإلغاء:**

و يقصد به إفناء أو شطب المعلومات الموجودة داخل النظام كليا أو جزئيا، و من الأمثلة الواقعية على هذا الفعل ما قم به احد العاملين في شركة السمسرة والتأمين على الحياة في فورت ورث (fort warth) بولاية تكساس (Texas) الأمريكية 1985 بعد فصله من العمل باختراق النظام المعلوماتي للشركة لمذكورة بهدف الانتقام، حيث تمكن من محو أكثر من مائة و ثمان و ستين ألف من سجلات الشركة عن طريق زرع فيروس معلوماتي و قد حكم عليه بالمراقبة لمدة سبع سنوات، و دفع تعويض قدره أحد عشر ألف و ثمان مائة دولار[1].

ج - **تعديل المعلومات:**

و يقصد به تغيير المعطيات الموجودة داخل النظام و لاستبدالها بمعطيات أخرى و لا تتطلب هذه العملية تغييرا في المعلومات أو استبدالها بمعلومات أخرى، بل يتحقق الركن المادي لهذه الجريمة بمجرد إجراء تعديل داخلي و من الأمثلة الواقعية على هذه الصورة ،قيام صبي ألماني عمره 16سنة بزرع فيروس معلوماتي في شبكة المعلومات الخاصة لمستخدمي النظام videotext مهمته التقاط و جمع بيانات ذات طبيعة شخصية بالإضافة إلى قيام هذا الفيروس بالتلاعب في هذه البيانات بالتعديل و التغيير والمحو و تغيير مفاتيح السر.

الفرع الثاني: جرائم الاعتداء الواقعة بواسطة النظام المعلوماتي

وهنا لا يكون النظام المعلوماتي هو محل الجريمة، بل يكون الحاسب الآلي هو الوسيلة لتسهيل النتيجة الإجرامية بإستخدام النظام المعلوماتي، ويكون الهدفمن ورائها

[1] - هلالي عبد الله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية دراسة مقارنة ، القاهرة ، النسر الذهبي للطباعة ، 1999 ، ص 10 .

الربح بطريق غير مشروع، الإعتداء على اموال الغير، الإعتداء على الأشخاص وسلامتهم وحياتهم الخاصة، أو في سمعتهم وشرفهم والإعتداء على امن الدولة وأسرارها .

1- **التجسس الالكتروني: Cyberespionnage**: يعد هذا النوع من الجرائم من الأنواع التي تتم بين الحكومات وليس الأفراد، إذ تستعين الحكومات بمجرمين معلوماتيين لاستيقاء معلومات عن الدول المنافسة لها في مختلف المجالات الاقتصادية، والعسكرية، والاجتماعية لتحقق السبق والأرباح، خاصة بين الدول المتقدمة التي عرفت تطورا تكنولوجيا منقطع النظير كالولايات المتحدة الأمريكية والصين.

يستنتج أن التجسس الالكتروني، وبالرغم من تصنيفه ضمن الجرائم المعلوماتية إلا ان الحكومات تتنافس لابتكار افضل برامج التجسس الرقمي، وتتعاون مع المجرمين المعلوماتيين من ذوي القدرات التقنية الكبيرة لتصميمها، ولاكتشاف الثغرات الأمنية في نظمها ،وهو ما يعن الاعتماد على مبدأ الغاية تبرر الوسيلة في هذا المجال، خاصة في ظل الـ مجتمعات المعلوماتية التي تسعى لتحقيق السبق العسكري والعلمي والسيطرة على الثروات.[1]

2-**الاحتيال عبر الانترنت:cyber fraud**: هو أي تحريف غير صادق للحقيقة يهدف إلى السماح لشخص ،أو منعه عن فعل شيء ما ويسبب خسائر، ويهدف إلى تحقيق فوائـ د مادية [15]. عادة ما يكون الاحتيال عبر بطاقات البنوك، والدفع المالي، و استعمالها بشكل غير قانوني للقيام ببعض المعاملات المالية، وهو يتشابه مع الاحتيال التقليدي عن طريق ايهام الافراد والشركات بتحقيق أرباح طائلة، ثم النصب عليهم وسرقته.

---

[1]- المجلة الجزائرية للابحاث والدراسات ، تأثير الجريمة الإلكترونية على المعلومات الرقمية ، المجلد 03 العدد 09 ديسمبر 2019 ص 01 .

3- غسيل وتبييض الأموال إلكترونيا: Cyberlaundering: تتمثل في استعمال الحاسوب للقيام بمعاملات أو علاقات تجارية تعود بالربح سواء كانت ملموسة أو غير ملموسة، والتي تم التحصل عليها عن طريق نشاط اجرامي.

تجدر الإشارة هنا إلى أن تبييض الأموال يشمل تلك الأموال القذرة الناتجة عن جميع الجرائم والأعمال غير المشروعة ،وليست فقط الاعمال الناتجة عن معاملات تجارة المخدرات.[17] إن أهم ما يميز هذه العملية طريقة تهريب الأموال، واخفائها في البنوك، وتحويلها عبر مجالات جغرافية متنوعة لتحويل الجانب غير القانوني منها إلى قانوني.

4- **الابتزاز والترصد الالكتروني أو السيبرياني**: Cyberstalkingand Cyber extortion :حيث يعرف قاموس أكسفورد الترصد على أنه متابعة أو ملاحقة بخلسة، ويتضمن متابعة تحركات شخص عبر الانترنت ويعتمد هؤلاء المطاردين على نشر رسائل تهديدية في المواقع التي يزورها الضحية، وفي لوحات الاعلانات، وعبر مواقع الدردشة والبريد الالكتروني.

أما الابتزاز، فيتشابه مع ذلك التقليدي الذي يشمل التهديد للأفراد باستخدام معلوماتهم الشخصية بهدف الحصول على الأموال.

5-**الإرهاب الالكتروني:Cyber terrorism**: يشمل جميع أصناف الج رائم الالكترونية، ما زاد من فرص الإرهاب تطور أسلحته ،وسهل عل المجموعات الإرهابية عملية الترصد والايقاع بضحاياها، وبالتالي أصبحت اهداف الهجمات الارهابية سهلة سواء على الخط أو في الواقع، كما أصبح التأثير على الشباب للالتحاق بمجموعاتها سهلا يقتصر على نقرة زر.

6-**السطو والسرقة عبر الانترنت:Cyber theft**: من الجرائم التي تعتمد كثيرا على سرقة الأقراص الصلبة والمرنة للحصول على المعلومات المخزنة بها، ثم بيعها

والمتاجرة بها فيما بعد، خاصة عمليات السطو على بطاقات الائتمان، وهو ما قد يسبب زوال وإفلاس بعض الشركات الائتمانية والبنكية.[1]

7-القرصنة: Hacking :هي"جماعات تؤمن بالحرية المطلقة في الرأي والتعبير والاستخدام"، تستعمل طرق خاصة لاختراق أجهزة الحاسوب، الأرقام السرية للأشخاص وبريدهم الالكتروني، وبالتالي معرفة أسرار الناس وخصوصياتهم. يذكر على سبيل المثال ما قام به موقع ويكيليكس من خلال نشر حوالي ربع مليون وثيقة رسمية، مما سبب توتر كبير في العلاقات الدولية.

8-انتحال الشخصية:Identity theft: حيث يمكن القيام بهذه العملية عن طريق الحصول على المعلومات الأساسية حول شخص ما بهدف انتحال صفته والقيام بجرائم متعددة باستخدام اسمه ،إلى جانب المعلومات الأساسية مثل الاسم، رقم الهاتف والعنوان الشخصي. فالمنتحلون يستطيعون من خلالها الحصول على أرقام الضمان الاجتماعي، وأرقام رخصة القيادة، وحتى أرقام البطاقات الائتمانية، وأرقام جوازات السفر، مما يسمح للمجرمين بالقيام بمختلف أنواع السرقة والاحتيال. لذلك، فهي" من أخطر الجرائم التي يتعرض لها الأفراد"' والتي يجب التوعية حولها خاصة في الدول المتقدمة التي تعتمد اعتمادا كليا على الحكومات الالكترونية .

المطلب الثاني: جرائم الإعتداء على مكونات (البرامج) النظام المعلوماتي:

تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة، وقد تنفع هذه الجرائم إما على البرامج التطبيقية وإما على برامج التشغيل وسنتطرق لهاتين الصورتين فيما يأتي

[1] – المجلة الجزائرية للابحاث والدراسات ، مرجع سابق، ص 01.

الفرع الأول : الجرائم المعلوماتية الواقعة على البرامج التطبيقية :

1 – تعديل البرنامج : الهدف الرئيسي من تعديل هذه البرنامج يتمثل في اختلاس النقود وتكثر هذه الجرائم في مجال الحسابات.

ومن أمثلة ذلك قيام مبرمج بأحد البنوك الأمريكية بإدارة الحسابات بتعديل برنامج إضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بقيد المصاريف الزائدة في حساب خاص به أطلق عليه اسم zzwick وحصل على إثر ذلك على مئات الدولارات كل شهر وكان من الممكن أن يستمر هذا العمل الإجرامي لولا أن البنك أراد بمناسبة تأسيس شركة جديدة للدعاية أن يكافئ أول وآخر عميل له ليكشف عدم وجود ما يدعى zzwick [1]

وهناك نظام آخر يسمى سلامي salami ويتم الإختلاس بموجب هذا النظام باستقطاع مبالغ زهيدة وعلى فترات زمنية طويلة ومتباينة من خلال صفقات عديدة يترتب عليها تحقيق فائدة كبيرة وقد حقق بموجب هذا البرنامج أحد المستخدمين الأمريكيين بإحدى المنشآت التجارية الكبرى يدعى E . Royce في خلال 6 سنوات مايقرب من 2 مليون دولار . [2]

2–**التلاعب في البرنامج :** يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية أو عن طريق قيام أحد المبرمجين زرع برنامج فرعي غير مسموح به في البرنامج الأصلي يسمح له بالدخول غير المشروع في العناصر الضرورية لأي نظام معلوماتي، ويصعب اكتشاف هذا البرنامج لصغره ودقته.

[1] – أحمد خليفة الملط ، الجرائم المعلوماتية ، دار الفكر الجامعي ، الطبعة الثانية 2006 ، ص 173 .

[2] – المرجع نفسه، ص 174 .

الفرع الثاني: الجرائم المعلوماتية الواقعة على برامج التشغيل :

تعد برامج التشغيل تلك البرامج المسؤولة عن نظام معلوماتي، من حيث قيامها بتنظيم وضبط ترتيب التعليمات الخاصة بالنظام .

وتقوم الجريمة المعلوماتية في هذه الصورة عن طريق تزويد البرنامج كمجموعة تعليمات إضافية يسهل الوصول إليها وبواسطة شفرة تسمح الحصول على جميع المعطيات التي يتضمنها النظام المعلوماتي .[1]

ويتحقق هذا النوع من الجرائم المعلوماتية في شكلين :

1-**المصيدة:**

تتمثل هذه الصورة في إعداد المبرمج برنامج به أخطاء وعيوب عمدا، لا يكشف بعضها عند استخدام البرنامج، إذ يترك المبرمج ممرات خيالية وفواصل وتفرغات في البرنامج حتى يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال تفرغات إضافية أو إحداث مخارج وسيطة للولوج داخل النظام المعلوماتي والوصول إلى كل المعلومات التي تحويها الذاكرة .

وبهذه التقنية يمكن للمبرمج استخدام البرنامج في أي وقت وفق أهوائه، وبذلك يصبح هو المهيمن على النظام وعلى صاحب العمل المعتدى عليه.[2]

2-**تصميم برنامج وهمي:**

وتقوم هده الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه مخصص خصيصا لارتكاب الجريمة ومراقبة تنفيذها، ومن أمثلة ذلك قيام إحدى شركات التامين الأمريكية في لوس انجلوس بواسطة مبرمجها تصميم برنامج وهمي يقوم بتصنيع وثائق

---

[1] – أحمد خليفة الملط ، الجرائم المعلوماتية ، نفس المرجع ، ص 175.

[2] – محمد سامي الشوا ، ثورة المعلومات وانعكاساتها على قانون العقوبات ، دار النهضة العربية ، 1994 ، ص 82

تأمين لأشخاص وهميين بلغ عددهم 46.000 بهدف تقاضي هذه الشركة من إتحاد شركات التامين عمولات من نظيراتها.

ملخص الفصل الأول:

من خلال الفصل الأول تناولنا الإطار المفاهيمي للجريمة الإلكترونية بحيث عرفناها بمفهوميها الواسع والضيق، وهي فعل إجرامي يتم من خلال الحواسيب أو الشبكات كعمليات الإختراق والقرصنة كما تضم أشكال الجرائم التقليدية التي يتم تنفيذها عبر الانترنت، وتطرقنا كذلك إلى أركان الجريمة الإلكترونية المتمثلة في السمات الخاصة بالجريمة الإلكترونية والمجرم الإلكتروني، وأنواع الجريمة الإلكترونية المتمثلة في الجريمة الإلكترونية المرتكبة من خلال إستخدام النظام المعلوماتي، والجريمة الإلكترونية الواقعة على النظام المعلوماتي التي تشمل جريمتي الدخول والبقاء غير المشروعان في منظومة معلوماتية وجريمة المساس بمنظومة معلوماتية.

الفصل الثاني

إثبات الجريمة الإلكترونية

المبحث الأول: مفهوم الدليل الرقمي

المبحث الثاني: ضبط الجريمة الالكترونية وطرق اثباتها

المبحث الثالث: حجية الدليل الرقمي

الفصل الثاني: إثبات الجريمة الإلكترونية

الجريمة الإلكترونية نوع جديد ومستحدث من الجرائم له خصوصيته والمتمثلة في الدليل الناتج عنه، وهو الدليل الرقمي، وللحصول على هذا الدليل لابد من ان يقوم رجال الضبطية القضائية بعدة إجراءات خاصة تحكمها ضوابط وقواعد عامة

ولكي يتم الوصول إلى الحقيقة في مرحلة الحكم لابد أن يتم الآمر عن طريق أدلة متوفرة لدى القاضي يمارس سلطته التقديرية عليها، وفي مجال الجريمة الالكترونية يكون الدليل الالكتروني هو الأوفر، وهو دليل خاضع للقواعد العامة فيما يخص حجيته .

ونظرا للطبيعة الخاصة التي يتمته بها الدليل الالكتروني، فإن حجيته على مستوى الاثبات الجنائي قد تثير عدة مشاكل خاصة فيما يتعلق بمصداقيته وعليه نقسم هذا الفصل الى مبحثين

المبحث الأول: مفهوم الدليل الرقمي

لدراسة مفهوم الدليل الرقمي، لا بد من التطرق إلى تعريف الدليل الرقمي وخصائصه من خلال المطب الأول ثم التعرف على تقسيمات الدليل الرقمي في المطلب الثاني .

المطلب الأول: تعريف الدليل الرقمي وخصائصه

إن الدليل الرقمي من الأدلة الجنائية المستحدثة في نطاق الإثبات الجنائي جاء بغرض التصدي لنوع مستحدث من الجرائم، ألا وهي الجرائم الإلكترونية، وفي سبيل دراسة الدليل الإلكتروني كغيره من الأدلة الجنائية، لابد من التطرق لماهية الدليل الإلكتروني، فقبل كل شيء لابد من التعرف على ماهية الشيء المراد دراسته . [1]

الفرع الأول: تعريف الدليل الرقمي:

لتعريف الدليل الرقمي، لابد أولا من التطرق إلى الدليل بصفة عامة كأول شيء، وهذا بهدف التعرف على الدليل الرقمي، وإذا باعتبار أنه من المنطقي وجوب دراسة الأصل العام المتمثل في الدليل بصفة عامة، ثم التطرق إلى الفرع المتمثل في الدليل الرقمي.

وعليه سنتناول في هذا الفرع معنى الدليل الجنائي، من خلال التكلم عنه لغة، وكذا إيراد المعنى الاصطلاحي.

ثم سيكون التكلم عن معنى الدليل الإلكتروني، من الجانب الفقهي، من خلال مايلي.

---

[1]– عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2010، ص، 49.

أولا: معنى الدليل الجنائي

سيكون الحديث عن معناه اللغوي، وأيضا المعنى الاصطلاحي .

أ- **المعنى اللغوي للدليل الجنائي:** يعرف الدليل لغة على أنه المرشد، والدليل هو ما يستدل به، والدليل الدال أيضا، ويقال دله على الطريق يدله بالضم ودلالة بفتح الدال وكسرها، ودلولة بالضم والفتح أعلى، ويقال أدل فأمل والاسم الدالة بتشديد اللام وفلان يدل بفلان أي يثق به[1] .

فهو المرشد وما به الإرشاد، وما يستدل به، والدليل الدال والجمع أدلة ودلالات.

وقد قال أبو عبيد " الدال قريب المعنى من المعنى من الهدي وهما في السكينة والوقار في الهيئة والمنظر وغير ذلك" [2] .

ومنه نقول أن التعريف اللغوي للدليل الجنائي يعني بصفة عامة الإرشاد، وكذلك يأخذ معنى ما يتم الاستدلال به في إطار الإثبات.

ب-المعنى الاصطلاحي القانوني للدليل الجنائي:

يعرف على انه: «ما يلزم من العلم به شيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة المنشودة " [3].

فإذا أعلم المدعي القاضي بحجته فيما يخص دعواه، هنا يلزم على من أعلم القاضي بالحجة المطروحة، ويحكم عليه به .

[1] – ابن منظور: لسان العرب، دار صادر، الطبعة الثالثة، المجلد الحادي عشر، لبنان، 1414 هـ، 1994 م، ص، 248، 249 .

[2] – عائشة بن قارة مصطفى : حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2010، ص، 50.

[3]- المرجع نفسه، ص، 51.

والدليل في الاصطلاح الشرعي يأخذ معنى البينة، والتي يقصد بها الحجة والبرهان، أي ما يثبت، فهي كل ما يبين الحق ويظهره، وهذا باتفاق الفقهاء، وجاءت كلمة الدليل في القرآن الكريم في قوله تعالى: " ألم تر على ربك كيف مد الظل ولوشاء لجعلها ساكنا ثم جعلنا الشمس عليه دليلا "

وعليه فإن التعريف الاصطلاحي للدليل الجنائي، يتمثل عموما في العلم والوصول إلى اليقين، ومعرفة الحقيقة المنشودة، من خلال هذا الدليل.

وبالنظر إلى غالبية التشريعات نجد أنها لم تعرف الدليل، وإنما اكتفت بتعداد الأدلة، سواءا كان هذا التعداد على سبيل الحصر، أو المثال، إلا أن هناك بعض القوانين التي عرفته مثل قانون أسس الإجراءات الجنائية السوفيتية، إذ عرف الأدلة بأنها: " المعلومات الحقيقية التي على ضوئها يحدد المحقق، أو المحكمة طبقا للطرق المقررة قانونا توافر، أو تخلف فعل خطر اجتماعيا وتأثيم الشخص الذي ارتكب الفعل "[1].

فقد تعددت وجهات نظر القانونيين في معنى الدليل، ومن التعاريف ما جاء بها الخبراء الذين عرفوه بأنه " البرهان القائم على المنطق والعقل في إطار من الشرعية الإجرائية لإثبات صحة افتراض أو لرفع درجة اليقين الاقناعي في واقعة محل خلاف "[2]

كما تعددت محاولات الفقهاء في وضع تعريف له، حيث عرفه البعض على أنه: " الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها "[3].

---

[1]– سامي جلال فقي حسين: **الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي**، دار الكتب القانونية، مصر، 2011، ص، 16

[2] – أحمد مسعود مريم: **(آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04/09)**، رسالة ماجستير، منشورة، جامعة قاصدي مرباح، كلية الحقوق والعلوم السياسية، قسم الحقوق، الجزائر، 2013، ص، 81.

[3] – عائشة بن قارة مصطفى: المرجع السابق، ص، 51.

والحقيقة المقصودة هنا هي التي تتعلق بالوقائع المعروضة على القاضي، والتي من خلالها يعمل حكم القانون عليها .

كما تم تعريف الدليل على أنه: " الوسيلة التي يستعين بها القاضي في تكوين قناعته القضائية للوصول إلى الحقيقة من خلال تقديره السليم لها "[1].

ومن خلال ما سبق نقول أن غالب هذه التعريفات تتمحور حول الوصول للحقيقة، باستعمال المنطق السليم، سواء كان المنطق القانوني، أو العقلي، فهو وسيلة القاضي التي يصل من خلالها للحقيقة، ويكون بها اقتناعه، فالدليل الجنائي عبارة عن معلومة يثبت من خلالها ارتكاب الشخص للجريمة، أو عدم ارتكابه لها، فهو عنوان الحقيقة التي من خلالها يثبت الأمر أو يدحض، من خلال النظر في الواقع من جهة، وكذا النظر في القانون من جهة أخرى .

ثانيا : معنى الدليل الرقمي

إن التعاريف التي جاءت فيما يخص الدليل الإلكتروني، كانت متباينة، فمنها ما جاء واسعا، ومنها ما جاء ضيقا، وهذا راجع للعلم الذي ينتمي إليها هذا الدليل، فهناك تعاريف وردت من طرف الباحثين في المجال التقني، وتعاريف من جانب الباحثين في المجال القانوني، كما قامت بتعريفه المنظمة الدولية لأدلة الحاسوب، وعليه سنورد فيما يلي كلا من التعاريف الفقهية للدليل الإلكتروني، ثم سيكون الحديث عن تعريف المنظمة الدولية لأدلة الحاسوب .

[1]– سامي جلال فقي حسين، المرجع السابق، ص، 16.

أ – المعنى الفقهي للدليل الرقمي:

هناك عدة تعريفات من اهما : عرفه البعض على انه: " كل بيانات يمكن إعدادها أوتخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما " [1] .

وأيضا هناك من يعرفه بأنه: " معلومات يقبلها المنطق، والعقل، ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية، وعلمية، بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي، وملحقاتها، وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق، أو المحاكمة لإثبات حقيقة فعل، أو شيء له علاقة بجريمة، أوجان، أو مجني عليه " [2] .

بمعنى أن الدليل الإلكتروني يستخلص من البرامج المعلوماتية الموجودة في الحاسوب، وكذا ما يمكن استخلاصه من معدات، وأدوات الحاسوب الآلي، وهذا مربوط بأن يكون هذا الدليل قد استخرج بطريقة قانونية، هذا بهدف تحليلها، وتقديمه للقضاء في شكلها النهائي .

كما نجد التعريف الذي قال به الأستاذ " كيسي "، الذي عرفه على أنه: " يشمل جميع البيانات الرقمية التي يمكن أن تثبت أن هنالك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني، أوبين الجريمة، والمتضرر منها .

والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات، بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت، والصورة " [3]

---

[1]– عائشة بن قارة مصطفى: المرجع السابق، ص، 53.

[2]– المرجع نفسه، ص، 53.

[3]– المرجع نفسه، 54 .

الملاحظ على هذه التعاريف الفقهية، أن هناك خلط بين الدليل الإلكتروني، وبرامج الحاسوب الآلي، حيث تم اعتبار الدليل الإلكتروني كبيانات يتم إدخالها إلى جهاز الحاسوب، وهذا مفهوم يتماشى تماما مع ما يقصد به ببرامج هذا الجهاز، وبالنظر نجد أن كليهما لها آثار معلوماتية، وهذا باعتبار أن البيانات التي تخزن في جهاز الكمبيوتر مهما كانت صورتها نصوص، أو أرقام، أو صور، وغيرها، تتحول إلى طبيعة رقمية، وهذا مرده إلى أن التكنولوجيا الحديثة تعتمد على تقنية الترقيم، إلا أن هناك فرق بين الدليل الإلكتروني، وبرامج الحاسوب الآلي، حيث يكمن هذا الفرق في الوظيفة التي يؤديها .

أما الدليل الإلكتروني، فيكمن دوره في التعرف على طريقة وقوع الجريمة الإلكترونية، وهذا بغرض إثباتها وكشف الحقيقة، ونسبتها لمرتكبيها، خاصة في هذه البيئة الافتراضية، بحيث يمكن مثلا تفتيش محتوى القرص الصلب بهدف تبيان المراحل التي مر بها المجرم، لكي يحقق الغرض من فعله الإجرامي .

وما لا ينبغي إغفاله فيما يخص الفرق بين كل من الدليل الإلكتروني، وبرامج الحاسوب الآلي، أن الدليل الإلكتروني لا يقتصر دوره في إثبات الجرائم الإلكترونية فقط، كسرقة الملكية الفكرية، وإنما يمتد أيضا إلى الجرائم التقليدية، كالقتل، والاختطاف، أيضا الاتجار بالمخدرات، وغيرها من الجرائم التي تستخدم فيها التقنية الإلكترونية للتسهيل فيها، هذا من جهة .

ومن جهة أخرى نجد أن هذه التعريفات قد حصرت الأدلة الإلكترونية في الحاسوب، وملحقاته فقط، ولكن بالنظر لما تم التوصل إليه نجد أن هناك وسائل أخرى ترتبط بالحواسيب، كالهواتف النقالة، والبطاقات الذكية، وكذا المساعد الرقمي الشخصي .[1]

[1] – عائشة بن قارة مصطفى: المرجع السابق، ص – ص، 55 – 60.

ومنه نقول أن هذه التعاريف لا تحتوي على تعريف جامع مانع للدليل الإلكتروني، باعتبار أن هذه التعاريف عرفته على أساس جهاز الحاسوب فقط، في حين أن هناك اجهزة أخرى يمكن أن يستخرج منها الدليل الرقمي، وهذا ما يحتمه الوقت الراهن، فهذه التعاريف تقتصر على زمن معين، كما انه حصر تعريف هذا الدليل على هذا الجهاز معناه أن الدليل الرقمي يثبت الجرائم الإلكترونية فقط، غير أنه يمكن أن ترتكب جرائم تقليدية باستخدام التكنولوجيا الحديثة، وهذا للاستفادة من مزاياها، وعليه يمكن أن نقول أن الدليل الرقمي هو مجموع المعلومات التي تستخرج بطريقة قانونية، من جهاز الحاسوب، أو أي تقنية معلوماتية حديثة، بغرض إثبات جريمة معينة، ومنه نسبتها لشخص معين .

الفرع الثاني: خصائص الدليل الرقمي

للدليل الرقمي خصائص تميزه عن باقي الأدلة الجنائية التقليدية، وهذا يعود للبيئة التي يستخلص منها هذا النوع من الأدلة المتمثلة في البيئة الافتراضية، وما يمكن أن يقال عن هذه البيئة أنها متطورة بطبيعتها، بحيث تتوفر على أنواع متعددة من البيانات الرقمية التي قد تكون منفردة، أو مجتمعة حتى تكون دليلا، ومنه فإن هذه البيئة انعكست على هذا الدليل، وأضفت عليه خصائص لا تتوافر في باقي الأدلة الجنائية، وهذا ما سنوضحها من خلال ما يلي :

أولا: الدليل الرقمي دليل علمي وتقني

الدليل الإلكتروني كما سبق تبيانه هو الواقعة التي تنبئ عن وقوع جريمة أو فعل غير مشروع، وهذه الواقعة مرجعها أومبناها علمي، باعتبار أن مبنى العالم الافتراضي علمي أيضا، وهذه الخاصية مفادها أن الدليل الرقمي لا يمكن الحصول عليه ولا الإطلاع على ما يحتويه إلا باستخدام طرق علمية [1].

---

[1]– فتحي محمد أنور عزت: **الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية**، دار الفكر والقانون للنشر والتوزيع، الطبعة الأولى، مصر، 2010، ص، 648 .

وتفيد هذه الخاصية أيضا أنه عن قيام رجال الضبطية القضائية، أو سلطات التحقيق، بالتعامل مع هذا الدليل سعيا لإظهار الحقيقة بطريقة علمية، أي يكون البحث بسبل علمية، وهذا مرده إلى أن الدليل العلمي يخضع لقاعدة لزوم تجأوبه مع الحقيقة كاملة وفقا لقاعدة في القانون المقارن هي قاعدة " أن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة"، وعلى الرغم من الانتقادات التي وجهت لهذه القاعدة على أساس الإلزامية التي يوجبها القانون المقارن على أعضائه بضرورة وجود معرفة علمية، إلا أنه لا يمكن التمييز بين ما هوقانوني، وما هو علمي .

كذلك ما يمكن استنباطه من هذه الخاصية فيما يخص موضوع حفظه هو وجوب حفظ هذا الدليل على أسس علمية، ومنه ضرورة السعي وراء تحديث أسلوب تحرير المحاضر في هذا الشأن، فتحرير محضر يتنأول دليلا علميا مختلف عن المحضر المتناول اعتراف شخص مثلا، فالمحضر بالدليل العلمي يعني وجوب توافر طريقة علمية متوافقة مع ظاهرة الدليل العلمي أثناء تحريره، فمن غير المنطقي أن يتخذ صورة المحضر التقليدي[1] .

ومنه نقول أن هذه الخاصية التي يتميز بها الدليل الإلكتروني يترتب عنها عدة نتائج مهمة أهمها تحديث طرق، وكيفيات التعامل مع هذا الدليل بما يتماشى مع هذه الخاصية، وكذا بما يتماشى مع التطور التكنولوجي الراهن، حتى تكون لهذا الدليل حجية أكبر.

ثانيا: الدليل الرقمي يصعب التخلص منه

وتعتبر هذه الخاصية أو الميزة من أهم خصائص الدليل الرقمي، ويتمتع بها عن باقي الأدلة التقليدية، فنجد أنه يمكن التخلص بكل سهولة من الأوراق، والأشرطة المسجلة إذا كانت تحتوي علة اعتراف شخص بارتكابه للجريمة، وذلك بحرقها أو تمزيقها مثلا، كما

---

[1] – عائشة بن قارة مصطفى: المرجع السابق، 64.

انه من المستطاع التخلص من بصمات الأصابع بمسحها من موضعها، كما أن هناك بعض الدول التي يتم فيها التخلص من الشهود عن طريق قتلهم، أو تهديدهم لعدم الإدلاء بشهاداتهم، هذا فيما يتعلق بالأدلة التقليدية، وبالنسبة للأدلة الرقمية فإن الأمر مختلف، حيث انه يمكن استرجاعها بعد محوها، وإصلاحها بعد تلفها، وإظهارها بعد إخفائها، مما يؤدي لصعوبة التخلص منها، وهذا يعود إلى أن هناك العديد من البرامج الحاسوبية تتمثل وظيفتها في استعادة البيانات التي تم إلغائها، مثل : RecoverLost Data، سواء كان هذا الإلغاء عن طريق الأمر، أوبإعادة تهيئة، أوتشكيل للقرص الصلب باستخدام الأمر، وسواء كانت هذه البيانات في شكل صور أو رسومات أوكتابات أو غيرها، فكل هذا يشكل صعوبة إخفاء الجاني لجريمته، أو التخفي عن أعين العدالة، وهذا بشرط العلم بوقوع الجريمة من رجال البحث والتحقيق الجنائي .

كما يعتبر نشاط الجاني في سبيل محوالدليل الذي يدينه دليلا أيضا، وهذا لأن فعله هذا أي محاولة لإخفاء الدليل يتم تسجيله في الكمبيوتر، ويمكن استخلاصا كدليل إدانة ضده.

بمعنى أن الإلغاء أوالحذف للدليل الإلكتروني، هو في الحقيقة واقعة إخفاء لها مادام أن القاعدة المشار إليها ثابتة .

فهذه الخاصية في حقيقة الأمر تعد حافزا لمواصلة البحث في الجريمة الإلكترونية، ومنه تعد دافعا لاتخاذ الحيطة.

ومن هذه الخاصية تجدر الإشارة لأمر مهم، هو إمكانية استفادة مرتكب الجريمة من الضمانات الممنوحة له بمقتضى القانون، وهذا عند ارتكابه للجرائم الإلكترونية، على الرغم من وجود قصور في العلاقة بين المؤسسة القضائية، والمؤسسة التقنية .

وبالتالي فإن خاصية صعوبة التخلص من الدليل الإلكتروني تقابلها مسألة أخرى هي أن هذا الدليل نتيجة لمرونته وضعفه، فإنه يسهل إتلافه أو فقدانه أو كما يطلق عليه " Spoliation of Evidence "، بمعني إمكانية التخلص منه بغير الحذف والإلغاء، وبالنظر في هذه المسألة أي إمكانية إتلاف الدليل الإلكتروني، هي في الواقع ليست حقيقية، وإنما القول بإمكانية إتلافه معناه أنه يوجد قصور في القدرات التكنولوجية لدى مؤسسات العدالة، مما ينبغي معه وجوب العمل على التطوير المستمر لنظم العدالة، بالإضافة لتطوير قدرات القائمين على مهامها وأعمالها[1].

ثالثا: الدليل الرقمي دليل متنوع ومتطور وقابل للنسخ

على الرغم من أن الدليل الرقمي في أساسه يعتبر متحدا في تكوينه، أي في مجال الحوسبة والرقمية، إلا أنه يتخذ أشكالا مختلفة، فمصطلح الدليل الرقمي يشمل كافة أنواع البيانات الإلكترونية الممكن تداولها رقميا، ويكون بينها وبين الجريمة رابطة من نوع ما، بالإضافة إلى أن تكون متصلة بالضحية مما يتحقق معه وجود رابطة بينها وبين الجاني ففيما يخص التنوع المتعلق بالدليل الإلكتروني، نجد انه قد يظهر بطريقة علانية في هيئات مختلفة الأشكال، كأن يكون بيانات غير مقروءة، كما هو الأمر في حالة المراقبة عبر الشبكات والملقمات أو الخوادم، وقد يكون الدليل الإلكتروني مفهومها للأشخاص كما لوكان وثيقة معدة بنظام المعالجة الآلية للكلمات بأي نظام، كما يمكن أن يكون صورة ثابتة أو متحركة، أو معدة بنظام التسجيل السمعي المرئي، أو أن تكون مخزنة في نظام البريد الإلكتروني، وهذه الخاصية تستوجب مواكبة التطور في عالم التكنولوجيات [2].

كما أن الدليل الإلكتروني يعتبر دليلا قابلا للنسخ، وهذا مرده لإمكانية استخراج نسخ من الأدلة الجنائية الإلكترونية مطابقة للأصل، ولها نفس القيمة العلمية، وهذه

[1] – فتحي محمد أنور عزت: المرجع السابق، ص، ص، 655، 656.

[2]– فتحي أنور عزت: المرجع السابق، ص، ص، 651، 652.

الخاصية لا تتوافر في باقي الأدلة الجنائية التقليدية، وهذا يأتي معه بالضرورة وجود ضمانة شديدة الفعالية للحفاظ عل هذا النوع من الأدلة ضد الفقد والتلف والتغيير، عن طريق النسخ المطابق للأصل من الدليل، وهذا ما نص عليه القانون البلجيكي (نوفمبر 2000) في المادة 39، التي سمحت بضبط الأدلة الإلكترونية، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية .

كما نجد أن الدليل الإلكتروني يمتاز بالسعة التخزينية العالية، فآلة الفيديو الرقمية يمكنها تخزين مئات الصور، ودسك صغير يمكنها تخزين مكتبة صغيرة .

بالإضافة إلى أن الدليل الإلكتروني له خاصية رصد معلومات عن الجاني، وتحليلها في ذات الوقت، من خلال إمكانية تسجيلها لتحركات الفرد، وتسجيل عاداته وسلوكياته وبعض الأمور الشخصية، لذا فإن البحث الجنائي قد يجد غايته من الدليل المادي [1] .

ومنه نقول أن الدليل الرقمي، يتمتع بمجموعة من الخصائص، والمميزات التي جعلته يتميز عن باقي الأدلة الجنائية التقليدية، كما جعلته يفرض نفسه في مجال الإثبات الجنائي.

وبالنظر لهذه الخصائص نجد أنه يجب العمل على تطوير كل ما يتعلق بهذا الدليل، باعتبار أنه دليل علمي، وهذا عن طريق مواكبة التكنولوجيا الحديثة، فيما يخص إجراءات جمعه ودراسته وتحليله، لتتماشى مع طبيعة الدليل الإلكتروني، وكذا ضرورة أن يكون الأشخاص القائمين على هذا الدليل أشخاصا أكفاء، وعلى دراية بأن هذا النوع من الأدلة له ميزات خاصة تستوجب التعامل معه بطريقة خاصة .[2]

---

[1]- عائشة بن قارة مصطفى: المرجع السابق، ص، 64.

[2] – المرجع نفسه، ص، 66، 67.

المطلب الثاني: تقسيمات الدليل الرقمي :

إن فقهاء القانون الجنائي لم يتوسعوا في دراسة الدليل الرقمي، ومرد ذلك للحداثة النسبية لهذا الدليل من جهة، وتطوره بصفة دائمة من جهة أخرى، ومن المحاولات الفقهية أنه تم تقسيم الدليل الرقمي لأربعة أقسام هي: الأدلة الرقمية المتعلقة بجهاز الكمبيوتر وشبكاته، الأدلة الرقمية المتعلقة بالإنترنت، الأدلة الرقمية المتعلقة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات، الأدلة الرقمية المتعلقة بالشبكة العالمية للمعلومات [1] .

والملاحظ على هذا التقسيم أنه مطابق لتقسيم الجريمة عبر الكمبيوتر، وهذا ما سنوضحه.

الفرع الأول: التقسيمات الفقهية للدليل الرقمي

أولا: الأدلة الرقمية المتعلقة بالكمبيوتر وشبكاته:

وهي تتماشى مع جرائم الكمبيوتر الواقعة على أجهزة الكمبيوتر بسلوك غير مشروع، سواء كان هذا الأمر على المكونات المادية له، أو المكونات المعنوية، أو قواعد البيانات الرئيسية، مثل تخريب مكونات الكمبيوتر كالشاشات.

ثانيا: الأدلة الإلكترونية المتعلقة بالشبكة العالمية للمعلومات:

وهي متماشية مع الجرائم المتعلقة بهذه الشبكة، وهي فعل غير مشروع قانونا يقع على أي وثيقة أو نص موجود بالشبكة، مثل قرصنة المعلومات، وسرقة بطاقات الائتمان، وانتهاك الملكية الفكرية للبرامج وغيرها، فهذا النوع من الجرائم يتطلب الاتصال بالإنترنت.

---

[1] – ممدوح عبد الحميد عبد المطلب: **البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت**، دار الكتب القانونية، مصر، 2006، ص، 88.

ثالثا: الأدلة الإلكترونية المتعلقة بالإنترنت:

وهي تتطابق مع جرائم الإنترنت، وهي أيضا سلوك غير مشروع يقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات، مثل الدخول غير المشروع لمواقع يمنع الدخول إليها واستخدام عناوين (IP) غير حقيقية للدخول إلى الشبكة العالمية للمعلومات وغيرها.

رابعا: الأدلة الرقمية المتعلقة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات:

وهي متعلقة بالجرائم التي ترتكب باستخدام الكمبيوتر، حيث أنه لا يعتبر استعمال الكمبيوتر أو الشبكة العالمية للمعلومات أو الإنترنت، في هذه الجرائم من طبيعة الفعل الجرمي، وإنما تعتبر كوسيلة مساعدة لارتكاب الجريمة، مثل غسيل الأموال أو نقل المخدرات من مكان لآخر وغيره، وجهاز الكمبيوتر في هذه الحالة يحتفظ بآثار إلكترونية قد ترشد للفاعل[1] وإن هذا التقسيم الفقهي للدليل الإلكتروني، مع أنه يتناسب مع تقسيم الجرائم عبر الكمبيوتر، لكنه غير متناسب مع مفهوم التقنية الحديثة، فكل هذه التقسيمات تدور حول موضوع واحد وهو الدليل الإلكتروني، رغم أنها ميزت بين شبكات الكمبيوتر والإنترنت وبرتوكول تبادل المعلومات والشبكة العالمية للمعلومات التي هي في الأصل واحد ولكنها تختلف في المصطلحات .

ومنه نقول أن هذا التقسيم بالرغم من أنه جاء متماشيا مع الجرائم الواقعة عن طريق الكمبيوتر، وهذا جانب من الصحة فيه، إلا أنه لم يشمل كافة ما يتعلق بالدليل الإلكتروني، وخاصة وأنه لم يأخذ بعين الاعتبار وبصورة كبيرة التقنية الحديثة التي تعتبر ركيزة هامة لمعالجة موضوع الدليل الإلكتروني، باعتبار أن هذا الدليل ظهر بظهور التقنيات الحديثة .

---

[1] – عائشة بن قارة مصطفى: المرجع السابق، ص، ص، 72، 73.

الفرع الثاني: التقسيمات التشريعية والقضائية للدليل الرقمي

برزت عدة تشريعات حاولت تقسيم الدليل الرقمي، وإحاطة كل ما يتعلق به، والقضاء أيضا كان له دور في معالجة موضوع الدليل الرقمي، وكذا العمل على إعطاء تقسيمات إلا أن تشريع الولايات المتحدة الأمريكية كان من السباقين الذين تطرقوا لهذا الموضوع أي الدليل الرقمي، ولهذا ستكون كنموذج لدراستنا مع إبراز التقسيم المعتمد من قبلها للدليل الرقمي، سواء كان هذا الأمر على مستوى التشريع أو القضاء .

فهي تعتبر ثاني دولة بعد السويد في إصدار القوانين الخاصة بها التي تجرم عن طريقها نوعا مستحدث من الجرائم وهي الجرائم الإلكترونية، ومن أهم هذه القوانين قانون تقرير الأشخاص الصادر في 1970، بالإضافة إلى قانون الخصوصية الصادر في 31 ديسمبر 1974، وكذا قانون حرية المعلومات عام 1976، وأيضا قانون خصوصية الاتصالات سنة 1986، وغيرها من القوانين .

كما أن الولايات المتحدة الأمريكية قامت بإنشاء المنظمة الدولية لأدلة الحاسوب (ICOE)، ورافقتها بالفريق العامل على مستوى الأدلة الإلكترونية (SWGDE)، وهذا بغرض توحيد الجهود التي تقوم بها هذه المنظمة [1].

ومنه سنبرز من خلال ما يلي تقسيمات وزارة العدل الأمريكية للدليل الإلكتروني لسنة 2002:

أولا: السجلات المحفوظة في الحاسوب :

وهي عبارة عن وثائق مكتوبة ومحفوظة، والمقصود بالكتابة الإلكترونية أنها كل حروف أو أرقام أو رموز أو أي علامات أخرى، تثبت على دعامة إلكترونية أو رقمية أو ضوئية أوأية وسيلة مشابهة وتعطي دلالة قابلة للإدراك [2].

---

[1] – عائشة بن قارة مصطفى: المرجع السابق، ص، ص، 73، 74.

[2] – محمد حسين منصور: **الإثبات التقليدي والإلكتروني**، دار الفكر الجامعي، مصر، 2006، ص، 272.

من أمثلتها البريد الإلكتروني الذي عرف على انه : " طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات[1]

ففكرة البريد الإلكتروني تقوم على تبادل الرسائل الإلكترونية والملفات والرسوم والصور والبرامج وغيرها، عن طريق إرسالها من المرسل إلى شخص أو أكثر، وهذا باستعمال البريد الإلكتروني للمرسل إليه، فهو عبارة عن صندوق تتواجد به كل الرسائل المرسلة إلى صاحب البريد والتي سبق له إرسالها، والملغاة وغيرها من الأمور التي يحتوي عليها البريد الإلكتروني

وهناك أيضا ملفات برامج معالجة الكلمات، وكذا رسائل غرف المحادثة على الإنترنت .

ثانيا: السجلات المحفوظة جزئيا في الحاسوب :

هذا النوع من السجلات يتم إنشاؤها بواسطة الحاسوب أي هي عبارة عن مخرجات برامج الحاسوب، معنى ذلك أنها لم يتم لمسها من الأشخاص مثل (Log Files)، بالإضافة لسجلات الهاتف، وكذا فواتير أجهزة السحب الآلي (ATM) .

ثالثا: السجلات المحفوظة للإدخال والمنشأة بواسطة الحاسوب :

ومن أمثلة هذا النوع من الأدلة الإلكترونية أوراق العمل المالية التي تحتوي على مدخلات يتم تحويلها لبرامج أوراق عمل مثل (Excel) ثم تتم معالجتها بإجراء العمليات الحسابية .

فالتنوع في الدليل الإلكتروني مفاده أنه لا توجد وسيلة واحدة للحصول عليه، وإنما هي متعددة، وفي كل الأحوال يبقى الدليل إلكترونيا حتى وإن اتخذ هيئة أخرى، وفي هذه

---

[1]– خالد ممدوح إبراهيم: **التقاضي الإلكتروني**، دار الفكر الجامعي، الطبعة الأولى، مصر، 2007، ص، ص، 101، 102

الحالة فإن اعتراف القانون بهذا النوع من الأدلة يكون على أساس افتراضي يبنى على أساس الدليل الإلكتروني في حد ذاته وضرورته إلا أنه لكي يكون هناك تناسق بين القانون والدليل الإلكتروني، فإنه لابد من اتخاذ مسلك الافتراض باعتبار هذا الدليل دليلا أصليا، وهذا مرده إلى نقص توافر الإمكانيات الإلكترونية في المحاكم الجنائية التي تنظر في هذا النوع من الأدلة وهذا التقسيم هونفس التقسيم الذي أخذ به القضاء الأمريكي، فسجلات الحاسوب المقبولة أمام القضاء الأمريكي هي التي تكون في شكل نصوص، وهذا إما في هيئة سجلات الحاسوب المتوالدة، أو سجلات الحاسوب المخزنة، ويكمن

الفرق بينهم فيما إذا كان الشخص هو المنشئ لمحتوى هذه السجلات أو الآلة، فسجلات الحاسوب المخزنة تحتوي على كتابات شخص أو بعض الأشخاص في شكل إلكتروني مثل البريد الإلكتروني، أما ما يخص سجلات الحاسوب المتوالدة فالكمبيوتر هو الذي يصدرها، فهي عبارة عن مخرجات برامج الحاسوب مثل سجلات الدخول على الإنترنت التي يكون مصدرها مزود خدمة الإنترنت، كما أن هناك نوعا ثالثا من السجلات الذي يجمع بين التدخل الإنساني ومعالجة الكمبيوتر، مثلا كأن يدخل متهم معين بيانات ويطلب من الكمبيوتر معالجتها للوصول إلى نتائج يمسح بها هذا البرنامج المستخدم، كالشخص الذي يتهرب من الضرائب فيسجل بيانات غير صحيحة تتعلق بدخلها وربحها، ويطلب من الكمبيوتر حساب الضريبة المستحقة [1].

إلا أن ما يؤخذ على هذه التقسيمات أنها لا تشمل الدليل الإلكتروني، فهي حصرته في نوع واحد وهو سجلات الحاسوب المحتواة على نص، رغم أن الدليل الإلكتروني يتعلق بكافة البيانات الإلكترونية التي يمكن تداولها إلكترونيا، كالصور والأصوات والرسوم وغيرها، فنجد في الوقت الراهن بروتوكولات الاتصالات والتطبيقات المعلوماتية التي تستعمل في التحقيق فيما يخص الجرائم الإلكترونية، حيث يعتبر نظام (TCP /IP) من

[1] – عائشة بن قارة مصطفى: المرجع السابق، ص – ص، 74 – 76.

أكثر البروتوكولات المستعملة في شبكات الإنترنت، فهي تعتبر جزءا مهما منه، فهي تدل بصفة يقينية عن مصدر الجهاز الذي استخدم في الجريمة، كما تقوم بتحديد الأجهزة التي أصابها الضرر من هذا الفعل الإجرامي [1].

ومنه نقول أن التقسيم الذي جاء به كل من التشريع الأمريكي، وكذا القضاء الأمريكي فيه جانب من الصحة، باعتبار أنه تحدث عن نوع مهم من الأدلة الإلكترونية، والتي تعتبر أدلة قوية .

إلا أن هذا التقسيم تقسيم ناقص ولا يشمل كل الأدلة الإلكترونية، حيث نستطيع أن نقول أنه حصر تقسيمه في الأدلة الإلكترونية المكتوبة فقط في حين أن هناك أدلة إلكترونية أخرى، فهو لم يخرج في تقسيمه هذا عن السجلات المتعلقة بالحاسوب فقط .

[1]– عائشة بن قارة مصطفى: المرجع السابق، ص، 76 .

المبحث الثاني: ضبط الجريمة الإلكترونية وطرق إثباتها

لقد تطورت وسائل التحقيق الجنائي في عصر المعلوماتية تطورا ملموسا يواكب حركة الجريمة وتطور أساليب ارتكابها، فبعد إن كان الطابع المميز لوسائل التحقيق العنف والتعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية الحديثة القائمة على الإستعانة بالأساليب العلمية، وإستخدام شبكة الإنترنيت هي الصفة المميزة والغالبة .[1]

ولدراسة كيفية ضبط وطرق إثبات الجريمة الإلكترونية قسمنا مبحثنا إلى مطلبين: المطلب الأول: ضبط الجريمة الإلكترونية ونتناول في المطلب الثاني طرق إثبات الجريمة الإلكترونية وسنوضحه من خلال ما يلي :

المطلب الأول: ضبط الجريمة الإلكترونية

من البديهي أن تظهر أنماط جديدة من الجرائم لم تكن معهودة في السابق، وهذا ليس مقتصرا على أسباب التقدم التقني فقط، بل يحدث دوما وبصفة مستمرة فالمجرم والجريمة في تقدم وتجدد مستمرين .

ولا شك أن ظهور أنماط جديدة من الجرائم لم تكن مألوفة في السابق، ونحن لا نزال في بداية عصر الانفجار المعلوماتي، يعني توقع ظهور المزيد من الانماط الجديدة، والتي يتوجب معه تحديث الانظمة والتعليمات والجهات الامنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الانماط الجديدة، وهوما يتبع بتطوير اسلوب التحقيق فيها وكيفية اثباتها .

---

[1]– محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، مطبعة جامعة القاهرة، القاهرة، 2000 ص 75 .

ولدراسة هذا المطلب تطرقنا إلى القواعد العامة التي تحكم إثبات الجريمة الإلكترونية في الفرع الأول ومن ثم إنتقلنا إلى تبيان ضوابط إثبات الجريمة الإلكترونية في الفرع الثاني، ونختم المطلب بالتطرق إلى عناصر إثبات الجريمة الإلكترونية في الفرع الثالث .

الفرع الأول: القواعد العامة التي تحكم إثبات الجريمة الإلكترونية

تتنوع قواعد إثبات الجريمة الإلكترونية، حيث يمكن أن تصنف على النحو التالي :

أولا: من زاوية قوتها الثبوتية: هناك أدلة مباشرة تثبت الجريمة بصورة مباشرة، وأدلة غير مباشرة تنصب على وقائع لا تشير إلى الجريمة مباشرة، وإنما يحتاج الأمر إلى إعمال العقل والمنطق لإستخلاص الأدلة منها .

ثانيا: من زاوية النتيجة القضائية المستخلصة منها: هناك دليل يدل على وقوع الجريمة، ودليل على تحديد شخص مرتكبها، ودليل يثبت إرتكابها على المتهم .

ثالثا: من زاوية وظيفة الدليل الإثباتية: فهناك أدلة تنصب على إثبات توافر أحد ركني الجريمة المادي أو المعنوي، وهناك أدلة تنصب على تحديد شخصية المتهم فأما التحديد القاطع فيشير إلى تحديد شخصية الجاني دون أدنى شك كالبصمات وأثار الأقدام العارية والشهادة بالرؤية والإعتراف وضبط محصلات الجريمة في حوزة المتهم .

رابعا: من زاوية مضمون الدليل: هناك أدلة مادية محسوسة بإحدى الحواس، وهناك أدلة معنوية مثل الشهادة وأدلة قوية مثل أقوال المتهم .

الفرع الثاني: ضوابط إثبات الجريمة الإلكترونية

تنقسم ضوابط إثبات الجريمة الإلكترونية إلى ضوابط إثبات الجريمة بالأدلة العلمية، وضوابط إثبات الجريمة بالأدلة الإجرائية ويمكن توضيحها كما يلي :

أولا: ضوابط إثبات الجريمة الإلكترونية بالأدلة الإلكترونية :

يحتاج إثبات الجرائم الإلكترونية إلى دليل رقمي، كوسيلة لإثبات إرتكاب جريمة الإختراق والتعدي على البيانات والمعلومات، سواء بسرقتها أو إتلافها أو تزويرها، أو سرقة المنظومة الإلكترونية الخاصة بفرد معين أو منظمة معينة لصالح الفرد أو الغير والدليل العلمي يتطلب استخدام طرق غير تقليدية في الإثبات، والدليل العلمي يقتصر على إجراء تجارب علمية ومعملية على جهاز الحاسب الآلي الذي إستخدم في الإختراق أوالتعدي، لتعزيز دليل سبق تقديمه سواء بالنفي أو الإثبات للواقعة التي ثار الشك بشأنها [1].

والدليل العلمي هو النتيجة التي تسفر عنها التجارب العلمية والمعملية لتعزيز دليل سبق تقديمه .

إن عدم الإعتداد بالخبرة الفنية كوسيلة لإثبات الجريمة الالكترونية، واعتبارها بمثابة قرائن فقط، يضيف صعوبة اخرى إلى صعوبات إكتشاف المجرم وتحديده، في ضوء عدم تسليم الامور التي تحكم الدليل الرقمي في الفكر الجنائي خارج نطاق تلك الجرائم .

ومن خلال ذلك، يمكن توضيح الأدوات العلمية لضبط إثبات الجريمة على انها من ادوات تقوم بضبط الجريمة كغالبية برامج الحماية، وأدوات المراجعة وأدوات مراقبة المستخدمين للشبكة وأدوات التصنت على الشبكة والتقارير التي تنتجها نظم أمن البيانات، وأدوات الضبط الاخرى، ويمكن استخدام الأدوات المستخدمة في الجريمة كأداة ضبط مثل ادوات جمع المعلومات عن الزائريين للمواقع .

---

[1] – محمد علي العريان، الجرائم المعلوماتي ة، مرجع سابق ص 45 .

ثانيا: ضوابط إثبات الجريمة الإلكترونية بالأدلة الإجرائية :

الضوابط الإجرائية هي الأساليب التي تستخدم لإثبات وقوع الجريمة وتحديد شخصية مرتكبها وهذه الاساليب ذات فاعلية في التحقيق الفني، حيث تساهم في إثبات الجريمة وبيان الغموض وإيجاد العلاقة بين الجانيي والمجني عليه من قبل المحقق الفني، بإستخدام تقنيات وبرامج التتبع الإلكتروني والتفتيش الإلكتروني والضبط الإلكتروني، التي تتميز بقدرات فائقة على القيام بالمهام التتبع والإسترجاع للبرامج والأدوات التي إستخدمت في الإختراق والتعدي وإرتكاب الجريمة، ويمكن توضيح هذه الضوابط حسب الطريقة المتبعة للوصول وحسب البرنامج المتبع ومن تلك الطرق .[1]

- الإطلاع على عمليات النظام المعلوماتي ومكوناته من الشبكات والتطبيقات والخدمات وكذلك قاعدة البيانات وإدارتها، وخطة تأمينها، وموارد النظام، والمستفيدين والملفات والإجراءات وتصنيف الموارد العامة ومدى مزامنة الأجهزة والوقت المخصص لكل مستفيد في حالة تعدد المستخدمين واجراءات امن العاملين واسلوب النسخ الإحتياطي وبرامج الحماية المتوفرة .

إظهار الحقائق:

يجب على المحقق إظهار الحقائق خلال مرحلة جمع الإستدلالات الإلكترونية وإثباتها في محضره نظرا لأهميتها في تحديد الجريمة، ورسم خطوات البحث من خلال التثبيت من توافر اركان الجريمة، وتحديد مكان الجريمة ووصفه، وتحديد وقت وقوع الجريمة، وتحديد اسلوب ارتكاب الجريمة، واداة إرتكاب الجريمة، والظروف المحيطة بالجريمة، ودوافع الجريمة .

[1] – محمد فاروق عبد الحميد كامل، القواعد الفنية الشرطية للتحقيق والبحث الجنائي، جامع نايف العربية للعلوم الأمنية الرياض 2012، ص 35 .

التحقق من توافر اركان الجريمة :

يحدد وقوع جريمة ما توفر ركنيين اساسيين وهما الركن المادي ويقصد به الواقعة أو الضرر المادي للجريمة، ويتمثل في نشاط الفاعل والنتيجة التي يحققها والعلاقة السببية بينهما والركن الآخر هو الركن المعنوي ويقصد به الإدارة التي إقترن بها الفعل المرتكب، ويأخذ صورة القصد الجنائي في الجريمة المتعددة، وصورة الخطأ في الجريمة غير المقصودة .

إتباع القواعد الفنية لكشف الجريمة :

إن عمل المحقق يبدأ منذ الوقت الذي يصله فيه خبر وقوع جريمة، ويقوم بالإجراءات التي يتخذها عقب ذلك من معاينة وتفتيش وانتداب الخبراء، وسماع شهود واستجواب لأطراف الجريمة، وجمع التحريات وهومن كل هذه الإّجراءات يستخلص العديد من الادلة، ويحاط علما بكثير من الوقائع المتصلة بالجريمة والتي تختلف في قوة ثبوتيتها، وتأتي في أعقاب ذلك مرحلة يجد فيها المحقق نفسه وامامه مجموعة ضخمة من الأدلة والوقائع التي تمكن من جمعها .[1]

المطلب الثاني: طرق اثبات الجريمة الالكترونية

إن التطور التقني في شبكة الانترنت سوف يقود دون شك الى تغيير كبير، ان لم يكن كليا في المفاهيم السائدة حول الدليل ويقود مثل هذا القول في الحقيقة الى اعلان انضمام الخبرة التقنية الى علم الخبرة المتميزة للتعامل مع موضوع الدعوى، من حيث ضرورة الاستعانة بالمختصين في مجال النزاع .

ويعد كل من المعاينة والتفتيش والشهادة والاقرار، أحد وسائل جمع الادلة ولكل منها قواعده يتم اتباعها وعليه نقسم المطلب إلى فروع :

[1] – محمد علي العريان: الجرائم المعلوماتية، المرجع سابق، ص، 47 .

الفرع الأول: الإستدلالات الأولية لاثبات الجريمة الالكترونية :

يمكن توضيح طرق الإستدلالات الأولية لإثبات الجلاريسمة الإلكترونية من خلال ما يلي :

أولا: تلقي وضع البلاغ :

يعرف ضبط البلاغ على انه وضع اليد على شيئ يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها والضبط بهذا المعنى ينصرف إلى الأشياء دون الأشخاص وبنذل على ذلك يجب توضيح مدى صلاحية الجرائم المرتكبة في البيئة الالكترونية .

ثانيا: المعاينة

يقصد بالمعاينة مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف الحافظة عليها خوفا من اتلافها أو محوها أو تعديلها والمعاينة من اجراءات التحقيق الابتدائي ويجوز للمحقق للجوء اليه متى رأى لذاك ضرورة تتعلق بالتحقيق والاصل ان يحضر اطراف الدعوى المعاينة وقد يقرر المحقق أن يجربها في غيابتهم ولا يلتزم المحقق بدعوى محامي المتهم للحضور ومجرد غياب المتهم عند اجراء المعاينة ليس من شأنه أن يبطلها وتظهر اهمية المعاينة وقوع جريمة من الجرائم التقليدية حيث يوجد مسرح فعلي للجريمة يحتوى على اثار مادية فعلية يهدف القائم بالمعاينة الى التحفظ عليها تمهيد لفحصها لبيان مدى صحتها في الاثبات وليس الحال كذلك بالنسبة للجرائم الالكترونية حيث يتخلف عن ارتكابها اثار مادية وقد تطول فترة الزمانية بين وقوع الجريمة واكتشافها مما يعرض اثار الناجمة عنها الى المحو أو التلف أو العبث بها واذا تمت معاينة بعد وقوع الجريمة في مجال الالكتروني .[1]

---

[1] – ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، المرجع السابق ص 65 .

ثالثا: التحري وكشف غموض الجرائم الإلكترونية

تتسم الجرائم ذات الصلة بالحاسب الآلي بحداثة أساليب ارتكابها، وسرعة تنفيذها وسهولة إخفائها ودقة وسرعة محو اثارها هذه الخصائص العامة تقتضي أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وكيفية تشغيلها وأساليب إرتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي إستخدمت في إرتكابها، والتحفظ على البيانات أو الأجهزة التي إستخدمت في إرتكابها أو تلك التي تكون محلا للجريمة .[1]

وأساليب التحري أوالتحقيق التقليدية قد لا تصلح لكشف الجريمة وضبط مرتكبيها، والتحفظ على أدلتها، ويمكن إجراء بعض التحريات المبدئية قبل عملية التفتيش أو الضبط والتحقيق، توصلا لكشف غموض الجريمة تمهيدا لضبط مرتكبيها، وجميع الادلة المتعلقة بها .

رابعا: التفتيش:

التفتيش هو البحث في مستودع سر المتهم، وهو إجراء من إجراءات التحقيق يتطلب أوامر قضائية لمباشرته ويجب على المحقق الجنائي المبادرة لإجراء التفتيش وذلك قبل قيام الجاني بطمس معالم الجريمة وإخفاء كل ما يتعلق بها، وهو يستطيع ذلك إذا إتسع له الوقت وسنحت له الفرصة .[2]

[1]– ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية، ورقة عمل مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة، كلية الملك فهد الأمنية، الرياض، 2001 ص 185.

[2]– رمزي رياض عوض، مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها، دراسة تحليلية تأصيلية مقارنة، دار الفكر العربي، القاهرة 2000 ص 75 .

والتفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الاجراءات الجزائية، فيقصد به أنه 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 الى ادلة تفيد اثبات الجريمة ونسبتها إلى المتهم بإرتكابها [1].

لكن توجد بعض الصعوبات الإجرائية التي تعيق خضوع البيانات المخزنة آليا لقواعد التفتيش التقليدية، والتي منها تعدد الاماكن التي يوجد بها النظام المعلوماتي داخل أوخارج الدولة وهناك صعوبة في تحديد الأشياء التي يهدف إلى ضبطها من عملية التفتيش، وغيرها من الصعوبات مثل عدم إكتمال المعرفة المعلوماتية والتقنية لتنفيذ عملية التفتيش كما ينبغي أن تكون .

خامسا: الضبط

الغاية من التفتيش ضبط شيئ يتعلق بالجريمة ويفيد في التحقيق الجاري بشأن الجريمة الإلكترونية، سواء أكان هذا الشيء أدوات إستعملت في إرتكاب الجريمة أو شيئا نتج عنها أوغير ذلك مما يفيد في كشف الحقيقة ونظرا لكون الضبط في مجال الجرائم الالكترونية هوضبط بيانات المعالجة الكترونيا فقد اثير التساؤل هل يصلح هذا النوع من البيانات لأن يكون محلا للضبط ؟

وقد انقسم الفقه القانوني الى اتجاهين عند الاجابة على هذا التساؤل :

الاتجــاه الأول: يـرى الـبعض ان بيانـات الحاسـب لا تصـلح لأن تكـون محـلا للضـبط، لانتقـاء الكيـان المـادي عنهـا، ولا سـبيل لضـبطها الا بعـد نقلهـا علـى كيـان

[1] –نبيل عبد المنعم جاد، اسس التحقيق والبحث الجنائي العلمي، مطبعة كلية الشرطة 2002 ص 70 .

مادي ملموس عن طريق التصوير الفوتوغرافي، أو بنقلها على دعامة أو غيرها من الوسائل المادية ويستند هذا الرأي إلى أن النصوص القانونية المتعلقة بالضبط محل تطبيقها الاشياء المادية الملموسة .[1]

الاتجاه الثاني: ويرى الإتجاه الثاني أن البيانات المعالجة الكترونيا ما هي إلى ذبذبات الكترونية تقبل التسجيل والحفظ والتخزين على وسائط مادية فوجودها المادي لا يمكن انكاره ويستند هذا الاتجاه الى ان بعض النصوص القانونية تنص على ان التفتيش وضبط الدفاتر الخاصة بمؤسسات مالية يقتصر على تفتيش المكان بغرض تفقده واخذ نسخة من المواد المكتوبة، حتى ولو كانت السجلات المكتوبة في شكل الكتروني .

وخوفا من محو أو إتلاف أو نقل أو ضياع الأدلة التي يتم الحصول عليها بطريق التفتيش، فالمحقق التحفظ على هذه الادلة .

ويتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق، ويبقى تحت تصرفها الى حين انتهاء المحاكمة ويرى البعض ضرورة حفظ نسخة أخرى خوفا من تلف أو ضياع النسخة الوحيدة الموجودة تحت تصرف جهة التحقيق أو المحكمة .

سادسا: التسرب:

استحدث المشرع الجزائري في مجال مكافحته جرائم المساس بأنظمة الحاسب الآلي عدة إجراءات للكشف عن الجريمة ومرتكبيها، وتقديمهم للعدالة لينالوا جزاءا عما اقترفوه من جرم في حق المجتمع وترجع العلة في استحداث مثل هذه الاجراءات إلى عجز

---

[1] – ثنيان ناصر آل ثنيان، إثبات الجريمة الإلكترونية، المرجع السابق 2012، ص، 54

اساليب البحث والتحري التقليدية، والتي لم تعد كافية وفعالة للكشف عن الجرائم المستحدثة، والتي من بينها الجرائم الإلكترونية .[1]

ويقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الاشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك ويلجأ إلى هذا الاجراء عادة عندما تقتضي عملية التحري أو التحقيق في إحدى الجرائم المذكورة في ق إ ج .

الفرع الثاني: إثبات الجريمة الإلكترونية بالشهادة والاعتراف

سنقوم في هذا الفرع بدراسة إثبات الجريمة الإلكترونية بكل من الشهادة والاعتراف كل على حدى .

أولا: إثبات الجريمة الإلكترونية بالشهادة :

تعرف الشهادة بصفة عامة على أنها الإدلاء بمعلومات متعلقة بالجريمة من طرف الشاهد، أمام سلطة التحقيق، فحدوثها أمام هذه السلطة بالشكل القانوني هو الذي يضفي عليها صفة إجراءات التحقيق، وللمحقق أن يسمع شهادة من يرى لزوم سماعه من الشهود عن الوقائع التي تثبت أو تؤدي لثبوت الجريمة، وظروفها وإسنادها للمتهم أو براءته منها[2].

فهي في الأصل اختبار الشخص بما قد يكون رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه، فهي دليل مباشر في الدعوى، وعلى العموم هي ترجع إل تقدير قاضي الموضوع فيما يخص الأخذ بها من عدمه .

---

[1]– مهدي شمس الدين، النظام القانوني للتسرب في القانون الجزائري، مذكرة لنيل شهادة الماستر في الحقوق، جامعة محمد خيضر، بسكرة 2013 ص 37 .

[2]– أحمد المهدي، أشرف الشافعي: **التحقيق الجنائي الابتدائي وضمانات المتهم وحمايتها**، دار الكتب القانونية، مصر، 2000 ص 95

فالشهادة من أقدم وأبرز وسائل الإثبات وتحصيل الأدلة، فهي موجودة في كل تشريع إجرائي، نظرا للأهمية الكبيرة لها في مجال الإثبات الجنائي، وهذا راجع لطبيعة الجريمة التي تعتبر تصرف غير قانوني ليس من الممكن في الغالب إثباته بالكتابة، فالجاني يكب كل جهده حتى يخفي الجرم المقترف، وكثيرا ما يكون للسهادة أثناء جمع الاستدلالات أو التحقيق الابتدائي الأثر الكبير في الحكم بالإدانة أو البراءة .

وفي نطاق الجريمة الإلكترونية أيضا لشهادة أهمية كبيرة بصفة عامة، إلا أن الشاهد فيما يتعلق بالجريمة الإلكترونية الأمر مختلف، وهذا باعتبار أن الشاهد الإلكتروني مختلف في

صفته عن غيره من الشهود في الجرائم التقليدية، ومنه سيكون تركيز الحديث عن الشاهد الإلكتروني من خلال الآتي .

أ –تعريف الشاهد الإلكتروني :

إن الشاهد في الجريمة الإلكترونية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسوب، والذي تكون لديه جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله ويطلق على هذا النوع من الشهود مصطلح الشاهد الإلكتروني [1] .

فهو ذلك الشخص الذي يقرر أمام القضاء أو سلطة التحقيق ما يكون قد رآه أو سمعه أو أدركه على وجه العموم بحواسه، ويختلف الخبير عن الشاهد في أن الأخير يقدم إلى القاضي معلومات حصلها بالملاحظة الحسية، أما الخبير فإنه يقدم إلى القاضي تقارير وآراء توصل إليها بتطبيق قوانين علمية أو فنية.

[1] – علي عدنان الفيل: المرجع السابق، ص، 62.

فالشاهد الإلكتروني إذا تكون لديه خبرة وتخصص فيما يتعلق بتقنيات الكمبيوتر وعلومه، فالاختلاف الجوهري فيه عن الشاهد في الجرائم التقليدية، هو في صفته .

طوائف الشاهد الإلكتروني: فالشاهد الإلكتروني بمفهومه يشمل عدة طوائف:

القائم على تشغيل الحاسوب الآلي :

وهو المسؤول عن تشغيل الحاسوب الآلي والمعدات المتصلة به ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح، في إدخال البيانات كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج [1] .

المبرمجون:

وهم الأشخاص المتخصصون في كتابة البرامج، ويمكن تقسيمكم لفئتين، الفئة الأولى تتمثل في مخططي برامج التطبيقات، والفئة الثانية تتمثل في المخططين .

حيث يقوم مخطط وبرامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أما مخطط وبرامج النظم فيقومون باختيار وتعديل وتصحيح برامج نظام الحاسوب الداخلية، أي أنه يقوم بالوظائف الخاصة بتجهيز الحاسوب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج، ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج .

المحللون:

المحلل هو الشخص الذي يحلل الخطوات، ويقوم بتجميع بيانات نظام معين ودراستها وتحليلها، وذلك بتقسيم النظام إلى وحدات، واستنتاج العلاقات الوظيفية من تلك

---

[1] – عائشة بن قارة مصطفى: المرجع السابق، ص، 127.

الوحدات، كما يقوم بتتبع البيانات داخل النظم عن طريق ما يسمى بمخطط تدفق البيانات وإضافة على ذلك القيام باستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسوب [1] .

مهندسو الصيانة والاتصالات:

وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسوب بمكوناته وشبكات الاتصال المتعلقة به.

مديرو النظم:

وهم الذين توكل إليهم الأعمال الخاصة بالإدارة في النظم المعلوماتية .

بالإضافة إل ى هذه الفئات هناك أشخاص آخرون يعتبرون بمثابة الشهود في الجريمة الإلكترونية، ولهم دور كبير في توصيل المستهلك إلى شبكة الإنترنت، من بينهم مقدمو الخدمات الوسطية في مجال المعلوماتية والإنترنت، أيضا متعهدو الوصول ومتعهدو الإيواء والمسؤولين عن نقل المعلومات والمسؤولين عن متعهد الخدمات، كذلك مورد المعلومات.

ثانيا: إثبات الجريمة الإلكترونية بالاعتراف والإقرار

لم يستقر الفقه القانوني على رأي واحد في تحديد معنى الإقرار والاعتراف في المفهوم الاصطلاحي، فقد عرفه البعض بانه إقرار المتهم على نفسه بارتكاب الوقائع المكونة للجريمة كلها أو بعضها من خلال اقرار المتهم بكل أو بعض الوقائع المنسوبة إليه.

وهناك من وضع تعريقا يشمل شروط صحة الإقرار القانوني يعني الإقرار على النفس بحرية وإدراك بإرتكاب الأفعال المكونة للجريمة أو بعضها دون تأثير أو إكراه .

1 – خالد ممدوح إبراهيم: المرجع السابق، ص، 264.

ومن خلال ما سبق، يمكن القول أن الإقرار يقصد به إقرار المرء على نفسه فيما نسب إليه، وقد عرف سيد الأدلة في المواد الجزائية ولا يؤثر في الإقرار أن يرد مجملا، إذ لا يشترط أن يكون مفصلا شاملا كافة ظروف الجريمة ودوافعها، والعوامل التي أثرت في تكوينها، فإذا جاء الإعتراف مجملا فإنه يكون صحيحا طالما كان دالا على ارتكاب الجريمة .

إقرار المتهم إما يكون شفهيا إما مكتوبا، أي منهما كاف في الإثبات ويمكن تقسيم الإقرار إلى عدة أنواع وهي كما يلي:

الإقرار القضائي: وهو الإقرار الذي يصد ر أمام المحكمة التي تنظر الدعوى الجنائية بالفعل، ويجيز هذا الإقرار للمحكمة الإكتفاء به والحكم على المتهم بغير سماع الشهود، فيبدئ التحقيق في الجلسة بالمناداة على الخصوم والشهود

الإقرار غير القضائي: وهو الإقرار الذي يصدر خارج المحكمة التي تنظر الدعوى الجزائية، فإذا صدر الاقرار الجزائي في تحقيق النيابة أو أمام إحدى جهات التحقيق يعتبر إعتراف غير قضائي .

ويعتبر الإقرار غير قضائي الإقرار الذ يرد ذكره في التحقيقات نقلا عن أقوال منسوبة إلى المتهم خارج مجلس القضاء .[1]

الفرع الثالث: إثبات الجريمة الإلكترونية بالخبرة الفنية :

إن الاستعانة بالخبراء تعتبر من بين الإجراءات التي يلجأ إليها القضاة وسلطة التحقيق على حد السواء، وذلك كلما استعصى عليهم فهم موضوع معين يتميز بالتقنية ومن بين المجالات التي تستدعي اللجوء إل الخبرة الحصول على الدليل الإلكتروني،

[1] – جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية القاهرة 2011 ص 70 .

حيث أنه لا يستطيع التعامل مع هذا النوع من الأدلة إلا شخص ذودراية وخبرة في مجال تقنيات الحاسوب وشبكاته .

فالخبرة هي وسيلة لتحديد التفسير الفني للأدلة عن طريق الاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا عن الدليل المادي وإنما تقييم فني لهذا الدليل .

وإذا كانت الخبرة مهمة في الجرائم التقليدية، فإن أهميتها تصبح أكبر في سبيل الحصول على الدليل الإلكتروني لإثبات الجرائم الإلكترونية، وهذا لأنها تتعلق بأدلة فنية غاية في التعقيد ومحل الجريمة فيها في الغالب غير مادي، والتطور فيها سريع ولهذا لا يستطيع كشف غموضها إلا متخصص، وهذا ما يسمى بالخبرة التقنية التي تعتبر أقوى مظاهر التعامل القانوني والقضائي مع تكنولوجيا المعلومات .

يقصد بالخبرة: " مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرا إلى معرفة فنية أو دراية علمية لا تتوافر لديه " [1]

فهي بحث في المسائل المادية أو الفنية التي يصعب على المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات .

كما يعرف الخبير الإلكتروني بأنه الشخص الذي تعمق في دراسة الأعمال الإلكترونية، وتخصص في أدائه فترة زمنية طويلة مما أكسبه خبرة عملية، بحيث أصبح ملما بتفصيلاته مما جعله متفوقا على الشخص العادي، وجعله قادرا على إبداء الرأي الإلكتروني في الأمور المتصلة بهذا العمل، ويشترط في هذا الخبير أن يكون لديه المؤهل

[1] – صغير يوسف **(الجريمة المرتكبة عبر الإنترنت)**، ماجستير، منشورة، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، الجزائر، 2013، ص، 88.

العلمي والخبرة العلمية، إلا أن الشخص الذي يعمل في هذا المجال لمدة طويلة من الزمن وأصبح يتقن القواعد الفنية يمكن اعتباره خبيرا حتى وإن لم يتوفر فيه الجانب العلمي، عكس الذي يكون لديه المؤهل العلمي ولا يزاول هذه المهنة فلا يستطيع أن يكون خبيرا .

وعلى الخبراء الذين تكون لهم علاقة بالتحقيق الجنائي الإلكتروني أن يكونوا على معرفة بلغات البرمجة وأنظمة التشغيل الجديدة، وكذا تصميم البرامج وتشغيلها ومعرفة الجديد منها، وكذلك تحليل البرامج أو أنظمة التشغيل، وأيضا أن يؤمن بوجود أشخاص آخرين مثله لديهم القدرة على اختراق الشبكة .[1]

[1] – مصطفى محمد موسى، المرجع السابق، ص، 221، 222.

المبحث الثالث: حجية الدليل الرقمي في الإثبات الجنائي :

يخضع الدليل الإلكتروني كباقي الأدلة الجنائية للقواعد المقررة لباقي الأدلة فيما يخص حجيته، من حيث قبوله على مستوى أنظمة الإثبات الجنائي، سواء تعلق الأمر بنظام الإثبات الحر أوالمقيد أو المختلط، وفيما يتعلق بسلطة القاضي في قبول هذا النوع من الأدلة وتقديره والإقتناع به، وهذا بإعتبار أن القاضي لا يقدر إلا الدليل المقبول، وهذا على مستوى القضاء الجنائي .[1]

ولدراسة هذا الأمر نقسم مبحثنا إلى مطلبين: المطلب الأول: حجية الدليل الرقمي على ضوء نظم الأدلة الجنائية، أما المطلب الثاني: حجية الدليل الرقمي أمام القاضي الجزائي .

المطلب الأول: حجية الدليل الرقمي على ضوء نظم الأدلة الجنائية

إن أنظمة الإثبات الجنائي تعتبر ركيزة لا غنى عنها في مجال الإثبات الجنائي، باعتبار أنها أول من وضع قواعد وركائز الإثبات الجنائي .

فنظام الإثبات الجنائي المقيد كان يقوم على تقييد سلطة القاضي الجنائي، بوضع الأدلة من قبل المشرع وما على القاضي الجنائي إلا رؤية مدى توفر هذه الأدلة والأخذ بها، دون تدخل من قبله، فدور القاضي كان سلبيا بحتا، ولا يخرج عن نطاق تطبيق القانون وما جاء به القاضي دون زيادة أو نقصان عن ما جاء به المشرع . وهذا ما سنتطرق إليه من خلال ما يلي:

---

[1] – أمنة هلال، الإثبات الجنائي بالدليل الإلكتروني، مذكرة مكمل لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، ك لية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر بسكرة، سنة 2014-2015 ، ص 72 .

الفرع الأول: حجية الدليل الرقمي في نظام الإثبات المقيد :

إن نظام الإثبات المقيد بصفة عامة هو ذلك النظام الذي يطلق عليه نظام الأدلة القانونية، أو نظام الإثبات المحدد، بمعنى آخر أن المشرع هو الذي يحدد فيه الأدلة مسبقا، والقاضي بدوره لا يجوز له أن يخرج عن هذه الأدلة المحددة من قبل المشرع [1].

فالقاضي دوره في هذا النظام يظهر كمطبق للقانون، بمراعاة توافر الدليل أو شروطه، حيث أنه إذا لم تكن هذه الشروط والشكل المطلوب من القانون للدليل، فإن القاضي لا يستطيع أن يحكم على أساسه، كما أنه لابد أن يصرف النظر عن اقتناعه الشخصي حتى ولو اقتنع يقينيا بما هو متوفر أمامه [2].

فهذا النظام يحدد طرق الإثبات الجائز قبوله أمام القضاء، كالكتابة والبينة والقرائن، فالقانون يحدد الطريقة التي يتم بها إثبات الحق، كما أنه لا يجوز للخصم إثبات الحق الذي يدعيه بأي طريقة أخرى، وعلى القاضي أن يتقيد بطرق الإثبات التي يفرضها عليه القانون، ويلتزم بها وبالقيمة التي يعطيها القانون لكل دليل من أدلة الإثبات، فالقاضي في ظل هذا النظام دوره سلبي تماما يقتصر على تقدير ما يقدمه الخصوم من أدلة قانونية، وليس له أن يكمل الأدلة إذا كانت ناقصة [3] .

---

[1]- بن فردية محمد، " **الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي** "، مقال في المجلة الأكاديمية للبحث القانوني، الصادر عن كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة عبد الرحمان ميرة، بجاية، الجزائر، عدد 2014، جانفي، 2014، ص، 287.

[2]- مروك نصر الدين: **محاضرات في الإثبات الجنائي**، دار هومة للطباعة النشر والتوزيع، الطبعة الثالثة، الجزء الأول، الجزائر، 2009، ص، 56.

[3]- محمد حسين منصور: **قانون الإثبات**، دار الجامعة الجديدة للنشر، مصر، 2002، ص، ص، 08، 09.

الفرع الثاني: حجية الدليل الرقمي في نظام الإثبات الحر

إن نظام الإثبات الحر جوهره يتمثل في أن الاقتناع الشخصي هو وحده الذي يتحكم في قرار القاضي الجنائي، وهذا الاقتناع بدوره من اللزوم أن يصدر بكل حرية من ضمير القاضي، الذي يجب أن يكون حرا من ناحية إختيار الدليل من جهة، وكذا أن يكون حرا في تقييم هذا الدليل من جهة أخرى .

بصفة عامة نظام الإثبات الحر يكرس مبدأ حرية القاضي في الاقتناع، بمعنى أن القاضي حر في تكوين عقيدته من أي دليل يراه يقينيا ويقتنع به .

فهذا النظام لا يحدد طرقا معينة للإثبات، وإنما يكون للخصوم حرية كاملة في إختيار الأدلة المؤدية إلى اقتناع القاضي ومساعدته في الوصول إلى الحقيقة، دون التقيد بطرق محددة، فالقاضي في هذا النظام له دور إيجابي في تسيير الدعوى وتكوين الأدلة والحكم بناءا على ما يصل إليه من حقائق.

وفيما يتعلق بالدليل الإلكتروني فإن التشريعات التي تأخذ بهذا النظام لم تفرد نصوصا خاصة فيما يتعلق بقبول هذا الدليل، على أساس أن هذه التشريعات تستند لمبدأ حرية الإثبات في المسائل الجنائية، هذا المبدأ الذي يمثل أساس نظام الإثبات الحر، فمن خصائص هذا النظام عدم تحديد الأدلة، وكذا حرية القاضي في الأخذ بالأدلة وتقييمها وهذا ما يبين أن القاضي الجنائي يمكنه أن يستند إلى الدليل الإلكتروني لإثبات الفعل الجنائي في سائر الجرائم بصفة عامة، والجرائم الإلكترونية بصفة خاصة في ظل هذا النظام .

في نظام الإثبات الجنائي الحر لا يتم تحديد طرق معينة للإثبات، وتترك الحرية لأطراف الدعوى لتقديم إثباتاتهم إلى قاضي الموضوع، حيث يمكن للأطراف تقديم أدلة

كتابية أو شهادات شهود وغيرها من الأدلة، والقاضي بدوره يتولى فحصها وتقييمها ومن ثم إصدار حكمه وفقا للقناعة التي يتوصل إليها من تلك الأدلة [1] .

فالأدلة في ظل هذا النظام لا تكون محددة مسبقا، ولا وجود لأدلة يفرض على القاضي قبولها مقدما، والمشرع يقتصر دوره على تحديد الشروط اللازمة لصحة الدليل، وأيضا كيفية تقديمها، وهذا كلها ضمانا للحرية الفردية وكفالة لحسن سير العدالة، وللقاضي أن يتخذ أي إجراء يراه ضروريا ومناسبا للفصل في الدعوى (1) .

وبالنسبة للمشرع الجزائري فقد أقر بمبدأ حرية الإثبات الجنائي في المادة 212 ق.إ.ج التي جاء في فحواها: " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه " [2] .

فالمشرع الجزائري من الواضح في هذه المادة أنه يكرس مبدأ حرية الإثبات الجنائي أمام جهات الحكم، وهذا لا يدع شكا في تطبيق هذا المبدأ أمام كل الجهات القضائية .

وهناك عدة أسباب تجعل من الضروري العمل بهذا المبدأ في مجال الإثبات الجنائي، فحرية الإثبات تعد نتيجة منطقية لمبدأ قضاء القاضي بمحض اقتناعه، وهذا الأمر يترتب عليه السماح للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع ويطمئن إليها القاضي .

[1] – سامي جلال فقي حسين: المرجع السابق، ص، 75.

[2] – المادة 212 من قانون الإجراءات الجزائية الجزائري.

كما أن الإثبات في الدعوى الجنائية يكون على وقائع قانونية سواء كانت مادية أو معنوية، مما يصعب الحصول على دليل مسبق لهذه الوقائع، عكس الدعوى المدنية التي يسهل الحصول على دليل مسبق لوقائعها.

بالإضافة إلى أن حرية الإثبات يعد بمثابة إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية في مواجهة الجرائم المستحدثة، ومنها الجريمة الإلكترونية، وفتح المجال أمام الأدلة الحديثة للاستفادة من الوسائل العلمية الحديثة للكشف عن الأدلة ومنها الأدلة الإلكترونية.

وكذا طبيعة المصلحة التي تحميها الدعوى الجنائية تختلف عن المصلحة التي تحميها الدعوى المدنية، فالأولى في غالب الأحيان تتعلق بمصلحة المجتمع في أمنه واستقراره، أما الدعوى المدنية فالمصلحة فيها تتعلق بأفرادها، ومن المسلم به أن قرينة البراءة تقر بأن عبء الإثبات يقع على عاتق سلطة الإتهام، وهذا خلق صعوبة في مهمة هذه السلطة، هذا ما جعل من الضروري تسهيل مهمتها بإقرار مبدأ حرية الإثبات .

وعلى ذلك فإن الدليل الإلكتروني شأنه شأن الأدلة الأخرى، فهو مقبول مبدئيا في الإثبات الجنائي بصفة عامة، والإثبات في مجال الجرائم الإلكترونية بصفة خاصة، بشرط أن يتم الأخذ في عين الإعتبار ضابط المشروعية، فالحرية في هذا النظام لا تعني الإعتماد على وسائل غير قانونية، فحرية الأطراف في مجال الإثبات مقيدة بضوابط المشروعية التي لا يجب أن تخالف، وإلا ترتب على هذه المخالفة عدم مشروعية الدليل ومنه عدم قبول الدليل وبطلانه[1].

[1] – عائشة بن قارة مصطفى: المرجع السابق، ص – ص، 187 – 189.

الفرع الثالث: حجية الدليل الرقمي في نظام الإثبات المختلط

إن نظام الإثبات المختلط بصفة عامة هو النظام التوفيقي، أي النظام الوسط بين نظام الإثبات المقيد ونظام الإثبات الحر، حيث تتراوح أحكامه بين التقييد والإطلاق [1].

فهذا النظام يسعى إلى الجمع بين مفهومي كل من نظام الإثبات المقيد وكذا الحر للوصول إلى الحقيقة القضائية، وكذا محاولة التوفيق بينهما، أي إعمال كلا من النظامين معا .

فحتى يتسنى للقاضي إصدار حكمه ليكون حكما صحيحا وقويا لا بد عليه في هذا الإطار أن يكون اقتناعه اقتناعا شخصيا من جهة، أي تكون له الحرية في الأخذ بالدليل وبناء اقتناعه على أساس

شخصي ودون أي قيود، بالإضافة إلى أنه يجب عليه أن يحوز القناعة القانونية كما أقرها المشرع من جهة أخرى، أي يأخذ في عين الإعتبار ما جاء به المشرع وما تم النص عليه في القانون[2].

فهذا النظام يتجنب ما وجه من انتقادات إلى نظام الإثبات الحر من خشية تعسف القاضي الجنائي، وخروجه عن الصواب، وهذا عن طريق تحديد طرق الإثبات التي يعتمد عليها.

وكذلك تجنب الانتقادات التي وجهت لنظام الإثبات المقيد الذي يجعل دور القاضي سلبيا في عملية الإثبات، وهذا عن طريق إعطاء القاضي الجنائي الحرية في تقدير ما يعرض عليه من أدلة ثبوتية في الدعوى المعروضة عليه، وأبرز نموذج لنظام الإثبات المختلط هو الذي اقترحه "روبسبير" في إجتماع الجمعية التأسيسية الفرنسية عام 1791،

---

1 – سامي جلال فقي حسين، المرجع السابق، ص، ص، 79، 80.

2 – المرجع نفسه، ص، 93.

الذي كان يحتوي على جزأين، حيث تمثل الجزء الأول في عدم الحكم بالإدانة على المتهم إذا لم تتوفر ضده أدلة حددها القانون، أما الجزء الثاني فهو عدم الحكم بالإدانة على المتهم حتى وإن توافرت الأدلة القانونية ما لم تحقق قناعة القاضي .

ومن التشريعات التي أخذت بهذا النظام القانون الإجرائي الياباني الذي حدد سلفا أدلة ووسائل الإثبات، وأيضا أخذ بقاعدة الاقتناع الذاتي للقاضي [1] .

وفيما يخص الدليل الإلكتروني سيكون التكلم عنه في ظل مبادئ نظام الإثبات المختلط، وكذا حجيته في هذا النظام .

المطلب الثاني: حجية الدليل الرقمي أمام القضاء الجزائي

إن الدليل الإلكتروني كغيره من الأدلة الجنائية مأخوذ به أمام القضاء الجنائي، والقاضي يستند إلى هذا الدليل في العديد من القضايا خاصة في الجرائم الإلكترونية .

كما أن التطور التكنولوجي الحاصل في الوقت الراهن حتم على القضاء الجنائي أن يأخذ بهذا النوع من الأدلة المستحدثة، بالإضافة إلى أن القاضي الجزائي حر في الأخذ بالأدلة الإلكترونية، خاصة فيما يتعلق بالجرائم الإلكترونية .

والدليل الإلكتروني من الوجوب أن يكون مقبولا في الإثبات الجنائي، وأمام القضاء الجنائي باعتبار أنه دليل ذو مصداقية كبيرة، وهذا راجع لطبيعته العلمية والتقنية، وهذا ما يحتم على القضاء الجزائي أن ينظر في موضوع الأخذ بالدليل الإلكتروني، ويعطي له الحجية والقوة الثبوتية اللازمة، آخذا في عين الإعتبار أهمية هذا الدليل في إثبات العديد من الجرائم بصفة عامة، والجرائم الإلكترونية بصفة خاصة فالقاضي الجنائي بالنظر للتطور التكنولوجي الحاصل، يجد نفسه مضطرا إلى النظر في موضوع الدليل الإلكتروني

[1]– سامي جلال فقي حسين، المرجع السبق، ص، 95.

ولهذ سلطة القاضي الجزائي في قبول الدليل ا فإننا في سبيل دراسة الدليل الإلكتروني، من ناحية حجيته أمام القضاء الجنائي، الممثل بدوره في القاضي الجزائي، سنتناول ما يلي:

سلطة القاضي الجزائي في قبول الدليل الرقمي في الفرع الأول وبعدها ضوابط قبول وإقتناع القاضي الجزائي بالدليل الرقمي في الفرع الثاني واخيرا مشكلات الدليل الرقمي واثرها على الاقتناع الشخصي للقاضي الجنائي في الفرع الثالث .

الفرع الأول: سلطة القاضي الجزائي في قبول الدليل الرقمي

سنتطرق في هذا الفرع الى ما يلي:

أولا : حرية القاضي الجنائي في القبول والاقتناع بالدليل الإلكتروني

يقول الفقيه بيكاريا في مؤلفه الشهير الجرائم والعقوبات : " إن فكرة اليقين الذاتي المطلوبة في المواد الجزائية لا يمكن أن تتقيد بقواعد إثبات محددة سلفا تسلبها حقيقة مضمونها، ولا يمكن الوصول إلى الحقيقة بجزم ويقين إذا انحصر القاضي في دائرة مغلقة من الأدلة التي يحددها القانون "[1].

فحرية القاضي الجنائي بصفة عامة هي ما يتمتع بها القاضي الجنائي من اختيار النشاط الذهني الذي يسلكه بغية الوصول إلى حل ما يطرح عليه من قضايا [2] .

فالقاضي الجنائي له الحرية في تقدير قيمة كل دليل طبقا لقناعته القضائية، وله من خلال هذا التقدير أن يستقي هذه القناعة من أي دليل يطمئن له، ولا يلزمه المشرع

---

[1]- العربي شحط عبد القادر، نبيل صقر: الاثبات في المواد الجزائية، دار للهدى للنشر والتوزيع، الجزائر، ص، 22، 23.

[2]- محمد علي الكيك: **السلطة التقديرية للقاضي الجنائي**، دار المطبوعات الجامعية، مصر، 2007، ص، 28 .

بحجيته المسبقة، كماله طرح الأدلة التي لا يطمئن إليها، وله في النهاية سلطة التنسيق بين الأدلة المعروضة عليه [1].

والدليل الإلكتروني بدوره خاضع للمبدأ العام في الإثبات الجنائي، وهو حرية القاضي الجنائي في الاقتناع، وحريته في هذا الشأن بالغة الأهمية، باعتبار أن القاضي الجنائي هو وحده الذي يقدر قيمة الدليل الإلكتروني، وهذا تبعا للأثر الذي يحدثه في وجدانه من إرتياح ومن جهة أخرى نجد أن دور الإثبات العلمي أصبح له أهمية كبيرة، خاصة مع ظهور الدليل الإلكتروني المطلوب للإثبات في الجرائم الإلكترونية، بسبب إضطرار القاضي إلى التعامل مع هذا النوع من الأدلة الضرورية لكشف نوع جديد من الجرائم، وهذا مع وجود عائق نقص الثقافة المعلوماتية، وهذا الأمر تنجر عنه عدة مشاكل خاصة فيما يتعلق بالدليل الإلكتروني، مما يؤدي إلى نقص قيمته من جهة، ونقص الإعتماد عليه في إثبات الجرائم الإلكترونية من جهة أخرى ولهذا فإننا سنتطرق إلى الطبيعة العلمية للدليل الإلكتروني، وأثرها على اقتناع القاضي الجنائي، كما سيكون الحديث عن مشكلات الدليل الإلكتروني، وتأثيرها على اقتناع القاضي الجنائي .

إن الطبيعة العلمية للدليل الإلكتروني لها أهمية بالغة في الإثبات الجنائي، والميزة الأساسية له، ولذلك قبل كل شيء لابد من معرفة معنى الاقتناع القضائي، أو الاقتناع الوجداني، حيث يبنى الوجدان الخالص للقاضي الجزائي على الحق المخول له في ممارسة عملية الإثبات وهذا عن طريق تقدير ما إذا كانت الأدلة المطروحة في ملف القضية، تقوم على نسبة الفعل الإجرامي للشخص الذي شكك في أمره، أم أنها مقتصرة على إثبات ذلك واستيفاء كل الطرق المؤدية إلى جمع وسائل الإثبات المطلوبة لإظهار الحقيقة .

---

[1]– فاضل زيدان محمد: **سلطة القاضي الجنائي في تقدير الأدلة**، دار الثقافة للنشر والتوزيع ، الطبعة الأولى، الأردن، 2006، ص، 94.

وهذا ما يجعل من سلطة القاضي الجنائي في الإثبات الجنائي، أساسا لتكوين وجدانه الضروري للحكم في القضية المطروحة أمامه، وفق آليات معينة ومضبوطة [1] .

وبالنسبة لمعنى الاقتناع القضائي فقد اختلفت الاتجاهات الفقهية في تحديد المدلول القانوني للقناعة القضائية، إلا أنها تتفق على أنها تعني بأن القاضي بإمكانه أن يستحضر عقيدته من أي دليل يراه مناسبا ويطمئن إليه، وهذه الأدلة قد تكون من طرف الخصوم أو النيابة العامة أومن القاضي بنفسه، والتي عن طريقها تتكون قناعة هذا القاضي، والجدير بالذكر أن هذه الحرية الممنوحة للقاضي الجنائي ليست بهدف توسيع سلطته، وإنما لصعوبة الحصول على الدليل في المواد الجزائية خاصة فيما يتعلق بالأدلة العلمية، ومنها الدليل الإلكتروني .

وهذا المبدأ تم النص عليه لأول مرة من طرف المشرع الفرنسي الذي أقر بأن القضاة لا يحاسبون على الأدلة التي اقتنعوا بها، كما نص على أن هذا المبدأ يطبق أمام جميع الجهات القضائية الجنائية [2].

أما المشرع الجزائري فقد كرس مبدأ الاقتناع القضائي في المادة 307 من قانون الإجراءات الجزائية، وهي مستوحاة من المادة 353 من القانون الفرنسي .

كما أن المشرع الجزائري كرس مبدأ الاقتناع القضائي صراحة في المادة 212 من قانون الإجراءات الجزائية التي جاء في فحواها أنه من الجائز إثبات الجرائم بأي طريقة في الإثبات الجنائي، كما أنه للقاضي أن يصدر حكمه بناءا على اقتناعه الخاص،

---

[1]– برهان عزيزي، **إثبات الجريمة في أحكام مجلة الإجراءات الجزائية**، مجمع الأطرش للكتاب المختص، الطبعة الأولى، تونس، 2013، ص، 77.

[2]– فاضل زيدان محمد، المرجع السابق، ص، ص، 106، 107.

بالإضافة إلى أن المحكمة العليا أكدت على ضرورة مراعاة مبدأ الاقتناع القضائي، وتوصي بإعماله أمام المحاكم الجنائية [1] .

وبالنسبة لنطاق مبدأ الاقتناع القضائي فقد ثار خلاف حوله، فهناك من يرى أن هذا المبدأ يمتد إلى كافة أنواع المحاكم الجنائية، أي محاكم الجنايات والجنح والمخالفات، والمشرع الجزائري لم ينص صراحة على هذا الأمر بخلاف المشرع الفرنسي الذي نص عليه .

وهناك من يرى أن مبدأ الاقتناع القضائي وجد أصلا ليطبق أمام قضاء الحكم، ولكن هذا لا يعني أن نطاق تطبيقه مقتصر فقط على هذه المرحلة، وإنما يشمل أيضا مرحلة التحقيق الإبتدائي، فقضاة التحقيق والإحالة بدورهم يقدرون مدى كفاية الأدلة أو عدم كفايتها للاتهام، ويخضعون في سبيل هذا الأمر لضمائرهم واقتناعهم الذاتي فحسب[2].

وبالنسبة للدليل الإلكتروني وموقعه من هذا المبدأ، يتحتم علينا التكلم أولا عن قيمة الدليل الإكتروني كدليل علمي، ثم التطرق إلى تقدير القضاء للدليل العلمي .

أ – قيمة الدليل الإلكتروني كدليل علمي:

إن الدليل الإلكتروني لا تختلف قيمته ولا تزيد حجته عن غيره من الأدلة، وهذا من آثار إعمال مبدأ حرية القاضي الجنائي في الاقتناع، ومنه فإن القاضي الجنائي يستطيع أن يبني اقتناعه على الدليل الإلكتروني، كما يستطيع إبعاده وبالتالي لا يجوز إجبار القاضي على الاقتناع بالدليل الإلكتروني حتى وإن لم تكن هناك أدلة غيره .

---

[1]– عائشة بن قارة مصطفى، حجية الدليلي الإلكترونية في مجال الإثبات الجنائي، المرجع السابق، ص، 242، 243.

[2]– المرجع نفسه، ص، 244، 245.

وتجدر الإشارة إلى أن الفقه الفرنسي تطرق إلى حجية مخرجات الكمبيوتر في المواد الجنائية وهذا في مسألة قبول الأدلة المتحصلة من الآلة العلمية، وأقر بأن لها قيمة الأدلة الأخرى وبالتالي يمكن الإطمئنان إليها وتصلح للإثبات أمام القضاء الجنائي [1] .

كما أن أغلب التشريعات ذات الأصل اللاتيني وإن كانت تتفق حول قبول الدليل الإلكتروني، استنادا إلى قاعدة الاقتناع الحر للقاضي الجنائي، إلا أنها تختلف في طريقة تقديم هذا الدليل أمام المحكمة .

وبما أن الدليل الإلكتروني تطبيق من تطبيقات الدليل العلمي، ويتميز بالموضوعية والحياد والكفاءة، مما يجعل اقتناع القاضي الجنائي أكثر جزما ويقينا، وهذا الأمر يؤدي إلى التقليل من الأخطاء القضائية، والتوصل بدرجة كبيرة نحو الحقيقة .

وهذه الصفات التي يتمتع بها الدليل الإلكتروني، تؤدي إلى الاعتقاد بأنه بمقدار اتساع مساحة الأدلة العلمية، ومن بينها الدليل الإلكتروني، بمقدار ما يكون نقص في دور القاضي الجنائي في التقدير، خاصة أمام نقص الثقافة الفنية للقاضي، حيث يصبح الدور الكبير للخبير الذي يسيطر على العملية الإثباتية، وهذا الأمر لا يثير مشكلة كبيرة خاصة إذا قلنا بأن نظام الإثبات السائد يقوم على التوازن بين الإثبات العلمي من جهة، والاقتناع القضائي من جهة أخرى، حيث يتم العمل بالإثبات العلمي في إطار مبدأ الاقتناع القضائي[2] .

---

[1]– عائشة بن قارة مصطفى، حجية الدليلي الإلكترونية في مجال الإثبات الجنائي، المرجع السابق، ص، 246.

[2]– المرجع نفسه، ص، 247، 248

ب-تقدير القضاء للدليل العلمي :

إن الدليل العلمي يخضع لتقدير القاضي الجنائي، وبالتالي فهو يخضع لاقتناعه، ومنه فهذا الدليل يخضع لأمرين مهمين هما القيمة العلمية للدليل الإلكتروني كما سبق ذكرها، والأمر الثاني هو الظروف والملابسات التي وجد فيها هذا الدليل .

فتقدير القاضي لا يتناول الأمر الأول، لأن قيمة الدليل تقوم على أسس علمية دقيقة، بمعنى أنها لا حرية للقاضي في مناقشة الحقائق العلمية الثابتة، أما الظروف والملابسات التي وجد فيها الدليل، فإنها تدخل في نطاق تقديره الذاتي، فهي من صميم وظيفته القضائية، بحيث يكون في مقدوره أن يطرح مثل هذا الدليل رغم قطعيته، إذا تبين بأنه لا يتفق مع ظروف الواقعة وملابساتها، حيث تولد الشبهة لدى القاضي، ومن ثم يقضي في إطار تفسير الشك لصالح المتهم .

فمجرد توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أو البراءة، دون بحث الظروف والملابسات، فالدليل العلمي ليس آلية معدة د لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة، بل هو دليل إثبات قائم على أساس من العلم والمعرفة وللقاضي النظر إليه على ضوء الظروف والملابسات المحيطة بالواقعة التي ينظر فيها القاضي الجنائي [1] .

الفرع الثاني: مشكلات الدليل الرقمي وأثرها على اقتناع القاضي

إن الدليل الإلكتروني يثير العديد من المشكلات، وهذه المشكلات تتعلق بطبيعته التكوينية من جهة، وبإجراءات الحصول عليه من جهة أخرى، وهذه المشكلات تنقص من حجيته في مجال الإثبات الجنائي إن لم يتم إيجاد حلول لها، وسيكون الحديث عن هذه المشكلات من خلال التطرق إلى المشكلات الموضوعية، وكذا المشكلات الإجرائية .

[1] - فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، دار الفكر والقانون للنشر والتوزيع مصر، سنة 2000 ص، 596، 597.

أولا: المشكلات الموضوعية للدليل الإلكتروني:

وهي في الغالب تتعلق بطبيعة الدليل الإلكتروني في حد ذاته، وهذا بسبب الخصائص التي يتميز بها هذا الدليل وهي كالآتي .

أ- الدليل الإلكتروني غير مرئي:

فهذا الدليل هو عبارة عن سجل كهرومغناطيسي مخزن في نظام حاسوبي في شكل ثنائي، وبطريقة غير منظمة، فمثلا تتضمن الأقراص الصلبة مزيجا من بيانات مختلطة فيما بينها، والتي لا تكون كلها ذات صلة بالمسألة المطروحة بمعنى اختلاط الملفات البريئة مع الملفات المجرمة، وبالتالي فالدليل الإلكتروني يختلف عن الآثار المادية الناتجة عن الجرائم التقليدية التي يسهل على رجال العدالة إثباتها، بعكس الجرائم الإلكترونية، حيث أن الدليل فيها وهوالدليل الإلكتروني عبارة عن نبضات إلكترونية كما أن هذا الدليل غالبا ما يكون مشفرا ويمكن تعديله والتلاعب فيه، مما يقطع الصلة بين المجرم وجريمته، كما أنه يشكل عائقا أمام رجال التحري والتحقيق خاصة أنهم معتادون على الإثبات المادي للجرائم .[1]

ب- مشكلة الأصالة في الدليل الإلكتروني :

الأصالة في الدليل الإلكتروني لها طابع افتراضي لا يرتقي إلى مستوى الأصالة في الدليل المادي، باعتبار أن الدليل المادي ملموس، وهذه الأصالة أثارت العديد من المشكلات خاصة فيما يتعلق بالاعتداد بالنسخة التي تشكل دليلا كاملا ونجد أن موضوع الأصالة على المستوى القانوني جعل المشرع يعتمد على منطق افتراض أصالة الدليل الإلكتروني، حيث أن قانون الإجراءات الجنائية الفدرالي في الولايات المتحدة الأمريكية، نص صراحة على قبول الدليل الإلكتروني على أنه مستند أصلي وهذا كاستثناء، مادام أن البيانات قد صدرت من كمبيوتر أو جهاز مماثل له، وهذا سواء كانت هذه البيانات

[1] - فتحي محمد أنور عزت، المرجع السابق، ص، 596، 597.

مطبوعة أو مسجلة على دعامات أخرى تعبر عن البيانات الأصلية بشكل دقيق، وبهذا تتساوى الكتابة المادية من حيث الأصالة مع الكتابة عبر الحاسوب، رغم أن هذه الأخيرة مجرد نسخ للأصل الموجود رقميا في الحاسوب، أو عبر الإنترنت [1].

ج- الدليل الرقمي له طبيعة ديناميكية :

معناه أن الدليل الإلكتروني ينتقل عبر شبكات الاتصال بسرعة فائقة، ومنه إمكانية تخزين المعلومات أو البيانات في الخارج بواسطة شبكة الاتصال عن بعد، وينتج عن هذا الأمر صعوبة تعقب الأدلة الإلكترونية وضبطها، لأن هذا المشكل يستوجب القيام بإجراءات خارج حدود الدولة التي ارتكبت فيها الجريمة كتفتيش نظم الحاسوب وهذا كله يعيقه مشكل الحدود والولايات القضائية، باعتبار أن هذا النوع من الإجراءات فيه مساس بسيادة الدولة المقصودة، وهذا ما ترفضه غالبية الدول، ما تأتى عنه إبرام العديد من الاتفاقيات والمعاهدات الدولية في مجال التعاون الدولي، الذي يهدف إلى التقريب بين القوانين الجنائية، بغرض تسهيل عملية جمع هذا النوع من الأدلة العابرة للحدود لمكافحة الجرائم الإلكترونية [2] .

ثانيا: المشكلات الإجرائية للدليل الرقمي :

إن الدليل الإلكتروني له مشكلات موضوعية تؤثر على اقتناع القاضي، ولكن هناك أيضا مشكلات إجرائية لها تأثير على اقتناع القاضي الجنائي، وهي ارتفاع تكاليف الحصول على هذا الدليل من جهة، بالإضافة إلى نقص الخبرة الفنية والتقية لدى سلطات الاستدلال والتحقيق والقضاء بمجال تقنية المعلومات، وسيكون الحديث عن هاتين المشكلتين كالآتي .

[1] – عائشة بن قارة مصطفى، المرجع السابق، ص، 251، 252.

[2] – المرجع نفسه، ص، ص، 253، 254.

أ- ارتفاع تكاليف الحصول على الدليل الإلكتروني :

في مجال الدليل الإلكتروني في أغلب الأحيان يتم الإعتماد على الخبرة للتعامل مع هذا الدليل الفني المتوفر في مجال تكنولوجيا المعلومات والإنترنت، فالخبرة لها دور لا يستهان به خاصة مع نقص معرفة رجال القانون بالجوانب التقنية فيما يتعلق بالجرائم الإلكترونية، ولكن هذه الخبرة في المقابل تشكل عبئا بسبب حجم وضخامة المصاريف المتعلقة بها بغرض الحصول على الدليل الإلكتروني، فالإشكال الأساسي هنا يتعلق بطبيعة الدليل الإلكتروني وما يتطلب إثباته من تكاليف باهضة، خاصة مع غياب مؤسسات متخصصة في هذا الشأن خصوصا في الدول العربية، التي تضطر للجوء لمؤسسات أجنبية، مما يجعل التكاليف خاضعة للسعر العالمي المقرر في اللوائح المالية لهذه المؤسسات.

ب- نقص المعرفة التقنية عند رجال القانون:

إن الطبيعة الخاصة التي يتمتع بها الدليل الإلكتروني، كان لها أثر على عمل رجال القانون، سواء على مستوى التحقسق أو المحاكمة، وهذا راجع إلى أن الكشف عن الجرائم الإلكترونسة وإثباتها يستلزم استراتجيات خاصة، حيث أنه يتوجب عليهم اكتساب مهارات خاصة في سبيل مواجهة تقنيات الحاسوب وشبكاته، لما يكتسي هذه التقنيات المتعلقة بارتكاب هذه الجرائم من تعقيد، الأمر الذي يستوجب معه الإعتماد على تقنيات جديدة تتماشى مع طبيعة هذه الجرائم، وهذا بغرض معرفة نوع الجريمة المرتكبة وشخصية مرتكبها، وكيفية ارتكابها، وكذلك ضبط الجاني والحصول على الأدلة التي تدينه .

وبسبب هذا الأمر فإن الجهات المكلفة بالقبض والتحقيق تجد صعوبة كبيرة في التعامل مع هذه الجرائم عن طريق الوسائل الاستدلالية والإجراءات التقليدية، ولهذا كثيرا ما تفشل جهات التحقيق في جمع الأدلة الإلكترونية، كما أنه قد يتم تدمير الدليل عن غير قصد بسبب نقص المعرفة التقنية، ولهذا كان من الضروري إنشاء إدارة متخصصة

بهذا النوع من الجرائم والأدلة، وهوما تم فعلا، وهذا على المستوى الدولي وكذا على المستوى المحلي فعلى المستوى الدولي وبعد التأكد من أن الجرائم الإلكترونية عابرة للحدود، ولا يمكن القضاء عليها من طرف دولة واحدة، وضرورة التعاون بين الدول لمواجهة هذه الأنشطة الإجرامية المستحدثة، خلق تعاون دولي فعلا خاصة التعاون الدولي في مجال الشرطة وهو أهم تعاون في هذا الخصوص، أي مكافحة الإجرام الإلكتروني بصفة خاصة [1].

وقد تم تحقيق هذا التعاون من خلال عدة أجهزة متخصصة في هذا الشأن من أهمها المنظمة الدولية للشرطة الجنائية " الأنتربول "، التي تهدف بدورها إلى تشجيع التعاون بين أجهزة الشرطة في الدول الأعضاء، وهذا عن طريق تجميع البيانات والمعلومات التي تتعلق بالمجرم والجريمة، من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول الأعضاء، والقيام بتبادل هذه المعلومات بين الدول الأعضاء .

كما أنه توجد منظمات أخرى لا يقل دورها أهمية عن دور الأنتربول، وتهدف هي أيضا لمواجهة هذا النوع المستحدث من الجرائم على المستوى الدولي والحصول على الأدلة، مثل منظمة التعاون الإقتصادي والتنمية (OECD)، ومجموعة الثمانية الإقتصادية .

وأيضا أنشأ المجلس الأوروبي في " لوكسمبورغ " سنة 1991 شرطة أوروبية تسمى " الأوربول "، والتي تهدف هي الأخرى إلى الربط بين أجهزة الشرطة الوطنية في الدول المنظمة، وملاحقة الجناة في الجرائم العابرة للحدود، ومنها الجرائم الإلكترونية، وقد كان لها دور كبير وفعال في مكافحة هذا النوع من الجرائم، عن طريق تسهيل التحقيقات في

[1] – عائشة بن قارة مصطفى، المرجع السابق، ص، 256، 257.

هذه الجرائم، وتم إنشاء "الأورجست" من طرف الإتحاد الأوروبي بهدف التعاون القضائي خاصة فيما يتعلق بالجرائم المرتبطة بالإنترنت .

وعلــى المسـتوى العربــي قــام مجلـس وزراء الداخليــة العـرب بإنشــاء المكتــب العربـي للشـرطة الجنائيـة، الـذي يهـدف إلـى تنميـة التعـاون بـين أجهـزة الشـرطة فـي الدول الأعضاء [1] .

أما على المستوى الداخلي فقد بادرت مختلف الدول إلى إنشاء وحدات متخصصة لمكافحة الإجرام الإلكتروني على المستوى الوطني، كالولايات المتحدة الأمريكية التي قامت بإنشاء إدارة متخصصة لمتابعة الجرائم الإلكترونية في مكتب التحقيقات الفدرالي (FBI) .

وفرنسا التي قامت باتباع مخطط محكم لتحقيق الأمن المعلوماتي، أما " هونغ كونغ " فقد أسست قوة مكافحة قرصنة الإنترنت في ديسمبر 1999، وفي الصين تأسست القوة المضادة للهكرة سنة 2000، وفي الدول العربية قامت وزارة الداخلية المصيرية بإنشاء إدارة مكافحة جرائم الحاسوب وشبكات المعلومات أما فيما يخص الجزائر فلم يتم إنشاء إدارة متخصصة في مكافحة الجرائم الإلكترونية، ولكن مع ازدياد معدل الجريمة، وهذا بازدياد التقدم العلمي في المجال التكنولوجي، واستخدام الجناة للوسائل العلمية الحديثة في ارتكاب جرائمهم، اضطر المشرع الجزائري إلى تعديل قانون الإجراءات الجزائية، وذلك بموجب القانون (06 – 22)، واستحدث فيه فصلين وهما الفصل الرابع والخامس من الباب الثاني من الكتاب الأول، حيث يتمثل الفصل الرابع في" اعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور "، أما الفصل الخامس فقد جاء بعنوان " في التسرب "

---

[1]– عائشة بن قارة مصطفى، المرجع السابق، ص، 257 – 261.

ومن حيث التكوين والتأهيل في مجال مكافحة الجرائم الإلكترونية، قامت الجزائر ببعث إطارات من الدرك الوطني للتكوين والتخصص في البحث والتنقيب، وكذا ملاحقة المجرمين المعلوماتيين إلى بلدان أجنبية، كما تم استحداث شبكة اتصالات وطنية موحدة لجمع البيانات المتعلقة بشبكات الجريمة المنظمة [1] .

ومنه نقول أن الدليل الإلكتروني كغيره من الأدلة الجنائية خاضع لحرية القاضي الجنائي في الاقتناع، من خلال حريته في الأخذ به أو تركه وكذا تقديره، فالاقتناع القضائي مبدأ ذو أهمية كبيرة في الإثبات الجنائي، والدليل الإلكتروني هو الآخر يخضع لهذا المبدأ، بل إن أهمية هذا المبدأ تزيد عندما يتعلق الأمر بالدليل الإلكتروني، نظرا للطبيعة الخاصة لهذا الدليل المستحدث وصعوبة الحصول عليه.

إلا أن هذا الاقتناع من طرف القاضي الجنائي في مجال الدليل الإلكتروني يتأثر بعوامل معينة تترتب على الطبيعة الخاصة لهذا الدليل كما سبق وقلنا، خاصة التعقيد فيه فالدليل الإلكتروني كما سبق توضيحه هو دليل علمي وهذا الأمر له تأثير على اقتناع القاضي الجنائي، باعتباره دليل يقيني وموضوعي مما يؤدي بسهولة لاقتناع القاضي، إلا أنه يخضع لتقدير القاضي الجنائي وفي إمكانه الأخذ به كما في إمكانه عدم الأخذ به .

كما أن هذا الدليل تنجر عنه عدة مشاكل نابعة من طبيعته الخاصة لها تأثير على اقتناع القاضي الجنائي كمشكل أصالة الدليل الإلكتروني، وارتفاع تكاليف الحصول عليها، إلا أن مبدأ الاقتناع القضائي وحرية القاضي الجنائيه دور كبير في مواجهة هذه المشاكل، بإخضاع هذا الدليل لهذه المبادئ نظرا لصعوبة الحصول علية، وبالتالي إعماله والأخذ به وإعطائه الحجية المطلوبة من خلال هذه المبادئ الجوهرية في الإثبات الجنائي، والتي من شأنها أن تساعد بشكل كبير في مسألة الأخذ بالدليل الإلكتروني،

---

[1] – عائشة بن قارة مصطفى، المرجع السابق، ص، 825.

وليس بهدف توسيع سلطة القاضي الجنائي، وإنما تسهيل الوصول إلى الحقيقة المنشودة من كل هذا .[1]

[1] – أمنة هلال، الإثبات الجنائي بالدليل الإلكتروني، المرجع السابق، ص 78 .

ملخص الفصل الثاني:

وفي خلاصة هذا الفصل يجدر بنا القول أنه لإثبات الجريمة الإلكترونية لابد من إتباع طرق الإثبات المتعارف عليها، والتي تخضع للقواعد العامة للإثبات الجنائي .

ولكن ما يميز الجريمة الإلكترونية أنه عند تطبيق طرق الإثبات في مجالها ينتج دليل خاص بها وهو الدليل الإلكتروني، والذي يتميز بكونه دليل ذو هيئة إلكترونية غير ملموسة، ويخضع شأنه شأن الأدلة الجنائية الأخرى للسلطة التقديرية للقاضي الجزائي .

وكما رأينا أن الدليل الإلكتروني له حجيته أمام القاضي الجزائي بالرغم من المشاكل التي تنجر عن الطبيعة الخاصة التي يتمتع بها هذا الدليل الالكتروني .

خاتمة

خاتمة:

تعد هذه الدراسة حصيلة جهد قمنا به بهدف التصدي لموضوع إثبات الجريمة الإلكترونية، غير انه لا يجب أن يكون الطابع التقني لمثل هذا النوع من الجرائم عقبة تمنعنا محاولة التوسع في قاعدة النقاش حول الإجرام المعلوماتي .

ونظرا لإلمامنا بالجوانب التقنية والجوانب القانونية لهذا الموضوع، إلا أن ذلك لا يمنعنا أيضا القول بأنه توصلنا في ختام هذه الدراسة إلى عدة جوانب يمكن بلورتها في عدة نتائج وتوصيات إتضحت من خلال تحليل وتفسير البيانات التي تم الحصول عليها من خلال هذه الدراسة وفي هذا الصدد سيتم عرض ملخص لأهم النتائج والتوصيات المتوصل إليها وذلك على النحو التالي :

النتائـــج:

هناك العديد من النتائج التي توصلت إليها هذه الدراسة، علما انه ما تم التوصل إليه من نتائج الآن ربما يتغير مستقبلا بحكم طبيعة الجريمة الإلكترونية المرتبطة بالتقنية التي تتطور بشكل كبير، ويمكن إيجاز هذه النتائج كما يلي :

- أظهرت هذه الدراسة غياب مفهوم عام متفق عليه بين الدول حول التعريف القانوني للنشاط الإجرامي المتعلق بالجريمة المعلوماتية والأنماط المكونة لها .

- تتسم الجريمة الإلكترونية بصعوبة إكتشافها، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة، مقارنة بما يتم إكتشافه من جرائم تقليدية، ويمكن رد الأسباب التي تقف وراء صعوبة إكتشاف الجرائم الإلكترونية إلى عدم ترك هذه الجريمة لأي أثر خارجي بصورة مرئية، كما أن الجاني يمكنه إرتكاب هذه الجريمة في دول مختلفة.

- يعد الإثبات من اهم التحديات التي تواجه الاجهزة الأمنية ويزداد الإثبات صعوبة في الجرائم الإلكترونية، حيث أن إكتشاف الجريمة الإلكترونية ليس بالأمر السهل، وفي حال إكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كثير من الصعاب، مما يستلزم الكثير من الجهد والخبرة الفنية.

- إن الجريمة الإلكترونية قد تكون جريمة تقليدية تضم جانب إلكتروني، لاسيما في ضل إرتباط الناس بالتقنيات الحديثة التي إنتشرت بشكل كبير وأهما الحاسبات الآلية والهواتف الذكية، وقد تكون جريمة إلكترونية مستقلة بذاتها.

- تتطلب طبيعة الجريمة الإلكترونية بصفة عامة أساليب غير تقليدية في التحقيق لإكتشاف الدليل الرقمي ودعمه من طرف الفنيين المختصيين.

- تواجه طرق التحقيق في إثبات الجريمة الإلكترونية صعوبات متعددة، حيث تستدعي هذه الطرق في المقام الأول إكتشاف الجريمة الإلكترونية ومحلها وبيئتها والإبلاغ عنها، وأخذ إذن الجهات المختصة قبل القيام بالمعاينات والتفتيش للموقع أو الجهاز المشتبه به، وذلك للبحث عن الدليل الرقمي الإلكتروني بالطرق الفنية ومن ثم إجراء التحريات والأبحاث التي تساعد في عملية الإثبات.

- تمثل الشهادة أهمية كبيرة في إثبات الجريمة الالكترونية في المواد الجزائية، فهي ترد على وقائع مادية وترشد القاضي إلى تحري قيمتها.

- تساعد الخبرة الفنية في ‘ثبات الجريمة الالكترونية حيث تكمن أهمية الخبرة في أنها تنير الطريق أمام القاضي الذي يهتدي بها إلى تحقيق العدالة، لا سيما في المجال الجنائي، لذا فقد اهتمت مختلف القوانين بأهمية الاستعانة بالخبراء.

-

الإقتراحات:

على ضوء هذه النتائج المتوصل إليها يمكن وضع جملة من التوصيات يمكن أن تساهم في تفعيل إثبات الجريمة الإلكترونية وذلك كما يلي:

- تستدعي عملية التحقيق في الجرائم الالكترونية تطوير أساليب التحقيق الجنائي وإجرائاته بصورة تتلائم مع هذه الخصوصية.

- فيما يتعلق بمعاينة الجريمة الالكترونية، فيجب تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة وتحديد مواقعها بأسرع وقت ممكن، وفي حالة وجود شبكة إتصالات يجب البحث عن خادم الملفات بهدف تعطيل الاتصالات لمنع تخريب الأدلة المتحصل عليها.

- يجب التأكد ايضا من عدم وجود مجالات كهرومغناطيسية في المحيط الخارجي لمسرح الجريمة حتى لا يتم أي إتلاف للبيانات المخزنة.

- يجب فحص كل ما تحويه سلة المهملات في الجهاز ورفع البصمات التي قد تكون لها دلالة على مرتكب الجريمة.

- زيادة الإهتمام بتطوير دور الخبرة الفنية لما لها من دور فعال في إثبات الجريمة الإلكترونية، وهنا بعض العناصر التي نوصي بها بأن تتوفر في الخبرة الفنية حتى تساعد في إثبات الجريمة الإلكترونية وهي كما يلي:

- الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية، والأجهزة الملحقة به وكلمات المرور أو السر أو رموز التشفير.

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

- قدرة الخبير على إتفاق مأموريته دون أن يترتب على ذلك مشاكل أو تدمير الادلة المتحصلة من الوسائل الإلكترونية.

- إنشاء قاعدة بيانات لجرائم المعلومات من حيثّ أساليبها وأنواعها للرجوع إليها عند اللزوم.

- أهمية التنسيق المستمر بين الجهات القضائية والأمنية من جهة والجهات ذات العلاقة بالتكنولوجيا من جهة أخرى لمسايرة ما يستجد في هذا المجال.

- ضرورة النص صراحة على الأدلة الإلكترونية كأدلة إثبات في المجال الجنائي والاعتراف لها بحجية قاطعة.

- وجوب تعديل القواعد الإجرائية التي يؤخذ بها في تجميع الدليل الالكتروني بما يتماشى مع خصائص الدليل الالكتروني وطبيعته.

- لزوم أن يتوفر القضاة ومختلف من يعمل على الحصول على الدليل الإلكتروني على الثقافة المعلوماتية الكافية وكيفية التعامل مع هذا الدليل للاحتفاظ بقوته الثبوتية.

- من الضروري أن يكون هناك تنسيق وتعاون دولي أمني وقضائي للحصول على الدليل الإلكتروني، باعتبار أن الجرائم الإلكترونية من الجرائم العابرة للحدود، وهذا بغرض تسهيل إجراءات تحصيل هذا النوع من الأدلة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع

أولا: النصوص القانونية والقوانين:

1_ الأمر رقم 03-05 الصادر في 19 يوليو 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر، العدد 44.

2_ الأمر رقم 03-07 الصادر في 19 يوليو 2003، المتعلق ببراءات الإختراع، العدد44.

3_ الأمر رقم 09-04 الصادر في 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، العدد47.

4_ الأمر رقم 22/06 الصادر في 20 ديسمبر 2006 المعدل والمتمم لقانون الإجراءات الجزائية.

ثانيا: الكتب والمصادر:

1_ أحسن بوسقيعة، الوجيز في القانون الجزائري العام، الديوان الوطني لإنشغال التربوية، 2002، ط 01، الجزائر.

2_ أحمد المهدي، أشرف الشافعي، التحقيق الجنائي الإبتدائي و ضمانات المتهم و حمايتها، دار الكتب القانونية، مصر، 2006 .

3_ أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي ، الطبعة الثانية ، مصر ، 2006.

4_ بن زيطة عبد الهادي، حماية برامج الحاسوب في التشريع الجزائري، دار الخلدونية للنشر والتوزيع، الجزائر، 2007، ط1.

5_ جلال محمد الزعبي، أسامة أحمد المناعسة، جرائم تقنية نظم المعلومات الإلكترونية، دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان الأردن، 2010، ط1، ص189.

6_ خثير المسعود، الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الطبعة 2010.

7_ زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري الدولي، دار الهدى للطباعة والنشر، الجزائر، 2011.

8_ طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2009.

9_ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنيت، دار الكتب القانونية، مصر، 2002.

10_ فيفي كامل عقيقي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، 2000، ط2، دون بلد نشر.

11_ محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، مكتبة دار الثقافة للنشر والتوزيع، عمان الأردن، 2004، الطبعة 1.

12_ محمد علي العربان، الجزائر المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004.

13_ محمد علي قطب، الجرائم المعلوماتية وطرق مواجهتها، مركز الإعلام الأمني، الأكاديمية الملكية للشرطة، الجزء الأول.

ثالثا: الرسائل العلمية:

1_ حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، بحث مكمل لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام والعقاب، جامعة باتنة، 2012/2011، ص13، نقلا عن نائلة عادل محمد فريد قورة، جرائم الحاسب الإقتصادية، القاهرة، 2004.

2_ دردور نسيم، جرائم المعلوماتية على ضوء القانون الجزائري والمقارن، مذكرة لنيل شهادة الماجستير، شعبة القانون الجنائي، جامعة منثوري، قسنطينة، 2012-2013.

3_ رصاع فتيحة، الحماية الجنائية للمعلومات على شبكة الأنترنت، مذكرة لنيل شهادة الماجستير في القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2012/2011.

4_ سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر، باتنة، 2012-2013، نقلا عن عبد القادر المومني، الجرائم المعلوماتية، ط02، 2010.

5_ سمية مزغيش، جرائم المساس بالأنظمة المعلوماتية، مذكرة مكملة من متطلبات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2013-2014.

6_ سوير سفيان، جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام، جامعة أبو بكر بلقايد، تلمسان، 2010-2011.

7_ صغير يوسف، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، جامعة مولود معمري، تيزي وزو، 2013/3/6، نقلا عن كحلوش علي، جرائم الحاسوب وأساليب مواجهتها، مجلة صادرة عن مديرية الأمن الوطني، العدد 84، 2007.

8_ صغير يوسف، (الجريمة المرتكبة عبر الإنترنت)، ماجستير، منشورة، جامعة مولود معمري، كلية الحقوق و العلوم السياسية، قسم الحقوق، تيزي وزو، الجزائر، 2013.

9_ عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي ، دار الجامعة الجديدة، مصر، 2010 .

10_ عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية، (دراسة مقارنة)، رسالة مكملة للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط، 2014.

11_ مصطفى محمد موسي التحقيق الجنائي في لجرائم الإلكترونية ، مطابع الشرطة ، الطبعة الأولى، مصر، 2008 .

12_ ممدوح عبد الحميد عبد المطلب: البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الإنترنت، دار الكتب القانونية، مصر، 2006 .

رابعا: المقالات والمجلات :

1_ بن دعاس فيصل، إجراءات التحري في الجرائم المعلوماتية، محاضرة في إطار التكوين المحلي المستمر للقضاة، مجلس قضاء قسنطينة.

2_ بوعناد فاطمة زهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، سيدي بلعباس، 2013، العدد 1.

3_ سمير سعدون مصطفى وآخرون، الجريمة الإلكترونية عبر الأنترنت وسبل مواجهتها، بحث مقدم بتاريخ 2010/09/20، بدون سنة.

4_ عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحية القانونية والفنية (دراسة مقارنة)، المؤتمر العربي الأول لعلوم الأدلة الجنائية والطلب الشرعي، الرياض، 2007.

5_ كامل فريد السالك، الجريمة المعلوماتية، ندوة التنمية ومجتمع المعلوماتية، حلب، 23/21 تشرين الأول، 2000.

6_ كوثر فرام، الجريمة المعلوماتية على ضوء العمل القضائي المغربي، بحث نهاية التدريب، المعهد العالي للقضاء، 2009/2007.

7_ مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، مجلة علمية، نقلا عن الطاهر روابنية، المسائلة، مقال، العدد 01، 1991.

8_ موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة مقدمة إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا، طرابلس، 2009.

خامسا: المواقع الألكترونية :

سميرة بيطام، الجريمة الإلكترونية وتقنية الإجرام المستحدث:

hyyp://www.culture/net.alukah.br

:موقع ويكيبيديا، الموسوعة الحرة، التاريخ 2022/05/14، 13:48 .2

http//ar .wkiped.org/wiki

فهرس المحتويات

فهرس المحتويات

الفصل الثاني : إثبات الجريمة الإلكترونية

ملخص:

بتطور وسائل التواصل وعصر المعلوماتية الذي نعيشه، تطورت الجرائم التي أصبحت تمارس في فضاء حكومي، هذا ما اضطر التشريعات الوطنية والاتفاقيات الدولية لوضع عقوبات لمكافحة الجرائم الالكترونية بحيث حاولت الجزائر استحداث آليات قانونية تسمح بالحد من انتشار هذه الجرائم من خلال وضع منظومة قانونية متكاملة ترتكز أساسا على كل من قانوني العقوبات والإجراءات الجزائية.

الكلمات المفتاحية: الجريمة الالكترونية، النظام المعلوماتي، الدليل الرقمي، اثبات الجريمة الالكترونية.

Abstract :

With the development of means of communication and the information age in which we live, crimes that have become practiced in a governmental space have evolved, which has forced national legislation and international conventions to set penalties to combat cybercrime. Both legal penalties and criminal procedures.

Keywords: cybercrime, information system, digital evidence, proof of cybercrime.

.