جامعـــــــة قاصـــدي مربـــــاح ـ ورقلـــــــة ـ
كليـــة الحقـــوق و العلـــوم السياسيـــة
قســـــــم الحقـــــوق

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر

الميدان: حقوق وعلوم سياسية

الشعبة: حقوق

التخصص: قانون جنائي

من إعداد الطالبين: لبيض عادل ـ نزلي بشرى

بعنوان:

إثبات الجريمة الإلكترونية

نوقشت وأجيزت بتاريخ:07 جوان 2018

أمام اللجنة المكونة من السادة الأعضاء

. الأستاذ/ شنين صالح ـ أستاذ محاضر "أ" ـ جامعة قاصدي مرباح ورقلة ـ رئيسا

. الأستاذ/ خويلدي السعيد ـ أستاذ محاضر "أ" ـ جامعة قاصدي مرباح ورقلة ـ مشرفا

. الأستاذ/ بن عمر ياسين ـ أستاذ مساعد "ب" ـ جامعة قاصدي مرباح ورقلة ـ مناقشا

السنة الجامعية: 2018/2017

جامعـــــــة قاصـــدي مربـــــاح ـ ورقلـــــــة ـ
كليـــة الحقـــوق و العلـــوم السياسيـــة
قســـــــم الحقـــــوق

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر

الميدان: حقوق وعلوم سياسية

الشعبة: حقوق

التخصص: قانون جنائي

من إعداد الطالبين: لبيض عادل ـ نزلي بشرى

بعنوان:

إثبات الجريمة الإلكترونية

نوقشت وأجيزت بتاريخ:...../...../.....

أمام اللجنة المكونة من السادة الأعضاء

. الأستاذ/شنين صالح ـ أستاذ محاضر "أ" ـ جامعة قاصدي مرباح ورقلة ـ رئيسا

. الأستاذ/ خويلدي السعيد ـ أستاذ محاضر "أ" ـ جامعة قاصدي مرباح ورقلة ـ مشرفا

. الأستاذ/ بن عمر ياسين ـ أستاذ مساعد "ب" ـ جامعة قاصدي مرباح ورقلة ـ مناقشا

السنة الجامعية: 2018/2017

شكر وعرفان:

إن الشكر في البدء والمنتهى للمولى عز وجل الذي وفقنا في إنجاز هذا العمل.

ثم الشكر لأستاذنا المحترم الدكتور: **خويلدي السعيد** لإشرافه على هذه المذكرة، ولم يبخل علينا بالنصح والإرشاد.

وإلى كافة أساتذتنا الأفاضل الذين تتلمذنا على أيديهم، كل باسمه.

ونتوجه بالشكر أيضا للسيد: **نزلي مصطفى** على مجهوداته التي بذلها لإخراج عملنا على هذا الوجه.

ولا ننسى زميلنا السيد: **بوخزنة مبروك**، الذي نتوجه بالشكر الجزيل له على ما قدمه لنا من مساعدات وتسهيلات في سبيل الحصول على المراجع.

إليكم جميعا نتقدم بشكرنا الخالص.

عادل _ بشرى

مقدمة

المقدمـــــة

مقدمة:

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

وعمدت عدة دول في سبيل مواجهة الجرائم الإلكترونية إلى وضع سياسات جنائية تتنوع بين الوقاية والمواجهة من خلال سن مجموعة من القوانين من أجل وضع حد للانفلات في مجال الجرائم المعلوماتية، هذه الأخيرة أحدثت انقلابا هاما في النظريات التقليدية بما فيها نظرية الإثبات الجنائي، من منطلق أن أهم خاصية تتميز بها الجريمة الإلكترونية هي صعوبة إثباتها باتفاق الفقهاء والدارسين في مجال المعلوماتية، وما انعكس سلبا على العملية الإثباتية للجرائم المعلوماتية هو عدم تناسب النصوص المنظمة لطرق الإثبات التقليدية مع طبيعة الجريمة المعلوماتية وتطورها، بسبب سرعة إخفائها وطمس معالمها في زمن قياسي ومن أي مكان في العالم، ما استلزم على المشرعين تبني أنواع جديدة من الأدلة تسمى بالأدلة الرقمية مع حرصهم على توفير الغطاء التشريعي لها.

نظرا للطابع الخاص والتقني للجرائم الإلكترونية فهي تتم في بيئة غير مادية لا علاقة لها بالمستندات وتتم عبر نظام الحاسب الآلي أو شبكة الانترنت، فإن عملية إثباتها تقتضي البحث عن الدليل المناسب في ظل عجز وعدم قدرة الأدلة الجنائية العادية في الغالب إثبات هذه الجرائم .

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 الاستغناء عنها، وأصبحت المجتمعات المعاصرة تعتمد على البيئة الرقمية وازداد التوجه نحو التخلي عن الوثيقة في المعاملات المختلفة بما فيها عملية الإثبات، مما أدى إلى استحداث أشكال جديدة من الأدلة في الإثبات الجنائي، استوجب توفرها على شروط معينة لاعتبارها دليلا كاملا يمكن من خلالها دحض قرينة البراءة واثبات عكسها عندما يصل اقتناع القاضي إلى حد الجزم واليقين.

المقدمـــــة

أهمية الموضوع:

تكمن أهمية هذه الدراسة في التعرف على الجريمة الإلكترونية لاسيما من حيث ضبطها وإثباتها، لأنه لا يختلف اثنان في أن أساس توقيع العقوبة على المتهم يكمن في إثبات إدانته وذلك بإقامة الأدلة عليه، لذا فإن الإثبات يعتبر موضوعا في غاية الأهمية، علما أن أهمية 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 أخرى معرفتها لإثبات وقوع هذه الجرائم.

كما أن الإثبات الجنائي بالدليل الإلكتروني له أهمية بالغة تتضح من خلال صلته بطائفة جديدة من الجرائم اصطلح عليها تسمية الجرائم الإلكترونية، هذه الأخيرة انتشرت في الوقت الحالي بشكل يستدعي التوقف عندها، باعتبار أنها من المواضيع التي أثارت العديد من المشاكل في نطاق الإثبات الجنائي، وهذا ما يستوجب الاعتماد 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 الأدلة الرقمية وكذا الكشف عن مدى حجية الدليل الإلكتروني في مجال الإثبات الجنائي.

أسباب اختيار الموضوع:

تتمثل أسباب اختيار الموضوع في ما يلي:

1: أسباب ذاتية:

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

2: **أسباب موضوعية:**

نظرا لتفشي ظاهرة الإجرام الإلكتروني بشكل سريع، وتطور الوسائل المستخدمة في ارتكاب الجريمة الإلكترونية، 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:

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

الدراسات السابقة:

معظم الدراسات السابقة التي اطلعنا على محتواها ونحن بصدد انجاز مذكرتنا هذه، جاءت بمعظم الأفكار التي يجب التطرق إليها في هذا الموضوع، فمثلا مذكرة رسالة الماجستير "**إثبات الجريمة الإلكترونية**"، جامعة نايف العربية للعلوم الأمنية، بالرياض، سنة 2012، وكذا مذكرة شهادة الماستر "**الإثبات الجنائي بالدليل الإلكتروني**" جامعة بسكرة، سنة 2015.

إلا أننا وفي دراستنا هذه تناولنا زيادة عن المذكرتين السابقتين، موقف المشرع الجزائري من الجريمة الإلكترونية، وكذا حجية الدليل الرقمي أمام القاضي الجزائي الجزائري.

المقدمـــــة

الإشكالية:

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

هل يخضع إثبات الجريمة الإلكترونية بصفتها جريمة مستحدثة لنفس المعايير التي يخضع لها إثبات الجريمة التقليدية أم هناك اختلاف يميز بينهما.

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

_ ما المقصود بكل من الجريمة الإلكترونية والدليل الرقمي ؟

_ ما هي طرق إثبات الجريمة الإلكترونية ؟

_ هل يعتبر الدليل الرقمي دليلا كاملا للإثبات الجنائي ؟

ولمعالجة الإشكالية المطروحة والإجابة عن التساؤلات الفرعية التابعة لها، قسمنا موضوعنا إلى فصلين اثنين هما:

- الفصل الأول: مفهوم الجريمة الإلكترونية والدليل الرقمي.

- الفصل الثاني: إثبات الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي.

الفصل الأول

مفهوم

الجريمة الإلكترونية والدليل الرقمي

الفصل الأول: مفهوم الجريمة الإلكترونية والدليل الرقمي

تمهيد:

الجريمة الإلكترونية جريمة مستحدثة نشأت نتاج التطور التكنولوجي الذي شهده العالم، وبالتالي وجب إثباتها والتوصل إلى مرتكبيها.

ولما كان رجال القضاء يرنون إلى إيجاد طرق إثبات هذه الجريمة تتماشى وطبيعتها، وتضمن الإحاطة بجميع ملابساتها، كان لزاما علينا قبل الخوض في سرد هذه الطرق أن نتعرض إلى مفهوم كل من الجريمة الإلكترونية والدليل الرقمي وذلك من خلال المبحثين التاليين:

المبحث الأول: مفهوم الجريمة الإلكترونية.

المبحث الثاني: مفهوم الدليل الرقمي.

المبحث الأول: مفهوم الجريمة الإلكترونية:

عصر الانترنت أو عصر التكنولوجيا الرقمية أو عصر المعلوماتية، كل هذه الأوصاف إنما تعبر عن مدى ضخامة القفزات العلمية الهائلة التي تحققت ومدى تنوع الانجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الآونة الأخيرة. وفي الواقع إن هذا الوجه المشرق لتقنية المعلومات لا يخلُو من الجانب المظلم الذي يمثل الإجرام المعلوماتي، والذي كان موجودا ليستغل هذه التقنيات المتطورة لتحقيق مصالح ومآرب تتنوع وتتعدد[1]. وأضافت المعلوماتية الكثير من الجوانب الإيجابية إلى حياتنا، إلا أنها في المقابل جلبت معها نسلا جديدا من المجرمين اصطلح على تسميتهم مجرمي المعلوماتية[2].

وعليه نقسم مبحثنا هذا إلى ثلاثة مطالب: نتطرق للتعريف بالجريمة الإلكترونية في (المطلب الأول)، وإلى الطبيعة القانونية للجريمة الإلكترونية وخصائصها في (المطلب الثاني)، وأخيرا إلى مواجهة الجريمة الإلكترونية في التشريع الجزائري في (المطلب الثالث).

[1]- نهلا عبد القادر المومني: **الجرائم المعلوماتية**، (ط1)، دار الثقافة للنشر و التوزيع، عمان،2008، ص46.

[2]- محمد سامي الشوا: **الثورة المعلوماتية و انعكاساتها على قانون العقوبات**، (ط2)، دار النهضة العربية، القاهرة، 1998، ص:33.

المطلب الأول: التعريف بالجريمة الإلكترونية:

في تعريفنا بالجريمة الإلكترونية نتطرق إلى تعريف الجريمة الإلكترونية (الفرع الأول)، أنواع الجريمة الإلكترونية (الفرع الثاني)، المجرم المعلوماتي (الفرع الثالث).

الفرع الأول: تعريف الجريمة الإلكترونية:

بذل الفقه جهودا مضنية في محاولة لوضع تعريف محدد لماهية الجريمة الإلكترونية، فانقسم الفقه بين اتجاهين[1]: الأول يضيّق من مفهوم الجريمة الإلكترونية والآخر يوسّع من مفهومها.

ومن التعريفات التي وضعها أنصار الاتجاه المضيّق، أن الجريمة الإلكترونية هي: "كل فعل غير مشروع يكون العلم بتكنولوجيا الكمبيوتر بقدر كبير لازما لارتكابه من ناحية وملاحقته من ناحية أخرى".

كما عرفها هذا الاتجاه بأنها: "هي التي تقع على جهاز الكمبيوتر أو داخل نظامه فقط". أو هي: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الكمبيوتر، أو تلك التي يتم تحويلها عن طريقه".

بينما عرف أصحاب الاتجاه الموسّع الجريمة الإلكترونية بأنها: "كل سلوك إجرامي يتم بمساعدة الكمبيوتر".

أوهي: "كل جريمة تتم في محيط أجهزة الكمبيوتر". أو هي : "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها"[2].

وبعد التطرق إلى تعاريف كلا الاتجاهين، اتضح لنا أن أشمل تعريف للجريمة الإلكترونية هو: "هي الجريمة التي تتم باستخدام الحاسب الآلي، أو تلك التي تقع على الحاسب الآلي ذاته"[3].

الفرع الثاني: أنواع الجريمة الإلكترونية:

تقسم الجريمة الإلكترونية إلى:

---

[1]- نائلة عادل محمد فريد: **جرائم الحاسب الآلي الاقتصادية**، (د.ط)، منشورات الحلبي الحقوقية، 2005، ص:28.

[2] . Aderian Roben , Computer crime and the law , C.L.J. 1991, vol.15, p 399.

[3]. محمد علي قطب: **الجرائم المعلوماتية وطرق مواجهتها**، وزارة الداخلية، الأكاديمية الملكية للشرطة، مملكة البحرين، 2010، ص: 02.

أولا: جريمة التخريب ونقل الأموال: وهي بدورها تنقسم إلى:

1- جريمة إتلاف معطيات الحاسوب أو تخريبها: المقصود بهذه الجريمة، هو الإتلاف أو التخريب الذي يقع على بيانات ومعلومات وبرامج الحاسوب لا على الكيان المادي له، فهذا الجانب لا يثير صعوبة في تحديد الجريمة ووسائل حمايتها. فمن خلال هذا التعريف لهذه الجريمة، فإنه لا بد من عرض صور ووسائل ارتكاب هذه الجريمة، فجانب من الفقه يرى أنها تتخذ صورتين هما:

أ): محو المعلومات كليا وتدميرها إلكترونيا.

ب): تشويه المعلومة أو البرنامج على نحو يجعلها غير صالحة للاستعمال.

2- الجرائم المصرفية "نقل الأموال": إن جريمة التعدي –بواسطة الكمبيوتر– تتم عن طريق أفراد، يتمتعون بخبرة ودراية طويلة في التعامل مع هذه الأجهزة المتطورة. إن ارتكاب هذه الجريمة (التعدي) يتم في الغالب لأسباب شخصية أو سياسية أو اقتصادية، حيث يعمد المجرم إلى الدخول إلى المصارف وتحويل الأموال من حسابات إلى حسابات أخرى، وهي أصعب الجرائم التي ترتكب في الوقت الحالي لكونها لا تعرف الحدود، أو المكان أو الزمان. وقد امتدت هذه الجرائم لتشمل التلاعب في بطاقات الائتمان التي تمت سرقتها، واستخدامها للشراء بواسطة الانترنت، وتعد عمليات السطو على بطاقات الائتمان أحدث أنماط السلوك الإجرامي التي ارتبطت بشبكة الانترنت، من بنوك أو مؤسسات مالية أو أفراد. وقد زاد خطر انتشار هذا النوع من الجرائم صعوبة التوصل إلى مرتكبيها، ففي كثير من الأحيان يكتشف حامل بطاقة الفيزا في دولة ما أن بطاقته قد استخدمت في شراء سلعة من أحد المحلات في دولة ثانية، ويكون الفاعل في دولة ثالثة وقد تمت الواقعة من خلال موقع المحل البائع على شبكة الانترنت.

ثانيا: جرائم أخرى متعلقة بالحاسوب والانترنت: تنقسم إلى:

1. جريمة التزييف والتزوير: إن تزييف العملة وما يصاحبها من جرائم أخرى يعاقب عليها القانون لما تسببه من أضرار للمواطنين في معاملاتهم اليومية المستمرة، ولآثارها المدمرة في الاستقرار والاطمئنان الاقتصادي. وباعتبارها تشكل عدوانا مباشرا على سيادة الدولة في حق من صميم حقوقها، يستوجب مقاومتها بشدة وتوعية المواطنين وتنبيه المسؤولين لهذه الظاهرة التي غزت المجتمعات الإنسانية منذ أن عرف الإنسان العملة كوسيلة للمبادلات. وقد انتشر تزييف العملة انتشارا خطيرا في العصر الحديث، لسهولة وسرعة المواصلات وتداخل الحدود بين الدول. كما تطورت هذه الجريمة وأخذت في طابعها الشكل الدولي.

2. التشهير: توجد بعض الظواهر السلبية التي برزت على شبكة الانترنت، مثل تسهيل الدعارة وبث المواد الإباحية وخدش الحياء، ونشر بعض القيم السلبية وغير ذلك. وبالرغم من الإيجابيات الهائلة لشبكة الانترنت، فإن المخاطر الناجمة عن هذه الشبكة بالغة الحد والعمق خاصة بالنسبة للأحداث صغار السن، حيث أن الأحداث يميلون إلى التقليد والمحاكاة وإثبات الذات، والحدث المهيأ للانحراف يكون مستعدا للاستجابة لأي مؤثر خارجي يؤجج استعداده الداخلي وميله الذاتي للانحراف. وشبكة الانترنت توفر لهؤلاء المادة الخصبة من المواد الإباحية، والصور الخليعة، والتراسل مع الأقران سيئي الخلق منحرفي الميول. كما تعد شبكة الانترنت الفضاء الرحب لنشر أي فضائح على اختلاف أنواعها أو التشهير بأي شخص دون أي ضابط قانوني.

3. النسخ غير المرخص للمصنفات الرقمية: المصنفات الرقمية عبارة عن برمجيات، وقواعد البيانات وطبوغرافيا الدوائر المتكاملة، وهي مصنفات جاءت وليدة علوم الحوسبة مستقلة عن علوم الاتصال وتبادل المعطيات وشبكات المعلومات.

ومع ظهور شبكات المعلومات، والتي ارتبطت في الذهنية العامة بشبكة الانترنت، كمعبر عنها وعن التفاعل والدمج بين وسائل الحوسبة والاتصال، ظهرت أنماط جديدة من المصنفات الممكن الحصول عليها خاصة مع وجود شبكات الانترنت. إلا أنه في واقع الأمر تعتبر هذه المصنفات مؤلفات خاصة، كل نشر أو نسخ أو استفادة منها يعتبر تعدي على حقوق الملكية الفكرية للمؤلف. وتعتبر هذه الجريمة من الجرائم المنتشرة بصفة واسعة خاصة في دول العالم الثالث، أين يجد الفرد صعوبة في اقتناء المصنف الأصلي

فيلجأ إلى الحصول عليه بطرق غير مشروعة. وقد تقدر خسائر شركة "ميكروسوفت" حوالي 16.000.000 دولار سنويا من جراء القرصنة والتداول غير المشروع لمنتجاتها[1].

ثالثا: جرائم إلكترونية أخرى: تتعدد وتتنوع الجرائم الإلكترونية مما لا يسعنا لذكرها بالتفصيل، لذا سنورد بعض منها بإيجاز:

1: إنشاء المواقع السياسية والدينية المعادية.

2: إنشاء المواقع المعادية للأشخاص أو الجهات السياسية أو الفكرية.

3: جرائم القرصنة.

4: جرائم التجسس الإلكتروني.

5: الإرهاب الإلكتروني: يقوم الإرهابيون بإنشاء وتصميم مواقع لهم على شبكة الانترنت لنشر أفكارهم والدعوة إلى مبادئهم.

6: الجرائم الجنسية والممارسات غير الأخلاقية.

7: الجرائم المنظمة عبر الانترنت: تتمثل في: تجارة المخدرات وغسيل الأموال، السطو على أموال البنوك وقيادة الجماعات الإرهابية عن بعد[2].

الفرع الثالث: المجرم المعلوماتي: رغم الصعوبات التي قد تظهر عند تحديد سمات معينة للمجرم المعلوماتي، فإنه يرتكب جرائمه وهو يمارس وظيفته في مجال الحاسبات الآلية، فلا بد وأن يكون إنسانا اجتماعيا يحيا وسط المجتمع، يقوم بواجباته ويمارس حقوقه الاجتماعية والسياسية دون وجود أي عائق في حياته العملية. وأيضا لابد أن يكون الشخص الذي يرتكب جريمته المعلوماتية إنسانا محترفا يتمتع بذكاء[3]، ولذلك نعرض هذه السمات على النحو التالي:

أولا: المجرم المعلوماتي هو إنسان اجتماعي بطبعه : المجرم المعلوماتي لا يضع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به، بل إنه إنسان متكيف اجتماعيا، ذلك أنه أصلا مرتفع الذكاء ويساعده

---

[1]- العربي قندوز وآخرون: **جرائم الحاسوب**، مذكرة مقدمة للتخرج"الدفعة الثانية لمفتشي الشرطة"، مدرسة الشرطة طيبي العربي، سيدي بلعباس، الجزائر، 2008، ص: 25 وما بعدها.

[2]- عادل عبد الجواد محمد: **الانترنت والإجرام المنظم**، مجلة الأمن والحياة، العدد 303، 26 **سبتمبر** 2007، (د.ب.ن)، ص: 30 . 32.

[3]- محمد علي العريان: **الجرائم المعلوماتية**، (د.ط)، دار الجامعة الجديدة للنشر، الإسكندرية،2011، ص:77.

على ذلك عملية التكيف وقد يزيد تكيفه مع توافر الشخصية الإجرامية لديه[1]. وكثير من الجرائم المعلوماتية ترتكب بدافع الكبرياء أو النصب أو الحسد أو بدافع اللهو، ولإظهار مدى تمتعه بقدرة التفوق في مواجهة أمن الأنظمة المعلوماتية[2].

ثانيا: المجرم المعلوماتي من النوابغ، محترف وذكي: يذكر عادة أن الإجرام المعلوماتي هو إجرام الأذكياء وذلك بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف[3]. والإجرام المعلوماتي يتميز بأنه ينشأ من تقنيات التدمير الناعمة، بمعنى آخر أن يقوم المجرم المعلوماتي بالتلاعب في بيانات وبرامج الحاسوب الآلي، لكي يمحو هذه البيانات أو يعطل استخدام البرامج، وليس عليه سوى أن يلجا إلى زرع الفيروسات في هذه البرامج، أو باستخدام القنابل المنطقية أو الزمنية أو برامج الدودة، لكي يشل حركة النظام المعلوماتي ويجعله غير قادر على القيام بوظائفه الطبيعية[4].

والمجرم في جرائم الكمبيوتر والانترنت ليس مجرما عاديا، ويصنف ضمن نوابغ المجرمين أو نوابغ المعلوماتية، والذي يخشى عليهم من التحول من مجرد الهواية إلى الاحتراف في أفعال اختراق النظم، فقد تتربص به منظمة غير مشروعة تعتمد على المعلوماتية في جرائمها وتقوم بتجنيده، الأمر الذي يجعله مجرما معلوماتيا محترفا[5].

المطلب الثاني: الطبيعة القانونية للجريمة الإلكترونية وخصائصها:

تعتبر الجرائم التي ترتكب من خلال شبكة الانترنت، جرائم ذات طبيعة خاصة وخصائص منفردة، لا تتوافر في الجرائم التقليدية، سواء من حيث أسلوب وطرق ارتكابها، أو شخص مرتكبيها.

نقسم مطلبنا هذا إلى: الطبيعة القانونية للجريمة الإلكترونية في (الفرع الأول)، وخصائص الجريمة الإلكترونية في (الفرع الثاني).

---

[1]- عبد الفتاح بيومي حجازي: **علم الجريمة و المجرم المعلوماتي**، (ط1)، توزيع منشأة المعارف، الإسكندرية،2009، ص: 97.

[2]- محمد علي العريان: **الجرائم المعلوماتية**، المرجع السابق، ص: 77.

[3]- عبد الفتاح بيومي حجازي: **علم الجريمة و المجرم المعلوماتي**، المرجع السابق، ص:98.

[4]- محمد علي العريان: **الجرائم المعلوماتية**، المرجع السابق، ص78.

[5]- عبد الفتاح بيومي حجازي: **علم الجريمة و المجرم المعلوماتي**، المرجع السابق، ص: 99 . 100.

الفرع الأول: الطبيعة القانونية للجريمة الإلكترونية:

تكمن الطبيعة الخاصة لهذه الجرائم في قدرة شبكة المعلومات على نقل وتبادل معلومات ذات طابع شخصي وعام في آن واحد، مما يؤدي إلى ارتكاب الفعل، والسبب في ذلك توسع بنوك المعلومات بأنواعها، علاوة على رغبة الأفراد وسعيهم إلى ربط حواسيبهم بالشبكة، على أساس أن هذه الجرائم ترتكب ضمن نطاق المعالجة الإلكترونية للبيانات، سواء أكان في تجميعها أو تجهيزها أم في إدخالها إلى الحاسب المرتبط بشبكة المعلومات، ولغرض الحصول على معلومات معينة، كما قد ترتكب هذه الجرائم في مجال معالجة النصوص.

وصعوبة التكييف القانوني لهذه الجرائم تكمن في طبيعتها الخاصة، بحيث أن القواعد التقليدية لم تكن مخصصة لهذه الظواهر الإجرامية المستحدثة، وبالتالي تطبيقها على هذا النوع من الجرائم يثير مشاكل عديدة في مقدمتها مسألة الإثبات، ومتابعة مرتكبيها. وعلى ضوء الاعتبارات السابقة يمكن القول بأن هذه الجرائم تتمتع بطبيعة قانونية خاصة[1].

الفرع الثاني: خصائص الجريمة الإلكترونية:

أولا: جريمة عالمية: بمعنى أنها تتعدى الحدود الجغرافية للدول. إنها جرائم عابرة للقارات، لأنه مع انتشار شبكة الاتصالات العالمية والانترنت، أمكن ربط أعداد هائلة لا حصر لها من الحواسيب عبر العالم بهذه الشبكة، حيث يمكن أن يكون الجاني في بلد والمجني عليه في بلد آخر[2].

ثانيا: جرائم صعبة الإثبات: صعوبة متابعتها واكتشافها بحيث لا تترك أثرا، فهي مجرد أرقام تتغير في السجلات. فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها. ويلاحظ أن الجرائم التي لم تكتشف هي أكثر بكثير من تلك التي كشف عنها على أساس أنها تفتقر إلى الدليل المادي التقليدي كالبصمات، كما يصعب الاحتفاظ الفني بآثارها أن وجدت، وتحتاج لخبرة فنية خاصة يتعذر على المحقق التقليدي منالها أو التعامل معها، لأنها تعتمد غالبا على قمة الذكاء المصحوب بالخداع والتضليل

[1]- محمد زكي أبو عامر ـ علي عبد القادر القهوجي: **قانون العقوبات، القسم الخاص** ، (د.ط)، دار النهضة العربية القاهرة، 1993 ، ص9.

[2]. عبد الفتاح مراد: **شرح جرائم الكمبيوتر والانترنت**، (د.ط)، دار الكتب والوثائق المصرية ، 2005، ص: 42.

بدس برامج أو وضع كلمات سرية ورموز تعوق الوصول إلى الدليل، وقد يلجا مرتكبها لتشفير التعليمات لمنع إيجاد أي دليل يدينه[1].

ثالثا: جرائم ناعمة: إذا كانت الجريمة التقليدية تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة، وغيرها، فالجرائم الالكترونية لا تتطلب أدنى مجهود عضلي ممكن، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة، على أساس أن الجاني في الجرائم الالكترونية هو إنسان متوافق مع المجتمع، ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو لمجرد إظهار تفوقه على آلة الكمبيوتر أو على البرامج التي يشتغل بها، وأكيد لتحقيق مصلحة ما[2].

رابعا: عدم التبليغ: عند وقوع الجريمة بواسطة الانترنت، نجد أن بعض المجني عليهم يمتنعون عن إبلاغ السلطات المختصة خشية على السمعة والمكانة، وعدم اهتزاز الثقة في كفاءتهم، خاصة إذا كان كيان أو هيئة معينة. وقد اقترح في (و م أ) بأن تفرض النصوص المتعلقة بجرائم الحاسوب التزاما على عاتق موظفي الجهة المجني عليها، بالإبلاغ عما يقع عليها من جرائم متى وصل إلى علمهم ذلك، مع تقرير جزاء في حالة إخلالهم بهذا الالتزام.

المطلب الثالث: مواجهة الجريمة الإلكترونية في التشريع الجزائري:

حاول المشرع الجزائري إصدار قوانين عامة وهياكل و أجهزة للتصدي للجريمة الإلكترونية، ومحاربة قراصنة الانترنت و إحالتهم قانونيا على المحاكم، متأثرا بجل الدول العربية التي وضعت قوانين لمكافحة الجريمة الإلكترونية.

الفرع الأول: القوانين العامة الموضوعية المنظمة للجريمة الإلكترونية:

أولا: الدستور الجزائري: كفل دستور الجزائر لسنة 1996 بالتعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية الحقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان. وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات

[1]- هشام محمد رستم: **الجرائم المعلوماتية**، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد(2)،1999 ، ص:24.

[2]- عبد الفتاح مراد: **شرح التحقيق الجنائي الفني والبحث الجنائي** ،(د.ط)، دار الكتب والوثائق المصرية، مصر، 2006، ص: 46.

والإجراءات الجنائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق. ومن أهم المبادئ الدستورية العامة:

***المادة 38**: الحرّيّات الأساسيّة وحقوق الإنسان والمواطن مضمونة.

***المادة 44**: حرّيّة الابتكار الفكريّ والفنّي والعلمي مضمونة للمواطن. حقوق المؤلّف يحميها القانون. لا يجوز حجز أيّ مطبوع أو تسجيل أو أيّة وسيلة أخرى من وسائل التّبليغ والإعلام إلاّ بمقتضى أمر قضائيّ. الحريات الأكاديمية وحرية البحث العلمي مضمونة وتمارس في إطار القانون. تعمل الدولة على ترقية البحث العلمي وتثمينه خدمة للتنمية المستدامة للأمة.

لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون، سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة". أن القانون يحمي حقوق المؤلف ولا يجوز حجز أي مطبوع أو تسجيل أو أية وسيلة أخرى من وسائل التبليغ والإعلام إلا أمر قضائي[1].

ثانيا: قانون العقوبات: لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي، وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام، مما دفع بالمشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ – في 10 **نوفمبر** 2004 المتمم لأمر رقم: 66-156 المتضمن قانون العقوبات تحت عنوان: "المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن هذا القسم ثمانية مواد من المادة (394) مكرر إلى (394 **المادة مكرر**7) من **(ق.ع)**.

وفي عام 2006 أدخل المشرع الجزائري تعديلا آخرا على قانون العقوبات بموجب قانون: **رقم** 06-23 المؤرخ في 20 **ديسمبر** 2006، حيث مسّ هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص الواردة في هذا القسم من القانون 04-15، وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام، باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى، وشيوع ارتكابه ليس فقط

[1]. القانون رقم 16-01 المؤرخ في 6-03-2016 المعدل للدستور عدد الجريدة الرسمية 14.

من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم، نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الإنترنت كوسيلة لنقل المعلومات[1].

ثالثا: قانون الإجراءات الجزائية: بالنسبة لمتابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة، غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة (37) من قانون الإجراءات الجزائية[2].

كما نص على التفتيش في المادة (45 **الفقرة** 7) من نفس القانون المعدلة حيث أعتبر إن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه في القواعد الإجرائية العامة، من حيث الشروط الشكلية والموضوعية، فالتفتيش، وإن كان إجراء من إجراءات التحقيق، قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة (44) من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية[3].

ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة (51 **الفقرة** 6)، وكذا على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة (65 **مكرر** 5/ 10)، كما أن قانون الإجراءات الجزائية نصّ على ألا يجوز ضبطها إلا في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة، غير أنه طبقا لقانون الإجراءات المعدل والمتمم في الفصل الرابع تحت عنوان "في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"، نصّت المادة (65 **مكرر**5/3) على أنه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، يجوز لوكيل الجمهورية المختص أن يأذن بالاعتراض ووضع ترتيبات تقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به، بصفة خاصة أو سرية، في أماكن خاصة أو عامة. أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة فتطبق عليها نفس إجراءات الجريمة التقليدية[4].

---

[1]- فضيلة عاقلي: **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري**، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017، ص: 115

[2]- أنظر المادة 37 من الأمر 15-02 المؤرخ في 23 جويلية 2015 ، المعدل والمتمم للأمر 66-155 المؤرخ في 8 يونيو المتضمن قانونه الإجراءات الجزائية ، الجريدة الرسمية المؤرخة في 23 يونيو 2015 ، العدد 40.

[3]- أنظر المادتين 44 . 45 من **ق.إ.ج.ج.**

[4]- أنظر المواد 51 و 65 من **ق.إ.ج.**

الفرع الثاني: القوانين والهياكل الخاصة للتصدي للجرائم الإلكترونية:

أولا: القوانين الخاصة للتصدي للجرائم الإلكترونية:

1: :**قانون البريد والاتصالات السلكية واللاسلكية:** باستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات بحيث لاحظنا أنه تسارع مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان إجراء التحويلات المالية عن الطريق الالكتروني ذلك ما نصت عليه المادة 87 منه، كما نصت المادة 84 **الفقرة** 2 منه على استعمال حوالات دفع عادية أو الكترونية أو برقية، كما نص في المادة 105 منه على احترام المراسلات، بينما أتت المادة 127 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات[1].

2: **قانون التأمينات:** قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي في نصوص قانونية عديدة تخص البطاقة الالكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج، وهي صالحة في كل التراب الوطني، وكذا الجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا، أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الالكترونية حسب المادة 93 **مكرر** 2 من **(ق.ت)**[2].

3:**القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:** جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكل ما يتعلق بالمنظومة المعلوماتية، والمعطيات المعلوماتية، ومقدمو الخدمات، والمعطيات المتعلقة بتسيير الاتصالات الإلكترونية، من مراقبة وتفتيش للمنظومات المعلوماتية عند الضرورة، وحجز المعطيات المعلوماتية، وحفظ المعطيات المتعلقة

---

[1]- أنظر المواد: 84 . 87 . 105 . 127 من قانون البريد والاتصالات السلكية واللاسلكية رقم 03- 2000 المؤرخ 2000/08/05، الجريدة الرسمية **عدد**48.

[2]- أنظر المواد: 6 **مكرر**1، والمادة 65**مكرر**1، من القانون رقم 08/01 المؤرخ في 2008/01/23 المعدل والمتمم لقانون 83/01 المتعلق بالتأمينات.

بحركة السير على الالتزامات الخاصة بمقدمي خدمة الإنترنت، وأخيرا على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1].

ثانيا: الهياكل الخاصة للتصدي للجرائم الإلكترونية:

1: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال :

وأنشئت بموجب القانون رقم04-09 المؤرخ في 5 **أوت** 2009 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. ومن مهام الهيئة الوطنية تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقاية، ولمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية، في حالة الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني.

2: الهيئات القضائية الجزائية المتخصصة: أنشئت بموجب القانون 14/04 المؤرخ في 10/11/2004 المعدل والمتمم لقانون الإجراءات الجزائية، تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 37،329، و40 من **ق.إ.ج.ج.** تتمتع اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06 المؤرخ في 05/01/2006 بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09/04.

3: المعهد الوطني للأدلة الجنائية وعلم الجرائم: يتكون من إحدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، ودائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات (الدرك الوطني).

4: المديرية العامة للأمن الوطني: تتصدى هذه المديرية للجريمة الإلكترونية من عدة جوانب ومنها الجانب التوعوي، بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية التوعوية وهذا من خلال برمجتها

[1]- أنظر المواد من المادة الثانية حتى 14من قانون **رقم** 04-09 المؤرخ في 2009/08/05 والمتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

لتنظيم دروس توعوية في مختلف الأطوار الدراسية، وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

حيث عمدت القيادة العليا للأمن الوطني استحداث مخابر، فصائل وخلايا مختصة في مكافحة الجرائم الإلكترونية، أهمها:

_ في سنة 2007 استحدثت في مخابر الشرطة العلمية الكائن مقرها بالجزائر العاصمة، قسنطينة ووهران أقسام مختصة في تتبع الأدلة الرقمية، من خلال استغلال الأجهزة الإلكترونية، قصد استخراج وتتبع ما من شأنه أن يفيد في التحقيق، ويساعد العدالة في تقرير الأحكام في القضايا التي تكون من هذا النوع.

_ كما خلقت المديرية العامة للأمن الوطني سنة 2010 على جميع مصالح أمن ولايات الوطن، خلايا مختصة بمكافحة الجريمة الإلكترونية.

ودائما في إطار مكافحة الجريمة الالكترونية، ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم، فأكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائية INTERPOL هذه الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا[1].

[1]- عبد الرحمان حملاوي: **مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية**، جامعة بسكرة، كلية الحقوق ، 2016.

المبحث الثاني: مفهوم الدليل الرقمي:

لدراسة مفهوم الدليل الرقمي، لابد من التطرق إلى تعريف الدليل الرقمي وخصائصه (المطلب الأول)، ومن ثم التعرف على تقسيمات الدليل الرقمي (المطلب الثاني).

المطلب الأول: تعريف الدليل الرقمي وخصائصه:

الفرع الأول: تعريف الدليل الرقمي:

لتعريف الدليل الرقمي (الإلكتروني) لا بد من التطرق إلى الدليل الجنائي بصفة عامة كأول شيء، وهذا اعتبارا أنه من المنطقي وجوب معرفة الأصل العام المتمثل في الدليل بصفة عامة، ثم التطرق إلى الفرع المتمثل في الدليل الإلكتروني[1].

أولا: تعريف الدليل الجنائي:

الدليل في اصطلاح الشرعيين هو: "ما يلزم من العلم به العلم بشيء آخر، فإذا أعلم المدعي القاضي بحجته على دعواه لزم متى علم القاضي بتلك الحجة مع اقتناعه بها، علمه بصدق دعوى المدعي فيها ادعاءه والحكم له به"[2].

أما الدليل في اصطلاح القانونيين فقد تعددت التعريفات التي أعطيت له، غير أن التعريف الذي يصلح للإفصاح عن مفهوم الدليل هو ما جاء به الدكتور **مأمون سلامة**: "الدليل هو الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه"[3].
وعرف الدليل الجنائي بأنه : "البرهان القائم على المنطق والعقل في إطار من الشريعة الإجرائية لإثبات صحة افتراض أو لرفع درجة اليقين الإقناعي أو حفظها في واقعة محل خلاف".

ومن هذا التعريف تظهر السمات الأساسية المحددة للدليل الجنائي، والتي تتمثل بأنه برهان يقوم على المنطق والعقل، ويهدف إلى الإقناع بما يكفل الحرية في أسلوبه وشكله ونوعه، ويرفض القيود على إطلاقه

---

[1]- خولة عباسي: **الوسائل الحديثة للإثبات الجنائي في القانون الجزائري**، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، بإشراف الأستاذ: دبابش عبد الرؤوف، جامعة محمد خيضر، بسكرة، 2013، ص: 9.

[2]- أحمد إبراهيم: **طرق الإثبات الشرعية**، كلية الحقوق، مصر، العدد01، 1مارس 1993.

[3]- هلالي عبد الإله أحمد: **النظرية العامة للإثبات في المواد الجنائية**، دار الكتاب الحديث، ص:339.

إلا بما كان مرتبطا بالتشريعات القانونية. وهناك أنواع من الأدلة الجنائية الإجرائية، أدلة قانونية، وأدلة مادية وأدلة قولية، وأدلة فنية. فالأدلة الشرعية (القانونية) هي مجموع الأدلة التي حددها المشرع وعين قوة كل منها، بحيث لا يمكن الإثبات بغيرها، كما لا يمكن للقاضي أن يعطي القوة لأي دليل منها أكثر مما أعطاها المشرع.

أما الدليل المادي فهو الذي ينبعث من عناصر مادية، والدليل القولي هو الذي يتمثل فيما يصدر عن الغير من أقوال تؤثر في قناعات القاضي (مثل اعتراف المتهم وشهادة الشهود..). أما الدليل الفني فالمقصود به ما ينبعث من رأي الخبير حول تقدير دليل مادي أو قولي قائم في الدعوى، وهو عادة ما يقدمه الخبراء من نتائج حاسمة في مسائل فنية لا تستطيع المحاكم بحكم تكوين أعضائها الوصول إليها.

ويلاحظ أن هناك خلط لدى الكثير من رجال القانون، بما فيهم العاملين في الأجهزة الأمنية، بين المقصود بالدليل المادي والأثر المادي، وهذا ما أدى إلى استحداث تعريف لكل منهما، حيث يعرف الدليل المادي بأنه (حالة قانونية تنشأ من استنباط أمر مجهول من نتيجة فحص علمي أو فني لأثر مادي تخلف عن جريمة وله من الخواص ما يسمح بتحقيق هويته أو ذاتيته). أما الأثر المادي فقد عرف بأنه: (كل ما يمكن إدراكه ومعاينته بالحواس، سواء كان جسما ذا جرم أو مجرد لون أو شكل أو رائحة) كأثر استعمال آلة ووجود بقع دموية أو غيرها، وبذلك يكون الأثر المادي مصدرا للدليل المادي وقد يشكل هذا الأثر دليلا بعد الفحص والمعالجة[1].

ثانيا: تعريف الدليل الرقمي:

عرف البعض الدليل الرقمي بأنه: "الدليل المأخوذ من أجهزة الحاسب الآلي. ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية، يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة. ويتم تقديمها في شكل دليل يمكن اعتماده أمام القضاء، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل: النصوص المكتوبة أو الصور، والأصوات والرسوم والأشكال، وذلك من أجل الربط بين الجريمة والمجرم والمجني عليه، وبشكل قانوني يمكن الأخذ به أمام أجهزة إنفاذ وتطبيق القانون"[2].

---

[1] - http://diae.net/1379310:37 تاريخ التصفح 25 03 2018 على الساعة

[2] - عبد الناصر محمد محمود فرغلي . محمد عبيد سيف سعيد المسماري: **الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة**، المؤتمر الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية، الرياض، 2007، ص:13.

أو هو: "معلومات يقبلها العقل والمنطق 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 أو شخص له علاقة بجريمة أو جان أو مجني عليه"[1].

في حين عرفه البعض الآخر بأنه: "الدليل الذي يجد له أساس في العالم الافتراضي ويقود إلى الجريمة"[2].

أما التعريف المقترح للدليل الرقمي أو الإلكتروني من قبل المنظمة الدولية لأدلة الحاسوب (OCEI)[3] فهو: "المعلومات المخزنة أو المتنقلة في شكل ثنائي، ويمكن أن يعتمد عليها في المحكمة"[4]. وهو نفس المعنى تقريبا المتبنى من قبل الفريق العلمي العامل على مستوى الأدلة الرقمية (SWGDE)[5]، باعتبار هذا الأخير أنشئ من أجل توحيد الجهود التي تقوم بها المنظمة الدولية لأدلة الحاسوب (OCEI)، وتطوير مختلف التخصصات والمبادئ التوجيهية من أجل استرداد، المحافظة، ودراسة الأدلة الرقمية بما فيها الصوتية والمصورة[6].

---

[1]- محمد الأمين البشري: **التحقيق في الجرائم المستحدثة**، جامعة نايف للعلوم الأمنية، الرياض، 2004، ص: 234.

[2]- عمر محمد بن يونس: **مذكرات في الإثبات الجنائي عبر الانترنت**، ندوة الدليل الرقمي بمقر جامعة الدول العربية بمصر، الفترة من 5 إلى 8 مارس 2006، ص:5.

[3] -Organization of Computer Evidence International .

[4] -Electronic evidence is" information stored or transmitted in binary from that may be relied upon in court ". Eoghan Casey : op.cit.p,261.

[5] -Standard Working Group on Digital Evidence .

[6]- عائشة بن قارة مصطفى: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، دار الجامعة الجديدة، الإسكندرية، 2010، ص:54 . 55.

الفرع الثاني: خصائص الدليل الجنائي الرقمي:

يتميز الدليل الجنائي الرقمي عن الدليل الجنائي العادي أو التقليدي بالخصائص التالية:

1: الأدلة الرقمية تتكون من بيانات ومعلومات ذات هيئة إلكترونية غير ملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية، واستخدام نظم برامجية حاسوبية.

2: الأدلة الرقمية ليست أقل مادية من الأدلة المادية فحسب، بل تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن[1]. وذلك لأن مصطلح الدليل الرقمي يشمل كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميا، بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني[2].

3: يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها ذات القيمة العلمية والحجية الثبوتية، الشيء الذي لا يتوفر في أنواع الأدلة الأخرى، مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد، والتلف والتغيير، عن طريق عمل نسخ طبق الأصل من الدليل[3].

4: الأدلة الرقمية يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد اختفائها، مما يؤدي إلى صعوبة الخلاص منها وهي خاصية من أهم خصائص الدليل الرقمي بالمقارنة بالدليل التقليدي، فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغاؤها، سواء تم ذلك بالأمر supprimer وحتى ولو تم عمل إعادة تهيئة أو تشكيل للقرص الصلب بالأمر formater والبرامج التي تم إتلافها أو إخفاؤها سواء أكانت صورا أو رسوما أو كتابات أو غيرها، مما يعني صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة، طالما تم علم رجال البحث والتحقيق الجنائي بوقوع الجريمة.

5: الأدلة الجنائية الرقمية ذات طبيعة ديناميكية فائقة السرعة، تنتقل من مكان إلى آخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان[4].

---

[1]. محمد الأمين البشري:**التحقيق في الجرائم المستحدثة**، المرجع السابق، ص: 237 وما بعدها.

[2]- Eoghan Casey : Digital evidence and forensicscience, computer and the internet, computer crime, 1st ed Academic Press_ USA UK 200 .P ;9 .

[3]- عمر محمد بن يونس: **مذكرات في الإثبات الجنائي عبر الانترنت**، المرجع السابق، ص: 12.

[4]- عبد الناصر محمد محمود فرغلي . محمد عبيد سيف سعيد المسماري: **الإثبات الجنائي بالأدلة الرقمية**، المرجع السابق، ص: 15.

6: يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت، فالدليل الرقمي يمكنه أن يسجل تحركات الفرد، كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي[1].

المطلب الثاني: تقسيمات الدليل الرقمي:

تختلف الجريمة الإلكترونية عن الجريمة العادية في كون الأولى تتم في بيئة غير مادية عبر نظام حاسب آلي، أو شبكة المعلومات الدولية –الانترنت- حيث يمكن للجاني عن طريق (نبضات إلكترونية رقمية) لا ترى أن يعبث في بيانات الحاسب أو برامجه وذلك في وقت قياسي قد يكون جزءا من الثانية، كما يمكن محوها في زمن قياسي كذلك قبل أن تصل يد العدالة إليه، مما يصعب الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على الدليل المتوافر[2].

الفرع الأول: التقسيمات التشريعية والقضائية للدليل الرقمي:

برزت عدة تشريعات حاولت تقسيم الدليل الرقمي وإحاطة كل مل يتعلق به، والقضاء أيضا كان له دور في معالجة موضوع الدليل الإلكتروني، وكذا العمل على إعطاء تقسيمات له، إلا أن تشريع الولايات المتحدة الأمريكية كان من السباقين الذين تطرقوا لهذا الموضوع.

وفقا لما قررته وزارة العدل الأمريكية سنة 2002 فإن الدليل الرقمي يمكن تقسيمه إلى ثلاث مجموعات هي كالتالي:

1: **السجلات المحفوظة في الحاسوب:** وهي الوثائق المكتوبة والمحفوظة مثل البريد الإلكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الانترنت.

2: **السجلات التي تم إنشاؤها بواسطة الحاسوب:** وتعتبر مخرجات برامج الحاسوب وبالتالي لم يلمسها الإنسان، مثل سجلات الهاتف وفواتير أجهزة السحب الآلي.

---

[1]- أنظر: ممدوح عبد الحميد عبد المطلب: **استخدام بروتوكول TCP IP في بحث وتحقيق الجرائم على الكمبيوتر**، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، رقم العدد:4، المحور الأمني الإداري، تاريخ الانعقاد: 26أفريل 2003، دبي، الإمارات العربية المتحدة، ص: 649 . 650.

[2]- نبيل عبد المنعم جاد: **جرائم الحاسب الآلي**، بحث منشور بندوة المواجهة الأمنية للجرائم المعلوماتية، مركز دعم اتخاذ القرار بالقيادة العامة لشرطة دبي، مطبعة بن دسمال، دبي، 2005، ص: 128.

3: **السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشاؤه بواسطة الحاسوب:** ومن الأمثلة عليها: أوراق العمل المالية التي تحتوي على مدخلات تم تلقيمها إلى برامج أوراق العمل مثل Excel ومن ثم تمت معالجتها من خلال البرنامج بإجراء العمليات الحسابية عليها، ويلاحظ أن التنوع في الدليل الرقمي يفيد بالضرورة أنه ليس هناك وسيلة واحدة للحصول عليه، وإنما تتعدد وسائل التوصل إليه.

في كل الأحوال يظل الدليل المستمد منه رقميا، حتى وإن اتخذ هيئة أخرى، ففي هذه الحالة فإن اعتراف القانون بهذه الهيئة الأخرى يكون مؤسسا على طابع افتراضي، مبناه أهمية الدليل الرقمي ذاته وضرورته، إلا أنه لكي يحدث تواصل بين القانون وبين الدليل المذكور ـ نتيجة لنقص توافر الإمكانيات الرقمية في المحاكم ـ فإنه يلزم اتخاذ مسلك الافتراض من حيث اعتباره دليلا أصليا[1] .

الفرع الثاني: تقسيمات أخرى للدليل الإلكتروني (الرقمي):

هناك تقسيمات أخرى للدليل الرقمي، فقد أعطى الفقهاء احتمالات عديدة للدليل الرقمي، وهذا ما سنحاول إيضاحه من خلال ما سيقدم، لمحاولة الإلمام بجميع أنواع الدليل الإلكتروني:

أولا: قسم الدليل الرقمي في إحدى التقسيمات تبعا لمكوناته إلى:

1: **الأشرطة المغناطيسية:** وهذا الشريط هو عبارة عن شريط بلاستيكي مغطى بمادة قابلة للمغنطة، وهذا الشريط قد يكون ملفوفا على بكرة مثل التي تستخدم في أجهزة التسجيل الصوتي، وكذا قد يكون داخل علبة على هيئة شريط فيديو مثلا، وكل الأشرطة الممغنطة بها رأس للقراءة والكتابة يسجل البيانات، على شكل نقطة مغناطيسية على الشريط بشفرة خاصة تدل على البيانات المستخرجة من الحاسوب، كما يتمكن هذا الرأس من الإحساس بوجود هذه النقطة ويقوم بإرسال النبضات الكهربائية المقابلة لشفرة البيانات داخل الحاسوب.

2: **الأقراص المغناطيسية:** تعد من أفضل وسائط التخزين التي يمكن استخدامها للتخزين المباشر أو العشوائي، وهذا راجع لقدرتها الاستيعابية الكبيرة، ولها خاصية مهمة هي إمكانية القراءة أو التسجيل على أي قطاع من السطوح، وكذا إمكانية تغيير أو تعديل أي ملف عليها دون الحاجة إلى إنشاء ملف جديد، حيث يتم تعديل التسجيل وهو في موضعه.

[1]- عمر محمد بن يونس: **مذكرات في الإثبات الجنائي عبر الانترنت**، المرجع السابق، ص: 12.

ثانيا: تقسم الأدلة الإلكترونية بحسب مكان وجودها إلى:

1: أدلة ورقية مثل: مخرجات الحاسوب والتقارير والرسوم البيانية.

2: أجهزة الحاسبات: وهي التي تحتوي على ملحقات الحاسوب من شاشات وغير ذلك.

3: الأقراص المرنة والصلبة: تعتبر من أهم الأدلة الرقمية لاحتوائها على بيانات وكلمات المرور، وصور وتقارير وخطط ارتكاب الجريمة وغيرها.

4: أشرطة تخزين المعلومات: تستخدم لحفظ النسخ الاحتياطية.

5: القطع الإلكترونية: مثالها أجهزة الإرسال التي يجب أن تفحص للتأكد من طبيعتها خاصة في قضايا التجسس.

6: أجهزة المودم: وهي التي تستخدم في نقل المعلومات، ويمتاز بعضها بإمكانية أن يعمل كجهاز الرد على رسائل الهاتف، ويجب تسجيل الكابلات المتصلة به عند ضبطه.

7: البرامج: وهي التي تمثل الأدوات الرئيسية التي يستغلها المجرم في ارتكاب جريمة نظم المعلومات.

8: الطابعات والأجهزة الخاصة بتصوير المستندات، وما قد تحتويه من أوراق مطبوعة ومصورة، أو ما هو مخزن في ذاكرتها من معلومات[1].

من جهة أخرى يمكن اعتبار الأدلة الصوتية المخزنة إلكترونيا أدلة إثبات قاطعة، وهذا يعتمد على دقة الأجهزة المستخدمة في كشف التلاعب، وهذا عن طريق المراقبة الإلكترونية للمحادثات التليفونية مثلا، والمقصود بها التصنت على الأحاديث الخاصة بالمشتبه به، فهي من ناحية تشمل التصنت على المحادثات، ومن ناحية تسجيلها عن طريق أجهزة التسجيل، وهذا عن طريق إما استقبال المراسلات التليفونية، أو في مواجهة الرسائل اللاسلكية[2].

فإذا كانت الأجهزة المستخدمة في تخزين الأدلة الصوتية إلكترونيا دقيقة، وتكشف التلاعب عن طريق خبير تعتبر دليلا قاطعا، فهذا يكون وفقا لشروط، أولها: أن تكون منطوية على اعتداء على حق يحميه القانون، وثانيها: أن يكون هناك تحديد دقيق للشخصية المسجل صوتها أو البريد الإلكتروني الخاص بها، وثالثها: أن يكون تحديد الحديث المراد التقاطه وفق الجريمة المتعلقة بها وكذا الجريمة المصرح بها[3].

---

[1]- علي جبار الحسيناوي: **جرائم الحاسوب والانترنت**، (د.ط)، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009، ص: 143.

[2]- محمد الأمين خرشة: **مشروعية الصوت والصورة في الإثبات الجنائي**، (ط.1)، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص: 48 . 49.

[3]- علي جبار الحسيناوي: المرجع نفسه، ص: 144.

نقول أن هذه التقسيمات قد ألمت بجانب كبير ومهم من الأدلة الإلكترونية التي تعتبر من الأدلة القاطعة، ففي تقسيم الدليل الرقمي لا بد من الأخذ بعين الاعتبار التطور المستمر الذي يطرأ على هذا النوع من الأدلة من جهة، وعلى البيئة الافتراضية أو الإلكترونية من جهة أخرى، فهي أدلة متطورة بطبيعتها، كما تتطور وسائل الحصول عليها والتي يجب مراعاتها قانونيا، حتى يكون من الإمكان الاعتماد عليها كدليل إثبات في مختلف القضايا.

ملخص الفصل الأول:

وفي خلاصة هذا الفصل، يجدر بنا القول أن الجريمة الإلكترونية هي جريمة وليدة التطور العلمي والتكنولوجي الكبير الذي وصل إليه العالم. فرغم الوجه المشرق الذي يقدمه إلا أن له جانب آخر سلبي عندما يستعمل في غير الغرض الذي وجد من أجله، وهذا النوع المستحدث من الجرائم مرتكب من طرف أصناف يعرفون بالمجرمين المعلوماتيين الذين يتميزون بالذكاء والفطنة ومدى تكيفهم بالمجتمعات الأخرى. ورأينا أن هذه الجريمة يتولد عنها نوع جديد من الأدلة الجنائية، وهو الدليل الرقمي الذي هو عبارة عن معلومات مخزنة في الحاسبات الآلية وغيرها من الإلكترونيات، أي أنه ذو هيئة إلكترونية غير ملموسة لا تدرك بالحواس، وهذه أهم خاصية تميز الدليل الرقمي عن غيره من الأدلة الجنائية.

الفصل الثاني

إثبات الجريمة الإلكترونية

وحجية الدليل الرقمي

في الإثبات الجنائي

الفصل الثاني: إثبات الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي

تمهيد:

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

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

ونظرا للطبيعة الخاصة التي يتمتع بها الدليل الإلكتروني، فإن حجيته على مستوى الإثبات الجنائي قد تثير عدة مشاكل خاصة فيما يتعلق بمصداقيته.

وعليه نقسم هذا الفصل إلى مبحثين وهما:

المبحث الأول: ضبط الجريمة الإلكترونية وطرق إثباتها.

المبحث الثاني: حجية الدليل الرقمي في الإثبات الجنائي.

المبحث الأول: ضبط الجريمة الإلكترونية وطرق إثباتها:

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

ولدراسة كيفية ضبط وطرق إثبات الجريمة الإلكترونية قسمنا مبحثنا هذا إلى مطلبين اثنين:

المطلب الأول: ضبط الجريمة الإلكترونية.

المطلب الثاني: طرق إثبات الجريمة الإلكترونية.

[1]- محمود محمود مصطفى: **الإثبات في المواد الجنائية في القانون المقارن**، (د.ط)، مطبعة جامعة القاهرة، القاهرة، 1977، ص: 139.

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 هذه الأنماط الجديدة، والتي يتوجب معها تحديث الأنظمة والتعليمات والجهات الأمنية المختصة بمعالجة القضايا الناتجة عن ظهور هذه الأنماط الجديدة، وهو ما يتبع بتطوير أسلوب التحقيق فيها وكيفية إثباتها[1].

ولدراسة هذا المطلب تطرقنا إلى القواعد العامة التي تحكم إثبات الجريمة الإلكترونية في (الفرع الأول)، ومن ثم انتقلنا 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 لاستخلاص الأدلة منها.

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

ثالثا: من زاوية وظيفة الدليل الإثباتية: فهنالك 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، وآثار الأقدام العارية، والشهادة بالرؤية، والاعتراف، وضبط محصلات الجريمة في حوزة المتهم، آثار المقاومة على جسده أو بأظافر المجني عليه، أو التحديد غير القاطع يشير إلى مجرد احتمال لتحديد شخصية الجاني وهي مجرد قرائن.

[1]- محمد علي العريان: **الجرائم المعلوماتية**، المرجع السابق، ص: 31.

رابعا: من زاوية مضمون الدليل: هناك أدلة مادية محسوسة بإحدى الحواس، وهناك أدلة معنوية مثل الشهادة، وأدلة قولية مثل أقوال المتهم[1].

ولذلك فقواعد الإثبات النظامية يقصد بها الأدلة التي حددها المنظم وعين حالات استخدامها ومدى حجيتها، وبالرغم من أن هناك من يعد تلك الأدلة الإلكترونية مرحلة متقدمة من الأدلة المادية، أو أدلة فنية لأنها تنبعث من رأي خبير فني، إلا أنها تعد نوعا متميزا من وسائل الإثبات، وذلك بسبب كونها نبضات غير محسوسة، وأن حجمها وشكلها تخيلي وأنها سريعة الانتقال، ويمكن استخراج نسخ من الأصل والحصول على نفس الدليل الموجود بمسرح الجريمة التقليدي بالمسرح الإلكتروني أو بمسرح الكتروني آخر، وقد يكون بمقدور المحققين استرجاع الدليل بعد حذفه[2].

الفرع الثاني: ضوابط إثبات الجريمة الإلكترونية:

تنقسم ضوابط إثبات الجريمة الإلكترونية إلى ضوابط إثبات الجريمة بالأدلة العلمية، وضوابط إثبات الجريمة بالأدلة الإجرائية.

ويمكن توضيحهما كما يلي:

أولا: ضوابط إثبات الجريمة الإلكترونية بالأدلة الإلكترونية: يحتاج إثبات الجرائم الإلكترونية إلى دليل رقمي، كوسيلة لإثبات ارتكاب جريمة الاختراق 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 استخدم في الاختراق أو التعدي، لتعزيز دليل سبق تقديمه سواء بالنفي أو الإثبات للواقعة التي ثار الشك بشأنها[3]، ويحتاج إجراء هذه التجارب إلى محقق جنائي

---

[1]- ثنيان ناصر آل ثنيان: **إثبات الجريمة الإلكترونية**، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، إشراف: الدكتور/ جلال الدين محمد صالح، جامعة نايف للعلوم الأمنية، الرياض، 2012، ص: 72 . 73.

[2]- محمد الأمين البشري: **التحقيق في جرائم الحاسب والانترنت**، المجلة العربية للدراسات العربية والتدريب، المجلد:15، العدد: 30، جامعة نايف للعلوم الأمنية، الرياض، 2001، ص: 115.

[3]- عبد الفتاح بيومي حجازي: **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت**، (د.ط)، دار الكتب القانونية، مصر، (د.س.ن)، ص: 49 . 50.

وفني متخصص لديه مهارات فنية وتقنية لاستخلاص الأدلة الرقمية، لأن الفصل في الدعوى الجزائية في هذه الحالة يتوقف على الرأي الفني الذي يثبت أو ينفي ارتكاب الجريمة من قبل المشتبه به[1].

والدليل العلمي هو النتيجة التي تسفر عنها التجارب العلمية والمعملية لتعزيز دليل سبق تقديمه، سواء للإثبات أو نفي واقعة ثارت شكوك حولها. وهو لا يعدو كونه رأيا فنيا يعتمد على الخبرة ومهارة فني متخصص يحدد إذا كان الاختراق والتعدي قد تم من حاسب المشتبه به أم لا[2].

إن عدم الاعتداد بالخبرة الفنية كوسيلة لإثبات الجريمة الإلكترونية، واعتبارها بمثابة قرائن فقط، يضيف صعوبة أخرى إلى صعوبات اكتشاف المجرم وتحديده، في ضوء عدم تسليم الأمور التي تحكم الدليل الرقمي في الفكر الجنائي خارج نطاق تلك الجرائم.

وهناك ضرورة لاعتبار الخبرة الفنية في الجرائم الإلكترونية دليلا ماديا، فهي وسيلة علمية في مواجهة الجريمة الإلكترونية في ضوء طبيعة هذه الجريمة التي تعتمد على نبضات إلكترونية، يتم من خلال التلاعب بقواعد البيانات في المنظمات، وذلك بالإضافة أو الحذف أو التعديل وإخراج مخرج أو وثيقة إلكترونية مزورة بصورة صحيحة، مستغلا مهاراته في الدخول على النظام والقيام بالجرائم الإلكترونية والتلاعب التي يصعب كشفها بالطرق التقليدية، مما يحتم الاستعانة بأساليب علمية وخبرات فنية ذات فاعلية في إثبات الجريمة الإلكترونية، والعمل على تطويرها والاستفادة من فاعليتها في إثبات هذه الجرائم.

ومن خلال ذلك، يمكن توضيح الأدوات العلمية لضبط إثبات الجريمة على أنها: (أدوات تقوم بضبط الجريمة كغالبية برامج الحماية، وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وأدوات التصنت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات، وأدوات الضبط الأخرى، ويمكن استخدام الأدوات المستخدمة في الجريمة كأداة ضبط مثل: أدوات جمع المعلومات عن الزائرين للمواقع)[3].

---

[1]- محمود نجيب حسني: **شرح قانون الإجراءات الجنائية**، (ط.2)، دار النهضة العربية، القاهرة، 1987، ص: 474.

[2]- محمد حماد الهيتي: **جرائم الحاسوب: ماهيتها،أهم صورها والصعوبات التي تواجهها**، (د.ط)، دار المناهج للنشر والتوزيع،عمان، 2005،ص: 232. وما بعدها.

[3]- محمد علي العريان: **الجرائم المعلوماتية**، المرجع السابق، ص: 44 . 45.

ثانيا: ضوابط إثبات الجريمة الإلكترونية بالأدلة الإجرائية:

الضوابط الإجرائية هي الأساليب التي تستخدم لإثبات وقوع الجريمة وتحديد شخصية مرتكبها. وهذه الأساليب ذات فاعلية في التحقيق الفني، حيث تسهم في إثبات الجريمة وبيان الغموض وإيجاد العلاقة بين الجاني والمجني عليه من قبل المحقق الفني، باستخدام تقنيات وبرامج التتبع الإلكتروني والتفتيش الإلكتروني والضبط الإلكتروني، التي تتميز بقدرات فائقة على القيام بمهام التتبع والاسترجاع للبرامج والأدوات التي استخدمت في الاختراق والتعدي وارتكاب الجريمة، ويمكن توضيح هذه الضوابط حسب الطريقة المتبعة للوصول وحسب البرنامج المتبع. ومن تلك الطرق:

1- الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته:

يجب على المحقق الفني الاطلاع على 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، وإجراءات أمن العاملين وأسلوب النسخ الاحتياطي، وبرامج الحماية المتوفرة[1].

2- إظهار الحقائق:

يجب على المحقق إظهار الحقائق خلال مرحلة جمع الاستدلالات الإلكترونية، وإثباتها في محضره نظرا لأهميتها في تحديد الجريمة، ورسم خطوات البحث من خلال التثبت من توافر أركان الجريمة، وتحديد مكان الجريمة ووصفه، وتحديد وقت وقوع الجريمة، وتحديد أسلوب ارتكاب الجريمة، وأداة ارتكاب الجريمة، والظروف المحيطة بالجريمة، ودوافع الجريمة[2].

3- التحقق من توافر أركان الجريمة:

يحدد وقوع جريمة ما توفر ركنين أساسيين وهما: الركن المادي: ويقصد به الواقعة أو الضرر المادي للجريمة، ويتمثل في نشاط الفاعل والنتيجة التي يحققها والعلاقة السببية بينهما. والركن الآخر هو: الركن

[1]- محمد علي العريان: **الجرائم المعلوماتية**، المرجع السابق، ص: 81.

[2]- محمد فاروق عبد الحميد كامل: **القواعد الفنية الشرطية للتحقيق والبحث الجنائي**، جامع نايف العربية للعلوم الأمنية، الرياض، 1999، ص: 66 .67.

المعنوي: ويقصد به الإرادة التي اقترن بها الفعل المرتكب، ويأخذ صورة القصد الجنائي في الجريمة المتعمدة، وصورة الخطأ في الجريمة غير المقصودة.

4- 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 للخبراء، وسماع شهود واستجواب لأطراف الجريمة، وجمع التحريات، وهو من كل هذه الإجراءات يستخلص العديد من الأدلة، ويحاط علما بكثير من الوقائع المتصلة بالجريمة والتي تختلف في قوة ثبوتيتها، وتأتي في أعقاب ذلك مرحلة يجد فيها المحقق نفسه وأمامه مجموعة ضخمة من الأدلة والوقائع التي تمكن من جمعها[1].

الفرع الثالث: عناصر إثبات الجريمة الإلكترونية:

هناك العديد من العناصر المختلفة لإثبات الجريمة الإلكترونية، والتي يمكن توضيحها فيما يلي:

أولا: العنصر الأول: إظهار الركن المادي للجرائم الإلكترونية:

إن النشاط أو السلوك المادي في جرائم الانترنت يتطلب وجود بيئة رقمية واتصال بالانترنت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته. فمثلا: يقوم مرتكب الجريمة بتجهيز الكمبيوتر لكي يحقق له حدوث الجريمة، فيقوم بتحميل برامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد مخلة بالآداب العامة وتحميلها على جهاز المضيف، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها.

لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الإجرامي في نطاق الجرائم الإلكترونية، حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تكنولوجيا المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق، وبرامج فيروسات، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور مخلة بالآداب للأطفال، فمثل هذه الأشياء تمثل جريمة في حد ذاتها[2].

---

[1]- محمد سامي الشوا: **ثورة المعلومات وانعكاساتها على قانون العقوبات**، (د.ط)، دار النهضة العربية، القاهرة، 2000، ص: 74.

[2]- ممدوح عبد الحميد عبد المطلب: **جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية: الجريمة عبر الانترنت**، (د.ط)، مكتبة دار الحقوق، الشارقة، 2001، ص: 226.

ثانيا: العنصر الثاني: إظهار الركن المعنوي للجرائم الإلكترونية:

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني. ويتحد الركن المعنوي للجريمة الإلكترونية من خلال مبدأ الإرادة ومبدأ العلم، فالمجرم المعلوماتي تارة يستخدم الإرادة للتخطيط للجريمة، وتارة يستخدم العلم من أجل تنفيذ الجريمة الإلكترونية[1].

ثالثا: العنصر الثالث: تحديد وقت ومكان ارتكاب الجريمة الإلكترونية:

تثير مسألة النتيجة الإجرامية في جرائم الانترنت مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الإجرامية، فلو قام أحد المجرمين في أمريكا اللاتينية باختراق جهاز خادم أحد البنوك في الإمارات، وهذا الخادم موجود في الصين، فكيف يمكن معرفة وقت حدوث الجريمة، هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في الصين؟ وهذا بالتالي يثير مشكلة أخرى وهي مكان ارتكاب الجريمة الإلكترونية، ويثار أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن، حيث أن هناك بعد دولي في هذا المجال ذلك أن الجريمة الإلكترونية جريمة عابرة للحدود[2].

رابعا: العنصر الرابع: علانية التحقيق:

إن علانية التحقيق من الضمانات اللازمة لتوافر العدالة، ولهذا قيل أن العلانية في مرحلة المحاكمة لا يقتصر فيها الأمر على وضع الاطمئنان في قلب المتهم، بل أن فيها بذاتها حماية لأحكام القاضي من أن تكون محلا للشك أو الخضوع تحت التأثير، كما فيها اطمئنانا للجمهور على أن الإجراءات تسير في طرق طبيعية. والعلانية المقررة للتحقيق في الإجراءات الجنائية هي من بين الضمانات الخاصة به، وهي تختلف في التحقيق الابتدائي عنها في مرحلة المحاكمة. ففي الابتدائي تعتبر العلانية نسبية قاصرة على الخصوم في الدعوى الجنائية، والعلانية في التحقيق النهائي أو مرحلة المحاكمة هي علانية مطلقة، بمعنى أنه يجوز لأي فرد من أفراد الجمهور الدخول إلى قاعة الجلسة وحضور المحاكمة[3].

---

[1]- محمد علي العريان: **الجرائم المعلوماتية**، المرجع السابق، ص: 157.

[2]- محمد محمد شتا: **فكرة الحماية الجنائية لبرامج الحاسب الآلي**، (د.ط)، دار الجامعة الجديدة، القاهرة، 2000، ص: 192.

[3]- فهد إبراهيم السبهان: **استجواب المتهم بمعرفة سلطة التحقيق**، (د.ط)، مطبعة بن دسمال، دبي، 1995، ص: 52.

المطلب الثاني: طرق إثبات الجريمة الإلكترونية:

إن التطور التقني في شبكة الانترنت سوف يقود دون شك إلى تغيير كبير، إن لم يكن كليا في المفاهيم السائدة حول الدليل. ويقود مثل هذا القول في الحقيقة إلى إعلان انضمام الخبرة التقنية إلى علم الخبرة المتميزة للتعامل مع موضوع الدعوى، من حيث ضرورة الاستعانة بالمختصين في مجال النزاع[1].

ويعد كل من المعاينة والتفتيش والشهادة والإقرار، أحد وسائل جمع الأدلة ولكل منها قواعده يتم إتباعها[2].

وعليه نقسم المطلب إلى ثلاثة فروع:

الاستدلالات الأولية لإثبات الجريمة الإلكترونية في (الفرع الأول)، إثبات الجريمة الإلكترونية بالشهادة والاعتراف في (الفرع الثاني)، وإثبات الجريمة الإلكترونية بالخبرة الفنية في (الفرع الثالث).

الفرع الأول: الاستدلالات الأولية لإثبات الجريمة الإلكترونية:

يمكن توضيح طرق الاستدلالات الأولية لإثبات الجريمة الإلكترونية من خلال ما يلي:

أولا: تلقي وضبط البلاغ: يعرف ضبط البلاغ على أنه: "وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها"[3]. والضبط بهذا المعنى ينصرف إلى الأشياء دون الأشخاص. وبناء على ذلك، يجب توضيح مدى صلاحية الجرائم المرتكبة في البيئة الإلكترونية لضبط البلاغ. ويعد البلاغ هو المشكلة الحقيقية التي تواجه الجريمة الإلكترونية، فغالبية المنظمات تخشى من الإبلاغ لكي لا تفقد ثقة عملائها، ومن ثم يفلت مرتكب الجريمة الإلكترونية بفعله نتيجة إحجام المنظمات والشركات والمؤسسات المالية عن الإبلاغ خوفا على سمعتها، حيث تفضل هذه المرافق عدم إبلاغ السلطات المختصة للمحافظة على ثقة عملائها أكثر من اهتمامها بكشف الجريمة، ويفضلون الترضية المالية لعملائهم ومنحهم الأموال التي سلبت منهم نتيجة الاختراق والتعدي[4].

---

[1]- هشام فريد رستم: **الجوانب الإجرائية للجرائم المعلوماتية**، (د.ط)، مكتبة الآلات الحديثة، أسيوط، مصر، 1994، ص: 141ومابعدها.

[2]- عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري: **الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة**، المرجع السابق، ص:16.

[3]- عبد الفتاح مصطفى الصيفي: **تأصيل الإجراءات الجنائية**، (د.ط)، دار المعرفة الجامعية، الإسكندرية، 2002، ص: 225.

[4]- محمد حماد الهيتي: **جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها**، المرجع السابق، ص: 218

ومن خلال ما تقدم، يمكن تلقي وضبط البلاغ كما يلي:

1. بالنسبة للجرائم الواقعة على المكونات المادية للبيئة الإلكترونية:

بالنسبة للجرائم الواقعة على المكونات المادية للبيئة الإلكترونية فإن الأمر لا يثير أي صعوبة تذكر، ذلك أن الضبط يرد بالأساس على الأشياء المادية محل الجريمة المرتكبة[1].

2. بالنسبة للجرائم الواقعة على المكونات غير المادية للبيئة الإلكترونية:

فيما يتعلق بهذه الجرائم فإن الأمر يثير العديد من الإجراءات، يمكن توضيحها كما يلي:

أ): بالنسبة للبرامج التطبيقية ونظم التشغيل: وفي هذه الحالة يمكن ضبط أدلة الجريمة إذا كان محلها سرقة الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في نسخه بصورة غير مشروعة أو إتلافه بوسائل تقليدية. ولكن الأمر يزداد صعوبة في حال استخدام وسائل فنية في إتلاف البرامج كالفيروسات مثلا، ويتمثل مكمن الصعوبة في هذه الحالة في قلة الخبرة لدى الجهات الأمنية باعتبارها الجهة الأصلية المختصة بالضبط. وهناك صعوبة ثانية تتصل باتساع الشبكة الإلكترونية، فقد يؤدي الضبط إلى عزل النظام الإلكتروني بالكامل عن دائرته لمدة زمنية طويلة، وهو ما يسبب حتما أضرارا بالجهة مستخدمة النظام، هذه النتيجة المتوقعة من عملية الضبط ستؤدي حتما إلى امتناع مستخدمي الأنظمة الإلكترونية من التعاون الكامل والفعال مع سلطة التحقيق، الأمر الذي يخلق إشكالية كبيرة تواجه إجراءات الضبطية القضائية[2].

ب): بالنسبة للبيانات الرقمية: في هذه الحالة يصطدم المحقق الجنائي بعوامل عدة تحول دون ضبطه للبيانات التي تعد دليلا على ارتكاب الجريمة، وتكمن هذه العوامل في عدم وجود دليل مرئي يمكن فهمه بالقراءة، بالإضافة إلى عدم وجود آثار مادية يمكن على أساسها الاستدلال على وجود دليل ارتكاب الجريمة. ويتجلى ذلك في جرائم الاختلاس والتزوير التي تستعمل فيها التقنية الالكترونية، وحتى البيانات

[1]- عبد الفتاح مصطفى الصيفي: **تأصيل الإجراءات الجنائية**، المرجع السابق، ص: 119.

[2]- سعيد عبد اللطيف حسين: **إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت: الجرائم الواقعة في جرائم تكنولوجيا المعلومات**،(د.ط)، دار النهضة العربية، القاهرة، 1999، ص: 42.

التي يمكن الوصول إليها يستطيع الجاني أن يدمرها في فترة زمنية قصيرة تعد بالثواني، بالإضافة إلى الخبرة الفنية المتطلبة لفحص هذه الأدلة لتحديد البيانات التي تصلح كأدلة إدانة للجاني من عدمها[1].

ومن خلال ما سبق، فالبلاغ إجراء يصدر عن الغير أو عن المجني عليه في غير الجرائم التي يتوقف تحريك الدعوى الجنائية فيها على الشكوى، بهدف إحاطة المختص علما بوقوع جريمة أو واقعة مخالفة للقانون.

والأصل أن يقبل رجل الضبط الجنائي جميع البلاغات والشكاوى التي ترد إليه بشأن الجرائم بغض النظر عن شخصية الشاكي أو صفته، فقد يكون المتقدم بالبلاغ أو الشكوى الجاني أو المجني عليه، أو أي فرد من عامة الناس[2].

ومن خلال ما تقدم، يجب على رجال الضبطية، كل على حسب اختصاصه، أن يقبلوا البلاغات والشكاوى التي ترد إليهم في جميع الجرائم، وأن يقوموا بفحصها وجمع المعلومات المتعلقة في محضر رسمي، ومن ثم إرسالها إلى الجهة المختصة[3].

ثانيا: المعاينة:

يقصد بالمعاينة: "مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها، أو محوها، أو تعديلها". والمعاينة من إجراءات التحقيق الابتدائي. ويجوز للمحقق اللجوء إليها متى رأى لذلك ضرورة تتعلق بالتحقيق. والأصل أن يحضر أطراف الدعوى المعاينة، وقد يقرر المحقق أن يجريها في غيبتهم، ولا يلتزم المحقق بدعوة محامي المتهم للحضور، ومجرد غياب المتهم عند إجراء المعاينة ليس من شأنه أن يبطلها.

وتظهر أهمية المعاينة عقب وقوع جريمة من الجرائم التقليدية، حيث يوجد مسرح فعلي للجريمة يحتوي على آثار مادية فعلية، يهدف القائم بالمعاينة إلى التحفظ عليها تمهيدا لفحصها لبيان مدى صحتها في الإثبات. وليس الحال كذلك بالنسبة للجرائم الإلكترونية، حيث يتخلف عن ارتكابها آثار مادية، وقد تطول الفترة الزمنية بين وقوع الجريمة واكتشافها، مما يعرض الآثار الناجمة عنها إلى المحو أو التلف أو العبث بها.

---

[1]. محمد حماد الهيتي: **جرائم الحاسوب: ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها**، المرجع السابق، ص: 239.

[2]- مأمون محمد سلامة: **الإجراءات الجنائية في التشريع المصري**، (د.ط)، دار الفكر العربي، القاهرة، 1991، ص: 474.

[3]- ثنيان ناصر آل ثنيان: **إثبات الجريمة الإلكترونية**، المرجع السابق، ص: 54 . 55.

وإذا تمت المعاينة بعد وقوع الجريمة في المجال الإلكتروني، فيجب مراعاة ما يلي:

1. تصوير الحاسب والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل صورة.
2. العناية بملاحظة الطريقة التي تم بها إعداد النظام.
3. ملاحظة وإثبات حالة التوصيلات والكابلات المتصلة بكل مكونات النظام حتى يمكن إجراء عمليات المقارنة والتحليل حين عرض الأمر فيما بعد على المحكمة.
4. عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء اختبارات للتأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.
5. التحفظ على المعلومات سلة المهملات من الأوراق الملقاة أو الممزقة وأوراق الكربون المستعملة والشرائط والأقراص الممغنطة غير السليمة وفحصها، ويرفع من عليها البصمات ذات الصلة بالجريمة.
6. التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة، لرفع ومضاهاة ما قد يوجد عليها من بصمات.
7. قصر مباشرة المعاينة على الباحثين والمحققين الذين تتوافر لهم الكفاءة العلمية والخبرة الفنية في مجال الحاسبات الآلية[1].

ثالثا: التحري وكشف غموض الجرائم الإلكترونية:

تتسم الجرائم ذات الصلة بالحاسب الآلي بحداثة أساليب ارتكابها، وسرعة تنفيذها وسهولة إخفائها ودقة وسرعة محو آثارها. هذه الخصائص العامة تقتضي أن تكون جهات التحري والتحقيق بل والمحاكمة على درجة كبيرة من المعرفة بأنظمة الحاسب الآلي، وكيفية تشغيلها وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها من حيث كشفها وضبط الأدوات التي استخدمت في ارتكابها، والتحفظ على البيانات أو الأجهزة التي استخدمت في ارتكابها أو تلك التي تكون محلا للجريمة[2].

---

[1]- ممدوح عبد الحميد عبد المطلب: **أدلة الصور الرقمية**، ورقة عمل مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة: الجرائم الإلكترونية الملامح والأبعاد، المنعقدة بكلية الملك فهد الأمنية بالرياض في الفترة من 22 إلى 24 أفريل 2007، كلية الملك فهد الأمنية، الرياض، 2007، ص: 533.

[2]- محمد أبو العلا عقيدة: **التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية**، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في الفترة من 26 إلى 28 أفريل 2003، مركز البحوث والدراسات، أكاديمية شرطة دبي، 2003، ص: 6.

وأساليب التحري أو التحقيق 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 مرتكبها، وجميع الأدلة المتعلقة بها.

ولكي تنتج التحريات آثارها الإجرائية يجب أن تتسم بما يلي[1]:

1. أن تتعلق بجريمة ارتكبت فعلا، لأن إذن جهة التحقيق يصدر استنادا عليها وهو إجراء من إجراءات التحقيق، ولا يصدر عن جريمة لم تقع أو محتملة. فلصدور إذن التفتيش يجب إجراء تحريات جدية تشير بوضوح إلى ارتكاب شخص معين جريمة إلكترونية، وفق دلائل وأمارات قوية تحدده وتنسب الجريمة إليه دون غيره تجنبا للمساس بحريته وحرمة مسكنه.

2. استخدام الوسائل المشروعة في إجراء التحريات، وعلى ذلك فلا يجوز استراق السمع أو التجسس من ثقوب الأبواب.

3. عدم التدخل في جلب الجريمة بالتحريض عليها وذلك لكي يسهل على رجال الضبطية اكتشافها وتحدد مرتكبها، لكونه على علم مسبق بها.

4. التقيد بقواعد الاختصاص النوعي والمكاني، لكي تكون إجراءاته منسجمة مع ما تنص عليه التعليمات فلا تبطل التحريات.

5. كفاية التحريات وجديتها بحيث تضمن معلومات وافية وصحيحة وكاملة وغير مغلوطة، بحيث يتخذها المحقق أساسا لتحقيقه فيما بعد[2].

[1]- عبد الفتاح مصطفى الصيفي: **تأصيل الإجراءات الجنائية**، المرجع السابق، ص: 228.

[2]- ثنيان ناصر آل ثنيان: **إثبات الجريمة الإلكترونية**، المرجع السابق، ص: 61 . 62.

رابعا: التفتيش:

التفتيش هو البحث في مستودع سر المتهم، وهو إجراء من إجراءات التحقيق يتطلب أوامر قضائية لمباشرته[1]. ويجب على المحقق الجنائي المبادرة لإجراء التفتيش وذلك قبل قيام الجاني بطمس معالم الجريمة، وإخفاء كل ما يتعلق بها، وهو يستطيع ذلك إذا اتسع له الوقت وسنحت له الفرصة[2].

والتفتيش في مدلوله القانوني بالنسبة للجرائم الإلكترونية لا يختلف عن مدلوله السائد في فقه الإجراءات 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 إلى أدلة تفيد إثبات الجريمة ونسبتها إلى المتهم بارتكابها[3].

لكن توجد بعض الصعوبات الإجرائية التي تعيق خضوع البيانات المخزنة آليا لقواعد التفتيش التقليدية، والتي منها تعدد الأماكن التي يوجد بها النظام المعلوماتي داخل أو خارج الدولة، وهناك صعوبة في تحديد الأشياء التي يهدف إلى ضبطها من عملية التفتيش، وغيرها من الصعوبات مثل: عدم اكتمال المعرفة المعلوماتية والتقنية لتنفيذ عملية التفتيش كما ينبغي أن تكون[4].

1. شروط التفتيش:

أ). الشروط الموضوعية تتمثل في المحل والسبب:

يجب أن يكون للتفتيش محل، الذي قد يكون الشخص أو المكان. ويشترط فيه أن يكون محددا أو قابلا للتحديد، وأن يكون مشروعا أي يرد على محل جائز قانونا. وبناء على ذلك، لا يجوز تفتيش دور السفارات، ومنازل السفراء، ورجال السلك السياسي الأجنبي، ولا يجوز تفتيش المدافع عن المتهم أو الخبير الاستشاري لضبط أوراق أو مستندات سلمها له المتهم لأداء مهمته الدفاعية[5].

---

[1]- رمزي رياض عوض: **مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها: دراسة تحليلية تأصيلية مقارنة**، (د.ط)، دار الفكر العربي، القاهرة، 2000، ص: 85.

[2]- نبيل عبد المنعم جاد: **أسس التحقيق والبحث الجنائي العملي**،(د.ط)، مطبعة كلية الشرطة، (د.ب.ن)، 2006، ص: 112.

[3]- عبد الإله أحمد هلالي: **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي**،(د.ط)، دار النهضة العربية، القاهرة، 1997، ص: 73.

[4]- عفيفي كامل عفيفي: **جرائم الحاسب الآلي وحقوق المؤلف والمصنفات الفنية**، (د.ط)، منشأة المعارف، الإسكندرية، 2000، ص: 344.

[5]- أحمد فتحي سرور: **الوسيط في قانون الإجراءات الجنائية**، (ط.4)، المجلد الأول، دار النهضة العربية، القاهرة، 1981، ص: 423.

كما يجب أن يكون للتفتيش سبب، ولا يقوم سبب التفتيش إلا إذا كان هناك جريمة قد وقعت.

ب) . الشروط الشكلية للتفتيش:

فهي بحسب الأصل لا تملكه إلا سلطة التحقيق وهي النيابة العامة. وبالتالي فالتفتيش يخضع للخصائص العامة التي تخضع لها كافة إجراءات التحقيق الابتدائي، وهي وجوب التدوين بمعرفة كاتب، والسرية عن الجمهور، وحضور الخصوم ووكلائهم كلما أمكن ذلك. كذلك لا بد أن يكون أمر التفتيش مسببا، وهذا التسبيب ضمان لتوافر العناصر الواقعية التي يتوافر بها سبب التفتيش بالمعنى الدقيق، وحتى يكون ذلك التسبيب تحت رقابة هيئة الحكم، وكذلك الدفاع، حتى يمكن مراقبة ما إذا كان إذن التفتيش صدر وفقا للشروط القانونية من عدمه، وحتى يمكن تقدير جدية صدوره، وهو أمر يقدره المحقق تحت رقابة محكمة الموضوع. وفي جميع الأحوال يحق للدفاع مراقبة ذلك انبعاثا من كفالة حق الدفاع[1].

2. التفتيش في الجرائم الرقمية (الإلكترونية):

والتفتيش في الجرائم الإلكترونية يكون محله كل مكونات الحاسب الآلي، سواء كانت مادية أو معنوية، وكذلك شبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش. وتشمل جميع مكوناته المادية، والمكونات المعنوية التي تشمل برامج النظام وبرامج التطبيقات سابقة التجهيز طبقا لاحتياجات العميل. ويستلزم تفتيش الحاسب الآلي مجموعة من الأشخاص لديهم الخبرة والمهارة التقنية في نظم الحاسب الآلي، كمشغلي الحاسب الآلي وخبراء البرامج ومديري النظم المعلوماتية[2].

خامسا: الضبط:

الغاية من التفتيش ضبط شيء يتعلق بالجريمة ويفيد في التحقيق الجاري بشأن الجريمة الإلكترونية، سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئا نتج عنها، أو غير ذلك مما يفيد في كشف الحقيقة. ونظرا لكون الضبط في مجال الجرائم الإلكترونية هو ضبط بيانات المعالجة الكترونيا، فقد أُثير التساؤل: هل يصلح هذا النوع من البيانات لأن يكون محلا للضبط؟

وقد انقسم الفقه القانوني إلى اتجاهين عند الإجابة عن هذا التساؤل:

---

[1]- عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري: **الإثبات الجنائي بالأدلة الرقمية**، المرجع السابق، ص: 19.

[2]- عبد الفتاح بيومي حجازي: **مبادئ الإجراءات الجنائية في جرائم الحاسب الآلي والانترنت**، المرجع السابق، ص: 388 وما بعدها.

1. الاتجاه الأول: يرى البعض أن بيانات الحاسب لا تصلح لأن تكون محلا للضبط، لانتفاء الكيان المادي عنها، ولا سبيل لضبطها إلا بعد نقلها على كيان 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 الأشياء المادية الملموسة.

2. الاتجاه الثاني: ويرى الاتجاه الثاني أن البيانات المعالجة إلكترونيا ما هي إلا ذبذبات إلكترونية أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره. ويستند هذا الاتجاه إلى أن بعض النصوص القانونية تنُصُّ على أن تفتيش وضبط الدفاتر والسجلات الخاصة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخة من المواد المكتوبة، حتى ولو كانت السجلات مكتوبة في شكل إلكتروني. وهذا الخلاف دعا المنظم في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط، ليشمل فضلا عن أشياء مادية محسوسة، البيانات المعالجة إلكترونيا، أو إصدار تشريعات تتعلق بالجريمة الإلكترونية، تتضمن القواعد الإجرائية المناسبة لهذه الصورة من البيانات، وذلك من خلال الحجز على الأشياء المادية وعلى البيانات المعالجة إلكترونيا.

وخوفا من محو أو إتلاف أو نقل أو ضياع الأدلة التي يتم الحصول عليها بطريق التفتيش، فللمحقق التحفظ على هذه الأدلة، ويتم التحفظ على البيانات محل الجريمة، وكذلك الأدوات التي استخدمت في ارتكابها، أو الآثار المتخلفة عنها وتفيد في كشف الحقيقة.

ويتم استخراج نسخة من المعلومات المضبوطة على الوسائط الخاصة بجهة التحقيق، ويبقى تحت تصرفها إلى حين انتهاء المحاكمة. ويرى البعض ضرورة حفظ نسخة أخرى خوفا من تلف أو ضياع النسخة الوحيدة الموجودة تحت تصرف جهة التحقيق أو المحكمة[1].

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

[1]- ثنيان ناصر آل ثنيان: **إثبات الجريمة الإلكترونية**، المرجع السابق، ص: 66 . 67.

في استحداث مثل هذه الإجراءات إلى عجز أساليب البحث والتحري التقليدية، والتي لم تعد كافية وفعالة للكشف عن الجرائم المستحدثة، والتي من بينها الجرائم الإلكترونية.

1. مفهوم التسرب: عرف المشرع التسرب في المادة 65 **مكرر** 12 من قانون الإجراءات الجزائية، وإن كان في الأصل أن التعريفات من عمل الفقه، ويرجع سبب ذلك إلى حداثة وخطورة هذا الإجراء.

ويقصد بالتسرب: "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف. ويلجأ إلى هذا الإجراء عادة عندما تقتضي عملية التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 **مكرر** من هذا القانون، وهي:

- جرائم المخدرات.
- الجريمة المنظمة عبر الحدود الوطنية.
- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- جرائم تبييض الأموال والإرهاب.
- الجرائم المتعلقة بالتشريع الخاص بالصرف.

ويمكن تجسيد عملية التسرب في الجرائم الإلكترونية كإشراك ضابط أو عون الشرطة القضائية في محادثات غرف الدردشة، أو حلقات النقاش حول دعارة الأطفال، أو كلام يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتخذ المتسرب أسماء مستعارة ويظهر بمظهر طبيعي كما لو كان فاعل مثلهم، ويحاول الاستفادة من معرفتهم حول كيفية اقتحام الهاكر لموقع ما، أو مباشرة الحديث في الموضوع الجنسي حتى يتمكنوا من اكتشاف وضبط الجرائم التي تتم من خلالها كالدعوة للدعارة مثلا.

2. شروط صحة التسرب: التسرب كممارسة غير عادية للضابط أو عون الشرطة القضائية، بل يعد من أخطر الإجراءات مساسا بحرمة الحياة الخاصة للمتهم، لذلك اشترط المشرع ضمانات معينة يتعين مراعاتها عند اللجوء إلى هذا الإجراء، ويتمثل ذلك فيما يلي:

أ: صدور إذن التسرب من وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية.
ب: يجب أن يكون الإذن مكتوبا مع احتوائه على الأسباب التي تبرر صدوره.

ج: يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته.

د: يحدد في الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز **أربعة أشهر**، ويمكن أن تتجدد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية، وفي نفس الوقت أجاز القانون للقاضي الذي رخص بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدة المحددة[1].

سابعا: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

نظم المشرع الجزائري كل من اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في المواد من 65 **مكرر**5 إلى غاية 65 **مكرر** 10، التي تجيز لضباط الشرطة القضائية وأعوانهم القيام بهذه الأعمال إذا اقتضت ضرورة التحري في الجرائم المتلبس بها، أو بعض الجرائم وذلك بموجب إذن من وكيل الجمهورية المختص أو بموجب إذن من قاضي التحقيق.

1. تعريف اعتراض المراسلات:

عرفته لجنة الخبراء للبرلمان الأوروبي في اجتماع لها عقد "**بستراسبورغ**" في 06 **أكتوبر** 2006 حول موضوع أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية بأنه: "عملية مراقبة سرية للمراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجرائم وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم بارتكابهم الجرائم أو مشاركتهم فيها".

وتحدث المشرع الجزائري عن اعتراض المراسلات في نصوص المواد من65 **مكرر**5 حتى المادة 65 **مكرر**10 من قانون الإجراءات الجزائية، لكنه لم يورد تعريفا صريحا عن مفهوم اعتراض المراسلات[2].

2. تعريف تسجيل الأصوات والتقاط الصور:

إن المشرع الجزائري لم يعطي تعريفا صريحا لتسجيل الأصوات، بل عرفه ضمنيا في نص المادة 65 **مكرر**5 من قانون الإجراءات الجزائية على أنه: "وضع واستعمال الوسائل والترتيبات التقنية دون موافقة

---

[1]. عائشة بن قارة مصطفى : **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، المرجع السابق، ص: 119. 120. 121.

[2]. نور الدين لوجاني: **أساليب البحث والتحري وإجراءاتها**، يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية، الجزائر، يوم 2007/12/12، ص: 8.

المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية، من طرف شخص أو عدة أشخاص يتواجدون في أماكن خاصة أو عمومية"[1].

حيث يتم تسجيل الاتصالات الإلكترونية التي تكون تحت المراقبة ويتم تقديم هذه التسجيلات إلى السلطات المختصة دون سواها، وهذا ما نص عليه المشرع في المادة 25 من المرسوم الرئاسي 15-261 على أن "تسجل الاتصالات الإلكترونية التي تكون موضوع مراقبة، وتحرر وفقا للشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية"[2].

3. إجراءات وشروط اعتراض المراسلات وتسجيل الأصوات والتقاط الصور:

لا يجوز في الأصل التقاط الصور وتسجيل أصوات دون علم الأشخاص أو رضاهم، إلا أن المشرع ونظرا لضرورة التحقيق في بعض الجرائم سمح بالقيام بمثل هذه العمليات، حيث تكون مصلحة التحقيق وكشف المجرمين أولى بالرعاية من الحفاظ على أسرار الحياة الخاصة[3].

ولقد أتاح المشرع الجزائري من خلال نصوص المواد من 65 **مكرر**05 إلى غاية المادة 65 **مكرر**10 من قانون الإجراءات الجزائية، للضبطية القضائية حق استعمال الأساليب والوسائل التقنية في إطار البحث والتحري في الجرائم المستحدثة، حيث أخضعها للشروط والإجراءات التالية:

أ: تستخدم الأساليب والوسائل التقنية في الجرائم الخاصة فقط: وهي الجرائم التي نصت عليها المادة:65 مكرر05 من قانون الإجراءات الجزائية. وعليه فلا يصح أن تستعمل هذه الأساليب والوسائل التقنية في الجرائم الأخرى.

ب: الإذن: وهو شرط أساسي وضروري لمباشرة عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، إذ يجب أن يضمن جمع المعلومات والعناصر المكونة للجريمة والتي تسمح لوكيل الجمهورية أو لقاضي التحقيق بالتعرف على الاتصالات المطلوبة التقاطها والأماكن المقصودة سواء سكنية أو غيرها، وكذلك طبيعة الجريمة التي تبرر اللجوء إلى هذه التدابير. ويشترط لصحة الإذن ما يلي:

---

[1]- مهدي شمس الدين: **النظام القانوني للتسرب في القانون الجزائري**، مذكرة لنيل شهادة الماستر في الحقوق، جامعة محمد خيضر، بسكرة، 2014، ص: 27.

[2]. انظر: المادة 25 من المرسوم الرئاسي 15-261.

[3]. فوزي عمارة: **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجنائية** ، مجلة العلوم الإنسانية ، العدد 33 ، جامعة منتوري ، قسنطينة ، جوان 2010، ص 238 .

- أن يكون مكتوبا وهذا كمبدأ عام من الأعمال المخولة للضبطية القضائية حسب المادة 18 من قانون الإجراءات الجزائية.

- تحديد المدة الزمنية لعملية التسرب وهي **أربعة أشهر** قابلة للتجديد حسب مقتضيات التحري والتحقيق.

ج: وضع الترتيبات التقنية: بعد الحصول على رخصة الإذن، يستطيع رجال الضبطية القضائية مباشرة وضع الوسائل والترتيبات التقنية، دون موافقة وعلم الأشخاص المعنيين، وهذا للمحافظة على السرية وإلا ما الفائدة من هذا الإجراء إذا كان بموافقة وعلم الأشخاص المشتبه فيهم.

وللمحافظة على الطابع السري للعملية فإن المشرع سمح لأفراد الضبطية القضائية بإجراء وضع الترتيبات التقنية في أي وقت يرونه مناسبا، حتى ولو كان خارج المواعيد المحددة في نص المادة 47 من قانون الإجراءات الجزائية[1].

د: الرقابة القضائية: يجب أن تخضع جميع العمليات المسموح بها قانونا تحت المراقبة والإشراف المباشر لوكيل الجمهورية المختص بذلك، كما أنه إذا ما تم فتح تحقيق قضائي، فإن هذه العمليات تتم بإذن من قاضي التحقيق وتحت رقابته المباشرة.

هـ: الإطار المكاني لأساليب التقنية في التحري عن الجرائم: نصت المادة 65 **مكرر**05 من قانون الإجراءات الجزائية عن الأماكن التي يتم استعمال الوسائل التقنية فيها وتتمثل في الأماكن العمومية، الأماكن الخاصة، المحلات السكنية.

و: المحافظة على السر المهني: أثناء قيام الضبطية القضائية بمهمة استعمال الوسائل الحديثة كالتقاط وتسجيل الأصوات خاصة في الأماكن الخاصة والمتعلقة بأماكن العمل كمكاتب المحاماة أو التوثيق وغيرها من الأماكن والأشخاص الذين تخضع متابعتهم لإجراءات خاصة تتعلق باحترام السر المهني، فعلى القائم بهذه العملية مراعاة السر المهني وعدم المساس به، وهذا حسب نص المادة 65 **مكرر**06 من قانون الإجراءات الجزائية.

ز: تسخير الأعوان المؤهلين والمكلفين بالمواصلات السلكية واللاسلكية: أجاز المشرع الجزائري لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له باستعمال الوسائل الخاصة في البحث والتحري، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينوبه، أن يسخر ويكلف كل عون مؤهل وصاحب خبرة في مجال المواصلات يعمل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية

[1]- مهدي شمس الدين: **النظام القانوني للتسرب في القانون الجزائري**، المرجع السابق، ص: 28.

واللاسلكية، لاستخدامه بالتكفل بالجوانب التقنية لعمليات اعتراض المراسلات وتسجيل الأصوات، وهذا حسب ما جاء في نص المادة 65 **مكرر**08 من قانون الإجراءات الجزائية.

ح: تحرير محضر عن العملية: نص قانون الإجراءات الجزائية وفي المادة 18 منه، على وجوب التدوين وتحرير تقارير عن كل عملية وهذا كمبدأ عام لأعمال الضبطية القضائية، كما جاءت في المادة 65 **مكرر**09 من قانون الإجراءات الجزائية لتعزز ما جاء في المادة 18 من نفس القانون فيما يتعلق باعتراض المراسلات وتسجيل الأصوات والتقاط الصور. وعليه يجب على ضابط الشرطة القضائية أن يقوم بتحرير محضر عن كل عملية، يذكر فيها جميع تفاصيل العملية من بدايتها أي من وضع الترتيبات اللازمة لمباشرة العملية حتى نهايتها، كما يجب ذكر في المحضر تاريخ وساعة بداية العملية وتاريخ الانتهاء منها. أما نتائج التحريات التي تتعلق بمضمون المراسلات المسجلة أو الصور الملتقطة، فعلى ضابط الشرطة القضائية المأذون له أو المناب بهذه العملية أن ينسخ أو يصف المحتوى الضروري واللازم لإظهار الحقيقة في محضر ليودع بالملف. أما إذا كانت المكالمات باللغات الأجنبية، فإنه يتم الاستعانة بمترجم لترجمة محتوى المكالمات ونسخها[1].

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:

الشهادة في مجال الجريمة الإلكترونية لا تختلف من حيث ماهيتها عن الجريمة التقليدية، وأمر سماع الشهود متروك لفطنة المحقق ومرتبط بظروف التحقيق، والأصل أن يطلب من الخصوم سماع من يرون من الشهود، وللمحقق أن يدعو للشهادة من يقدر أن لشهادته أهمية، وله أن يسمع شهادة أي شاهد يتقدم من تلقاء نفسه.

والشاهد في الجريمة المعلوماتية هو ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية أو هامة لازمة للدخول في نظام المعالجة الآلية

[1]- نور الهدى السوفي: **التحقيق في الجريمة المعلوماتية**، مذكرة مقدمة استكمالا لمتطلبات نيل شهادة الماستر، شعبة الحقوق، تخصص قانون جنائي، بإشراف الأستاذ الدكتور: رضا الهميسي، جامعة قاصي مرباح، ورقلة، 2017، ص: 45 . 46.

للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله، ويطلق على هذا الشاهد اسم **(الشاهد المعلوماتي)**، وذلك تمييزا له عن الشاهد التقليدي[1].

والشاهد المعلوماتي بهذا المفهوم قد يكون واحدا من عدة طوائف أهمها:

1. مشغلو الحاسب الآلي: وهم الخبراء الذين تكون لهم الدراية التامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به، واستخدام لوحة المفاتيح في إدخال البيانات، وتكون لديهم معلومات عن قواعد كتابة البرامج[2].

2. المحللون: والمحلل هو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين وتحليلها إلى وحدات منفصلة، واستنتاج العلاقات الوظيفية منها، كما يقوم كذلك بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

3. المبرمجون: وهم الأشخاص المتخصصون في كتابة أوامر البرامج ويمكن تقسيمهم إلى فئتين:

أ): الفئة الأولى: هم مخططو برامج التطبيقات، ويقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم، ثم يقومون بتحويلها إلى برامج دقيقة وموثوقة لتحقيق هذه المواصفات.

ب): الفئة الثانية: هم مخططو برامج النظم ويقومون باختيار وتعديل وتصحيح برامج نظام الحاسب الداخلية وإدخال أية تعديلات أو إضافات لها[3].

4. مهندسو الصيانة والاتصالات: وهم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب وبمكوناته وشبكات الاتصال المتعلقة به.

5. مديرو النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية[4].

---

[1]- عبد الإله هلالي: **التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة**، (د.ط)، دار النهضة العربية، القاهرة، 2000، ص: 23.

[2]- محمد فهمي: **الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني**، (د.ط)، مطابع المكتب المصري الحديث، القاهرة، 1991، ص: 23.

[3]- عبد الله حسين علي محمود: **إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات**، بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور القانون الجنائي، دبي، من 26 إلى 28 أفريل 2003، ص: 616.

[4]- خالد محمد المهيري: **التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية**، (ط.2)، دار الغرير للطباعة والنشر، دبي، (د.س.ن)، ص: 508.

ثانيا: إثبات الجريمة الإلكترونية بالاعتراف (الإقرار):

لم يستقر الفقه القانوني على رأي واحد في تحديد معنى الإقرار(الاعتراف) في المفهوم الاصطلاحي، فقد عرفه البعض بأنه: "إقرار المتهم على نفسه بارتكاب الوقائع المكونة للجريمة كلها أو بعضها من خلال إقرار المتهم بكل أو بعض الوقائع المنسوبة إليه".

وهناك من وضع تعريفا يشمل شروط صحة الإقرار قائلا: "بأن الإقرار القانوني يعني الإقرار على النفس بحرية وإدراك بارتكاب الأفعال المكونة للجريمة أو بعضها، دون تأثير أو إكراه، وإن إقرار المدعي بارتكابه وقائع الجريمة كلها أو بعضها، وأنه هو الذي قام بهذا الفعل بنفسه وهذا ما أقره الفقه والقضاء. ويتضح بذلك أن الاعتراف في جوهره تقرير أو إعلان، وأن موضوعه هو الواقعة سبب الدعوى ونسبة هذه الواقعة إلى المتهم، وأنه يتعين أن يكون من صدر عنه الإقرار هو نفسه من تنسب إليه الواقعة، بما يترتب عليه من قيام المسؤولية الجنائية عنها، ويعني ذلك أن المتهم هو المقر أو المعترف، وهو نفسه الذي تنسب إليه الواقعة موضوع الإقرار.

ومن خلال ما سبق، يمكن القول أن الإقرار يقصد به إقرار المرء على نفسه فيما نسب إليه، وقد عرف بسيد 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 الاعتراف مجملا فإنه يكون صحيحا طالما كان دالا على ارتكاب الجريمة.

1. أشكال الإقرار وأنواعه:

أ): أشكال الإقرار:

إقرار المتهم إما يكون شفهيا وإما مكتوبا، وأي منهما كاف في الإثبات، ومن خلال ذلك يمكن توضيح أشكال الإقرار كما يلي:

. الإقرار الشفوي: يمكن أن يثبت بواسطة كاتب التحقيق أو كاتب الجلسة، ولا يلزم أن يكون الإقرار المثبت بمحضر التحقيق موقعا عليه من المتهم طالما أن المحضر قد وقع عليه المحقق أو الكاتب.
ولكن الإقرار الشفهي يعتبر أقل قيمة من الإقرار المكتوب، فكثير من المعترفين ينكرون اعترافاتهم الشفهية ويدعون أنهم أجبروا عليها باستعمال العنف معهم أو التهديدات والوعود.

. الإقرار المكتوب: لا يتطلب أن يكون له شكل معين، فقد يكون مكتوبا على الآلة الكاتبة أو باليد أو في صورة، حديث مسترسل أو في شكل أسئلة وأجوبة.

وقد نصت بعض التشريعات على أنه يجب لكي يقبل الإقرار في الإثبات أن يكون مكتوبا موقعا عليه من المتهم، وعلى أية حال فإن الإقرار سواء كان شفويا أو مكتوبا فأمره متروك لتقدير القاضي واقتناعه به[1].

ب): أنواع الإقرار:

يمكن تقسيم الإقرار إلى عدة أنواع، وهي كما يلي:

. الإقرار القضائي: وهو الإقرار الذي يصدر أمام المحكمة التي تنظر الدعوى الجنائية بالفعل، ويجيز هذا الإقرار للمحكمة الاكتفاء به والحكم على المتهم بغير سماع الشهود، فيبدأ التحقيق في الجلسة بالمناداة على الخصوم والشهود، ويسأل المتهم عن اسمه ولقبه وسنه، ثم يسأل المتهم عما إذا كان معترفا بارتكاب الفعل المسند إليه، فإن أقر جاز للمحكمة الاكتفاء باعترافه والحكم بغير سماع الشهود، وإلا فتسمع شهادة الشهود للإثبات[2].

. الإقرار غير القضائي: وهو الإقرار الذي يصدر خارج المحكمة التي تنظر الدعوى الجزائية، فإذا صدر الإقرار الجزائي في تحقيق النيابة أو أمام إحدى جهات التحقيق، أو قضاء الإحالة أو في محضر جمع الاستدلالات، يعتبر اعترافا غير قضائي.

كما يعتبر إقرارا غير قضائي الإقرار الذي يرد ذكره في التحقيقات نقلا عن أقوال منسوبة إلى المتهم خارج مجلس القضاء.

ويعتبر الإقرار غير القضائي مثل ما يقر به في تحقيق إداري، أو كمن يقر بارتكاب الجريمة أمام أحد الأشخاص ويشهد ذلك الشخص بالتحقيق بالإقرار الذي سمعه.

على أنه طبقا لمبدأ حرية القاضي في تكوين اعتقاده، فإن القاضي الجزائي حر في تقدير قيمة الاعتراف قضائيا كان أو غير قضائي، وليس هناك ما يمنع من أن يكون الإقرار غير القضائي سببا في الإدانة، لأنه لا يخرج عن كونه دليلا في الدعوى، ويخضع لتقدير القاضي كباقي الأدلة، وكل ما في الأمر أن

---

[1]- محمد نصير السرحاني: **مهارات التحقيق الجنائي الفني في جرائم الحاسب الآلي والانترنت**، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض،2004، ص: 75.

[2]- يونس عرب: **جرائم الحاسب الآلي والانترنت**، منشورات اتحاد المصارف العربية، (د.ب.ن)، 2002، ص: 304

الإقرار غير القضائي لا يصلح أن يكون سببا في اكتفاء المحكمة به والحكم على المتهم بغير سماع الشهود[1].

الفرع الثالث: إثبات الجريمة الإلكترونية بالخبرة الفنية:

تعد عملية الحصول على الأدلة الرقمية أمرا صعب الوصول إليه لما تتطلبه من خبرة ومهارة كبيرة في مجال الحاسب الآلي، ويرجع ذلك لتعدد صور وأشكال الجرائم الإلكترونية ما بين مهاجمة المعلومات بغرض تدميرها أو الاستيلاء عليها، أو قد يكون المقصود بالهجوم هو الأجهزة، كنشر فيروس يعمل على إتلاف وحداته الرئيسية مثلا، أو قد يكون الأمر مجرد اختراق لكلمة مرور خاصة ببنك أو مؤسسة كبرى بغرض الاحتيال والحصول على الأموال، وقد تكون لمجرد إثبات الذات وإظهار المقدرة العالية في مجال الحاسب الآلي[2]. ولما كانت عملية تجميع الأدلة الرقمية الجنائية في الجرائم الإلكترونية أو الرقمية تعد من أهم وأصعب الأمور التي تواجه عملية الإثبات الجنائي، فقد كان لزاما أن يتم اللجوء إلى خبير قضائي معلوماتي متخصص، لاشتقاق الدليل العلمي الفني الجنائي. ويرى البعض المتخصصين أن عملية تجميع الأدلة الرقمية في الجرائم الإلكترونية التي تتم عبر الشبكة العالمية (الانترنت) تتم عبر ثلاث مراحل:

. المرحلة الأولى: تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة، حيث تتبع الحاسبات الخوادم التي دخل المجرم منها ومحاولة إيجاد أي أثر له.

. المرحلة الثانية: وهي مرحلة المراقبة، فهناك فرضية تقول بأن المجرم لا بد وأن يعود أو يحوم حول مسرح جريمته، وتتعدد طرق مراقبة هذه الحواسيب، ويمكن توضيح هذه الطرق كما يلي:

1: استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر وتسجيل بيانات كل دخول وخروج بالموقع.

2: استخدام أجزاء توضع في الحاسب الآلي لمراقبته.

3: استخدام كاميرات مراقبة لشاشة الحاسب الآلي معدة للاستخدام التجاري، وأبسط الطرق لمراقبة الحاسب هي الدخول لمكان وجوده.

---

[1]- جميل عبد الباقي الصغير: **القانون الجنائي والتكنولوجيا الحديثة**، (د.ط)، دار النهضة العربية، القاهرة، 1992، ص: 97.

[2]- عبد الناصر محمد فرغلي و محمد عبيد المسماري: **الإثبات الجنائي بالأدلة الرقمية**، المرجع السابق، ص: 25.

4: وهناك وسيلة أخرى أصعب قليلا، وهي زرع فيروس كمبيوتر أو دودة من نوع حصان طروادة، وهذه الوسيلة لها ميزة أنها تستطيع مراقبة أكثر من جهاز واحد، ولكن يجب عدم السماح للفيروس بالانتشار وإلا سوف يصبح هدفا لبرامج الدفاع ضد الفيروسات.

. المرحلة الثالثة: ضبط الأجهزة المشتبه فيها وفحصها فحصا فنيا وشرعيا، حيث يبدأ في هذه المرحلة عمل الخبير المعلوماتي في فحص النظام الحاسوبي المشتبه فيه بمكوناته المادية ومكوناته البرمجية، سعيا لاشتقاق الدليل الرقمي لتقديمه لجهة التحقيق أو الحكم، لتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه، ولتقرير إدانة المتهم أو تأكيد براءته. ويتم ذلك وفق القواعد الفنية المتعارف عليها والمتبعة في مجال الخبرة المعلوماتية، مع مراعاة القواعد القانونية لمبدأ المشروعية.

ومن خلال ما سبق، يمكن إيجاز خطوات اشتقاق الدليل بمعرفة الخبير المعلوماتي من أجل إثبات الجريمة الإلكترونية كما يلي:

1: التأكد من مطابقة محتويات إحراز المضبوطات لما هو مدون عليها، مع التأكد من صلاحية وحدات النظام للتشغيل، وتسجيل بيانات وحدات المكونات المضبوطة، كالنوع والطراز أو الموديل والرقم التسلسلي.
2: استكمال تسجيل باقي بيانات الوحدات من خلال قراءات على الجهاز.
3: عمل نسخة أو نسخ مطابقة للأصل من كل وسائط التخزين المضبوطة، وعلى رأسها القرص الصلب، ويفضل البدء بذلك لإجراء عملية الفحص المبدئي على هذه النسخ لحماية الأصل من أي فقد، أو تلف أو تدمير، سواء من سوء الاستخدام أو لوجود فيروسات أو أفخاخ وقنابل برمجية.
4: تحديد أنواع وأسماء المجموعات البرمجية، برامج النظام وبرامج التطبيقات وبرامج الاتصالات، وما إذا كان هناك برامج معينة ذات دلالة بموضوع الجريمة، برامج إنشاء ومعالجة الصور في جرائم التزييف والتزوير والمونتاج.
5: تحديد ما إذا كان هناك برامج أو ملفات أو بيانات أو معلومات ذات دلالة ترابطية بموضوع الجريمة، كصور للعملات وصور للعملات المائية وشريط الضمان، والأرقام المسلسلة في جرائم تزييف العملة، أو للمستندات والتوقيعات، وبصمات الأختام وبصمات الأصابع بجرائم التزوير، ووجود رسائل التهديد في صندوق الصادر في البريد الإلكتروني، في جريمة القتل أو التهديد بالقتل وغير ذلك.
6: إظهار الملفات المخبأة والنصوص المخفية داخل الصور.

7: تحويل الدليل الرقمي إلى هيئة مادية وذلك عن طريق طباعة الملفات، أو تصوير محتواها إذا كانت صور أو نصوص، أو وضعها في أي وعاء آخر حسب نوع البيانات والمعلومات المكونة للدليل[1].

وندب الخبير من سلطات المحقق، فليس في القانون ما يلزمه بالاستجابة للمتهم ولا لغيره من الخصوم، ويحدد المحقق للخبير مهمته والميعاد الذي يقدم فيه تقريره، والأصل أن يباشر الخبير عمله في حضور المحقق وتحت إشرافه، والاستثناء يتم ذلك في غيابه، وللخصوم حق الحضور أثناء عمل الخبير، ويجوز مع ذلك أن يباشر الخبير عمله في غياب الخصوم، وأن يمنعهم كذلك من الحضور إذا كان للمنع سببا.

ومن خلال توضيح دور الخبرة الفنية في إثبات الجريمة الإلكترونية، فإن البحث عن المعلومات داخل جهاز الكمبيوتر ذاته يعد أمرا بالغ التعقيد ويحتاج إلى وجود خبير، وأهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم الإلكترونية هي:

1: **وصف الحاسبات وأثرها**: ويتضمن ما يلي:

أ: تركيب الحاسبات وصناعتها وطرازها ونوع التشغيل، وأهم الأنظمة الفرعية التي تستخدمها بالإضافة إلى الأجهزة الطرفية الملحقة بها، وكلمات المرور أو السر، ونظام التشفير.

ب: طبيعة بيئة الحاسب أو الشبكة من حيث التنظيم ومدى التركيز، أو توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات، وتردد موجات البث وأمكنة اختزانها.

ج: الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها.

د: أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام[2].

2: **بعض المعلومات والتقنيات المتعلقة بالحاسبات**: ويتضمن ذلك ما يلي:

أ: بيان كيف يمكن عند الاقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.

ب: بيان كيف يمكن عند الاقتضاء نقل أدلة الإثبات إلى أوعية ملائمة بغير أن يلحقها تلف.

---

[1]- ممدوح عبد الحميد عبد المطلب: **البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت**، دار الكتب القانونية، مصر، 2006، ص: 92 . 93.

[2]- عبد الناصر محمد فرغلي، محمد عبيد المسماري: **الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية**، المرجع السابق، ص: 27.

ج: كيفية تجسيد الأدلة في صورة مادية بنقلها إن أمكن إلى أوعية ورقية يتاح للقاضي مطالعتها وفهمها، مع إثبات أن المسطر على الورق مطابق للمسجل على الحاسب أو النظام أو الشبكة أو الدعامة الممغنطة[1].

[1]- محمود عبد الله حسين: **سرقة المعلومات المخزنة في الحاسب الآلي**، (د.ط)، دار النهضة العربية، القاهرة، 2002، ص: 39.

المبحث الثاني: 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 أو المقيد أو المختلط، وفيما يتعلق بسلطة القاضي في قبول هذا النوع من الأدلة وتقديره والاقتناع به، وهذا باعتبار أن القاضي لا يقدر إلا الدليل المقبول، وهذا على مستوى القضاء الجنائي[1].

ولدراسة هذا الأمر نقسم مبحثنا هذا إلى مطلبين:

المطلب الأول: حجية الدليل الرقمي على ضوء نظم الأدلة الجنائية.

المطلب الثاني: حجية الدليل الرقمي أمام القاضي الجزائي.

[1]- أمنة هلال: **الإثبات الجنائي بالدليل الإلكتروني**، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، بإشراف الأستاذ الدكتور: مستاري عادل، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2015، ص: 73.

المطلب الأول: حجية الدليل الرقمي على ضوء نظم الأدلة الجنائية:

في سبيل دراسة الدليل الرقمي أو الإلكتروني في ظل أنظمة الإثبات الجنائي أو نظم الأدلة الجنائية، وباعتبار أنه دليل مستحدث، نتطرق إلى بيان حجيته في أنظمة الأدلة الجنائية على النحو التالي:

حجية الدليل الرقمي في نظام الإثبات المقيد في (الفرع الأول)، وحجية الدليل الرقمي في نظام الإثبات الحر في (الفرع الثاني)، وأخيرا حجية الدليل الرقمي في نظام الإثبات المختلط في (الفرع الثالث).

الفرع الأول: حجية الدليل الرقمي في نظام الإثبات المقيد:

في ظل نظام الإثبات المقيد، لا يكون الدليل الإلكتروني مقبولا أمام القاضي الجنائي ما لم يتم النص عليه من قبل المشرع، حيث يتوجب عليه تحديد هذا النوع من الأدلة سلفا وبدقة، والقاضي الجنائي يتوجب عليه الأخذ بهذه الأدلة متى توافرت فيها شروط الدليل الصحيح، وقد حددت العديد من التشريعات التي تعمل بهذا النظام هذه الأدلة، أي الأدلة الإلكترونية، والمشرع لعب دورا مهما في تحديدها[1].

وقبول الدليل الإلكتروني في هذا النظام له شروط نص عليها المشرع الإنجليزي، حيث تعاقبت في إنجلترا العديد من القوانين التي تسمح بقبول الدليل الالكتروني، كقانون الإثبات الجنائي لسنة 1968، وقانون الشرطة والإثبات الجنائي لسنة 1984، الذي ترتب عليه قبول المشرع الإنجليزي للدليل الإلكتروني كدليل في الإثبات الجنائي، وهذا خروجا عن الأصل العام الذي يعمل به في القانون الإنجليزي الذي لا يقبل الشهادة السماعية. إلا أن هذا القبول تقيده شروط معينة نصت عليها المادة 69 من قانون 1984، ويتمثل **الشرط الأول** في عدم وجود أسباب معقولة للاعتقاد بأن البيان يفتقر إلى الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسوب.

أما **الشرط الثاني** فهو أن يعمل الحاسوب في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك فإن أي جزء لم يعمل فيه بصورة سليمة أو كان معطلا عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة محتوياته.

[1]- سامي جلال فقي حسين: **الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي**، (د.ط)،دار الكتب القانونية، مصر، 2011، ص: 91.

وفيما يتعلق **بالشرط الثالث**، فهو يتمثل في الوفاء بأية شروط متعلقة بالمستند، محددة طبقا لقواعد المحاكمة المتعلقة بالطريقة أو الكيفية التي يجب أن تقوم بها المعلومات الخاصة بالبيان المستخرج عن طريق الحاسوب[1].

وتجدر الإشارة إلى أن صحة الدليل الإلكتروني تتوقف على صحة برنامج التشغيل الذي يعمل الكمبيوتر بحسب تعليماته، ومن حق المتهم أن تتاح له الفرصة لإثبات أن برنامج التشغيل لا يعمل بطريقة صحيحة أو منتظمة.

كما أن القانون الإنجليزي لسنة 1984 تضمن كذلك توجيهات لكيفية تقدير قيمة أو وزن البيان المستخرج عن طريق الحاسوب، عن طريق مراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسوب والمقبولة في الإثبات.

ومنه نقول أن الدليل الإلكتروني في ظل نظام الإثبات المقيد مقبول ويؤخذ به، وهذا باعتباره كدليل إثبات جنائي، وله قوة ثبوتية أيضا. إلا أن الأخذ بالدليل الإلكتروني في هذا النظام تعترضه مشاكل خاصة فيما يتعلق بقواعد هذا النظام، وأهمها قاعدة استبعاد شهادة السماع وأيضا قاعدة الدليل الأفضل.

إلا أن غالبية التشريعات وحتى تتماشى مع هذا النوع الجديد والمستحدث من الأدلة، أوردت استثناءات على هذه القواعد، وتم قبول الدليل الإلكتروني والأخذ به في ظل هذا النظام، مع إيراد شروط أيضا للأخذ بالدليل الإلكتروني.

ومنه يمكن القول بأن الدليل الإلكتروني له حجية وقوة ثبوتية بالنسبة للتشريعات التي تأخذ بنظام الإثبات المقيد، وقد حاولت بشكل كبير إعطاء القوة الثبوتية لهذا النوع من الأدلة.

وبالرغم من أن الدليل الإلكتروني يتعارض بسبب طبيعته مع أهم قواعد نظام الإثبات الجنائي المقيد، إلا أنه كان من الضروري الخروج عن الأصل العام في هذه القواعد، وإيراد استثناءات عليها، حتى يكون في الإمكان الأخذ بالدليل الإلكتروني، وهذا تماشيا مع التكنولوجيا الحديثة وإثبات الجريمة الإلكترونية[2].

[1]- عائشة بن قارة مصطفى: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، المرجع السابق، ص: 209 . 210.

[2]- أمنة هلال: **الإثبات الجنائي بالدليل الإلكتروني**، المرجع السابق، ص: 78 . 79 . 80.

الفرع الثاني: حجية الدليل الرقمي في نظام الإثبات الحر:

إن نظام الإثبات الحر بصفة عامة لا يحدد طرقا معينة للإثبات، وإنما يترك الحرية لأطراف الدعوى بغرض تقديم أدلة إثبات دعواهم. والقاضي الجنائي بدوره يقوم بتقييم هذه الأدلة، ومنه التوصل إلى قناعة معينة بخصوص الأدلة المطروحة أمامه، وإصداره حكمه في ضوء القناعة التي توصل إليها. وإن كان هذا الأمر ينطبق على الأدلة التقليدية، فإن ذلك لا يثير مشكلة إذا ما تم تطبيقه على الأدلة الإلكترونية، حيث يقدم أطراف الدعوى أدلتهم، أو تقدم سلطة الاتهام أدلتها، ومن ثم فإن القاضي يصدر حكمه بناءا على قناعته التي توصل إليها. فالأدلة الإلكترونية هي تطبيق من تطبيقات الدليل العلمي بما يتميز به من موضوعية وحياد وكفاءة في إقناع القاضي الجزائي، هذه الصفات التي دفعت بالبعض إلى الاعتقاد إلى أنه كلما اتسعت مساحة الأدلة العلمية ومنها الأدلة الإلكترونية، كلما قل دور القاضي الجنائي في التقدير.

لكن هذا الأمر لم يكن مستبعدا باعتبار أنه عند مناقشة دليل علمي ما كالدليل الإلكتروني، يلزم التمييز بين أمرين مهمين، حيث يتمثل الأمر الأول في القيمة العلمية القاطعة للدليل الإلكتروني، والأمر الثاني هو الظروف والملابسات التي وجد فيها هذا الدليل.

فالقاضي الجنائي عند تقديره للدليل الإلكتروني لا يتطرق إلى القيمة العلمية للدليل، لأنها حقيقة علمية ثابتة، ولأنه أيضا ليس من اختصاصه مناقشة الأمور العلمية البحتة، وإنما هي من اختصاص الخبراء المختصين في هذا المجال، وفي إمكان القاضي الاستعانة بهم بهدف معرفة حقيقة هذا الدليل العلمي وهو الدليل الإلكتروني.

كما أن القاضي الجنائي بإمكانه رفض هذا الدليل عندما يرى أن وجوده لا يتناسب منطقيا مع ظروف وملابسات الواقعة. أما إذا اقتنع القاضي بأن الدليل المطروح صحيح، وأنه وجد في ظروف ملائمة لظروف وملابسات الواقعة يستطيع الأخذ به[1].

ومنه نقول أن حجية الأدلة الإلكترونية لا تثير صعوبات بسبب حرية تقديم الأدلة لإثبات الجرائم الإلكترونية، وكذلك حرية القاضي الجنائي في تقدير هذه الأدلة التي لها طبيعة خاصة، فهي كذلك تعتبر أدلة إثبات في المواد الجنائية.

[1]- سامي جلال فقي حسين:**الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي**، المرجع السابق، ص: 79 . 80.

فحتى إن أثيرت مشكلة حول المخرجات المتحصلة من الحاسوب فهي ليست بالمشكلة العويصة، باعتبار أنها تخضع لحرية القاضي في تقدير هذه الأدلة، الذي بمقدوره أن يطرح هذا النوع من الأدلة الإلكترونية رغم قطعيتها من الناحية العلمية، وهذا عندما يجد أن الدليل الإلكتروني لا يتماشى منطقيا مع ظروف الواقعة وملابساتها.

فهذا النظام يصلح فيه الأخذ بالدليل الإلكتروني دون وجود أي عائق في الغالب، على أساس أهم مبدأ فيه وهو حرية الإثبات الجنائي، الذي يقوم على أساس عدم تحديد طرق معينة للإثبات الجنائي، مع الأخذ في عين الاعتبار الدور الإيجابي الذي يلعبه القاضي في هذا النظام، والذي انطلاقا منه يمكن له أن يمحص أي دليل يطرح أمامه ليأخذ بالدليل الذي يستقر في وجدانه، ويبني على أساسه اقتناعه الشخصي بالقضية المطروحة أمامه، ومنه يقوم بإصدار الحكم سواء بالبراءة أو بالإدانة[1].

الفرع الثالث: حجية الدليل الرقمي في نظام الإثبات المختلط:

في ظل نظام الإثبات المختلط يحدد المشرع الأدلة الإلكترونية سلفا، عن طريق إصدار تشريع بهذه الأدلة، ويحدد فيه الأدلة المقبولة، ومن ثم فإنه يمنح القاضي الحق في تقدير هذه الأدلة المعروضة أمامه في القضية التي ينظرها، ومنه له الحق في استبعاد أي دليل لا يقتنع به، والأخذ بدليل قانوني آخر اقتنع به. فعلى سبيل المثال لو حدد المشرع الأدلة الإلكترونية المقبولة في المخرجات الورقية، وعرضت أمام القاضي الجنائي في قضية ما، يحق له الأخذ بأي دليل يقتنع به ويطمئن له، ويستبعد الدليل الذي لا يقنعه[2].

فالقانون الياباني مثلا حصر طرق الإثبات المقبولة في أقوال المتهم وأقوال الشهود والقرائن والخبرة، أما بالنسبة للأدلة الإلكترونية فقد قرر الفقه الياباني أن السجلات الإلكترومغناطيسية تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات، ففي هذه الحالة يتم قبول هذه الأدلة وهي الأدلة الإلكترونية سواء كانت الأصل أم كانت نسخة طبق الأصل.

---

[1]- أمنة هلال: **الإثبات الجنائي بالدليل الإلكتروني**، المرجع السابق، ص: 83 . 84.

[2]- سامي جلال فقي حسين:**الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي**، المرجع السابق، ص: 97.

كما نص قانون الإجراءات الجنائية الشيلي على إمكانية استخدام الأفلام السينمائية والحاكي والنظم الأخرى الخاصة بإنتاج الصورة والصوت والاختزال، أي وسيلة قد تكون ملائمة وتؤدي لاستخلاص المصداقية ويمكن أن تكون مقبولة كدليل إثبات.

كما أن الفقه الشيلي من جهة أخرى يرى بدوره أن الدليل الناتج عن الحاسوب والانترنت أو الدليل الإلكتروني، يمكن أن يكون مقبولا وهذا في المحكمة، باعتباره دليل كتابي، أو دليل مستندي كالنظم الحديثة الأخرى التي تهدف إلى جمع وتسجيل المعلومات.

وحجة الفقه الشيلي في هذا المجال تستهدف توسيع نطاق الوسائل العلمية الحديثة في الإثبات، بهدف تغطية العناصر الإثباتية الناتجة عن الجرائم المعلوماتية[1].

ومنه نقول أن الدليل الإلكتروني في ظل نظام الإثبات المختلط لا مشكل في الأخذ به، باعتبار أن هذا النظام يجمع بين كل من نظام الإثبات المقيد، ونظام الإثبات الحر، فهو يعمل على تحديد أدلة الإثبات الجنائية من جهة والدليل الإلكتروني حدد كاستثناء على هذه القاعدة، كما أنه يولي أهمية كبيرة لسلطة القاضي الجنائي في الأخذ بالأدلة وتقديرها، وهذا الأمر يسهل الأخذ بالدليل الإلكتروني على أساس حرية القاضي الجنائي في قبول أي دليل يراه مناسبا، وكذا استبعاد الدليل الذي لا يراه مناسبا[2].

المطلب الثاني: حجية الدليل الرقمي أمام القاضي الجزائي:

إن الدليل الرقمي 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 الجنائي 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 الجنائي أن ينظر في

[1]- علي حسن محمد الطوالبة: **التفتيش الجنائي على نظم الحاسوب والانترنت**، (ط.1)، عالم الكتاب الحديث للنشر والتوزيع، الأردن، 2004، ص: 198.

[2]- أمنة هلال: **الإثبات الجنائي بالدليل الإلكتروني**، المرجع السابق، ص: 86 . 87.

موضوع الأخذ بالدليل الإلكتروني، ويعطي له حجية والقوة الثبوتية اللازمة، آخذا في عين الاعتبار 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.

لهذا وفي سبيل دراسة الدليل الإلكتروني من ناحية حجيته أمام القضاء الجزائي الممثل بدوره بالقاضي الجنائي، سنتناول ما يلي:

سلطة القاضي الجزائي في قبول الدليل الرقمي في (الفرع الأول)، وبعدها ضوابط قبول واقتناع القاضي الجزائي بالدليل الرقمي في (الفرع الثاني)، وأخيرا مشكلات الدليل الرقمي وأثرها على الاقتناع الشخصي للقاضي الجنائي في (الفرع الثالث).

الفرع الأول: سلطة القاضي الجزائي في قبول الدليل الرقمي:

يقول الفقيه **بيكاريا** في مؤلفه الشهير **الجرائم والعقوبات**: "أن 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 به 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 بحجيته المسبقة، كما له طرح الأدلة التي لا يطمئن إليها، وله في النهاية سلطة التنسيق بين الأدلة المعروضة عليه[3].

والدليل الإلكتروني بدوره خاضع للمبدأ العام في الإثبات الجنائي، وهو حرية القاضي الجنائي في الاقتناع، وحريته في هذا الشأن لها أهمية بالغة، باعتبار أن القاضي الجنائي هو وحده الذي يقدر قيمة الدليل الإلكتروني، وهذا تبعا للأثر الذي يحدثه في وجدانه من ارتياح. ومن جهة أخرى نجد أن دور الإثبات العلمي أصبح له أهمية كبيرة خاصة مع ظهور الدليل الإلكتروني المطلوب للإثبات في الجرائم الإلكترونية،

---

[1]- العربي شحط عبد القادر، نبيل صقر: **الإثبات في المواد الجزائية**، (د.ط)، دار الهدى للنشر والتوزيع، الجزائر، (د.س.ن)، ص: 22 . 23.

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

[3]- فاضل زيدان محمد: **سلطة القاضي الجنائي في تقدير الأدلة**، (ط.1)، دار الثقافة للنشر والتوزيع، الأردن، 2006،ص: 94.

بسبب اضطرار 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 الاعتماد عليه من جهة أخرى.

إن الطبيعة العلمية للدليل الإلكتروني لها أهمية بالغة في الإثبات الجنائي، وهي الميزة الأساسية له. لذلك قبل كل شيء لا بد 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.

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 أو من القاضي نفسه، 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 نص 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

[1]- برهان عزيزي: **إثبات الجريمة في أحكام مجلة الإجراءات الجزائية**، (ط.1)، مجمع الأطرش للكتاب المختص، تونس، 2013، ص: 77.
[2]- فاضل زيدان: **سلطة القاضي الجنائي في تقدير الأدلة**، المرجع السابق، ص: 106 . 107.

أن يصدر حكمه بناءا على اقتناعه الخاص، 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 الجزائية، أي محاكم الجنايات والجنح والمخالفات، والمشرع الجزائري لم ينص صراحة على هذا الأمر بخلاف المشرع الفرنسي الذي نص عليه.

وهناك من يرى أ ن هذا المبدأ وجد أصلا ليطبق أمام قضاء الحكم، ولكن هذا لا يعني أن نطاق تطبيقه مقتصر فقط على هذه المرحلة، وإنما يشمل أيضا مرحلة التحقيق الابتدائي، فقضاء التحقيق والإحالة بدورهم يقدرون مدى كفاية الأدلة وكفايتها 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 الإلكتروني كدليل علمي، ثم التطرق إلى تقدير القضاء للدليل العلمي.

أولا: قيمة الدليل الإلكتروني كدليل علمي: إن الدليل الإلكتروني لا تختلف قيمته ولا تزيد حجيته عن غيره من الأدلة، وهذا من آثار إعمال مبدأ حرية القاضي الجنائي في الاقتناع، ومنه فإن القاضي الجنائي يستطيع إبعاده، وبالتالي لا يجوز إجبار القاضي على الاقتناع بالدليل الإلكتروني حتى وإن لم تكن هناك أدلة غيره.

وتجدر الإشارة إلى أن الفقه الفرنسي تطرق إلى حجية مخرجات الكمبيوتر في المواد الجنائية، وهذا في مسألة قبول الأدلة المتحصلة من الأدلة العلمية، وأقر بأن لها قيمة الأدلة الأخرى وبالتالي يمكن الاطمئنان إليها، وتصلح للإثبات أمام القضاء الجنائي[3].

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.

---

[1]- عائشة بن قارة مصطفى: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، المرجع السابق، ص: 242 . 243.

[2]- المرجع نفسه، ص: 244 . 245.

[3]- المرجع نفسه، ص: 246.

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[1].

ثانيا: 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 أنه 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.

فبمجرد توافر الدليل العلمي لا يعني أن القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أو البراءة، دون بحث الظروف والملابسات، فالدليل العلمي ليس آلية معدة 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[2].

---

[1]- عائشة بن قارة مصطفى: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، المرجع السابق ، ص: 247 - 248.

[2]- فتحي محمد أنور عزت: **الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية**، (ط.1)، دار الفكر والقانون للنشر والتوزيع، مصر، 2010 ، ص: 596 . 597.

الفرع الثاني: ضوابط قبول واقتناع القاضي الجنائي بالدليل الرقمي:

أولا: الضوابط التي تتعلق بمصدر الاقتناع: وتتمثل في:

1. ضابط أن يكون الدليل الإلكتروني مقبولا: وهذا الضابط مكملا لقيد مشروعية الدليل الإلكتروني، فعلى القاضي أن يستمد اقتناعه من أدلة مقبولة ومشروعة، فمن غير الجائز الاعتماد على طرق إثبات لا تأتلف واحترام الإنسان وحريته.

وكما سبق و أن ذكرنا، فإن القاضي الجنائي حر في تقديره للدليل الإلكتروني المقبول في الدعوى، الذي يتم الحصول عليه بطريقة مشروعة، ولهذا فإن مسألة قبول هذا الدليل لا بد أن تحظى بالأهمية، لاعتبارها ركيزة في مبدأ حرية القاضي الجزائي في تقدير الدليل الإلكتروني، لأن محل هذه الحرية هو الأدلة المقبولة، فالتطبيق الحسن للقانون يفرض على القاضي الجنائي أن يكون اقتناعه من دليل إلكتروني مقبول، ويستبعد في المقابل جميع الأدلة الإلكترونية غير المقبولة، لأنه من غير المعقول أن تكون عنصرا من عناصر اقتناعه.

لهذا على القاضي الجنائي أن يستمد اقتناعه الذاتي في مجال الإثبات المتعلق بالجرائم الإلكترونية من دليل إلكتروني مشروع ومقبول، فمن غير الجائز ومن غير المقبول أن يستمد القاضي الجنائي اقتناعه من دليل تم الحصول عليه عن طريق إجراء باطل وإلا بطل معه الحكم، لأن ما بني على باطل فهو باطل[1].

2. ضابط ضرورة طرح الدليل الإلكتروني في الجلسة للمناقشة: بصفة عامة يجب على القاضي أن يستمد قناعته من أدلة طرحت بالجلسة، وخضعت للمناقشة من طرف الخصوم، واستناد القاضي إلى أدلة لم تطرح للمناقشة موجب للبطلان.

فمن الأسس التي تقوم عليها الأدلة أن القاضي لا يمكن أن يباشر سلطته في تقدير هذه الأدلة ما لم تطرح في الجلسة، وبحضور الخصوم وتتم مناقشتها، والغاية من هذا الضابط أن يتاح لكل طرف في الدعوى أن يواجه خصمه بما لديه من أدلة ضده، وكذا يبين موقفه منها.

زيادة على أنه من مقتضيات هذا الضابط، أن تعرض أدلة الدعوى جميعها في جلسة المحكمة وتطرح للمناقشات، فالشاهد بشهادته والمتهم يذكر اعترافه وأيضا يقرأ تقرير الخبير.

[1]- عائشة بن قارة مصطفى: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، المرجع السابق، ص: 269.

فهذه القاعدة تعني أن القاضي لا يجوز أن يؤسس اقتناعه إلا على عناصر الإثبات التي طرحت في جلسات المحكمة، وخضعت لحرية مناقشة أطراف الدعوى إعمالا لمبادئ المحاكمة الجزائية المتمثلة في الشفوية بحسب المواد 300 ـ 304 ـ 353 من قانون الإجراءات الجزائية الجزائري، ومبدأ العلنية بحسب المواد 285 ـ 342 ـ 355 ـ 399 من نفس القانون.

وكذا مبدأ المواجهة بحسب المادة 2/212 من نفس القانون، وهذه المناقشة عليها أن تأخذ في عين الاعتبار ضرورة احترام حقوق الدفاع، بإعطاء فرصة للمتهم للاستفسار حول كل وسيلة من وسائل الإثبات المقدمة أمام القاضي الجنائي هذا من جهة، ومن جهة أخرى يتعين توافر المناقشة الحضورية لأنها تعتبر مطلبا منطقيا، وتنطوي على فحص شامل وجماعي لكل وسيلة إثبات[1].

ولا يختلف الأمر بالنسبة للدليل الإلكتروني، سواء كان على شكل بيانات معروضة على شاشة الكمبيوتر، أو مدرجة في حاملات البيانات أو اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مستخرجة في شكل مطبوعات، كل هذا عليه أن يكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة[2].

ثانيا: الضوابط التي تتعلق بالاقتناع ذاته: تتمثل في ما يلي:

1. ضابط بناء الاقتناع القضائي على اليقين: إن الخصومة الجنائية تهدف بصفة عامة إلى معرفة الحقيقة المطلقة، ولهذا يقتضي أن يصدر القاضي حكمه على اقتناع يقيني، عن طريق صحة ما ينتهي إليه من وقائع، لا بمجرد الظن والاحتمال، لأن الشك يفسر لصالح المتهم آخذا بقاعدة أساسية ومبدأ مهم في الإثبات الجنائي وهو الأصل في الإنسان البراءة، وشرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة التي يستقى منها اليقين أدلة تقليدية أو مستحدثة كالدليل الإلكتروني.

وإذا كان القاضي الجنائي يستطيع الوصول إلى اليقين بالأدلة التقليدية عن طريق المعرفة الحسية التي تدركها الحواس، أو المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج، فإن الجزم بوقوع جريمة إلكترونية ونسبتها إلى المتهم المعلوماتي تتطلب نوعا جديدا من المعرفة، وهي المعرفة العلمية للقاضي بالأمور المعلوماتية لا سيما و أن القاضي الجنائي يلعب دورا إيجابيا في الإثبات الجنائي، وقد يؤدي الجهل في بعض الأحيان إلى التشكيك في قيمة الدليل الإلكتروني ومن ثمة يقضي بالبراءة، خاصة

[1]- أمنة هلال: **الإثبات الجنائي بالدليل الإلكتروني**، المرجع السابق، ص: 107 ـ 108.

[2]- عائشة بن قارة مصطفى: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، المرجع السابق، ص: 269 ـ 271.

أن الشك يستفيد منه المتهم المعلوماتي في مرحلة المحاكمة، وهذا يؤدي إلى إفلات المجرمين من العقاب ومن تطبيق القانون.

2. ضابط ملائمة الاقتناع القضائي لمقتضيات العقل والمنطق: إن القاضي في تكوين اقتناعه و إن كان حرا في اختياره للأدلة التي يطمئن إليها، وهذا في حكمه، إلا أن هذا الأمر مشروط بأن يكون استنتاج القاضي لحقيقة الواقعة وما كشف عنها من أدلة لا يخرج عن مقتضيات العقل والمنطق[1].

فيلزم أن يكون استخلاص محكمة الموضوع لواقعة الدعوى استخلاصا معقولا سائغا، ومعيار معقولية الاقتناع هو أن يكون الدليل بما في ذلك الدليل الإلكتروني مؤديا إلى ما رتبه الحكم عليه، من غير تعسف في الاستنتاج، ولا تنافر مع مقتضيات العقل والمنطق.

ومع ذلك تجدر الإشارة إلى أن تقييد القاضي الجنائي عند تقديره للدليل الإلكتروني بضوابط معينة، سواء كانت متعلقة بهذا الدليل ذاته أو متعلقة بالاقتناع، غير كافية لضمانة منع الاستبداد والتحكم، بل من اللزوم وجود ضمانة أخرى أشد من سابقيها لتجعل سلطة القاضي الجنائي التقديرية تدور في إطار معتدل، بهدف الوصول إلى الحقيقة الواقعية، باعتبارها غرض الدعوى الجزائية، وتتمثل هذه الوسيلة في مراقبة المحكمة العليا لسلطة القاضي الجنائي[2].

وما نستنتجه في الأخير، أن القاضي الجنائي في سبيل اقتناعه بالدليل الإلكتروني من الواجب عليه أن يضع في الحسبان وفي عين الاعتبار مجموعة الضوابط التي رسمها له المشرع، مثله مثل اقتناعه بالأدلة الجنائية الأخرى، باعتبار أن الدليل الإلكتروني أصبح كغيره من الأدلة الجنائية، دليل لا يمكن الاستغناء عنه في خضم التطور التكنولوجي الذي نعيشه، والذي بدوره خلق جرائم مستحدثة وأدلة مستحدثة في سبيل مكافحتها ومنها الدليل الإلكتروني.

الفرع الثالث: مشكلات الدليل الرقمي وأثرها على الاقتناع الشخصي للقاضي الجزائي:

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.

---

[1]- العربي شحط عبد القادر، نبيل صقر: **الإثبات في المواد الجنائية**، المرجع السابق، ص: 29.

[2]- عائشة بن قارة مصطفى: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، المرجع السابق، ص: 281.

أولا: المشكلات الموضوعية للدليل الإلكتروني: وهي في الغالب تتعلق بطبيعة الدليل في حد ذاته وهذا بسبب الخصائص التي يتميز بها هذا الدليل وهي كالآتي:

1. 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 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].

2. 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 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 الانترنت.

3. الدليل الإلكتروني 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

[1]- عائشة بن قارة مصطفى: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، المرجع السابق، ص: 251 . 252.

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[1].

ثانيا: المشكلات الإجرائية للدليل الإلكتروني: تتمثل في ما يلي:

1. ارتفاع تكاليف الحصول على الدليل الإلكتروني: في مجال الدليل الإلكتروني في أغلب الأحيان يتم الاعتماد على الخبرة للتعامل مع هذا الدليل الفني المتوفر في مجال تكنولوجيا المعلومات والانترنت، 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.

2. نقص المعرفة التقنية عند رجال القانون: إن الطبيعة الخاصة التي يتمتع بها الدليل الإلكتروني كان لها أثر على عمل رجال القانون، سواء على المستوى التحقيق أو المحاكمة، وهذا راجع إلى أن الكشف عن الجرائم الإلكترونية 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 الاعتماد 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، وهو ما تم فعلا، وهذا على المستوى الدولي

[1]- عائشة بن قارة مصطفى: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، المرجع السابق، ص: 253 وما بعدها.

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 في مجال الشرطة، وهو أهم تعاون في هذا الخصوص.

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، والقيام بتبادل هذه المعلومات من خلال المكاتب الوطنية للشرطة الدولية الموجودة في أقاليم الدول الأعضاء.

ومع ازدياد معدل الجريمة الإلكترونية اضطر المشرع الجزائري إلى تعديل قانون الإجراءات الجزائية، وذلك بموجب القانون (06 ـ 22) الذي استحدثت فيه فصلين هما الفصل الرابع والخامس من الباب الثاني من الكتاب الأول، حيث يتمثل الفصل الرابع في:" **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور**"، أما الفصل الخامس فقد جاء بعنوان: "**في التسرب**".

ومنه نقول أن الدليل الإلكتروني كغيره من الأدلة الجنائية خاضع لحرية القاضي الجزائي 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 له وصعوبة الحصول عليه.

إلا أن هذا الاقتناع في مجال الدليل الإلكتروني يتأثر بعوامل معينة تترتب على الطبيعة الخاصة لهذا الدليل كما سبق وأشرنا، خاصة التعقيد لكونه دليل علمي، وهذا الأمر له تأثير على قناعة القاضي باعتباره دليل يقيني وموضوعي مما يؤدي بسهولة لاقتناع القاضي، إلا أنه يخضع لتقدير القاضي الجنائي.

كما أن هذا الدليل تنجر عنه عدة مشاكل نابعة من طبيعته الخاصة التي لها تأثير على اقتناع القاضي الجنائي كمشكل أصالة الدليل الإلكتروني، وارتفاع تكاليف الحصول عليه، إلا أن مبدأ الاقتناع القضائي وحرية القاضي الجنائي له دور كبير في مواجهة هذه المشاكل، بإخضاع هذا الدليل لهذه المبادئ نظرا لصعوبة الحصول عليه، 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، 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: 94 . 95.

ملخص الفصل الثاني:

وفي خلاصة هذا الفصل يجدر بنا القول أنه لإثبات الجريمة الإلكترونية لا بد 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 الإلكتروني.

الخاتمة

الخاتمة:

تعد هذه الدراسة حصيلة جهد قمنا به بهدف التصدي لموضوع إثبات الجريمة الإلكترونية، غير أنه 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 اتضحت من خلال تحليل وتفسير البيانات التي تم الحصول عليها خلال هذه الدراسة، وفي هذا الصدد سيتم عرض ملخص لأهم النتائج والتوصيات المتوصل إليها وذلك على النحو الأتي :

1: النتائــج:

هناك العديد من النتائج التي توصلت إليها هذه الدراسة، علما أنه 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 و الأنماط المكونة لها.

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

- يعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية ويزداد الإثبات صعوبة في الجرائم الالكترونية، حيث أن اكتشاف الجريمة الالكترونية أمر ليس بالسهل ، وفي حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كثير من الصعاب، مما يستلزم الكثير من الجهد والخبرة الفنية.

- إن الجريمة الالكترونية قد تكون جريمة تقليدية تضم جانب الكتروني، لاسيما في ظل ارتباط الناس بالتقنيات الحديثة التي انتشرت بشكل كبير وأهمها الحاسبات الآلية والهواتف الذكية، وقد تكون جريمة الكترونية مستقلة بذاتها.

- تتطلب طبيعة الجريمة الالكترونية بصفة عامة أساليب غير تقليدية في التحقيق لاكتشاف الدليل الرقمي ودعمه من طرف الفنيين المختصين، وذلك يستدعي اتخاذ إجراءات سريعة في هذا الخصوص، لأن الدليل الالكتروني غير مادي ويمكن التخلص منه من قبل مرتكبي هذه الجرائم، كما تختلف أساليب تلقي البلاغ وإجراء المعاينة والقيام بالتحريات والتفتيش في الجرائم التقليدية نظرا لطبيعة الجرائم الالكترونية وخصوصياتها.

- تواجه طرق التحقيق في إثبات الجريمة الالكترونية صعوبات متعددة، حيت تستدعي هذه الطرق في المقام الأول اكتشاف الجريمة الالكترونية ومحلها وبيئتها ثم الإبلاغ عنها، وأخذ إذن الجهات المختصة قبل القيام بالمعاينات والتفتيش للموقع أو الجهاز المشتبه به، وذلك للبحت عن الدليل الرقمي الالكتروني بالطرق الفنية ومن ثم إجراء التحريات والأبحاث التي تساعد في عملية الإثبات.

- تتسم الجرائم ذات الصلة بالحاسب الآلي بحداثة أساليب ارتكابها وسرعة تنفيذها وسهولة إخفائها ودقة وسرعة محو أثارها، هذه الخصائص العامة تقتضي أن تكون جهات التحري والتحقيق بل و حتى المحاكمة على دراية كبيرة بأنظمة الحاسب الآلي وكيفية تشغيلها وأساليب ارتكاب الجرائم عليها أو بواسطتها، مع القدرة على كشف غموض هذه الجرائم وسرعة التصرف بشأنها.

- تمثل الشهادة أهمية كبيرة في إثبات الجريمة الالكترونية في المواد الجزائية، فهي ترد على وقائع مادية وترشد القاضي إلى تحري قيمتها، حيث يكون للشهادة أثناء التحقيق أثر كبير في ما يتعلق بالبراءة والإدانة، كما لها أهميتها في الكشف عن الأدلة التي تساعد في إثبات الجريمة الالكترونية .

- تساعد الخبرة الفنية في إثبات الجريمة الالكترونية حيث تكمن أهمية الخبرة في أنها تنير الطريق أمام القاضي الذي يهتدي بها إلى تحقيق العدالة، لاسيما في المجال الجنائي، لذا فقد اهتمت مختلف القوانين بأهمية الاستعانة بالخبراء، وبالتالي فإنه يجوز للمحكمة المختصة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم.

- يعتبر فقدان الأثر من أهم المعوقات التي تواجه إثبات الجريمة الالكترونية، حيث تظل الجريمة الالكترونية عن طريق الحاسب الآلي مجهولة ما لم يبلغ عنها للجهات المكلفة بالتحريات وجمع الاستدلالات أو التحقيق القضائي، علما أن المشكلة التي تواجهها الجهات المختصة أن هذه الجرائم لا تصل إلى علمها بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية لا تخلف آثارا مادية كتلك التي تخلفها الجريمة العادية .

- لم تنص أغلب التشريعات والقوانين على الدليل الالكتروني أو الرقمي ومنهم المشرع الجزائري الذي بدوره لم ينص على الدليل الالكتروني في قوانينه، علما أنه يعتبر المساهم الأول في سبيل مواجهة الجرائم الالكترونية، وهذا يعتبر قصورا من طرف مختلف التشريعات والقوانين.

- إن محل الدليل الالكتروني ونطاق العمل به هو الجريمة الالكترونية، غير أنه يصلح كذلك لإثبات الجرائم التقليدية التي تم ارتكابها عن طريق تقنية الحاسب الآلي.

- قصور أغلب التشريعات من الناحية الإجرائية فيما يخص إجراءات الحصول على الدليل الالكتروني واقتصارها على القواعد العامة والإجراءات التقليدية .

- تمتع الدليل الالكتروني بيقينية كبيرة بسبب الحرص على العمل بمبدأ مشروعية الدليل الالكتروني .

2: **الاقتراحات:**

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

- تستدعي عملية التحقيق في الجرائم الالكترونية تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، بصورة تمكن رجال التحريات من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمة لذلك، ولتحقيق ذلك يجب زيادة الاهتمام بتدريب المكلفين بمباشرة التحريات والتحقيقات مع الاستعانة بذوي الخبرة الفنية المتميزة في هذا المجال.

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

- يجب التأكد أيضا من عدم وجود مجالات كهرومغناطيسية في المحيط الخارجي لمسرح الجريمة حتى لا يتم أي إتلاف للبيانات المخزنة، وهذا يتطلب اختبارات وفحوصات تقنية قبل نقل أي مادة معلوماتية من مسرح الجريمة.

- يجب فحص كل ما تحويه سلة المهملات في الجهاز ورفع البصمات التي قد تكون لها دلالة على مرتكب الجريمة، بالإضافة إلى ضرورة القيام بحفظ كل المستندات الخاصة بالإدخال والإخراج والتي قد تكون على صلة بالجريمة.

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

01/ الإلمام بتركيب الحاسب وصناعته وطرازه ونظم تشغيله الرئيسة والفرعية، والأجهزة الملحقة به وكلمات المرور أو السر أو رموز التشفير.

02/ طبيعة البيئة التي يعمل في ظلها الحاسوب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين و الوسائل المستخدمة في ذلك.

03/ قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك أي مشاكل أو تدمير الأدلة المتحصلة من الوسائل الالكترونية.

04/ التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بغير أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على دعائمها الممغنطة.

- إنشاء قاعدة بيانات لجرائم المعلومات من حيث 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 الالكترونية كأدلة إثبات في المجال الجنائي والاعتراف لها بحجية قاطعة، وكذلك النص على وسائل التأكد من سلامة الدليل الالكتروني التي تعتبر شرطا لقبوله.

- وجوب تعديل القواعد الإجرائية التي يؤخذ بها في تجميع الدليل الالكتروني بما يتماشى مع خصائص الدليل الالكتروني وطبيعته، وعدم الاكتفاء بالإجراءات التقليدية لجمع الدليل الالكتروني حيث أنه يجب أن تصاحبها إجراءات حديثة وهذا من طرف الدول التي لم تنص عليها صراحة واكتفت فقط بالإجراءات التقليدية ومنها المشرع الجزائري الذي يجب عليه تحديث إجراءات الحصول على هذا الدليل .

- لزوم أن يتوفر القضاة ومختلف من يعمل على الحصول على الدليل الالكتروني 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 الالكتروني، باعتبار أن الجرائم الالكترونية من الجرائم العابرة للحدود، وهذا بغرض تسهيل إجراءات تحصيل هذا النوع من الأدلة.

قائمة المصادر والمراجع

قائمة المصادر والمراجع:

أولا: المصادر:

1: القانون رقم 16-01 المؤرخ في 6-03-2016 المعدل للدستور عدد الجريدة الرسمية 14.

2: الأمر 15-02 المؤرخ في 23 **جويلية** 2015، المعدل والمتمم للأمر 66-155 المؤرخ في 8 **يونيو** المتضمن قانون الإجراءات الجزائية ، الجريدة الرسمية المؤرخة في 23 **يونيو** 2015 ، العدد40.

3: القانون رقم 04/09 مؤرخ في 5 **غشت سنة** 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال، الجريدة الرسمية، **العدد**47 المؤرخة في 16 **أغشت سنة** 2009.

4: المرسوم الرئاسي رقم 15-261 ومؤرخ في 28 **أكتوبر** 2015، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية المؤرخة في 8**أكتوبر** 2015، **العدد** 53.

5: الأمر 156/66 المتضمن قانون العقوبات، المؤرخ في 8 **يونيو** 1966، المعدل والمتمم بالقانون 15/04، المؤرخ في 10 **نوفمبر** 2004، الجريدة الرسمية المؤرخة في 24 **ديسمبر** 2006، **العدد** 71.

6: قانون البريد والاتصالات السلكية واللاسلكية رقم 03- 2000 المؤرخ 2000/08/05، الجريدة الرسمية **عدد**48.

7: القانون رقم 08/01 المؤرخ في 2008/01/23 والمعدل والمتمم لقانون 83/01 المتعلق بالتأمينات، الجريدة لرسمية **عدد**29.

ثانيا: المراجع:

أ): الكتب:

1: أحمد إبراهيم: **طرق الإثبات الشرعية**، كلية الحقوق، مصر، العدد01، 1مارس 1993.

2: أحمد فتحي سرور: **الوسيط في قانون الإجراءات الجنائية**، (ط.4)، المجلد الأول، دار النهضة العربية، القاهرة، 1981.

3: العربي شحط عبد القادر، نبيل صقر: **الإثبات في المواد الجزائية**، (د.ط)، دار الهدى للنشر والتوزيع، الجزائر، (د.س.ن).

4: برهان عزيزي: **إثبات الجريمة في أحكام مجلة الإجراءات الجزائية**، (ط.1)، مجمع الأطرش للكتاب المختص، تونس، 2013.

5: جميل عبد الباقي الصغير: **القانون الجنائي والتكنولوجيا الحديثة**، (د.ط)، دار النهضة العربية، القاهرة، 1992.

6: خالد محمد المهيري: **التحقيق الجنائي العملي في الجريمة التقليدية والمعلوماتية**، (ط.2)، دار الغرير للطباعة والنشر، دبي، (د.س.ن).

7: رمزي رياض عوض: **مشروعية الدليل الجنائي في مرحلة المحاكمة وما قبلها: دراسة تحليلية تأصيلية مقارنة**، (د.ط)، دار الفكر العربي، القاهرة، 2000.

8: سامي جلال فقي حسين: **الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي**، (د.ط)،دار الكتب القانونية، مصر، 2011.

9: سعيد عبد اللطيف حسين: **إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت: الجرائم الواقعة في جرائم تكنولوجيا المعلومات**،(د.ط)، دار النهضة العربية، القاهرة، 1999.

10: عائشة بن قارة مصطفي: **حجية الدليل الإلكتروني في مجال الإثبات الجنائي**، دار الجامعة الجديدة، الإسكندرية، 2010.

11: عبد الإله أحمد هلالي: **تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي**،(د.ط)، دار النهضة العربية، القاهرة، 1997.

12: عبد الإله هلالي: **التزام الشاهد بالإعلام في الجرائم المعلوماتية، دراسة مقارنة**، (د.ط)، دار النهضة العربية، القاهرة، 2000.

13: عبد الفتاح بيومي حجازي: **الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت**، (د.ط)، دار الكتب القانونية، مصر، (د.س.ن).

14: عبد الفتاح بيومي حجازي: **علم الجريمة و المجرم المعلوماتي**، ط1، توزيع منشأة المعارف، الإسكندرية،2009.

15: عبد الفتاح مراد: **شرح جرائم الكمبيوتر والانترنت**، (د.ط)، دار الكتب والوثائق المصرية ، 2005.

16: عبد الفتاح مراد: **شرح التحقيق الجنائي الفني والبحث الجنائي** ،(د.ط)، دار الكتب والوثائق المصرية، مصر، 2006.

17: عبد الفتاح مصطفى الصيفي: **تأصيل الإجراءات الجنائية**، (د.ط)، دار المعرفة الجامعية، الإسكندرية، 2002.

18: عفيفي كامل عفيفي: **جرائم الحاسب الآلي وحقوق المؤلف والمصنفات الفنية**، (د.ط)، منشأة المعارف، الإسكندرية، 2000.

19: علي جبار الحسيناوي: **جرائم الحاسوب والانترنت**، (د.ط)، دار اليازوري العلمية للنشر والتوزيع، الأردن، 2009.

20: علي حسن محمد الطوالبة: **التفتيش الجنائي على نظم الحاسوب والانترنت**، (ط.1)، عالم الكتاب الحديث للنشر والتوزيع، الأردن، 2004.

21: فاضل زيدان محمد: **سلطة القاضي الجنائي في تقدير الأدلة**، (ط.1)، دار الثقافة للنشر والتوزيع، الأردن، 2006.

22: فتحي محمد أنور عزت: **الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية**، (ط.1)، دار الفكر والقانون للنشر والتوزيع، مصر، 2010.

23: فهد إبراهيم السبهان: **استجواب المتهم بمعرفة سلطة التحقيق**، (د.ط)، مطبعة بن دسمال، دبي، 1995.

24: مأمون محمد سلامة: **الإجراءات الجنائية في التشريع المصري**، (د.ط)، دار الفكر العربي، القاهرة، 1991.

25: محمد الأمين خرشة: **مشروعية الصوت والصورة في الإثبات الجنائي**، (ط.1)، دار الثقافة للنشر والتوزيع، الأردن، 2011.

26: محمد حماد الهيتي: **جرائم الحاسوب: ماهيتها،أهم صورها والصعوبات التي تواجهها**، (د.ط)، دار المناهج للنشر والتوزيع،عمان، 2005.

27: محمد زكي أبو عامر ـ علي عبد القادر القهوجي: **قانون العقوبات، القسم الخاص** ، (د.ط)، دار النهضة العربية القاهرة، 1993.

28: محمد سامي الشوا: **الثورة المعلوماتية و انعكاساتها على قانون العقوبات**، (ط2)، دار النهضة العربية، القاهرة، 1998.

29: محمد سامي الشوا: **ثورة المعلومات وانعكاساتها على قانون العقوبات**، (د.ط)، دار النهضة العربية، القاهرة، 2000.

30: محمد علي العريان: **الجرائم المعلوماتية**، (د.ط)، دار الجامعة الجديدة للنشر، الإسكندرية،2011.

31: محمد علي الكيك: **السلطة التقديرية للقاضي الجنائي**، (د.ط)، دار المطبوعات الجامعية، مصر، 2007.

32: محمد علي قطب: **الجرائم المعلوماتية وطرق مواجهتها**، وزارة الداخلية، الأكاديمية الملكية للشرطة، مملكة البحرين، 2010.

33: محمد فهمي: **الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني**، (د.ط)، مطابع المكتب المصري الحديث، القاهرة، 1991.

34: محمد محمد شتا: **فكرة الحماية الجنائية لبرامج الحاسب الآلي**، (د.ط)، دار الجامعة الجديدة، القاهرة، 2000.

35: محمود عبد الله حسين: **سرقة المعلومات المخزنة في الحاسب الآلي**، (د.ط)، دار النهضة العربية، القاهرة، 2002.

36: محمود محمود مصطفى: **الإثبات في المواد الجنائية في القانون المقارن**، (د.ط)، مطبعة جامعة القاهرة، القاهرة، 1977.

37: محمود نجيب حسني: **شرح قانون الإجراءات الجنائية**، (ط.2)، دار النهضة العربية، القاهرة، 1987.

38: ممدوح عبد الحميد عبد المطلب: **جرائم استخدام الحاسب الآلي وشبكة المعلومات العالمية: الجريمة عبر الانترنت**، (د.ط)، مكتبة دار الحقوق، الشارقة، 2001.

39: ممدوح عبد الحميد عبد المطلب: **البحث والتحقيق الجنائي الرقمي في جرائم الحاسب الآلي والانترنت**، دار الكتب القانونية، مصر، 2006.

40: نائلة عادل محمد فريد: **جرائم الحاسب الآلي الاقتصادية**، (د.ط)، منشورات الحلبي الحقوقية، 2005.

41: نبيل عبد المنعم جاد: **أسس التحقيق والبحث الجنائي العملي**،(د.ط)، مطبعة كلية الشرطة، (د.ب.ن)، 2006.

42: نهلا عبد القادر المومني: **الجرائم المعلوماتية**، (ط1)، دار الثقافة للنشر و التوزيع، عمان،2008.

43: هشام فريد رستم: **الجوانب الإجرائية للجرائم المعلوماتية**، (د.ط)، مكتبة الآلات الحديثة، أسيوط، مصر، 1994.

44: يونس عرب: **جرائم الحاسب الآلي والانترنت**، منشورات اتحاد المصارف العربية، (د.ب.ن)، 2002.

ب): المقالات:

1: عادل عبد الجواد محمد: **الانترنت والإجرام المنظم**، مجلة الأمن والحياة، العدد 303، 26 **سبتمبر** 2007، (د.ب.ن).

2: فوزي عمارة: **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجنائية**، مجلة العلوم الإنسانية، العدد 33، جامعة منتوري، قسنطينة، جوان 2010.

3: محمد الأمين البشري: **التحقيق في جرائم الحاسب والانترنت**، المجلة العربية للدراسات العربية والتدريب، المجلد:15، العدد: 30، جامعة نايف للعلوم الأمنية، الرياض، 2001.

ج): الملتقيات:

1: عبد الله حسين علي محمود: **إجراءات جمع الأدلة في مجال جريمة سرقة المعلومات،** بحث مقدم للمؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، محور القانون الجنائي، دبي، من 26 إلى 28 أفريل 2003.

2:عبد الرحمان حملاوي، مداخلة بعنوان دور المديرية العامة للأمن الوطني في مكافحة الجرائم الالكترونية، جامعة بسكرة، كلية الحقوق ، 2016.

3: عبد الناصر محمد محمود فرغلي . محمد عبيد سيف سعيد المسماري: **الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، دراسة تطبيقية مقارنة،** المؤتمر الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف للعلوم الأمنية، الرياض، 2007.

4: عمر محمد بن يونس: **مذكرات في الإثبات الجنائي عبر الانترنت،** ندوة الدليل الرقمي بمقر جامعة الدول العربية بمصر، الفترة من 5 إلى 8 مارس 2006.

5: فضيلة عاقلي: **الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري،** كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017.

6: محمد الأمين البشري: **التحقيق في جرائم الحاسب والانترنت،** المجلة العربية للدراسات العربية والتدريب، المجلد:15، العدد: 30، جامعة نايف للعلوم الأمنية، الرياض، 2001

7: محمد أبو العلا عقيدة: **التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية،** المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، المنعقد في الفترة من 26 إلى 28 أفريل 2003، مركز البحوث والدراسات، أكاديمية شرطة دبي، 2003.

8: محمد فاروق عبد الحميد كامل: **القواعد الفنية الشرطية للتحقيق والبحث الجنائي،** جامع نايف العربية للعلوم الأمنية، الرياض، 1999.

9: ممدوح عبد الحميد عبد المطلب: **استخدام بروتوكول TCP IP في بحث وتحقيق الجرائم على الكمبيوتر،** المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة

دبي، مركز البحوث والدراسات، رقم العدد:4، المحور الأمني الإداري، تاريخ الانعقاد: 26أفريل 2003، دبي، الإمارات العربية المتحدة.

10: ممدوح عبد الحميد عبد المطلب: **أدلة الصور الرقمية**، ورقة عمل مقدمة ضمن فعاليات ندوة المجتمع والأمن في دورتها الخامسة: الجرائم الإلكترونية الملامح والأبعاد، المنعقدة بكلية الملك فهد الأمنية بالرياض في الفترة من 22 إلى 24 أفريل 2007، كلية الملك فهد الأمنية، الرياض، 2007.

11: نبيل عبد المنعم جاد: **جرائم الحاسب الآلي**، بحث منشور بندوة المواجهة الأمنية للجرائم المعلوماتية، مركز دعم اتخاذ القرار بالقيادة العامة لشرطة دبي، مطبعة بن دسمال، دبي، 2005.

12: نور الدين لوجاني: **أساليب البحث والتحري وإجراءاتها** ، يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية ، الجزائر، يوم 2007/12/12.

13: هشام محمد رستم: **الجرائم المعلوماتية**، أصول التحقيق الجنائي الفني مجلة الأمن والقانون، دبي العدد(2)،1999.

د): البحوث الجامعية:

1: مذكرات الماجستير:

_ ثنيان ناصر آل ثنيان: **إثبات الجريمة الإلكترونية**، رسالة مقدمة استكمالا لمتطلبات الحصول على درجة الماجستير، تخصص السياسة الجنائية، إشراف: الدكتور/ جلال الدين محمد صالح، جامعة نايف للعلوم الأمنية، الرياض، 2012.

_ محمد نصير السرحاني: **مهارات التحقيق الجنائي الفني في جرائم الحاسب الآلي والانترنت**، رسالة ماجستير، جامعة نايف للعلوم الأمنية، الرياض،2004.

2: مذكرات الماستر:

_ أمنة هلال: **الإثبات الجنائي بالدليل الإلكتروني**، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، بإشراف الأستاذ الدكتور: مستاري عادل، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2015.

_ خولة عباسي: **الوسائل الحديثة للإثبات الجنائي في القانون الجزائري**، مذكرة مكملة لمقتضيات نيل شهادة الماستر في الحقوق، تخصص قانون جنائي، بإشراف الأستاذ: دبابش عبد الرؤوف، جامعة محمد خيضر، بسكرة، 2013.

_ مهدي شمس الدين: **النظام القانوني للتسرب في القانون الجزائري**، مذكرة لنيل شهادة الماستر في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر، بسكرة، 2014.

_ نور الهدى السوفي: **التحقيق في الجريمة المعلوماتية**، مذكرة مقدمة استكمالا لمتطلبات نيل شهادة الماستر، شعبة الحقوق، تخصص قانون جنائي، بإشراف الأستاذ الدكتور: رضا الهميسي، جامعة قاصي مرباح، ورقلة، 2017.

ثالثا: المراجع باللغة الفرنسية:

_Aderian Roben , Computer crime and the law , C.L.J. 1991, vol.15.

_Electronic evidence is" information stored or transmitted in binary from that may be relied upon in court ". Eoghan Casey : op.cit. .

Eoghan Casey : Digital evidence and forensicscience , computer and the internet , computer crime, 1st ed Academic Press USA UK 200 .

رابعا: المواقع الإلكترونية:

_ http://diae.net/13793

قائمة المختصرات المستخدمة في المذكرة:

- ق.ع = قانون العقوبات
- ق.إ.ج = قانون الإجراءات الجزائية
- ق.ت = قانون التأمينات
- ط = طبعة
- د.ط = دون طبعة
- د.ب.ن = دون بلد نشر
- د.س.ن = دون سنة نشر

الفهرس

الفهرس: