الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة يحي فارس بالمدية

كلية الحقوق والعلوم السياسية

مذكرة نهاية الدراسة للحصول على شهادة الماستر

تخصص: القانون الجنائي والعلوم الجنائية

بعنوان: **الإثبات الجنائي في مجال الجرائم الالكترونية**

من إعداد الطالب:

❖ فرحات زين العابدين

تحت إشراف الأستاذ:

- الدكتور يحي تومي

السنة الدراسية: 2022- 2023

شكر وعرفان

في البداية، أحمد الله الذي أعطانا القوة والصبر لإتمام هذا العمل العلمي المتواضع.

ثم أتوجه بجزيل الشكر والامتنان إلى **الأستاذ الدكتور تومي يحي** الذي لم يبخل علي بتوجيهاته الهادفة وتدخلاته الصائبة.

كما أتقدم بالشكر إلى جميع أساتذة كلية الحقوق تخصص جنائي على وقوفهم مع الطلبة خاصة في محنة كوفيد 19.

كما أشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه الأطروحة.

ولا أنسى أن أشكر كل من قدم لي يد العون من قريب أو بعيد في إنجاز هذا العمل.

إهداء

إلى من لا يمكن للكلمات أن توفي حقهما، الوالدين الكريمين.

إلى من لا أستطيع الاستغناء عنهم، إخوتي وولدي.

إلى كل الاهل والاقارب وجميع الأصدقاء والزملاء

أهدي ثمرة جهدي.

زين العابدين

مقدمة

مقدمة |

لقد شهدت الوسائل التقنية الحديثة انتشارا واسعا في العصر الحالي فعلى سبيل المثال فقد تغلغلت الحاسبات الآلية وشبكة الانترنت في جميع جوانب الحياة ، بحيث أصبحت العديد من الدول تعتمد عليها في تسيير مرافقها الحيوية كالدفاع والأمن والاقتصاد، كما أن هذه الأخيرة عرفت انتشارا واسعا على المستوى الاجتماعي بحيث أصبح معظم الأفراد يلجؤون إلى استخدام العديد من التقنيات الالكترونية في تسيير شؤون حياتهم اليومية، كالتواصل وتبادل المعارف عبر شبكة الانترنت وانجاز الأعمال وتقديم الخدمات، فلا يقف أمامهم أي عائق لا مادي ولا جغرافي وهذا راجع للطبيعة الخاصة للنظم – المعلوماتية والتي يتم من خلالها ترجمة المعلومات المتبادلة عبر الانترنت في شكل أرقام ورموز الكترونية ويتم ذلك بمجرد كبسة زر على الحاسب الآلي.

ونظرا لما تتميز به النظم المعلوماتية من دقة وسرعة في تجميع المعلومات وتخزينها ومعالجتها، فإنها خلفت إنجازات وتطورات كبيرة في المجال التقني، وهذا راجع للاستخدامات الكثيرة لها في مختلف قطاعات الحياة إلا أن هذه التكنولوجيا أدت إلى ظهور نوع جديد من الجرائم ألا وهي الجرائم الالكترونية وقد تسببت هذه الأخيرة في العديد من الاعتداءات على الحياة الخاصة للأفراد، كما أنها أحدثت خسائر كبيرة لاقتصاد الدول. بالإضافة إلى ذلك فإن الوسائل العلمية الحديثة ساعدت المجرم المعلوماتي على القيام بمختلف الجرائم الالكترونية كاختراق شبكات الانترنت وتزييف النقود الالكترونية وتزوير المستندات الالكترونية ... الخ، بسرعة وبدقة عالية دون ترك أي أثر للكشف عنها أو معرفة مصدرها، كما أن هذا الاعتداء يمكن أن يكون على مجموعة من المجني عليهم في نفس الوقت وفي مختلف أنحاء العالم عن طريق ما يسمى بشبكة الانترنت.

كما أن الطبيعة الخاصة لمحل ارتكاب الجرائم الالكترونية والذي يتمثل في المعلومات صعبت | على السلطات المختصة بالبحث والتحري مباشرة مهامها والمتمثلة في القيام بإجراءات الاستدلال و التحقيق عبر البيئة الرقمية وهذا راجع لتعودهم على التعامل مع الجرائم التقليدية والتي تخلف أثارا مادية في مسرح الجريمة كالبصمات مما يسهل عليهم هذه المهمة على عكس الجرائم الالكترونية فإنها لا تخلف أثارا مادية وهذا لانعدام الدليل المرئي لها، وبفضل هذه الخاصية فإن الجاني في هذه الجرائم يمكنه إخفاء وطمس الدليل من مسرح الجريمة، مما يزيد الأمر تعقيدا على هذه السلطات ولذلك فإن عملية البحث والتحري لهذه الجرائم تحتاج إلى طرق الكترونية فنية وتقنية تتناسب مع طبيعتها بشكل يمكنها من ترجمة الأرقام والرموز الالكترونية إلى بيانات مقروءة تصلح بان تكون ادلة للإثبات لهذه الجرائم ونسبتها لفاعليها ويطلق عليها اسم الأدلة الالكترونية.

ونظرا للأهمية البالغة لموضوع الإثبات الجنائي في مجال الجرائم الالكترونية فقد كان محور دراستنا في هذه المذكرة بحيث تكمن هذه الأهمية في كون أن الجرائم الالكترونية من الجرائم المستحدثة والتي هي أخذت في تطور مستمر كما أن أساليب ارتكابها دائمة العمل على مواكبة التطور التكنولوجي الحاصل في ميدان المعلوماتية، لذلك فإن هذا النوع من الجرائم يرتبط بالمستجدات التي لم تكن معروفة في مجال القانون الجنائي سواء من الناحية الموضوعية أو الإجرائية. بالإضافة إلى ذلك فإن أهمية هذا الموضوع تتضح في كونه تناول أحدث الوسائل العلمية وأكثرها انتشارا في قضايا الإثبات الجنائي ألا وهو الدليل الالكتروني والذي جاء ليتلاءم مع الجريمة المستحدثة المرتكبة عبر تكنولوجيات الاعلام والاتصال.

كما أنه ومن دون منازع فإن أي محاولة للتعامل إجرائيا مع هذا النوع من الأدلة في إطار عملية البحث والتحري سبب عدة إشكالات إجرائية للأجهزة المكلفة بذلك، وينبغي أن تأتي الدراسات القانونية من أجل الشرح والإيضاح لذلك فقد سبب هذا الموضوع جدلا فقهيا كبيرا بين فقهاء القانون الجنائي، كون الجرائم الالكترونية تميزت بطبيعة خاصة من حيث الوسائل التي ترتكب بها، ومن حيث المحل الذي تقع عليه، ومن حيث الجناة الذين يرتكبونها، فالجناة في مثل هذه النوعية من الجرائم، هم من المجرمين المحترفين الذين يرتكبون جرائمهم دونما ثمة آثار دماء أو آثار طلقات نارية، ولكن هم يخططون لما يفعلون، ويستخدمون قدراتهم الفنية والعقلية لنجاح هذا التخطيط، وهم كذلك يحيطون أنفسهم بتدابير أمنية واقية تزيد من صعوبة كشفهم .

وإن السبب الرئيسي الذي دفعنا لاختيار موضوع الإثبات الجنائي في مجال الجرائم الالكترونية كونه من الموضوعات المستحدثة التي تعاني من نقص الدراسات كما أنه للتطرق لهذا الموضوع يتسنى لنا معرفة مدى مواكبة التطور القانوني للتقدم التكنولوجي الذي شهده العالم في منتصف القرن العشرين، لأن هذا التطور لم يخلف أثاراً إيجابية فحسب، بل تعدى إلى أبعد من ذلك، فقد استغل ذلك معظم الأشخاص للقيام بمختلف الجرائم وذلك بالاستعانة بالتقنيات التكنولوجية الحديثة.

أما بالنسبة لإشكالية هذا الموضوع فباعتبار أن الجريمة الالكترونية من الجرائم المستحدثة المتعلقة بالكيانات غير المادية، مما يؤكد على صعوبة الكشف عنها وإثباتها وهذا راجع للطبيعة الخاصة والمعقدة للدليل الالكتروني، مما خلف العديد من المشكلات فيما يخص مسألة الأخذ به وقبوله كوسيلة من وسائل الإثبات الجنائي وذلك لأن مستودع هذه الأدلة هو الوسائل الالكترونية مما يجعلها قابلة للتلاعب والتغيير في الحقيقة التي وجدت من أجل التعبير عنها مما يطرح التساؤل حول اشكالية الاثبات الجنائي في الجرائم الالكترونية وكيفية الحصول على الدليل الإلكتروني حتى يعرض أمام القضاء الجزائي، ويعد الاثبات بالأدلة

الرقمية من أبرز تطورات العصر الحديث في كافة النظم القانونية ومن هنا تبدو أهمية الاثبات الجنائي بالدليل الالكتروني في كون هذا الاخير الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم المستحدثة وعلى هذا الأساس فقد ارتأينا بأن تكون إشكالية دراستنا كالآتي:

- ❖ إلى أي مدى يمكن الاعتماد على الدليل الالكتروني في الإثبات الجنائي؟
- ❖ وتتفرع عن هذه الإشكالية عدة تساؤلات والمتمثلة فيما يلي:
- ❖ ما مفهوم الجريمة الالكترونية وخصائصها؟
- ❖ كيف يمكن استخراج الدليل الالكتروني لوصفه دليل إثبات أمام القضاء الجزائي؟
- ❖ ما هي الشروط اللازمة للاعتماد على الدليل الالكتروني كدليل إثبات؟

وإن الهدف المرجو من دراسة هذا الموضوع هو معرفة مدى مواكبة القانون للتطور التكنولوجي وتحديد طرق البحث والتحري في الجرائم الالكترونية ومن خلالها يمكننا التعرف على كيفية الحصول واستخلاص أدلة الإثبات الجنائي وهذا راجع لكون أن مسرح الجريمة الرقمي هو مسرح افتراضي لأن الجرائم الالكترونية ذات طبيعة معنوية ولا تترك آثارا مادية مما يؤكد لنا بلا شك أن التحقيق وجمع الأدلة في هذه الجرائم يختلف عما هو الحال في الجرائم التقليدية.

لكن عند دراستنا لهذا الموضوع وقفت أمامنا مجموعة من الصعوبات والمتمثلة أساسا في نقص المراجع المتخصصة والدراسات السابقة ويعود ذلك لكون أن هذا الموضوع موضوعا حديثا لم تسبق دراسته بتعمق من الناحية الجنائية بالتحديد ولو أن هناك مجموعة من المقالات والمراجع التي عالجت هذا الموضوع من الناحية المدنية أو التجارية أو حتى الجنائية ولكن بشكل جزئي دون تناول جميع جوانبه.

ولقد اتبعنا في دراستنا المنهج التحليلي الوصفي بحيث تتضح سماته من خلال قيامنا بوصف الجريمة الالكترونية وتحديد بعض المفاهيم التي تقوم عليها وكذلك تلك الخاصة بإجراءات البحث والتحري عنها من جهة، ومن جهة أخرى فقد قمنا بتحليل بعض المواد والمفاهيم التي تناولتها هذه الظاهرة وذلك لأن دراستنا تهتم بسيل الكشف وضبط أدلة الإثبات الجنائية في مجال الجرائم الالكترونية من الناحية الفنية والقانونية.

ومن أجل معالجة الإشكالات السابق طرحها ارتأينا تقسيم هذه الدراسة إلى فصلين ولكل فصل مبحثين: بحيث تناولنا في **الفصل الأول** "اجراءات تحصيل الدليل الالكتروني في الجريمة الالكترونية"، ففي المبحث الأول تطرقنا إلى الاطار المفاهيمي للجريمة الالكترونية ، أما المبحث الثاني فكان محور دراستنا اجراءات تحصيل الدليل الالكتروني، أما **الفصل الثاني** "القيمة الثبوتية للدليل الالكتروني أمام القضاء" بحيث

مقدمة |

تناولنا في المبحث الأول حجية الدليل الالكتروني امام القضاء الجنائي، أما المبحث الثاني تطرقنا فيه إلى سلطة القاضي في تقدير الدليل الإلكتروني.

الفصل الأول

إجراءات تحصيل الدليل الالكتروني في الجريمة الالكترونية

تمهيد:

يجب التأكيد ومنذ البداية أنه لا وجود لجريمة معلوماتية أو الكترونية بدون وجود جهاز حاسوب بمكوناته المادية والمعنوية أو البرامجية، ذلك أن الحاسوب قد يكون هدفا للجريمة أو أداة لها وبيئة لها وإما اداة للكشف عنها، ومجابهتها ومن هنا يمكننا القول بأن التطور السريع والمستمر في استخدام الحاسوب صاحبته ظاهرة تعد خطيرة للغاية وهي الجريمة المعلوماتية وهي ظاهرة اجرامية جديدة ومما يزيد من خطورتها أنها تطال الحياة الخاصة للأشخاص وتستهدف المعلومات لذلك فإن تحديد مفهومها وإدراك ماهية هذه الجريمة بمختلف صورها يتطلب استقراء أراء الفقهاء والوقوف على التعريف المستنبط لها، بما تتخذه من المصطلحات الدالة عليها ذلك أن هذا النوع من الجرائم يتميز بتعدد الأشكال منها جرائم اختراق شبكات المعلومات، واتلاف البيانات وتدمير البرمجيات وسرقة المعلومات وغير ذلك كثير.

وإذا كانت الجريمة المعلوماتية ظاهرة قائمة ومتفاقمة الآن فإن الجهود المتواصلة لمجابهتها تصطدم بعدة عراقيل، سيما على مستوى النص الإجرائي للوصول إلى مرتكبي هذه الجرائم وتقديمهم للعدالة نظرا الخصوصية هذا النوع من الجرائم وطابعها الخاص ومن هنا تثار الصعوبة حول إمكانية الحصول على الدليل الرقمي وهو أمر يشكل بحد ذاته تحديا كبيرا. وعلى ضوء ذلك سنتناول في هذا الفصل الإطار المفاهيمي للجريمة الالكترونية في المبحث الأول وإجراءات تحصيل الدليل الالكتروني في المبحث الثاني.

المبحث الأول: الإطار المفاهيمي للجريمة الالكترونية

يقصد بالجريمة الالكترونية تلك المتصلة بتكنولوجيات الإعلام والاتصال مما يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات أو الاستخدام غير المشروع للبيانات المخزنة في أنظمة الحاسوب والتلاعب بها أو تدميرها فهي ترتكب عن طريق الحاسوب الآلي والانترنت. ولقد بذلت جهود كبيرة من أجل الوصول إلى وضع تعريف مناسب وملائم للجريمة المعلوماتية بغية تطويقها وضمان تعاون دولي لمحاربتها. وللوقوف على تحديد مفهوم الجريمة المعلوماتية يستلزم علينا التطرق الى تعريف الجريمة المعلوماتية في المطلب الاول وتحديد خصائصها في المطلب الثاني ثم نستعرض أساليب الجريمة المعلوماتية والاثار الناجمة عنها في المطلب الثالث.

المطلب الأول: مفهوم الجريمة الالكترونية

الفرع الأول: تعريف الجريمة الالكترونية

أولا: التعريف الضيق للجريمة الالكترونية

لقد عرف أنصار التعريف الضيق للجريمة الإلكترونية أنها لا تتحقق إلا إذا كان الفعل الجرمي يستهدف النظم المعلوماتية في ذاتها(Target of anoffense)، وهو بذلك يستبعد الحالة التي تستغل فيها وسائل التكنولوجيا الحديثة في ارتكاب الجرائم التقليدية. ولعل أبرز مناصري هذا الرأي نجد الأستاذ Sieberحيث يعرف الجريمة الإلكترونية على أنها كل سلوك غير مشروع أو غير مرخص به يهم المعالجة الآلية للمعطيات أو إرسالها، إذ يقول:

"est considéré comme crime informatique tout comportement illégal ou non autorisé qui concerne un traitement automatique de données ou de transmission de donné".

وعرفها الفقيه rosblat: "هي كل نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلي والتي تحول طريقه."

أما الفقيه Friedman عرفها كالتالي: "أي جريمة ضد المال مرتبطة باستخدام المعالجة الآلية للمعلومات. ويرى الأستاذ Mass أنها " الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق ربح.[1]

[1] عبد الحميد المليحي، الجريمة الالكترونية: مدخل إلى الإطار المفاهيمي، كلية الحقوق طنجة،

ويرى الأستاذ Parker أن الجريمة المعلوماتية هي كل فعل إجرامي متعمد كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه، أو كسب يحققه الفاعل.

وفي نفس الاتجاه ذهبت الأستاذة قورة نائلة إلى تعريف الجريمة الالكترونية بقولها: " كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى، وقد سار على هذا المنوال الأستاذ فالي علال، حيث اعتبر أن الجريمة المعلوماتية: " تشمل فقط الجرائم التي تكون فيها المعلومات والمعطيات والبيانات والوثائق المضمنة والمخزنة بالحاسوب أو بالأنظمة المعلوماتية أو بالبرامج التطبيقية أو برامج التشغيل المتعلقة بها موضوعا أو محلا لها، وذلك سواء كانت هذه المعطيات متاحة للجمهور أو سرية يتطلب الأمر توفر شروط معينة لولوجها، وسواع كان مرتكبها مؤهل لهذا الولوج المشروع بتوفره على كلمات المرور مثلا أو كان يستعمل في ذلك أسلوب غير مشروع عن طريق الاختراع."

وقد تعرضت هذه التعريفات لجملة من الانتقادات لكونها قاصرة عن الإحاطة بأوجه ظاهرة الإجرام المعلوماتي، حيث هناك من ركز على موضوع الجريمة، وركز آخرون على وسيلة ارتكابها في حين ركز البعض على فاعل الجريمة، والجريمة الإلكترونية قد تقع على الحاسب الألى بشقيه المادي hardware والمعنوي software ممثلا بالكيان المنطقي logical، بالاعتداء على البيانات المخزنة والمتبادلة بين الحاسب الآلي وشبكاته الخاصة والعامة عبر خطوط قنوات الاتصال.

ثانيا: التعريف الواسع للجريمة الالكترونية

أما أنصار التعريف الواسع لمفهوم الجرائم الالكترونية فقد تم تعريفها على أن الأجرام الالكتروني هو: "كل سلوك سلبي أم إيجابي يتم بموجه الاعتداء على البرامج أو المعلومات الاستفادة منها بأية صورة كانت وفي نفس الاتجاه يرى الفقيهان Cerdo وMicheal أن سوء استخدام الحاسب أو جريمة الحاسب تسهل استخدامه كأداة لارتكاب الجريمة، بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، كما تمتد إلى الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع البطاقة الائتمان ماكينات الحاسب الآلية بما تتضمنه شبكات تحويل الحسابات المالية بطرق الكترونية وتزييف المكونات المادية والمعنوية للحاسب، وتمتد أيضا لتشمل جهاز الحاسب أو مكوناته[1].

[1] عبد الحميد المليحي، مرجع سابق الذكر،

أما خبراء منطقة التعاون الاقتصادي والتنمية في عام 1983، عرفوا الجريمة الالكترونية أنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها".

وفي تقرير الجرائم المتعلقة بالحاسوب، أقر المجلس الأوربي بقيام المخالفة (الجريمة) في كل حالة يتم فيها " تغير معطيات أو بيانات أو برامج الحاسوب أو محوها، أو كتابتها أو أي تدخل أخر في مجال إنجاز البيانات أو معالجتها، وتبعا لذلك تسببت في ضرر اقتصادي أو فقد حيازة ملكية لشخص أخر أو يقصد الحصول على كسب اقتصادي غير مشروع له أو لشخص أخر".

أما مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين فقد عرف الجريمة المعلوماتية بأنها: "أية جريمة يمكن ارتكابها بواسطة نظام حاسوب أو شبكة حاسوبية، أو داخل نظام حاسوب وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية".

ويمكن القول بأن هذا التعريف جامع لجرائم الحاسب الآلي وشبكاته، فهو حاول أن يشمل كافة أشكال الإجرام الإلكتروني، سواء المتمثلة في الاعتداء على الجانب المادي للحاسب الآلي وشبكاته المحلية (LAN) أو الممتدة (WAN) (كالأنترنت)، بالإضافة إلى الجانب المعنوي Software (غير المادي). ومراد ذلك أن نظام الحاسب الآلي تشمل كل مكونات الحاسب العادية Hardware المعنوية Software وشبكات الاتصال الخاصة networks بالإضافة إلى الأشخاص حيث يمكن من خلالها تحقيق وظيفة أو هدف محدد[1].

ثالثا: تعريف الجريمة الالكترونية في التشريع الجزائري

لما كانت الحاجة ملحة وضرورية لحماية المال المعلوماتي قد استقر الفكر القانوني على ضرورة وجود نصوص قانونية لهذا الغرض وقد استجابت عدة دول ومنها الجزائر. فبالنسبة للتشريع الجزائري تدارك المشرع الجزائري مؤخرا الفراغ القانوني في مجال الإجرام المعلوماتي وذلك باستحداث نصوص تحريمية لقمع الاعتداءات الواردة على المعلوماتية ضمن نصوص قانون العقوبات، قانون الملكية الفكرية والصناعية، وعليه سنعالج في هذا الجزء من الدراسة القوانين التي سنتها الجزائر لمواجهة الجريمة المعلوماتية والهيئات المكلفة بمحاربة هذه الجريمة.

1- تعريف وأنواع الجريمة المعلوماتية في التشريع الجزائري

لقد أطلق المشرع الجزائري تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على الجريمة المعلوماتية، ولقد عرفها في المادة الثانية من القانون رقم 09-04 المؤرخ في 5 أوت 2009 بأنها: "جرائم

[1] عبد الحميد المليحي،

المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية[1]."

وبالرجوع إلى الاتفاقية الدولية حول الجرائم المعلوماتية المنعقدة ببودابست سنة 2001، نجد أن المشرع الجزائري استمد تعريفه من الاتفاقية الدولية السالفة الذكر.

هذا بخصوص تعريف الجريمة الالكترونية أما فيما يتعلق بأنواعها والتي حددها قانون العقوبات الجزائري في القسم السابع ضمن المواد 394 مكرر إلى 394 مكرر 6 فيمكن إجمالها في:

- جرائم الحذف أو التغيير في معطيات نظام المعالجة الآلية ونصت على هذا النوع من الجرائم المادة 394 مكرر 1 من قانون العقوبات الجزائري "يعاقب بالحبس من ستة أشهر إلى ثلاثة سنوات وبغرامة مالية من 500000 دج إلى 2000000 د.ج كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

- جرائم حيازة أو إفشاء أو نشر أو استعمال المعطيات الآلية: وهذا ما نصت عليه المادة 394 مكرر 2 "يعاقب بالحبس من شهرين إلى 3 سنوات وبغرامة من 1000000 د.ج إلى 5000000 د.ج كل من يقوم عمدا أو عن طريق الغش بما يلي:

- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلومات يمكن ترتكب بها الجرائم المنصوص عليها في هذا التنظيم.
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا التنظيم."

2- القوانين المنظمة للجريمة المعلوماتية في التشريع الجزائري:

قامت الجزائر بسن قوانين خاصة بالجريمة المعلوماتية وهي تعتبر متأخرة مقارنة ببعض الدول العربية، بالرغم من احتلالها المراتب الأولى عربيا وإفريقيا، ومن بين التشريعات نذكر منها:

- قانون العقوبات: قامت الجزائر بتعديل قانون العقوبات بموجب القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004، والذي ادخل عليه تعديل في 20 ديسمبر 2006. ويتضمن قانون العقوبات الجزائري القسم السابع تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ضمن المواد من 394 إلى 394 مكرر 6، والتي تناولت أنواع الجرائم الالكترونية وعقوبتها والتي تم تناول بعضها من قبل.

[1] الجمهورية الجزائرية الديمقراطية الشعبية: الجريدة الرسمية، العدد 47، المتضمن قانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجزائر 16/8/2009، ص 05

- قانون رقم 09-04 المؤرخ في 16 أوت 2009: وهو القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، صدر هذا القانون في الجريدة الرسمية رقم 47 الصادرة بتاريخ 16 أوت 2009، يحتوي على 6 فصول تناولت التعريف بالجريمة، مراقبة الاتصالات الالكترونية، القواعد الإجرائية، الهيئة الوطنية للوقاية من الجرائم المعلوماتية والاختصاص القضائي وهذا في 19 مادة.

3- الهيئات المكلفة بمواجهة الجريمة المعلوماتية في الجزائر:

من أجل مواجهة الجريمة الالكترونية قامت الجزائر بوضع عدة أجهزة وهيئات نذكر منها:

أ- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال:

أنشئت هذه الهيئة بموجب القانون رقم 09-04 المؤرخ في 5 أوت 2009 والذي حددت المادة 14 منه مهام الهيئة والمتمثلة في:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال في ذلك تميع المعلومات وإنجاز الخبرات القضائية.

- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

ب- الهيئات القضائية الجزائية المتخصصة:

والتي تم إنشاؤها بموجب القانون 04-14 المؤرخ في 10 نوفمبر 2004 المعدل للقانون الإجراءات الجزائية وأن اختصاصها إقليمي موسع طبقا للمرسوم التنفيذي رقم 06-348 المؤرخ في 5 ماي 2006.

ج- المعهد الوطني للأدلة الجنائية وعلم الإجرام:

أنشئ هذا المعهد بموجب مرسوم رئاسي رقم 04-183 المؤرخ في 26 جوان 2004 وهو مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، ويوضع تحت وصاية وزير الدفاع الوطني.

يتكون المعهد من 11 دائرة متخصصة في مجالات مختلفة من بينها دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة كما تقدم مساعدة تقنية للمحققين في المعاينات.

4- التدابير الوقائية المستحدثة:

لقد جاء في القانون رقم 04-09 مجموعة من التدابير الوقائية التي يتم اتخاذها مسبقا من طرف مصالح معينة لتفادي وقوع جرائم معلوماتية أو الكشف عنها وعن مرتكبيها في وقت مبكر وهي كالتالي[1]:

أ- مراقبة الاتصالات الالكترونية:

لقد نصت المادة 1 علـــــــــى أربع حالات التي يجوز فيها لسلطات الأمن القيام بمراقبة المرسلات والاتصالات الالكترونية، وذلك بالنظر إلى خطورة التهديدات المحتملة وأهمية المصلحة المحتملة وهي:

- للوقاية من الأفعال التي تحصل وصف جرائم الإرهاب والتخريب وجرائم أمن الدولة.

- عندما تتوفر معلومات عن احتمال وقوع اعتداء على منظومـــــة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني أو النظام العام.

- لضرورة التحقيقات والمعلومات القضائية حينما يصعب الوصول إلـى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.

- في إطار تنفيذ طلبات المساعدات القضائية الدولية المتبادلة.

ب- إقحام مزودي خدمات الاتصالات الالكترونية في مسار الوقاية من الجرائم المعلوماتية :

وذلك من خلال فرض عليهم مجموعة من الالتزامات مذكورة في المواد التالية 10، 11 و 12:

- الالتزام بالتعاون مع مصالح الأمن المكلف بالتحقيق القضائي عن طريق جمع أو تسجيل المعطيات المتعلقة بالاتصالات والمراسلات ووضعها تحت تصرفها مع مراعاة سرية هذه الإجراءات والتحقيق.

- الالتزام بحفظ المعطيات المتعلقة بحركة السير وكل المعلومات التي من شانها أن تساهم في الكشف عن الجرائم ومرتكبيها، وهذين الالتزامين موجهين لكل مقدمي خدمات الاتصالات الالكترونية دون استثناء.

- الالتزام بالتدخل الفوري لسحب المحتويات التي يسمح لهم الاطلاع عليها بمجرد العلم طريقة مباشرة أو غير مباشرة بمخالفتها للقانون، وتخزينها أو جعل الوصول إليها غير ممكن.

[1] ابراهيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، المجلد 2 ، العدد 2 ، جامعة مولود معمري تيزي وزو الجزائر، 1997، ص 153-152.

- الالتزام بوضع ترتيبات تقنية للحد من إمكانية الدخول إلى الموزعات التي تحتوي على معلومات متنافية مع النظام العام والآداب العامة مع إخطار المشتركين لديهم بوجودها، وتشير إلى أن هذين الالتزامين يخصان فقط مقدمي الدخول إلى الانترنت.

الفرع الثاني: خصائص الجريمة الالكترونية

تتميز الجرائم الالكترونية عن الجرائم التقليدية بعدة خصائص ومميزات منها ما يلي:

أولا- أنها تتم في بيئة رقمية الكترونية مجالها الحاسب الآلي بمكوناته المادية من أجهزة ومعدات وتجهيزات الحاسب الآلي ومكوناته المعنوية من النظم البرامجية.

ثانيا- سرعة التنفيذ: إذا يمكن ارتكابها وبضغطه واحدة على لوحة المفاتيح فهي جريمة تتم في وقت ضئيل قد لا يتعدى ثانية واحدة.

ثالثا- التنفيذ عن بعد: خلافا لعملية سرقة معدات الكمبيوتر لا يتطلب تواجد الفاعل في مكان الجريمة بل يمكن للفاعل تنفيذ جريمته في دولة بعيدة عن مكان تواجده فهي جريمة عابرة للحدود اذ أن ربط العالم بشبكة الاتصالات عن طريق الأقمار الصناعية والفضائيات والانترنت مكن من عولمة الجريمة.

رابعا- أنها جريمة ناعمة تخلوا من أي عنف فنقل البيانات من جهاز حاسب إلى آخر يجرى بطريقة آلية سهلة.

خامسا- أنها جريمة صعبة الأثبات وذلك راجع إلى صعوبة الوصول إلى الدليل او أثار مادية يتركها المجرم كما هو الشأن في الجريمة التقليدية إذ يمكن وبسهولة محو الدليل أو تدميره في زمن قياسي[1]، ولما كانت الجريمة المعلوماتية تكتسي هذا الطابع الخاص بها والمميز عن الجريمة التقليدية فقد كان من الضروري أن يوضع لها إطار خاص من حيث الطبيعة القانونية لهذه الخصوصية ومن هنا وجدت التشريعات نصوصا خاصة لمواجهة الإشكالات القانونية التي قد تثار لا سيما بخصوص جمع الأدلة ومدى قبولها من طرف الجهات القضائية ثم تحديد الجهة القضائية التي يؤول إليها الاختصاص في محاكمة مرتكب هذا النوع من الجرائم[2].

[1] يونس خالد عرب العالم الالكتروني الوسائل و المحتوى و المزايا و السلبيات منشورات اتحاد المصاريف العربية: الأردن، 2001، ص 72-73.

[2] على حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الانبات الجنائي الجزء الأول مجلة الأكاديمية شرطة دبي، العدد 1، 2003، ص 197.

ويبدو أنه وبالرغم من إصدار ترسانة من القوانين والتشريعات على المستوى المحلي والدولي فإن الآثار السلبية للثورة المعلوماتية ما فتئت تتزايد من خلال ارتفاع نسبة الجرائم المستحدثة التي ترتكب عن طريق الوسائل التقنية الحديثة وبالذات الحاسوب الانترنت[1].

المطلب الثاني: أساليب الجريمة الالكترونية والآثار الناجمة عنها

إن اشكال وأنواع الجرائم الالكترونية متعددة ومتنوعة ولكنها في الغالب لا تخرج عن نطاق الحاسب الآلي ومكوناته وهي تتخذ أساليب وصور منها الاعتداء على أنظمة الحاسوب فتكون هذه الأخيرة هدفا أو محلا للجريمة أما الصورة الثانية فتتعلق بالاستعمال غير المشروع لنظم المعالجة الآلية للمعلومات[2].

ويلاحظ بأن الصورة الأولى يستخدم فيها الجاني الحاسب الآلي كوسيلة لارتكاب الجريمة ويكون ذلك بأي فعل يؤدي إلى تعطيل نظام المعالجة الآلية عن القيام بوظائفه ويتم ذلك بالاختراق أو الدخول غير المشروع في كل جزء من منظومة المعالجة الآلية للمعطيات وقد يتم ذلك بعدة طرق احتيالية منها استعمال رمز الدخول Code d'acces بصفة غير عادية أو باستعمال برامج أخرى مثل البرنامج المسمى حصان طروادة Cheval de troi.[3]

ويلاحظ أن المشرع الفرنسي يعد أول من بادر بوضع أليات قانونية لحماية المعالجة الالية للمعلومات وذلك عن طريق القانون رقم 19/88 الصادر في 5/01/1988 والخاص بالغش المعلوماتي[4].

أما المشرع الجزائري فقد انتهج نفس النهج كذلك حين بادر بتعديل قانون العقوبات بموجب القانون 15/04 المؤرخ في 10/11/2004 والذي تضمن ثماني مواد من المادة 394 مكرر إلى المادة 394 مكرر 7، كما أضاف المادة 394 مكرر8 بموجب القانون رقم 16-02[1] المعدل والمتمم لقانون العقوبات ونص في ذلك على عدة جرائم منها:

1- الدخول عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات.

2- البقاء عن طريق الغش في كل أو جزء من المنظومة.

3- عرقلة السير العادي للمنظومة المعلوماتية.

4- تكوين جمعية الأشرار في عالم الانترنت.

---

[1] عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية. بط. دار الفكر الجامعي الاسكندرية مصر. 2004، ص 14.

[2] بد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت الجرائم الالكترونية الدراسة مقاربة، الطبعة الأولى منشورات الحلبي الحقوقية بيروت لبنان 2007، ص 52.

[3] هشام محمد فريد رستم، قانون المطويات ومخاطر تقنية المعلومات نط مكتبة الآلات الحديثة: أسيوط مصر. 1994 ص 60.

[4] جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي الاحكام الموضوعية للجرائم المتعلقة بالأنترنت، الطبعة الأولى، دار النهضة العربية، مصر، 2001، ص23.

أما الصورة الثانية والمتعلقة بالاستعمال غير المشروع لنظم المعالجة الآلية للمعلومات فتتجلى هذه الحالة في وضعيتين أو صورتين منها الدخول أو البقاء غير المشروع، ونظام المعالجة الآلية الحالة الثانية هي سرقة منفعة الحاسب الآلي أو المال المعلوماتي[1]، كالدخول إلى نظام الحاسوب والوصول إلى محتوياته أو البقاء فيه بصورة غير مسموح بها ومثال على ذلك العامل المرخص له قانونا للدخول إلى المنظومة المعلوماتية في إطار عمله يقوم وباستعمال رموز الدخول المزيفة للاطلاع على معطيات لا تدخل في نطاق مهامه العادية ومن أمثلة ذلك أيضا قيام فريق مكون من خمسة أشخاص في شيكاغو بالولايات المتحدة الأمريكية يعملون بإحدى المراكز التعليمية باستغلال الحاسب الآلي التابع للمركز البرمجة أعمال عملائهم الخاصة بشركة خاصة أخرى لهم، ومثال أخر أنه تم اكتشاف استخدام الحاسب الآلي في أكبر معامل انتاج الصواريخ النووية وقاعدة FBI بالولايات المتحدة الأمريكية من قبل منتي مستخدم وذلك لأغراضهم الشخصية.[2]

ولم يبق الإجرام الالكتروني منحصرا على المجال المالي فقط بل امتد وبشكل خطير إلى مجالات عديدة كالتحايل المعلوماتي في البرامج والمعطيات، بل أن الجماعات الإجرامية وسعت نشاطها إلى أخطر من ذلك بما فيها تشكيل المجموعات الإرهابية وقد بات واضحا ما لهذه المجموعات من تأثير على الاستقرار المحلي والدولي سيما ضد أصبح يعرف بالحكومات الالكترونية، مما يدفع إلى القول بأن المعالم أضحى أمام حرب جديدة يمكن تسميتها بالحرب المعلوماتية ويتضح من خلال العديد من الاحصائيات مدى جسامة الإضرار التي خلفتها الجرائم الالكترونية فالتقرير الذي نشرته الجمعية الفرنسية لأمن المعلومات عام 1991 يبين بأن الخسائر بلغت 104 مليار فرنك فرنسي، في حين قدرت سنة 1996 بحوالي 12.72 مليار فرنك فرنسي.[3]

أما في الولايات المتحدة الأمريكية فإن احصائيات مكتب التحقيقات الفدرالي أكدت بأن الخسائر المترتبة عن الجريمة الالكترونية تفوق 150 مرة الجريمة العادية.

أما في الجزائر فإن الاحصائيات المتوصل إليها من سنة 2005 إلى 2010 أكدت بأن جرائم الدخول غير المشروع مع اتلاف المعطيات أو تعديلها بلغ عدد 13 بمعدل 34% في حين بلغت نسبة ادخال المعطيات خلسة 21% وبالمقابل كانت المؤسسات المستهدفة 60% بالنسبة للإدارات العمومية والمؤسسات ذات الطابع الصناعي والتجاري وبنسبة 20% للشركات الخاصة ونسبة 11% بالنسبة للشركات الخاصة الاجنبية، وكانت الدوافع المادية تشكل نسبة 65% ودوافع الفضول 15% و التحدي

[1] محمد رمضان بازة، قانون العلويات الليبي جرائم الاعتداء على الأموال بط. القسم الخاص، الجزء الثاني. منشورات جامعة ناصر طرابلس ليبيا 1992 ص 44.

[2] هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012، ص82.

[3] على القهوجي الحماية الجنائية لبرنامج الحاسب الآلي نط الدار الجامعية للنشر: بيروت، 1999، ص 157

05% وعلى العموم فإنه يصعب تقدير حجم الخسائر الناجمة عن الجرائم المعلوماتية كما تشير إليه الأبحاث التي أجريت بشأنها في معظم الدول الغربية، سيما فرنسا والولايات المتحدة الامريكية وانجلترا، كما أصدر المكتب الجنائي الاتحادي في المانيا في السنوات الأخيرة تقريرا يحذر فيه من خطورة استعمال الوسائل المعلوماتية من طرف الارهابيين لأنها أصبحت تشكل أهم وسية لهم[1].

المبحث الثاني: إجراءات تحصيل الدليل الإلكتروني (الاجراءات الإجرائية لاستخلاص الدليل الالكتروني)

باعتبار الدليل الإلكتروني صنف جديد من الأدلة لنوع مستحدث من الجرائم ألا وهو الجريمة الإلكترونية، فإنه يستلزم وجود إجراءات لتحصيله وتكون متلائمة مع طبيعة حداثته.

والأكيد أن التحقيق والبحث للحصول على هذا النوع من الأدلة المتعلق والمرتبط بالتقنية يشترط إجراءات معينة خاصة. ولهذا سنقوم بتناول إجراءات تحصيل الدليل الإلكتروني وسنوضحها في هذا المبحث بعرض مدى سريان إجراءات التحقيق المألوفة على عملية تحصيل الدليل الإلكتروني المطلب الأول ثم الإجراءات المستحدثة في عملية تحصيل الدليل الإلكتروني (المطلب الثاني).

المطلب الأول: إجراءات التحقيق المألوفة (الإجراءات التقليدية للحصول على الدليل الالكتروني)

هناك إجراءات مختلفة تتبع في سبيل الوصول إلى غاية معينة والتي تتمثل في استخراج الدليل في التحقيق الجنائي وأما عن الإجراءات التقليدية نجد التفتيش المعاينة، الضبط، سماع الشهود، وندب الخبراء.[2] وهي إجراءات تستعمل بصفة عامة لهدف الحصول على الدليل سواء في الجرائم التقليدية أو المستحدثة وسوف نتطرق إلى كل هذه الإجراءات ونحاول إبراز كل إجراء ودوره في مجال تحصيل الدليل الإلكتروني.

الفرع الأول: المعاينة والتفتيش في البيئة الإلكترونية

يهدف التفتيش التقليدي إلى جمع الأدلة المادية للكشف عن الجريمة، وبما أن نظم الحاسبات هي عبارة عن كيان معنوي يفتقر للخاصية المادية للأشياء، فهل يمكن تطبيق القواعد العامة التقليدية للتفتيش على نظم المعلوماتية؟[3]

أولا: المعاينة في الجريمة الإلكترونية

تعريف المعاينة: هي إجراء من أهم إجراءات التحقيق فهي ذات أهمية قصوى فيما يخص إثبات الواقعة.

---

[1] عبد الله عبد الكريم عبد الله، مرجع سابق، ص 21.
[2] هلال أمنة، الإثبات الجنائي بالدليل الإلكتروني مذكرة لنيل شهادة الماستر، جامعة محمد خيضر بسكرة، 2014، ص 28.
[3] طرشي نورة مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول علي شهادة الماجستير في القانون الجنائي، جامعة الجزائر، كلية الحقوق، 2012، ص107.

وتعرف المعاينة انه مشاهدة واثبات الحالة في مكان الجريمة أي مشاهدة واثبات الآثار المادية التي خلفها ارتكاب الجريمة ويطلق عليها في العادة إثبات الحالة بمعني إثبات حالة الشخص والأشياء ذات الصلة بالحادث.

وقد عرفها البعض الآخر بأنها إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة.

وتختلف المعاينة في الجريمة الإلكترونية مقارنة بالجريمة التقليدية فإجراء المعاينة التقنية لمسرح الجريمة الإلكترونية يقع إما خارج بيئة الحاسب الآلي وإما داخلها.

1- المعاينة التي تقع خارج بيئة الحاسب الآلي والانترنت

تكون بشكل رئيسي على المكونات لمادية المحسوسة للمكان الذي وقعت فيه الجريمة وهو أقرب ما يكون إلى مسرح أية جريمة تقليدية قد يترك فيها الجاني أثار عدة كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.

2- المعاينة التي تقع علي المسرح الافتراضي

والذي يقع داخل البيئة الإلكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنت وفي دائرة الأقراص الصلبة الموجودة بداخل[1]. ولنجاح المعاينة في الجرائم الإلكترونية وحتى تأتي بثمارها وتفي بأغراضها المنشودة فإنه يوصي ب:

- تصوير الحاسب الآلي ولأجهزة الطرفية المتصلة به على أن يتم تسجيل وقت وتاريخ ومكان التقاط كل الصور.

- إمكانية تلاعب الجاني في البيانات عن بعد أو محوها عن طريق التدخل من خلال التدخل من خلال وحدة طرفية. لذلك ينبغي على المشرع أن يقرر إجراءات جنائية على كل من يقوم بإجراء أو تغيير أو تعديل في المعلومات المسجلة في ذاكرة الحاسب أو وسائط التخزين أو في بنك المعلومات أو قاعدة البيانات قبل قيام سلطة التحقيق بإجراء المعاينة وهذا ما أقر به المشرع الجزائري في المادة 43 من قانون الإجراءات الجزائية حرصا على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي بنصها علي أنه: " يخطر في مكان ارتكاب جناية علي كل شخص لا صفة له، أن يقوم بإجراء أي

[1] زروقي فايزة، زيرام سوميه المرجع السابق، ص 42.

تغيير علي حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيئي منها قبل الإجراءات الأولية لتحقيق القضائي وإلا عوقب بغرامة من 100 الي 1000دج".[1]

- عدم نقل أي مادة معلوماتية من مسرح الجريمة قبل إجراء الاختبارات التأكد من المحيط الخارجي لموقع الحاسب الآلي مجال لقوي مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

- إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كافي حتى يستعد من الناحية الفنية والعلمية وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معينتها.

- التحفظ على معلومات سلة المهملات من الأوراق والملفات الممزقة وأوراق الكربون المستعملة، والشرائط والأقراص الممغنطة السليمة، وفحصها وترفع من عليها البصمات ذات الصلة بالجريمة.

كل الإجراءات السالفة الذكر يجب أن تتم بالمشروعية أي وفق ما ينص عليه القانون الجنائي، وقصر هذه الإجراءات على المحققين الذين لديهم كفاءة وجيزة في مجال التكنولوجيا الحديثة والذين تلق التدريب الخاص لمواجهة هذا النوع من الجرائم.

ثانيا: التفتيش

1- تعريف التفتيش: لا يختلف المدلول القانوني للإجراء التفتيش في البيئة الإلكترونية عن المدلول التقليدي السائد في قانون الإجراءات الجزائية رغم اختلاف المحل الذي يقع عليه التفتيش.

ويعرف التفتيش بأنه: إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية الجناية أو جنحة تحقق وقوعها في محل يتمتع بحرمة المسكن أو الشخص وذلك بهدف إثبات ارتكابها أو نسبتها إلى المتهم وفقا لإجراءات قانونية محددة[2].

وبالنسبة للمشرع الجزائري لم يعط تعريفا دقيقا وخاصا للتفتيش بقدر ما اعتبره إجراء من إجراءات التحقيق وأحاطه بضوابط صارمة نضرا لأهميته في كشف الأدلة وخطورته، فيما قد يترتب عنه من مساس بحرية الأشخاص وبكرامتهم ومما يؤكد ذلك اهتمام الدستور الجزائري 1996 المعدل بموجب القانون رقم 01/16 المؤرخ في 06 مارس سنة 2016، بهذه النقطة وذلك في المادة 40 منه التي تنص على: فلا تفتيش إلا بمقتضي القانون وفي إطار احترامه ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة ... كما نجد المادة 64 من ق إ ج ج تنص على ما يلي: لا يجوز تفتيش المساكن ومعاينتها

[1] قانون رقم 66-155، سابق الذكر.
[2] هلال امنة، مرجع سابق الذكر، ص 32.

وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات تقابلها المادة 47 من دستور (2016).

ويمكن تعريف التفتيش في نظم الحاسوب والانترنت أنه "البحث في مستودع سر المتهم عن أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبتها إليه".

كما يعرف أيضا أنه" الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو أنظمة أو الانترنت[1].

يتضح لنا من التعريفات السابقة أن التفتيش ما هو إلا وسيلة للإثبات المادي وذلك لأنه يستهدف ضبط أشياء مادية تتعلق بالجريمة أو تفيد في كشف الحقيقة، والهدف منه دائما هو الحصول على الدليل المادي، وهو ما يتعارض مع الطبيعة غير المادية للبيانات والمعطيات المخزنة بالحاسب الألي وكذلك شبكة الانترنت فهي مجرد بيانات الكترونية ليس لها أي مظهر مادي محسوس في العالم الخارجي.

2- أهمية التفتيش

التفتيش من أخطر الإجراءات الجنائية التي تمس حريات الناس، فهو بحث في مستودع أسرارهم التي يحرصون على الاحتفاظ بها لأنفسهم، واعتداء على حرياتهم في صون أسرار مساكنهم وأشخاصهم، ولذلك حرصت الدساتير على رفع بعض أحكام التفتيش إلى مصاف المبادئ الدستورية، خاصة بعد الإعلان العالمي لحقوق الإنسان في مادته الثانية عشر بنصها على لا يتعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أن مراسلاته أو الحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات.

3- خصائص التفتيش

ما يميز التفتيش هنا أنه تعرض قانوني لحرية المتهم الشخصية ولأسراره الموجودة في جهاز الحاسوب، كما انه يمتاز بأنه وسيلة للبحث عن الأدلة المادية والمعنوية.

حيث قررت المادة 81 من ق إ ج ج على أنه " انه يجري التفتيش في جميع الأماكن التي من شأنها أن تكون مفيدة، ويمكن الحصول منها على أشياء يكون كشفها مفيدا لإظهار الحقيقة، أي جميع الأماكن التي يرجح توفرها على دليل إثبات ما عن حقيقة الجريمة والمجرم الإلكتروني."[2]

[1] زبيحة زيدان، مرجع سابق الذكر، ص 130.
[2] انظر المادة 81 من قانون 6-155 مؤرخ في 08 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية معدل ومتمم بالأمر رقم 11-02 مؤرخ في 23 فبراير 2011.

فالمشرع الجزائري كان واضحا في هذه المادة إذ أجاز التفتيش في أي مكان من شأنه إظهار الحقيقة للسير في القضية ولم يخصص أمكنة معينة للتفتيش وبالنظر إلى هذه المادة فإنه يجوز التفتيش في مكونات وشبكات الحاسوب، حتى إن كان فيه اطلاع على الأمور الشخصية وهذا بهدف الوصول إلى الحقيقة المنشودة.

4- الضوابط التي تحكم إجراء التفتيش

يجب أن يتم التفتيش وفقا لضوابط قانونية والتي وضعها المشرع الإجرائي، وفي حالة الخروج عن الضوابط كان إجراء التفتيش باطلا وتتمثل في الضوابط الموضوعية والضوابط الشكلية.[1]

1- ضوابط موضوعية: السبب، المحل، السلطة المختصة بالقيام بالتفتيش.

أ- سبب التفتيش في البيئة الإلكترونية

سبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل من أجل الحصول إلى الحقيقة، ويتمثل في وقوع جريمة ما جناية أو جنحة واتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها، وتوافر قرائن وأمارات قوية على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو في مسكنه، وهو ما ينطبق على الجريمة الإلكترونية على النحو التالي:

- وقوع جريمة من الجرائم الإلكترونية بالفعل سواء كانت جناية أو جنحة

وتطبيقا لمبدأ شرعية الجرائم والعقوبات، فلا محل لإصدار الإذن بتفتيش نظم الحاسوب إلا إذا كان المشرع قد نص صراحة على الأفعال التي تشكل جرائم من هذا النوع، وذلك ما فعلته الكثير من التشريعات المقارنة وفعله المشرع الجزائري من خلال القانون رقم 05-15 المؤرخ في 10 نوفمبر 2004 حيث أدرج المشرع الجزائري فصلا خاصا -الفصل السابع- بجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

- اتهام شخص أو عدة أشخاص معنيين بارتكاب الجريمة أو المشاركة فيها:

ينبغي أن تتوافر في حق الشخص المراد تفتيش شخصه أو مسكنه دلائل كافية تدعوا للاعتقاد بأنه قد ساهم في ارتكاب الجريمة الإلكترونية أو شريكا فيها.[2]

أما الدلائل الكافية في الجرائم الإلكترونية، يقصد بها "مجموعة الظواهر أو الأمارات المعينة القائمة على العقل والمنطق والخبرة الفنية والحرفية للقائم بالتفتيش والتي تؤكد نسبة الجريمة الإلكترونية إلى

[1] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني لحماية المعلومات، دار الجامعة الجديدة للنشر الإسكندرية، د ت ن، ص 371
[2] طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 372.

شخص معين بوصفه فاعلا أو شريكا"، ومن أمثلتها: ارتباط عنوان انترنت[1]، البروتوكول الخاص بجهاز الحاسوب الذي يحتوي على صور فاضحة مع رقم حساب المتهم لدى مزود الخدمات، ووجود رقمين للتلفون لديه يستخدمان في ذلك.[2]

ب- محل التفتيش:

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء المادية التي تتضمن سره، والسر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة كالمسكن أو الشخص والرسائل ومحل التفتيش في الجريمة الإلكترونية هو الحاسوب والشبكة التي تشمل في مكوناتها الخادم والمزود الآلي والمصنف والملحقات التقنية.[3]

الفرع الأول: القيام بالتفتيش في الكيانات المادية والمعنوية للحاسوب وما يرتبط به

يشرع في إجراء عملية التفتيش الالكتروني في نظام المعالجة الألية للجرائم الالكتروني بغية جمع الادلة الالكترونية في الأجهزة المرتكبة عليها الجريمة أو بواسطتها تلك الأجهزة المتصلة بالحاسب الألي وشبكة الانترنت التي تشمل في مكوناتها مقدم الخدمة والمزود الألي والمضيف والملحقات التقنية وأيضا الهاتف النقال ، فالولوج في المكونات المادية للحاسب الألي بحثا عن دليل ما يتصل بالجريمة يفيد في كشف الحقيقة و عن مرتكبها ، فالمواد التي أسندها الجاني إلى المجني عليه قد تكون محفوظة في القرص الصلب وبالتالي فحص هذا الأخير قد يؤدي إلى ضبط أدلة تدين الفاعل[4]، و يثور السؤال عن مدى خضوع المكونات المادية والمعنوبة للحاسب الألي والشبكات المرتبطة به وقابلتها للتفتيش ؟

1- مدى خضوع مكونات الحاسب الالكتروني المادية للتفتيش : لا يختلف اثنان في أن الولوج إلى المكونات المادية للحاسب الالكتروني بحثا عن دليل يتصل بالجريمة ، ومنه يخضع تفتيش الكومبيوتر إلى أحكام تفتيش المكان الذي يوجد به ذلك الجهاز ، فإذا كان الكومبيوتر مودعا في مكان خاص ، كمسكن المتهم أو أحد ملحقاته فتأخذ حكم المسكن ، فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكن المتهم ، وبذات الضمانات المقررة قانونا في التشريعات المختلفة ، أما إذا كانت تلك النهايات مرتبطة في مكان أخر وتطلبت دواعي التفتيش الوصول إليها وتفتيشها ، فإنه يجب مراعاة الشروط التي يتطلبها المشرع لتفتيش تلك الأماكن[5]

[1] طارق إبراهيم الدسوقي عطية، مرجع سابق، ص 37.
[2] أشرف عبد القادر قنديل، ص 172.
[3] أشرف عبد القادر قنديل، ص 150.
[4] د، عادل عزام سقف الحيط، المرجع السابق، ص 244.
[5] تومي يحي، جرائم الاعتداء ضد الافراد باستخدام تكنولوجيا الاعلام والاتصال، أطروحة دكتوراه، جامعة الجزائر 1، 2018، الجزائر ص 193.

2- مدى خضوع مكونات الحاسب الالكتروني المعنوية للتفتيش

لقد أثار تفتيش المكونات المعنوية للحاسب الآلي خلافا كبيرا في الفقه بخصوص تفتيشها من عدمه، حيث ذهب رأي إلى جواز تفتيش البيانات الالكترونية بمختلف أشكالها، لأن الغاية من التفتيش هي ضبط الأدلة المادية التي تفيد في كشف الحقيقة، وفي هذا المعني نجد المادة 251 من قانون الاجراءات الجنائية اليوناني تعطي سلطات التحقيق إمكانية القيام " بأي شيء يكون ضروريا لجمع الدليل وحمايته " حيث يفسر الفقه اليوناني عبارة أي شيء بأنها تشمل البيانات المخزنة أو المعالجة إلكترونيا وعليه ضبط المعطيات الالكترونية بمختلف صورها المخزنة في الذاكرة الداخلية للحاسب الالكتروني لا تشكل أية مشكلة في اليونان إذ بمقدور المحقق أن يعطي أمرا للخبير بجمع البيانات التي يمكن أن تكون مقبولة كدليل في اثبات الجريمة[1]، أما بالنسبة لأصحاب الرأي الثاني يرون بعدم انطباق المفهوم المادي على بيانات الحاسب الألي غير المرئية أو غير الملموسة ويقترح أصحاب هذا الرأي مواجهة هذا القصور التشريعي بإضافة عبارة إلى القوانين ذات العلاقة وإلى مذكرات التفتيش مثل المواد المعالجة عن طريق الحاسوب الالكتروني أو بياناته[2]وعليه يمكننا القول أن البيانات والمعلومات المخزنة في الحاسب الالكتروني تصلح لأن تكون محلا للتفتيش يمكن ضبطها واستنساخها على الورق أو على أية دعامة الكترونية .

3- مدى خضوع شبكات الحاسب الالكتروني للتفتيش

شبكات الحاسب الالكتروني عبارة عن مجموعة مكونة من عدة أجهزة (الحاسب الألي) والمتصلة ببعضها البعض أتصالا سلكيا أو لا سلكيا بحيث توجد شبكات واسعة في أماكن متفرقة مرتبطة ببعضها البعض عن طريق الهاتف[3]. غير أن الطبيعة التقنية الرقمية قد زادت من الصعوبات التي تواجه القائمين على التفتيش والضبط في الجرائم المرتكبة عن طريق الأنترنت، فالبيانات التي تحوي أدلة قد تتوزع على شبكات الحاسب الألي في أماكن مختلفة بعيدة عن الموقع المادي الذي يتم فيه التفتيش هذا من ناحية ومن ناحية أخرى قد يكون الموقع الفعلي للبيانات والمعلومات يدخل ضمن الاختصاص القضائي لدولة أخرى مما يعيق التحقيق والوصول إلى الدليل[4].

وبعد معرفتنا لمدى قابلية الكيانات المادية والمعنوية للحاسب الالكتروني والشبكات المتصلة به للتفتيش ورأي الفقه المقارن في ذلك، نتعرض إلى تفتيش الكيانات المادية والمعنوية للحاسب الالكتروني على النحو الاتي.

---

[1] د هلالي عبد الاله، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة 1997، ص 27. نقلا عن على عدلان الفيل، المرجع السابق، ص 460.

[2] د أسامة بن غانم العبيدي، المرجع السابق، ص 90. .

[3] د أسامة بن غانم العبيدي، المرجع السابق، ص 90.

[4] د، أسامة بن غانم العبيدي، المرجع السابق، ص 91.

أولا: تفتيش المكونات المادية لنظام المعالجة الألية والمعنوية المتصلة به

إن التفتيش الذي يقع على المكونات المادية لنظام المعالجة الألية لا توجد فيه أي مشكلة في التنفيذ لسهولة ذلك ، مع الأخذ بعين الاعتبار الاجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وامكانية اتلافها، ومرد هذه السهولة في التفتيش كونه يرد على أشياء مادية لا خلاف حول خضوعها للتفتيش طبقا لقواعد قانون الاجراءات الجزائية ، وتفتيش الأجهزة التي استخدمت في ارتكاب الجريمة(الحاسب الألي) والموجودة بمسكن المشتبه فيه تخضع إلى شروط تفتيش المساكن المنصوص عليها قانونا كالحصول على إذن مسبق من وكيل الجمهورية المختص وقد نصت المادة 64 من نفس القانون التي نصت على أنه " لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الاجراءات.."

والتفتيش في أنظمة الحاسوب وشبكة الانترنت يختلف عن التفتيش العادي، بحيث تخضع المكونات المادية للحاسب الألي للتفتيش قصد البحث عن الشيء المتعلق بالجريمة وجمع الأدلة التي تثبت وقوع الفعل الجرمي للإجراءات القانونية الخاصة بالتفتيش[1]، غير أنه جواز تفتيش المكونات المادية يتوقف على طبيعة المكان الموجودة فيه هل هو مكان عام أم مكان خاص؟ إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت خاصة كمسكن المتهم أو أحد ملحقاته كانت لها حكمه فلا يجوز تفتيشها إلا بنفس الشروط المقررة قانونا لتفتيش المساكن والأماكن التي لها حرمة خاصة[2]، غير أن المشرع الجزائري قد استثنى تطبيق هذه الشروط عند اجراء التفتيش بمناسبة تحقيق بخصوص الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ،وذلك من خلال التعديل الذي ألحقه على قانون الاجراءات الجزائية بالقانون رقم 22/06 المؤرخ في 20 /2006/12 حيث ورد هذا الاستثناء في المادة 45 الفقرة الأخيرة وفي الفقرة الثالثة والرابعة من المادة 47 والفقرة الثالثة من المادة 64[3].

ويستخلص من قراءة هذه المواد أن المشرع الجزائري لا يشترط حضور الشخص الذي يشتبه في ارتكابه للجريمة عند تفتيش مسكنه، بل يجوز القيام بإجراء التفتيش في كل ساعة من ساعات النهار أو الليل[4] وبهذا يكون المشرع قد غلب المصلحة العامة على حريات الأفراد وذلك يرجع لاعتبارين :

- الخوف من امكانية اختفاء الجريمة بسرعة وذلك بمحو أدلتها أو اخفائها.

---

[1] تومي يحي، المرجع السابق، ص 194.

[2] تنص المادة 64 الفقرة الأولى من ق ا ج ج على أنه "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الاجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه ويذكر ذلك في المحضر مع الاشارة صراحة إلى رضاه".

[3] أنظر المادة 45 الفقرة الأخيرة، وأيضا المادة 47 الفقرة 2، وأيضا المادة 64 الفقرة 3 من قانون الاجراءات الجزائية.

[4] أنظر الفقرة الثالثة من المادة 47 من قانون الاجراءات الجزائية.

- أهمية الدليل الرقمي كونه الدليل الوحيد في الدعوى العمومية ومن ثم الارتكاز عليه والتعويل عليه في الاثبات. ومن جملة المكونات المادية والمعنوية وشبكات الانترنت التي يتم فحصها للحصول على الدليل الرقمي هي:

1- فحص القرص الصلب : يحتوي القرص بداخله مجموعة من البيانات الرقمية ذات الطابع الثنائي بحيث يكون الموظف المختص، أو الخبير المختص أمام إجراءين إما الفحص الكلي أو الجزئي على القرص الصلب وذلك من أجل معرفة محتوى البيانات ثنائية الرقم التي يؤدي التعامل معها على الكشف عن القيمة الاسترادادية للبيانات المخزنة في القرص سواء أكانت مكتوبة أو على هيئة صور أو أصوات[1]، ومن خلال استخدام برمجيات متخصصة في فحص القرص الصلب والتي تمكن المفتش من استعراض كافة صفحات الانترنت التي تم تصفحها حتى تاريخ قد يصل إلى ستة أشهر وكل الملفات التي قام مستخدم الجهاز بتنزيلها وغيرها من الملفات، وما تم حذفه من بيانات سواء كانت بيانات مكتوبة أو عبارة عن صور أو أصوات ..الخ[2].

2- فحص البرمجيات والنظام المعلوماتي

إن امتداد التفتيش إلى مكونات غير مادية محل جدل لدى الفقه حول مدى صلاحيتها لأن تكون موضوعا للتفتيش كون الخلاف الواقع يدور حول مسألة أن التفتيش التحقيقي وسيلة للبحث عن الأدلة المادية، وهو إجراء يسعى إلى ضبط الأدلة المتعلقة بالجريمة لتقديمها إلى المحكمة كدليل إدانة، غير أنه يثور تساؤل حول مدى امكانية اعتبار البحث عن أدلة الجريمة المرتكبة باستخدام تقنية المعلومات ووسائل الاتصال نوعا من التفتيش باعتبار أن البيانات الالكترونية أو البرامج ليس لها مظهر مادي محسوس في العالم الخارجي، ويستشعر الفقه صعوبة المسألة نظرا لغياب الطبيعة المادية للمعلومات في ذاتها مجردة من دعامتها المادية، وهناك اتجاهين للفقه بالنسبة لهذا الأمر هما:

الاتجاه الأول: يرى بعدم امكانية انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة وأحكام التفتيش في القانون الجنائي الاجرائي مع ما يتطلبه كشف الحقيقة في جرائم القذف والسب والتهديد المرتكبة عبر الانترنت من خلال المواقع الالكترونية ومواقع التواصل الاجتماعي فيها من بحث وتحري عن الأدلة الاثباتية الرقمية[3].

الاتجاه الثاني: يرى أصحاب هذا الاتجاه أن برامج الحاسوب يمكن أن تنطبق عليها سمات المادة وخصائصها وبالتالي تدخل في نطاق الأشياء المادية ويستوي في ذلك أن تكون برامج نظام أو برامج

[1] ممدوح خالد ابراهيم، المرجع السابق، ص 247.
[2] بن يونس عمر محمد أبو بكر، المرجع السابق، ص 101.
[3] تومي يحي، المرجع السابق، ص 196.

تطبيقات[1]، والتدليل على ذلك أن المادة هي كل ما يشغل حيزا ماديا في فراغ معين وأن هذا الحيز يمكن قياسه والتحكم فيه.

ويظهر لنا موقف المشرع الجزائري من إجراء التفتيش في الجرائم الالكترونية، وذلك من خلال القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها حين وضع الفصل الثالث منه تحت عنوان " القواعد الاجرائية " تفتيش المنظومات المعلوماتية من خلال ما جاءت به المواد 5 و6 و7 و8 و9 من القانون السالف الذكر، حيث أشارت المادة 5 منه على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في اطار قانون الاجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى منظومة معلوماتية..."[2] وفي هذا السياق دعت الاتفاقية الأوربية[3] في شأن جرائم تقنية المعلومات والمعطيات المعلوماتية المخزنة فيها بحق الدول الأعضاء في تفتيش النظم في إطار الاجراءات الجزائية أشارت المادة 19 منها، أن لكل دولة طرف الحق في سن القوانين التي تراها ضرورية من أجل تمكين السلطة المختصة بالتفتيش في نظام الحاسب الالكتروني، أو في الوسائط التي يتم تخزين معلومات الحاسوب بها ما دامت مخزنة في اقليمها[4].

أما التفتيش في ذاكرة التخزين يكون عن طريق فحص نظام الحاسوب من طرف عنصر الأمن المختص بالتفتيش أثناء الولوج عبر العالم الافتراضي، بحيث يمكنه ذلك من معرفة مواقع الانترنت التي زارها المعتدي فترات طويلة تصل إلى ستة أشهر حتى وإن قام الجاني بحذف كافة الملفات التي قام نظام التشغيل بتخزينها فيمكن للمحققين المختصين استخدام برمجيات معينة تمكنهم من استعادة كل الملفات المحذوفة.

هذا من جهة ومن جهة أخرى فإن فحص نظام الاتصال بالأنترنت، إذ يبدأ التفتيش بفحص مسار الانترنت كخطوة أولى بواسطة بروتوكول الأنترنت IP.Address هو الأخر يمكن سلطة التحقيق من تحديد حائز هذا البروتوكول.

ثانيا: تفتيش البريد الالكتروني

لقد صدر القانون الفرنسي رقم 575 الصادر عام 2004 المتعلق بشأن الثقة في الاقتصاد الرقمي حيث عرف البريد الالكتروني في المادة الأولى منه بأنه: "كل رسالة سواء كانت نصية أو صوتية أو مرفق

[1] هلالي عبد الاله أحمد، المرجع السابق، ص 75.
[2] تومي يحي، المرجع السابق، ص 198.
[3] الاتفاقية الأوروبية المتعلقة الجريمة الالكترونية، بودابست المجر 2001/11/13، ودخلت هذه الاتفاقية المتعددة الأطراف إلى حيز التنفيذ في يوليو سنة 2004، حيث شكلت أول محاولة قانونية لمعالجة مشكلة تزايد الجرائم السيبرالية كان الهدف الرئيس من تنظيم هذه الاتفاقية هو وضع سياسة جزائية مشتركة لمكافحة الجرائم الافتراضية، للمزيد من التفصيل أنظر د/ عادل عزام سقف الحيط، المرجع السابق، ص 365.
[4] أنظر المادة 19 من الاتفاقية الأوربية المتعلقة بالجريمة الالكترونية بودابست، المجر في 2001/11/23.

بها صور أو أصوات ويتم ارسالها عبر شبكة اتصالات عامة وتخزن عند أحد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها".[1]

وتتم عملية ضبط البريد الالكتروني من طرف المحقق وعنصر الأمن المختص باتباع خطوات معينة مع مراعاة أحكام التفتيش وضبط الأشياء المنصوص عليها في قانون الاجراءات الجزائية ، ، ويشرع في البحث عن الدليل متفحصا جميع الرسائل الموجودة فيه .كما يقوم بالنسخ على دعامة الكترونية ، حيث أشارت المادة 6 من قانون رقم 09-04 على كيفية حجز وضبط المعطيات المخزنة عندما تكون مفيدة في الكشف عن الجرائم ومرتكبيها[2]، بحيث يتم نسخ المعطيات محل البحث على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفق القواعد المقررة في قانون الاجراءات الجزائية وتوضع في كيس يضع عليه ضابط الشرطة القضائية شريطا من ورق ويختم عليه بختمه[3] بعد كتابة ساعة و تاريخ ومكان ضبطها والقائم بالضبط ورقم محضر الواقعة، تودع بعد قيدها في سجل خاص مخزن المضبوطات ضمانا لسلامتها وعدم العبث بها.

ثالثا: تمديد التفتيش للشبكات المعلوماتية الموصولة بالحاسوب " التفتيش عن بعد "

تثير طبيعة النظم المعلوماتية وشبكة الانترنت التحدي أمام أعمال الشرطة القضائية المختصة في التفتيش الالكتروني، فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة وبعيدة تماما عن الموقع المادي للتفتيش حتى وإن ظل من الممكن الوصول إليها من خلال حواسيب تقع في الأبنية الجاري تفتيشها[4]، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي أخر أو حتى في بلد أخر، غير أن السلطات في ذلك الاختصاص السيادي قد تشعر ببالغ الانزعاج مما يزيد في تعقيد الأمر الذي يزيد من مشاكل الجريمة المرتكبة عبر الشبكة المعلوماتية العابرة للحدود .

وقد أجاز المشرع الجزائري من خلال المادة 5 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها على أنه " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الاجراءات الجزائية وفي الحالات المنصوص عليها بغرض التفتيش ولو عن بعد: إلى منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها، منظومة تخزين معلوماتية.

ودائما في هذا السياق نجد المادة 5 الفقرة الثالثة من القانون السالف الذكر في حالة تخزين المعلومات خارج الاقليم الوطني فقد نصت على أنه: "إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي

---

[1] تومي يحي، المرجع السابق، ص 199.
[2] تومي يحي، المرجع السابق، ص 199.
[3] أنظر المادة 45/ ف 5 من قانون الاجراءات الجزائية.
[4] عبد الله بن عبد العزيز بن عبد الله الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض 2011، ص 38.

يمكن الدخول إليها انطلاقا من المنظومة الأولى مخزنة في منظومة معلوماتية تقع خارج الاقليم الوطني فإن الحصول عليها يكون بمساعدة السلطات الأجنبية".

ثالثا: ضبط الأشياء وتحرير محضر تفتيش

إضافة إلى الضمانات المتعلقة بالميقات الزمني للتفتيش والأشخاص المطلوب حضورهم يشترط كذلك أن يحرر محضر بالتفتيش تدون فيه كل الخطوات والإجراءات المتخذة أثناء عملية التفتيش وما أسفر عنها من أدلة لكي يكون حجة على الجميع.

ولا يستوجب القانون شكلا أو شروطا خاصة في محضر التفتيش، بل يكفي أن يتوفر فيه ما تستوجبه القواعد العامة في المحاضر عموما، كالكتابة باللغة الرسمية، تاريخ تحريره توقيع محرره، ويتضمن كافة إجراءات التفتيش.[1]

ومن الشروط الجوهرية التي ينبغي مراعاتها في محضر التفتيش، وجوب استعانة المحقق بكاتب يتم اصطحابه لتحرير المحضر و تدوين ما تم من إجراءات و التأشير عليه تحت طائلة البطلان، وهو ما نصت عليه المادة (2/68) قانون الإجراءات الجزائية الجزائري وتحرر نسخة من هذه الإجراءات وجميع الأوراق ويؤشر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة بمطابقتها للأصل"، وأكدت عليه المادة (79) من القانون نفسه بنصها على " يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو القيام بتفتيشها ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات".[2]

ولا يختلف محضر التفتيش في مجال الجرائم الالكترونية عن غيره في الجرائم التقليدية سوى انه بالإضافة إلى الشكليات السابقة لابد من إحاطة القائم بالتفتيش في الجرائم الالكترونية بتقنية المعلوماتية الرقمية، أو استعانته بأهل الخبر الفنية والاختصاص في هذا المجال ليساعده في صياغة وتحرير محضر يغطي كل الجوانب الفنية للتفتيش.

وأشير إلى انه بالإضافة إلى شرط تحرير محضر التفتيش حرصت معظم الدول على تضمين تشريعاتها الإجرائية نصوص تمنع فيها الاطلاع أثناء التفتيش على الأشياء والأوراق المختومة التي تمس الأسرار الشخصية للعائلة، وتفرض على القائم بالتفتيش اتخاذ الاحتياطات الضرورية لتفادي انكشاف مثل هذه الأسرار.

[1] فايز محمد راجح غلاب، مرجع سابق، ص 338
[2] أنظر الفقرة 2 من المادة (68) والمادة (79) من ق.ا.ج. ج)، مرجع سابق.

وقد نص القانون الجزائري على هذه الضمانة في المادة (84 من ق إ ج) على الشكل التالي: " إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فإن لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الاطلاع عليها قبل ضبطها مع مراعاة ما تقتضيه ضرورات التحقيق وما توجبه المادة (3/83 ق إ ج). ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة ولا يجوز فتح هذه الأحراز والوثائق إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا..."[1]

وأعتقد أن هذا القيد المتعلق بعدم جواز الاطلاع على الأشياء والأوراق المختومة أثناء التفتيش يمكن تطبيقه على محتوى أنظمة المعالجة الآلية للبيانات المشفرة والمحمية فنيا ضد الاطلاع غير المرخص لان العلة من تقرير هذا القيد بالنسبة للأوراق المختومة هي نفسها بالنسبة لبيانات أنظمة المعالجة الآلية المشفرة، ألا وهي المحافظة على الأسرار الخاصة بالشخص المراد تفتيشه، فكما يضفي الختم والتغليف والتحريز على تلك الأوراق مزيدا من السرية والحماية فكذلك التشفير يضفي السرية على البيانات وبرامج المعالجة آليا.

الفرع الثاني: الخبرة والضبط في الجريمة الإلكترونية

أولا- الخبرة التقنية في الجريمة الإلكترونية

تعرف بأنها مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرها إلى معرفة فنية أو علمية لا تتوفر لديه فهي بحث في المسائل المادية أو الفنية التي يصعب علي المحقق أن يشق طريقه فيها ويعجز عن جمع الأدلة بالنسبة لها بالوسائل الأخرى للإثبات[2].

ويتم انجاز الخبرات من طرف مخابر الشرطة العلمية التابعة للأمن الوطني وكذا المعهد الوطني للأدلة الجنائية وعلم الإجرام التابعة للدرك الوطني، إلى جانب خبراء الإعلام الآلي التابعين للمجالس القضائية المغيرين في الجداول، واستثناء يجوز تعيين خبير غير مقيد في الجدول بموجب قرار مسبب من قاضي التحقيق وهذا في حالة وجود خبراء.

كما تنص المادة 14 من القانون رقم 04-09 على تقديم المساعدة للسلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز خبرات قضائية التي تتولها الهيئة الوطنية للوقاية من الجرائم المتصلة

[1] أنظر المادتين (83/3 و84) من قانون الإجراءات الجزائية الجزائري، مرجع سابق.
[2] هلال امنة، مرجع سابق الذكر، ص 54.

بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز خبرات قضائية التي تتولها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها المنشأة بموجب هذا القانون والتي نصت عليها المادة 13.

ومن الأمثلة التي يحتاج فيها التحقيق ليندب الخبير، الجرائم الآتية:

- ✓ تزوير المستندات المخلة في أنظمة الحاسبات الآلية أو الناتجة بعد المعالجة.
- ✓ التلاعب في البيانات.
- ✓ التلاعب في البرامج الأساسية أو برامج التطبيقات.
- ✓ الغش أثناء نقل وبث البيانات.

الشروط الواجب توفرها في الخبير

من الشروط الواجب توفرها في الخبير التقني ما يلي:

- الإلمام بالمكونات المادية والبرمجية للحاسب الآلي.

- الإلمام بوسائل وبرامج وطرق فحص نظم الحاسب الآلي كبرامج كشف وإزالة الفيروسات.

- استرجع البيانات والمعلومات فك الشفرات وكلمات السر.

- الإلمام بوسائل وبرامج نسخ البرامج والملفات وعمل نسخ من القرص الصلب.

- الإلمام بكيفية الربط بين الدليل المادي والكليل الرقمي في الوقائع محل البحث[1].

القواعد الفنية التي تحكم عمل الخبير

يقتضي عمل الخبير التقني في سبيل البحث والتحري بخصوص عن الأدلة الرقمية في الجرائم الالكترونية وغيرها من الجرائم المرتكبة عن طريق تكنولوجيات الاعلام والاتصال بحيث تعد عملية تجميع الأدلة الرقمية من أصعب الأمور التي تواجه الخبير الفني، لكن قبل الحديث عن الأساليب التي يستخدمها لا بد من ذكر الصفات الواجب توافرها بالخبير المعلوماتي وهي على النحو التالي:

- الإلمام بتركيب الحاسوب ونظم تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به بالإضافة إلى كلمات المرور ورموز التشفير.

- القدرة على أداء المهام دون أن يترتب على ذلك عطب أو تدمير الأدلة المتحصلة من الرسائل الالكترونية

[1] زروقي فايزة، زيرام سومية، المرجع السابق، ص 50.

- الادراك والدراية بطبيعة البيئة التي يعمل في ظلها الحاسوب المتصل بشبكة الانترنت وكيفية المعالجة الألية وتحديد أماكن التخزين والوسائل المستخدمة في ذلك.

- الالمام بعملية التحقيق الفني الجنائي من رسائل ارتكاب الجرائم ومحاولة إخفاء الأدلة وطرق البحث للوصول إلى الجاني[1].

- التمكن من نقل أدلة الاثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعامتها لحين القيام بأعمال الخبرة دون أن يلحقها تدمير أو إتلاف.

- معرفته لوسائل وطرق فحص نظام الحاسب الآلي كبرامج كشف وإزالة الفيروسات وبرامج استرجاع البيانات والمعلومات وإصلاح المتلف وإظهار المخفي منها[2].وأن يكون مالكا للأدوات الاحترافية من برامج وأجهزة تمكنه من أداء عمله.

ومن الأمور التي قد يقوم بها الخبراء للبحث عن الدليل الرقمي هو الدخول إلى الموقع الالكتروني الذي حدثت فيه الجريمة ويتعرفون عن البقعة الجغرافية التي يبث منها الموقع وذلك من خلال مواقع تقنية متخصصة موجودة على الشبكة تعطي هذه المعلومات عن الموقع والشركة التقنية المشرفة عليه[3]، والخبير يتبع أساليب فنية أثناء القيام بعملة لاكتشاف الدليل الالكتروني.

الفرع الثالث: الوسائل الفنية المستخدمة من قبل الخبير للحصول على الدليل الالكتروني

إن من بين وسائل الخبير في اكتشاف الدليل الالكتروني هناك العديد من هذه الوسائل التي يستعين بها الخبير أثناء تعامله مع الأدلة من أجل الوصول إلى كشف الحقيقة وضبط الدليل الالكتروني والتوصل إلى المجرم، غالبا ما تكون هذه الأدوات الفنية التي تستخدم في بيئة تقنية المعلومات ووسائل الاتصال، والتي يتم استخدامها في تنفيذ اجراءات التحقيق المختلفة في اثبات ونذكر منها على سبيل المثال:

أ- بروتوكول الانترنتIP[4]: يرى خبراء الاتصالات الرقمية أن عنوان الانترنت هو المسؤول عن تراسل حزم البيانات عبر شبكة المعلومات العالمية و توجيهها إلى أهدافها وبالتالي فهو موجود بكل جهاز مرتبط

---

[1] خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، ط1 ،الاسكندرية 2010، ص 288 .

[2] فالخبرة في الجرائم المعلوماتية تساعد في مسائل عديدة منها، منها الكشف عن الدليل، اصلاح الدليل وإعادة تجميعه و عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل وجمع الأثار المعلوماتية الرقمية Cyber trail digital التي قد تكون تبدلت خلال الشبكة المعلوماتية، وكذلك استخدام الخوارزميات للتأكد من أن الدليل لم يتم العبث به أو تعديله . أنظر خالد ممدوح ابراهيم، المرجع السابق، ص 302 تابع... ص 176

[3] ابراهيم طه الزايد، نطاق المسؤولية الجزائية عن جرائم الذم والقدح والتحقير المرتكبة من خلال المواقع الالكترونية، مذكرة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2011، ص 101.

[4] عنوان بروتوكول الإنترنت (Internet Protocol)، وهو عنوان رقمي منطقي يتم تعيينه لكل كمبيوتر، أو طابعة، أو محول، أو جهاز توجيه، أو أي جهاز آخر يشكل جزءاً من شبكة TCP / IP، ويُعد عنوان IP المكون الأساسي الذي بنيت عليه بنية الشبكات؛ حيث لا توجد شبكة إنترنت دون عنوان IP، هو عنوان يُستخدم لتعريف كل عقدة في الشبكة بشكل فريد، ويربط شبكة الإنترنت العالمية ببعضها البعض.مراد الشوابكة ،ماذا تعنيIP مقال منشور على الموقعhttps://mawdoo3.com/%D9%85% تم الاطلاع عليه يوم 2023/5/22 الساعة 10 و30 د.

بالأنترنت[1]، وبالتالي أول ما يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بارتكاب الجريمة .

ب- نظام البروكسي Proxy : يقوم البروكسي بدور الوسيط بين الشبكة ومستخدميها بحيث يضمن مقدم الخدمة توفير خدمات الذاكرة الجاهزة ، كما تقوم فكرة البروكسي طلبا للبحث عن صفحة ما ضمن ذاكرة Cache فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد تم تنزيلها من قبل، فيقوم بإرسالها إلى المستخدم دون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، أما إذا لم يتم تنزيله من قبل فيتم ارسال الطلب إلى الشبكة العالمية، وهنا يستخدم البروكسي أحد عناوين IP ومن خصائص هذا النظام أن الذاكرة المتوفرة لديه يمكن أن تحتفظ بتلك العمليات التي تمت الامر الذي يجعل دوره قوي في الاثبات.[2]

جـ- اقتفاء الأثر: تتمثل عملية اقتفاء الأثر في الاجراءات التي يتم استخدامها في تنفيذ طرق التحقيق الثابتة والمتغيرة المحددة منها وغير المحددة التي تثبت وقوع الجريمة وتحدد هوية مرتكبها ، حيث أخطر ما يخشاه المجرم الالكتروني تقصي أثره أثناء ارتكاب الفعل الجرمي عبر الانترنت من خلال المواقع الالكترونية لما تقدمه نتائج البحث والتحري ويثبته تقرير الخبرة الفنية الصادر عن البحث الجنائي هوية الفاعل بالتحديد، وفضلا عن ذلك يمكن تقصي أثر المجرم الالكتروني بطرق عدة سواء بواسطة البريد الالكتروني الذي تم استقباله أو من خلال تتبع أثر الجهاز الذي تم استعماله للقيام بالفعل المجرم[3] أو من خلال المراقبة الالكترونية واعتراض المرسلات عندما تقتضي التحريات والتحقيقات القضائية ذلك[4]. أو من خلال حساب المشتبه فيه على الفاسبوك بحيث يمكن التوصل إلى جميع أنواع المعلومات الشخصية الخاصة بالفرد، فمن خلال تحليل محتوى الشبكات يمكن تحديد العلاقة بين المشتبه فيه والجريمة الناشئة عن استخدام شبكة التواصل الاجتماعي.

د- استعمال أدوات فحص ومراقبة الشبكات : يستخدم المحقق عدة أدوات في فحص بروتوكول TCP/IP لمعرفة ما قد يصيب الشبكة ومعرفة العمليات التي قد تتعرض لها وتتمثل هذه الادوات في:

1- أداة TRACER: تقوم هذه الأداة بإظهار العناوين التي زارها الجاني والوقت والفترات التي قضاها فيها، كما تسمح هذه الأداة برؤية المسار الذي اتخذه IP من مضيف إلى أخر.

---

[1] عادل عزام سقف الحيط ، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية ، ط 1 ، دار الثقافة للنشر والتوزيع ، عما ، الاردن 2011 ، ص 274 .

[2] تومي يحي ، جرائم الاعتداء ضد الأفراد باستخدام تكنولوجيات الاعلام والاتصال ، أطروحة دكتوراه ، كلية الحقوق ،جامعة الجزائر 1 ، 2018/2017 ، الجزائر ، ص 189 .

[3] محمد أمين البشري ، التحقيق في جرائم الحاسب والانترنت ، المجلة العربية للدراسات الأمنية والتدريب ، عدد 30 ، جامعة نايف العربية للعلوم الأمنية ، الرياض سنة 2004 ، ص 186. وأنظر أيضا عبد الفتاح حجازي، مبادئ الاجراءات الجنائية في جرائم الكومبيوتروالانترنت ، دار الكتب القانونية ، القاهرة 2007 ، ص 396 .

[4] أنظر المادة 4 الفقرة (ج) من قانون 09-04 المؤرخ في 5غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام والاتصال ومكافحتها .

2- أداة Net Stat: تستعمل هذه الأداة لفحص حالة الاتصال الحالي للبروتوكول TCP/IP لها عدة مهام أهمها اظهار جميع الاتصالات الحديثة ، ومنافذ التصنت وعرض المنافذ والعناوين بصورة رقمية وعرض كامل لجدول الوجيه .

3 - أداة ARP: تتمثل وظيفة هذه الاداة في تحديد الحاسب الالي وموقعه على الشبكة .

4 - برنامج VisualRoute: يلتقط أي عملية تم اتخاذها ضد الشبكة، حيث يبين المناطق التي مر فيها الهجوم وبعد أن يتعرف هذا البرنامج على عنوان IP[1].

برنامج التتبع: يمكن لبرنامج التتبع أن تقوم بالتعرف على محاولات الاختراق ومن قام بها واشعار الجهة المتضررة بعملية الاختراق.

ثانيا- الضبط في الجريمة الالكترونية

يعرف الضبط انه وضع اليد على أي شيء يتصل بالجريمة التي وقعت من اجل الكشف عن الحقيقة وعن مرتكبيها، بهدف ضبط الأدلة والوثائق والأشياء التي تفيد في كشف الجريمة وإماطة اللثام عن غموضها.

والضبط هو العثور على أدلة في الجريمة التي تباشر التحقيق بشأنها و التحفظ عليها و الضبط هو الغاية من التفتيش ونتيجة المباشرة المستهدفة حيث تنص المادة 64 من قانون إ ج- على ما يلي لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المشتبه للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات ، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه..."[2]

وما يجدر الإشارة إليه أن الضبط قد يقع على برامج الحاسب الآلي كما قد يقع على بيانات الحاسب الآلي.

1- فيما يخص ضبط بيانات الحاسب الآلي:

بحيث يقابل المحقق الجنائي أثناء ضبطه للبيانات العديدة من الصعوبات العملية التي تحول دون ضبطه لهذه البيانات التي تعد دليلا لارتكاب جريمة ما في بيئة المعالجة الآلية للبيانات ومن هذه الصعوبات نجد:

[1] خالد عياد الحلبي، اجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2011، ص 211
[2] قانون رقم 66-155، سابق الذكر.

- عدم وجود دليل مرئي يمكن فهمه بالقراءة، باعتبار أن بيانات الحاسب التي تقع عليها الجريمة أو قد تقع بواسطتها غير مرئية.

- تتسم الجرائم التي يكون محلها بيانات الحاسب بعدم تركها لأية أثار يمكن الاستدلال ليها عليها.

- البيانات التي يمكن التواصل إليها، يمكن للجاني محوها أو تدميرها في فترة زمنية قصيرة جدا لا تتعدي ثوان معدودة، كما يمكن للجاني تبرير وجود البيانات في حال التوصل إليها بوجود خطأ في نظام الحاسب وبالتالي يمكنه التنصل من المسؤولية.[1]

وبعد القيام بعملية ضبط البيانات الإلكتروني يتم تحريرها وتأمينها فنيا، خاصة أمام غياب الثقافة المعلوماتية عن المحقق الجنائي مما يجعل تلك الأدلة عرضة للإتلاف والإفساد، ومن خلال هذا يتعين اتخاذ بعض الإجراءات الخاصة للحفاظ عليها وصيانتها من العين.

ومن بين هذه الإجراءات نجد:

- ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخها.

- عدم تعريض الأشرطة الممغنطة والأقراص لدرجات الحرارة العالية ولا إلى رطوبة، مع الإشارة إلى أن درجة الحرارة المسموح بها تتراوح ما بين (2-32) درجة مئوية، أما بالنسبة للرطوبة المسموح بها فتتراوح ما بين (20% إلى 80%).

- منع الوصول إلى البيانات التي تم ضبطها أو رفعها من النظام المعلوماتي.

2- فيما يخص برامج الحاسب الآلي:

ليس من الصعب التقرير بإمكانية ضبط الجرائم وأدلتها والتي يكون محلها مثلا سرقة الدعامة المادية للبرامج أو الوسائل المادية المستخدمة في نسخة بصورة غير مشروعة أو إتلافه بوسائل تقليدية لكن الأمر يصعب بضبط الشيء في حال استخدام وسائل فنية في إتلاف الفيروس وحصان طروادة.

وتكمن الصعوبة في هذه الحالة في أن الخبرة الخاصة لرجال الشرطة لا تتماشي مع خبرات المتهم في تلك الجرائم، وخاصة أن المتهم في تلك الجرائم يقوم فيها باستحداث فيروسات أخري أو نظم تشغيل جديدة لم يتعرض لها رجال الضبط من قبل، فتكمن الصعوبة هنا في اكتشافها والتوصل إليها وجمع الأدلة في هذا الشأن.[2]

[1] منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات، رسالة الدكتوراه في الحقوق، القاهرة، 2007، ص ص 196-198.
[2] عائشة بن قارة مصطفي، مرجع سابق، ص 70- 72.

المطلب الثاني: الإجراءات المستحدثة لتحصيل الدليل الإلكتروني

نظرا لقصور الإجراءات التقليدية لتحصيل أدلة اثبات الجرائم الالكترونية نظرا لطبيعتها وخصوصيتها، اهتدت أغلب التشريعات إلى إجراءات أخرى جديدة تتناسب مع الطبيعة التقنية أو اللامادية للدليل الالكتروني والتي نتناولها على النحو الاتي:

الفرع الأول: التسرب الإلكتروني

يقصد 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[1].

ويلجأ إلى هذا الإجراء عادة عندما تقتضي عملية التحري أو التحقيق في إحدى الجرائم وهي جرائم المخدرات الجريمة المنظمة عبر الحدود الوطنية -الجرائم بأنظمة المعالجة الآلية للمعطيات جرائم تبييض الأموال والإرهاب وأيضا الجرائم المتعلقة بالتشريع الخاص بالصرف.

أما بالنسبة للمشرع الجزائري فقد عرق التسرب في المادة (65 مكرر 12) بأنه 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 عند القيام بعملية البحث والتحقيق في الجرائم المذكورة في المادة (65 مكرر 5) من نفس القانون المذكور أعلاه ويتم اللجوء إلى هذا الإجراء في الجرائم التالية جرائم المخدرات، الجريمة المنظمة عبر الوطنية الجرائم الماسة بأنظمة المعالجة الآلية، جرائم تبييض الأموال[2]

الفرع الثاني: المراقبة الالكترونية واعتراض المراسلات

أولا: المراقبة الالكترونية

إن التطور الحاصل في المجال العلمي والتكنولوجي أدي إلى بروز تقنيات ووسائل حديثة يمكن استعمالها لمراقبة أحاديث الأشخاص وترصد كل ما يقومون به، ما جعل من السلطات المكلفة بالتحقيق التمسك بها لاستخدامه كتقنيات لكشف الجريمة وإثبات الحقيقة.

وتعتبر المراقبة الإلكترونية من أساليب التحري الجديدة التي جاءت بها اتفاقية بودابست في إطار المكافحة الإجرائية للجريمة المعلوماتية.

[1] أشرف عبد القادر قنديل، مرجع سابق الذكر، ص 156.
[2] أشرف عبد القادر قنديل، مرجع سابق الذكر، ص 157.

1- مراقبة الاتصالات الإلكترونية

يمكن تعريف المراقبة الإلكترونية بأنها إجراء يعني التنصت على المحادثات التي تدور بين أكثر من شخص، سواء بأجهزة سلكية أو لا سلكية.[1]

وبالنسبة للمشرع الجزائري فقد نظم في قانون (09-04) المراقبة الإلكترونية من خلال المواد 03 04 حيث تنص المادة 03 على ما يلي مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات تفتيش والحجز داخل منظومة في المادة معلوماتية.

أما عن الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية فقد تناولتها المادة 4 من نفس القانون نصت على ما يلي يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 03 أعلاه:

أ- للوقاية من الأفعال الموصوفة بالجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.

ب- في حالة توفر المعلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

ج - للمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول الى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكتروني[2].

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة.

1- مشروعية المراقبة الإلكترونية

ويقصد بها مراقبة الاتصالات الإلكترونية، فالأصل يقضي أن اتصالات الأفراد تخضع إلى مبدأ السرية والخصوصية، بحيث أن الاتصالات والمراسلات هي حق شخصي لكل فرد ولا يجوز انتهاكه كون هذا الحق مضمون قانونا ودستوريا، فقد نص المادة 38 من الدستور على أن "الحريات الأساسية وحقوق الإنسان والمواطن مضمونة وهذا يؤكد عدم جواز التعدي على حقوق وحريات الأفراد.

[1] زهير الحاج الطاهر، اليات الوقاية من الجريمة المعلوماتية، مذكرة الحصول على شهادة الماجستير قانون جنائي، كلية الحقوق جامعة الجزائر 2013، ص177

[2] زهير الحاج الطاهر، مرجع سابق الذكر، ص 178.

كما نصت المادة أيضاً على سرية المراسلات ولاتصالات الخاصة بكل أشكالها مضمونة. وبهذا فإن الدستور قد نص وأكد على ضمان سرية المراسلات والاتصالات كونها تمس وتخص حياة الفرد الخاصة[1]، وليس غريبا القول بأن الأديان السماوية تحرص على كرامة الإنسان بشكل خاص كما جاء في الدين الإسلامي الحنيف في تهجين التصرفات الهادفة إلى المساس بحرمة الإنسان ونهي عن الغيبة والنميمة والتجسس كما جاء في الآية القرآنية: **"..... ولا تجسسوا ولا يغتب بعضكم بعضا[2]..... "**

2- إجراءات مراقبة الاتصالات الإلكترونية

تعرف الاتصالات الإلكترونية حسب نص المادة 2 من قانون 04/09 بأنها كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية.

تكون المراقبة عن طريق وضع ترتيبات تقنية دون موافقة المعنيين بها قصد التقاط وتسجيل وبث وتسجيل الكلام المتفوه به من طرف شخص أو أشخاص، وفي أماكن خاصة أو عمومية، أو التقاط صور لشخص أو عدة أشخاص من أجل التحري والوصول إلى أدلة تثبت وقوع جريمة إلكترونية.

ثانيا: اعتراض المراسلات (تسجيل الأصوات التقاط الصور)

اعتراض المراسلات يقصد به التقاط أو تسجيل أو نسخ المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية لجميع المراسلات الصادرة والواردة تحت شكل مكالمات هاتفية، راديو، تلكس، مراسلات إلكترونية[3].

وقد عرفت لجنة الخبراء للبرلمان الأوربي بستراسبورغ في يوم: 06/10/2006 في اجتماع حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية اعتراض المراسلات بأنه عملية مراقبة سرية للمراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة أو المعلومات حول الأشخاص المشتبه فيهم بارتكابهم أو مشاركتهم في الجرائم[4] واعتراض المراسلات يتم عن وسائل سلكية واللاسلكية.

أ- في المجال السمعي (تسجيل الأصوات)

[1] زهير الحاج الطاهر، مرجع سابق الذكر، ص 177.
[2] سورة الحجرات، الآية 12.
[3] زهير الحاج الطاهر، مرجع سابق الذكر، ص 178.
[4] بوشو ليلي قبول الدليل العلمي أمام القضاء الجنائي مذكرة من أجل نيل شهادة الماجستير، الجزائر، 2010 2011، ص 128.

تفرض الرقابة في هذا المجال التنصت على الأحاديث الشخصية من خلال التجسس على المكالمات الهاتفية وتسجيلها وذلك من خلال استخدام ميكروفونات خفية من أجل الحصول على تلك المكالمات موضوع الرقابة.

ولقد عرف الفقه الفرنسي الأصوات هي عبارة عن ترجمة للتغيرات المؤقتة لموجات الصوت الخاصة بالكلام أو أي نوع آخر من الموجات أو التغيرات الدائمة، وعادة ما يتم التسجيل بواسطة آلة تترجم موجات الصوت إلى اهتزازات خاصة ويتم تسجيل الصوت على الشريط المستخدم في جهاز التسجيل بواسطة آلة المغناطيسية ويجري التسجيل على سلك ممغنط.

وبالرغم من أن مراقبة المكالمات التليفونية تشكل انتهاك حرمة الحياة الخاصة باعتبارها تتجسس على أدق أسرار الناس التي يمكن أن يكشفوا عنها لغيرهم دون خوف أو حرج ضنا منهم أن الحديث في مأمن، إلا أنه لا يمكننا إنكار أهميتها في العملية الاثباتية[1].

وعن المشرع الجزائري وبالرجوع إلى المادة 05 مكرر 05 المقصود من تسجيل الأصوات والتقاط الصور هو تلك العملية التقنية التي تتم بغرض مراقبة وتسجيل المحادثات الشفوية التي يتفوه بها شخص أو عدة أشخاص بصفة خاصة أو سرية وذلك في مكان عام أو خاص أو التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص.

ب- في المجال البصري (التقاط الصور)

يعتبر حق الشخص في صورته عنصرا من عناصر حياة الإنسان الخاصة، فإذا كانت الصورة العادية تحتل تسجيلا حقيقيا لما تراه العين، وما يعجز الفكر الإنساني عن التعبير عنه، فإن التصور التقني لوسائل التصور تجاوز ذلك كما في التصوير الإسبكتوغرافي و قد يتم التصوير باستخدام أشعة غير مرئية أو تصوير ضوئيا.

وقد تزايد في الأونة الأخيرة اعتماد سلطات التحقيق أسلوب المراقبة عن طريق التقاط أو تسجيل الصور لشخص من مكان معين بهدف الوصول إلى الحقيقة وعليه يجب أن تتوفر في الصورة الفوتوغرافية بعض العوامل حتى تكون مقبولة مبدئيا منها:

- عامل فني يتعلق بمدى مراعاة الأصول العلمية المتعارف عليها في التصوير الضوئي.

[1] بن بلاغة عقيلة، حجية أدلة الإثبات الجنائية، مذكرة لنيل شهادة الماجستير في القانون فرع القانون الجنائي، جامعة الجزائر، 2011، ص 65.

- عامل موضعي يتعلق بالصورة من حيث وضوحها وخلوها من الخدع والحيل وقدرة دلالتها على مكان وزمان التقاطها والأشخاص الذين تمثلهم كمال الشخص يتعلق بالخبرة الفنية القائم بالتصوير.

- عامل اجرائي يتعلق بإثبات إجراءات التصوير في محاضر والتأكد من خلو أية مسجلات سابقة (جهاز التصوير والفيلم) ثم التحفظ عليه بعد استعماله لحين عرضه على سلطات التحقيق[1].

ثالثا- القيود الواردة على عملية المراقبة الإلكترونية واعتراض المراسلات

1- الحصول علي الإذن من السلطات المختصة: يجب لمشروعية الدليل المستمد من اعتراض المراسلات و تسجيل الأصوات و التقاط الصور أن يكون نتيجة لإذن صادر عن وكيل الجمهورية أو قاضي التحقيق -حسب الحالة - غير أن إصدار هذا الإذن ليس مطلقا، وإنما مقيد بمجموعة من الشروط التي يجب أن تتوافر فيه، وإلا نحد الدليل الناتج عنه دليلا غير مشروع و بالتالي غير مقبول في عملية الإثبات الجنائي.

2- ضرورة تعليق الإذن بجرائم معينة: حيث يحدد المشرع الجزائري الجرائم التي يجوز لوكيل الجمهورية أو قاضي التحقيق في إطار البحث والتحري عن أدلة إثباتها أو نفيها أن يلجأ إلى هذه الإجراءات[2]، وحسب المادة 65 مكرر 5 ن-ق-إ-ج

أ- جرائم المخدرات: وهي تلك الجرائم المنصوص هي عليها بموجب القانون رقم 04-18 المؤرخ في 13 ذي القعدة 1425هـ الموافق لـ 25- 12-2004م و المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والاتجار غير المشروعين بها.

ب - الجريمة المنظمة العابرة للحدود الوطنية.

ج- الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وهي تلك الجرائم المنصوص و المعاقب عليها بموجب المواد 394 مكرر 7 من القانون 06-01 المعدل المتمم للأمر 15666 المتعلق بقانون العقوبات والصادر في 20-12-2006.

د- جرائم تبييض الأموال: وهي الجرائم المنصوص عليها ينص 389 مكرر من القانون رقم 04 15 المؤرخ في 2-10-11-2004 المعدل و المتمم للأمر 66-156 المتعلق بقانون العقوبات ويقصد بتبييض الأموال إخفاء المصدر الإجرامي للممتلكات و الأموال.

ه- جرائم الإرهاب: وهي الجرائم المنصوص عليها ينص المادة 87 مكرر من الأمر -95 11 المؤرخ في 25-02-1995 المعدل والمتمم للأمر 6-156 المتعلق بقانون العقوبات.

[1] بن بلاغة عقيلة، مرجع سابق الذكر، ص 80.
[2] بوشو ليلى، مرجع سابق الذكر، ص 130.

و- الجرائم المتعلقة بالتشريع الخاص بالصرف.

ي- جرائم الفساد: وهي الجرائم المنصوص عليها في المواد من 25 إلى 47 من القانون رقم 06-01 المؤرخ في 21 محرم 1427 الموافق ل 20-20-2006 المتعلق بالوقاية من الفساد ومكافحته.

ويمكن هنا أن نقول إن المشرع قد أحسن بتحديده للجرائم التي يمكن عند حدوثها اللجوء 2 إلى هذه الإجراءات نظرا لخطورتها على الحياة الخاصة للأشخاص[1].

3- عدم جواز صدور الإذن إلا بصدد جريمة وقعت بالفعل: حيث أنه وباستقراء نص المادة 65 مكرر 5 من ق إ ج نجد أن هذه الإجراءات هي من إجراءات التحقيق لا الاستدلال، وبالتالي فهي لم تشرع لتستخدم كوسيلة للتحري عن الجرائم، وعليه لا يمكن القيام بها إلا في الجرائم المتلبس بها أو في التحقيق الابتدائي، وتكون في الأول بإذن وكيل الجمهورية، وفي الثانية بإذن قاضي التحقيق بعد اتصاله له بالدعوى عن طريق طلب فتح التحقيق وهذا يعني أنه لا يمكن اللجوء إلى هذا الإجراء إذا لم تكن الجريمة قد وقعت بعد حتى ولو كانت وشيكة الوقوع والقول بغير ذلك أمر تستباح معه حرمات الناس وتنتهك خصوصياتهم بدعوى التحري عن الجرائم.

4- ضرورة أن يكون الإذن مكتوب و مسبب: نظرا لخطورة هذه الإجراءات على حرية الأفراد و حياتهم الخاصة فقد أشترط المشرع للقول بمشروعيتها بمجموعة من الشكليات نصت عليها المادة 65 مكرر 7 من ق إ ج و التي يجب أن يتضمنها الإذن المذكور في المادة 65 مكرر 5 السالفة الذكر، وهي: أن يكون مكتوب و يحتوي على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها، والأماكن المقصودة للقيام بالإجراء سواء كانت سكنية أو غيرها، وأن يحدد الجريمة المبررة لهذا الإجراء[2].

5- ضرورة أن يكون الإذن محدد المدة: نظرا للطابع الاستثنائي للإجراء محل الإذن، فقد اشترط القانون أن يكون محدد المدة حتى لا يظل سيفا مسلطا على رقاب الأفراد، وقد حددتها المادة 65 مكرر 7 ق إ ج بأربعة أشهر كحد أقصى قابلة للتحديد إذا دعت ضرورة التحري والتحقيق ذلك بنفس الشروط الشكلية والزمنية.

[1] بوشو ليلى، مرجع سابق الذكر، ص 131.
[2] أشرف قنديل، مرجع سابق الذكر، ص 220.

الفرع الثالث: حفظ وإفشاء المعطيات

الحفظ السريع للمعطيات المخزنة وقد نص على هذا الإجراء كل من المادتين 16 و17 من اتفاقية بودابست ويقصد به الاحتفاظ بالمعلومات السابقة وتخزينها مع حمايتها من كل ما يمكن أن يفسدها أو يتلف نوعيتها[1].

والإجراءات المقررة فيها تبين المادتين لا تطبق إلا إذا كانت البيانات المعلوماتية أو بيانات الحاسب الموجودة من قبل و في صورة التخزين ، لكن لأسباب عديدة قد لا تكون هذه البيانات المراد التنقيب عنها جنائيا قد لا تكون موجودة، أو لم تعد مخزنة كان يجمع ثم لا يحفظ لها أو تدمر بعد استعمالها لذلك إجراء التحفظ على البيانات في المادتين 16 و 17 تمدد للبيانات المعلوماتية الموجودة من قبل و ثم تجميعها و تخزينها، و هو إجراء قانوني جديد للتنقيب عن الجريمة المعلوماتية وبالأخص ضد الجرائم المرتكبة بواسطة شبكة الانترنت وسبب استحداث هذا الإجراء الجديد هو سرعة تغير البيانات المعلوماتية وقابليتها للتلاشي والتلاعب بها بمحوها أو تدمرها، فيسهل بالتالي فقدان أدلة ارتكاب الجريمة و المادة 16 من اتفاقية بودابست يمكن للسلطات الوطنية المختصة من إصدار أمر بالحفظ أو حفظ البيانات عن طريق الأمر الوقائي أو أمر إداري أو أي طرق مماثل للتفتيش أو إصدار أمر بالاطلاع.

الفرع الرابع: معوقات إثبات الجريمة الإلكترونية

مما لا شك فيه أن هناك العديد من العراقيل والمعوقات التي تقف حجر عثرة أمام إثبات الجريمة الإلكترونية، سنبينها في النقاط الآتية:

1- المعوقات المتعلقة بالجريمة:

أ- اختفاء آثار الجريمة، وغياب الدليل المرئي، لأن الجناة في الجرائم الإلكترونية يتمتعون بقدرة فائقة على إخفاء أي آثار مادية ملموسة على جرائمهم.

ب- صعوبة الوصول إلى الدليل، للإحاطة بوسائل الحماية الفنية مثل كلمات السر التي تمنع الوصول إليه.

ج- سهولة محو وتدمير الدليل في زمن قصير جدا من قبل الجاني.

د- ضخامة حجم المعلومات التي يجب فحصها واحتمال خروجها عن نطاق إقليم الدولة.

ه- الجناة في الغالب لا يستخدمون في دخولهم على شبكة الإنترنت أجهزتهم، بل يعتمدون على مقاهي الإنترنت المنتشرة في الدولة، ولا يمكن معرفة مستخدميها.

[1] عباسي خولة، مرجع سابق الذكر، ص 46.

و- أغلب البيانات والمعلومات المتداولة عبر الحاسب الآلي هي رموز مخزنة على وسائط ممغنطة لا يمكن الوصول إليها إلا عن طريق الحاسب الآلي، من قبل اشخاص مؤهلين لذلك.

2- المعوقات المتعلقة بالجهات المتضررة من الجريمة:

أ- بعض المؤسسات يكون لديها رغبة في عدم الإبلاغ عن الجريمة الإلكترونية حفاظاً على سمعتها.

ب- التسارع لاستخدام الشركات لأحدث التقنيات في نظم المعلومات وتبسيط الإجراءات لزيادة المنتجات وعدم تركيزها على الجانب الأمني.

ج- قد يكون سبب عدم الإبلاغ عن الجريمة عدم معرفة الضحية بوجود جريمة أصلاً، وعدم قناعته أنها ممكن أن تحدث لمؤسسته.

3- المعوقات المتعلقة بجهات التحقيق:

أ- شخصية المحقق: وذلك عندما يتهيب من استخدام الكمبيوتر والإنترنت.

ب- عدم توافر الأجهزة والبرامج المناسبة للتحقيق

وهناك العديد من المعوقات التشريعية كعدم وضع تشريعات جديدة لتناسب مع التطور التكنولوجي لتقنية المعلومات وظهور أدلة رقمية حديثة في ارتكاب الجرائم الإلكترونية. يعيق إثبات الجريمة.

الفصل الثانـي

القيمة الثبوتية للدليل الالكتروني أمام القضاء

تمهيد:

إن القاضي الجنائي لا يمكنه أن يقضي بعلمه الشخصي في مجال الإثبات إلا بعد إحاطته بوقائع الدعوى والتي تطرح أمامه في شكل أدلة، وهذه الأخيرة هي الوسيلة التي يبني على أساسها قناعته، أما بالنسبة للدليل التقني في مجال الجرائم الالكترونية فقد لا يعبر عن الحقيقة نظرا لما يتعرض إليه من تخريب أو تزييف أو عبث وهذا ما يثير مسألة مشروعية الأخذ به إذ أنه وبوجه عام يشترط في الدليل الجنائي أن يكون مشروعا من حيث وجوده ومن حيث الحصول عليه من جهة ومن جهة أخرى فإنه يثير مسألة مصداقية الدليل الالكتروني في تعبيره عن الحقيقة التي تهدف إليه الدعوى ونظرا للتطور الحاصل في المجال التقني فإنه أصبح من السهل أن يتم العبث بهذا النوع من الأدلة مما يجعل مضمونها متناقض مع الحقيقة دون أن ننسى أنها تعرض على شخص غير مختص.

ولذلك ستكون محل دراستنا القيمة القانونية للدليل الالكتروني والتي سيتم تقسيمها إلى مبحثين، بحيث يتضمن المبحث الأول حجة الدليل الالكتروني أمام القضاء الجنائي، اما المبحث الثاني فيتضمن سلطة القاضي الجزائري في تقدير الدليل الالكتروني.

المبحث الأول: حجية الدليل الالكتروني أمام القضاء الجنائي

المطلب الأول: مشروعية الدليل الإلكتروني

يقصد بالمشروعية التقيد بأحكام القانون والعمل في إطاره، بهدف تقرير ضمانة أساسية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة بالتعدي عليها في غير الحالات المسموح فيها بذلك. واعتبارا لذلك فالدليل الجنائي لا يكون سليما ويقينيا يعوّل عليه القضاء في أحكامه إلا إذا تحلى وتغلف بالمشروعية[1].

الفرع الأول: مشروعية الدليل الإلكتروني في الوجود

تقتضي مشروعية وجود الدليل الالكتروني أن يعترف المشرع الجزائي بهذا الدليل بنصوص قانونية واضحة ويدرجه ضمن قائمة وسائل الإثبات التي يجوز للقاضي الاستناد إليها لتكوين عقيدته، إذ لا يسوغ لهذا الأخير بناء حكمه على دليل لم ينص عليه القانون صراحة، كما ليس له أن يتوسع في تفسير النصوص الجنائية أو تأويلها أو تحميلها بأكثر مما تتحمل لما قد ينجم عن ذلك من خلق أدلة إثبات أخرى لم يعرف لها وجود في القانون حتى ولو بلغت الأفعال المرتكبة درجة عالية من الخطورة. وفي هذا الإطار، تختلف طريقة الاعتراف بالدليل الالكتروني وقبوله كدليل إثبات من دولة إلى أخرى بحسب طبيعة نظام الإثبات السائد فيها، والذي لا يمكن أن يخرج عن الفئات الثلاث التالية:

أولا - نظام الإثبات المقيد: وفيه يقوم المشرع بتحديد سلفا وبشكل حصري الأدلة التي يجوز للقاضي قبولها والاستعانة بها في الإثبات، وكذا تحديد القوة الاستدلالية لكل دليل بناء على قناعته بها، في حين لا يكون للقاضي الجزائي في هذا النظام أي دور في تقدير الأدلة أو البحث عنها، وإنما يقتصر دوره على فحص الدليل للتأكد من مدى مشروعيته وتوفره على الشروط التي حددها القانون وفي حالة انتفاء الشروط التي يتطلبها القانون في الدليل فان القاضي لا يسع له الحكم بالإدانة حتى ولو تكونت لديه قناعة يقينية بارتكاب المتهم للجريمة المنسوبة إليه.

ومن هنا يتضح جليا بأن نظام الإثبات المقيد يقوم على مبدأين أساسيين، الأول يتمثل في الدور الايجابي للمشرع في عملية الإثبات لكونه الذي ينظم قبول الأدلة سواء عن طريق التعيين المسبق للأدلة المقبولة للحكم بالإدانة، أو باستبعاد أدلة أخرى، أو بإخضاع كل دليل لشروط معينة.

أما المبدأ الثاني، فيتمثل في الدور السلبي للقاضي الجزائي في الإثبات، إذ يلتزم التزاما صارماً بما يرسمه له المشرع سلفا من أدلة إثبات على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير

[1] هلالي عبد الله احمد، حجية المخرجات الكومبيوترية في المواد الجنائية، مرجع سابق، ص 104.

من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون.

ومن المسائل التي انتقدت في هذا النظام، قيامه بتقنين اليقين بنصوص قانونية سلفا رغم أن اليقين مسالة يطرحها الواقع ترتبط بالظروف الخاصة والمتغيرة لكل قضية وتترك لتقدير قاضي الموضوع.

ثانيا- نظام الإثبات الحر[1]: وهو نظام يسود فيه مبدأ حرية الإثبات، إذ لا يحدد فيه المشرع طرقا معينة للإثبات ولا حجيتها أمام القضاء، إنما يترك ذلك للقاضي الجزائي الذي يكون له دور ايجابي في البحث عن الأدلة المناسبة وتقدير قيمتها الثبوتية حسب اقتناعه بها. فلا يلزمه القانون بالاستناد إلى أدلة معينة لتكوين قناعته فله أن يبني هذه القناعة على أي دليل يقدم في الدعوى وإن لم يكن منصوصا عليه، بل أن المشرع في مثل هذا النظام لا يختص بالنص على أدلة الإثبات، فكل الأدلة تتساوى قيمتها في نظر المشرع، والقاضي هو الذي يختار من بين ما يطرح عليه من الأدلة ما يراه مفيدا للوصول إلى الحقيقة.[2]

وعلى عكس نظام الإثبات المقيد فان فلسفة هذا النظام ترتكز على مبدأين مختلفان هما: الأول يتمثل في الدور الصلبي للمشرع في عملية الإثبات، ومن خلاله يمتنع المشرع عن تحديد الأدلة التي تصلح للإثبات مسبقا، وهو ما يفتح المجال لأن تكون مقبولة وفقا لتقدير القاضي وليس المشرع، كما يمتنع عن تحديد القيمة الاقناعية للدليل أو إظهار أي تسلسل بين هذه الأدلة في الحجية أو يرجح أي دليل على الآخر فيقتصر دور المشرع على تحديد الشروط اللازمة لصحة الدليل وطريقة تقديمه، وذلك ضمانا للحرية الفردية وكفالة حسن سير العدالة[3].

أما المبدأ الثاني، فهو الدور الايجابي للقاضي الجزائي في الإثبات، ويبدو ذلك من ناحيتين: الأولى من خلال الحرية المطلقة التي يتمتع بها القاضي الجزائي في إثبات حقيقة الجريمة بكافة طرق الإثبات[4].

ومن ناحية أخرى فنظام الإثبات الحرّ يمنح للقاضي الجزائي سلطة تقديرية كبيرة في قبول الأدلة، وموازنتها وتقدير قيمتها التدليلية محتكما إلى ضميره ومعتمدا على ثقافته وخبرته القانونية. فله أن يأخذ بأدلة ويستبعد أخرى.

---

[1] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة و القانون، مرجع سابق، ص 140.

[2] ياسر محمد الكومى. أبو حطب، الحماية الجنائية والأمنية للتوقيع الالكتروني، منشاة المعارف، الإسكندرية، 2014، ص 303.

[3] أحمد يوسف الطحطاوي، أدلة الالكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة ، 2015.، ص 195.

[4] اقر المشرع الجزائري بحرية الإثبات الجزائي في نص المادة (212) من قانون الإجراءات الجزائية بالصيغة التالية يجوز إثبات الجرائم بأية طريقة من طرق الإثبات ... وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي". ونص المشرع الفرنسي كذلك على هذا المبدأ في المادة (427) من قانون الإجراءات الجزائية على النحو التالي: " ما لم يرد نص مخالف يجوز إثبات الجرائم بكافة طرق الإثبات ويحكم القاضي بناء على اقتناعه الذاتي.

ثالثا- نظام الإثبات المختلط: وهو نظام وسط بين نظام الإثبات المقيد ونظام الإثبات الحر، وفيه تم التصدي للانتقادات الموجهة لنظام الإثبات الحر حول خشية تعسف القاضي الجزائي و خروجه عن جادة الصواب، وذلك بأن حدد له وسائل الإثبات التي يلجأ إليها لتأسيس حكمه. كما تم تلاقى ما وجه من انتقادات لنظام الإثبات المفيد، لما جعل دور القاضي سلبيا في عملية الإثبات، وذلك من خلال إعطاء القاضي الجزائي الحرية في تقدير ووزن ما يعرض عليه من أدلة ثبوتية وفقا لاقتناعه الشخصي[1].

من هنا يتبين بأن منطق هذا النظام يرتكز من جهة على تحديد قائمة أدلة الإثبات والقيمة الاثباتية لكل منها سلفا من قبل المشرع ومن جهة أخرى منح القاضي الجزائي سلطة تقديرية واسعة في موازنة وقبول الأدلة المطروحة أمامه وفقا لاقتناعه الذاتي.[2]

وفي هذا الصدد نجد المشرع الجزائري وكغيره من التشريعات المنتمية إلى نظام الإثبات الحق لم يفرد نصوصا خاصة تملي على القاضي الجزائي مقدما بقبول أو عدم قبول أي دليل بما في ذلك الدليل الالكتروني، إذ جاء القانون رقم (04-09) المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها خاليا من أية أوضاع خاصة بالدليل الالكتروني ليترك الأمر بذلك للقواعد العامة، وعليه فالأصل في الأدلة مشروعية وجودها ومن ثم فالدليل الالكتروني سيكون مشروعا في الموجود اصطحابا للأصل.

الفرع الثاني: مشروعية الدليل الإلكتروني في التحصيل

يقصد بمشروعية التحصيل أن تتم عملية البحث عن دليل الإدانة وتقديمه للقضاء من طرف القائمين بالتحقيق وفقا للقواعد والإجراءات التي رسمها القانون لذلك، فمشروعية الدليل إذا تتطلب صدقه في مضمونه، وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة تدل على الأمانة والنزاهة.[3]

لذلك لما كان الدليل المستمد من الوسائل الالكترونية الحديثة أكثر الأدلة اقتحاما وتعديا على حقوق وحرمات الأفراد استوجب عدم قبوله في العملية الاثباتية إلا إذا تم الحصول عليه في إطار أحكام القانون واحترام مبادئ العدالة وأخلاقياتها. فرغم إقرار مبدأ حرية القاضي الجزائي في الإثبات إلا أن هذه الحرية يعني ألا تمتد الى قبول أدلة وليدة إجراء غير مشروع ليس لان ذلك يتعارض مع قيم العدالة فحسب، إنما لأنه يمس بحق المتهم في الدفاع أيضا. [4]

[1] سامي جلال فقي حسين، مرجع سابق، ص 93.
[2] عفيفي كامل عفيفي، مرجع سابق، ص 373.
[3] فهد عبد الله العازمي، ص 394.
[4] رمزي رياض عوض، سلطة القاضي الجنائي في تقدير الأدلة، دار النهضة العربية القاهرة 2004. ص 154.

وينبغي الإشارة هنا إلى أن شرط مشروعية الدليل مطلوب في حالة الإدانة فقط، إذ لا يجوز أن تبنى الإدانة الصحيحة على دليل باطل، أما في حالة البراءة فالمشروعية ليست شرطا واجب التوفر في الدليل، إذ في هذه الحالة يمكن للمحكمة أن تستند إلى دليل فقد شروط صحته كشهادة قاصر غير مميز أو كان ثمرة إجراء باطل لإقرار براءة المتهم.

والحقيقة أن معيار قبول أية وسيلة علمية مستمدة في مجال الإثبات الجنائي لإظهار الحقيقة يرتكز أساسا على عدم إهدارها للحريات العامة للفرد وكرامته الإنسانية، وهو الأمر الذي يحرص عليه القاضي الجنائي لكي يوازن بين ما هو مشروع فيقبله وما هو غير مشروع فيتصدى له.[1]

المطلب الثاني: موقف المشرع الجزائري من أنظمة الإثبات الجنائي

لقد حسم المشرع الجزائري موقفه من أنظمة الإثبات الجنائي بشكل واضح في نصي المادتين (212 و 307) من قانون الإجراءات الجزائية، وذلك حينما نص في المادة (212) على أنه " يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الاحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي ونص في المادة (307) بأن " القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما ، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، ويبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم هل لديكم اقتناع شخصي".

فبالنظر إلى نصي هاتين المادتين يتضح جليا أن المشرع الجزائري تبنى كأصل عام نظام الإثبات الحر أو الاقتناع الشخصي للقاضي الجزائي، والذي منح من خلاله للقاضي الجزائي حرية واسعة في مجال تقدير الأدلة وفقا لقناعته الذاتية، وفتح أمامه باب الإثبات على مصراعيه كي يستلهم عقيدته من أي موطن يراه، دون أن يطالبه بتقديم مبرر لذلك. وفي الوقت نفسه وعلى سبيل الاستثناء نجده أخذ بنظام الإثبات المقيد أو ما يسمى كذلك بنظام الأدلة القانونية في إثبات بعض الجرائم أين اشترط لإثباتها أدلة قانونية محددة مسبقا على سبيل الحصر كما هو الشأن بخصوص جريمة الزنا المنصوص عليها في المادة (339) من قانون العقوبات[2]. كما منع الأخذ ببعض وسائل الإثبات كالمراسلة المتبادلة بين المتهم ومحاميه وإن تضمنت اعتراف المتهم بأنه ارتكب الجريمة[3].

[1] أحمد يوسف الطحطاوي، مرجع سابق الذكر، ص 267.
[2] تنص المادة 341 من قانون العقوبات على أن " الدليل الذي يقبل في ارتكاب الجريمة المعاقب عليها في المادة 339 يقوم إما على محضر قضائي يحرره أحد رجال الضبط القضائي عن حالة التلبس وإما بإقرار وارد في رسائل أو مستندات صادرة عن المتهم وإما بإقرار قضائي.
[3] تنص المادة (217) من القانون الإجراءات الجزائية على أنه لا يستنبط الدليل الكتابي من المراسلة المتبادلة بين المتهم ومحاميه.

وقد تأكد الأخذ بمبدأ الإثبات الحر كذلك بطريقة غير مباشرة في عدة نصوص قانون الإجراءات الجزائية، فيما يخص جهات الحكم، نذكر منها الفقرة الأولى من المادة (235) التي تنص على أنه " يجوز للجهة القضائية إما من تلقاء نفسها أو بناء على طلب النيابة العامة أو المدعي المدني أو المتهم أن تأمر بإجراء الانتقالات اللازمة لإظهار الحقيقة ". وكذلك الفقرة الأولى من المادة (286) " ... له (أي لرئيس الجلسة) سلطة كاملة في ضبط حسن سير الجلسة وفرض الاحترام الكامل واتخاذ أي إجراء براه مناسبا لإظهار الحقيقة.....

ولعل ما يعزز توجه المشرع الجزائري هذا الاتجاه هو عدم سنه نصوصا تملي على القاضي الجزائي مقدما بقبول أو عدم قبول أي دليل من الأدلة المطروحة عليه في الدعوى أو ترسم له طرقا محددة للإثبات يتقيد بها، إنما فسح له المجال لكي يختار بحرية من كل طرقه ما يراه مفيدا وموصلا إلى الكشف عن الحقيقة ويستلهم عقيدته من أية وسيلة أو دليل يطمئن إليه وجدانه ويرتاح إليه ضميره، ولو تعلق الأمر بالأدلة الالكترونية، خاصة أنه لم يتضمن قانون رقم (09-04) المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أية استثناءات أو أوضاع خاصة بهذا الصدد، مما يوحي بأن الدليل الالكتروني مقبول مبدئيا في الإثبات الجنائي بصفة عامة، والإثبات في مجال جرائم الاعتداء على النظم المعالجة الآلية بصفة خاصة، يمثل مظهرا من مظاهر اعتناق المشرع لمبدأ حرية الإثبات والاقتناع[1].

وفي مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وضع المشرع الجزائري على عائق مقدمي خدمات الانترنت عددا من الالتزامات لمساعدة السلطات المختصة بالتحري والتحقيق بما من شأنه تسجيل وحفظ المعطيات المتعلقة بمحتوى الاتصال أو المراسلة في حينها، كالمعطيات التي تسمح بالتعرف على مستعملي الخدمة المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال خصائصها التقنية، وكذا تاريخ ووقت ومدة الاتصال والمعطيات التي تسمح بالتعرف على مرسل الاتصال والمرسل إليه، وكذا عناوين المواقع المطلع عليها[2]. وكل ذلك يعد إخبارا صريحا على أن المشرع الجزائري قد سار على نهج نظام الإثبات الحر.

وهناك أسباب أخرى عديدة تبرر أخذ المشرع الجزائري بنظام الإثبات والاقتناع الحر ولعل أهمها ظهور وتفشي الأدلة العلمية بمختلف أنواعها، كتلك المستمدة من الطب الشرعي والتحاليل العلمية الدقيقة (كالبصمات الشخصية والبصمة الوراثية) ومضاهاة الخطوط والأدلة الالكترونية الرقمية، والتي لا تقبل

[1] خنفوسي عبد العزيز " تجميد مبدأ حرية الإثبات الجزائي في القانون الجنائي الجزائري" ص 01-02، مقال منشور في الموقع الالكتروني: http://tit.com/images/no_image_card.pn

[2] انظر المادة (3/11) من القانون رقم (09-04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مرجع سابق،

بطبيعتها إخضاع القاضي لأية قيود بشأنها، بل بالعكس فهي تفرض أن يترك أمر تقديرها وتمحيصها لمحض إرادة واقتناع القاضي الجزائي.

المبحث الثاني: سلطة القاضي الجنائي في تقدير الدليل الالكتروني

من أهم النتائج التي تترتب عن مبدأ حرية القاضي في تكوين اقتناعه حرية القاضي في تقدير الأدلة بما في ذلك الدليل الرقمي وموازنتها وفقا لما يمليه عليه وجدانه، ومن دون أن يخضع في ذلك الرقابة المحكمة العلياء إلا أنه مع ذلك مقيد بضرورة تأسيس اقتناعه على الجزم واليقين دون الظن والاحتمال وأن يكون متوائما مع مقتضيات العقل والمنطق. إن سلطة القاضي في تقدير الدليل الرقمي يحكمه مبدأ الاقتناع القضائي الذي يؤدي إلى نتيجتين هما حرية القاضي في قبول الأدلة وحرية القاضي في تقدير الأدلة، حيث يجوز له الاستناد إلى الدليل الرقمي للإثبات الجرائم خاصة الجرائم المعلوماتية حيث أن المشرع حسم هذه المسالة بتحديد النموذج القانوني للدليل الخاضع التقدير القاضي، فمتى ما توافرت شروط هذا النموذج طبقا لمبدأ الشرعية الإجرائية، وجب على القاضي إخضاعه لعملية تقديره وهي موضعية محضة للقاضي أن يمارس سلطته التقديرية فيها بل هي المجال الطبيعي لهذه السلطة حيث أنها تتعلق بقيمة الدليل في الإثبات وصولا للحقيقة.

المطلب الأول: مبدأ الاقتناع الشخصي للقاضي بالدليل الرقمي

إن المبدأ العام في الإثبات الجنائي يخضع الدليل الرقمي الى حرية القاضي الجنائي في اقتناعه الشخصي، وحريته في هذا المقام بالغة السعة، فهو وحده الذي يقر قيمة الدليل الرقمي بحسب ما تحدثه من أثر في وجدانه من ارتياح واطمئنان ومع ذلك ولقد تعاظم دور الإثبات العلمي مع ظهور الدليل الرقمي المطلوب للإثبات في الجرائم الالكترونية، مما جعل القاضي أنه يضطر للتعامل مع هذا النوع المستحدث من الأدلة الضرورية لكشف أنماط جديدة من الجرائم في مقابل نقص الثقافة المعلوماتية من جهة و القيمة العلمية التي يتمتع بها هذا الدليل من جهة، وهذا الأمر تنجر عنه عدة مشاكل خاصة فيما يتعلق بالدليل الرقمي، مما يؤدي إلى نقص قيمته من جهة، ونقص الاعتماد عليه في إثبات الجرائم الإلكترونية من جهة أخرى.

الفرع الأول: مضمون مبدأ الاقتناع الشخصي للقاضي

وبغية الإلمام بهذا المبدأ سنقوم في هذا الفرع بتعريفه (أولا)، ثم الأساس الذي يقوم عليه (ثانيا)، ثم نبين مجال تطبيق هذا المبدأ (ثالثا).

أولا: تعريف مبدأ الاقتناع القضائي

تعددت الآراء فيما يتعلق ببيان مدلول الاقتناع القضائي، حيث عرفه الفقهاء على أنه حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث احتمالات على درجة عالية من التأكد الذي تصل إليه نتيجة لاستبعاد أسباب الشك بطريقة جازمة وقاطعة.[1]

وعليه فالاقتناع هو اعتقاد قائم على أدلة موضوعية، تمتاز بخاصية ذاتية نتيجة لتفاعل ضمير القاضي عند تقديره للوقائع، تجعل اقتناعه نسبيا فيما يصل إليه من النتائج، هذه النتائج التي قد تختلف من قاض لآخر لاختلاف اتصال كل قاض بالوقائع المعروضة عليه، وذلك حسب تكوينه وتجاربه وأخلاقه وثقافته والمحيط الذي عاش ويعيش فيها.[2]

وعليه فالمطلوب من القاضي أن يتوصل إلى التأكيد واليقين وأن يبني حكمه على الإثبات القطعي الذي يمثل معيارا موضوعيا، غير أنه يشعر في أغلب الأحيان في نفسه بإدانة المتهم دون أن يستطيع التدليل على ذلك بالأدلة الكافية، وفي ذلك يتوصل القاضي إلى درجة اليقين بصفة ذاتية، وهذا ما يعبر عنه بالاقتناع الشخصي، ولذلك فإن المشرع قد فضل المعيار الذاتي عن الموضوعي وإن صفة الذاتية هي أبرز ما تميز الاقتناع الشخصي[3].

ثانيا: الأساس القانوني لمبدأ الاقتناع الشخصي للقاضي الجزائي بالدليل الرقمي

لقد أقرت معظم التشريعات الحديثة هذا المبدأ وجسدته في قوانينها الإجرائية، كما تم الأخذ به في أحكام محاكمها، وعليه سوف نحاول إبراز الأساس القانوني لهذه المبدأ، وذلك بإبداء موقف التشريع الفرنسي أولا، ثم موقف التشريع الجزائري، وهذا وفق ما يلي:

1- الأساس القانوني لمبدأ الاقتناع الشخصي للقاضي الجزائي في القانون الفرنسي

لقد لقي مبدأ الاقتناع الشخصي أول تعبير قانوني عنه بموجب نص المادة 342 من تقنين التحقيقات الجنائية الفرنسي القديم وذلك من خلال العبارات التي نقر على مسمع المحلفين عند المداولات حول اتهام الشخص. إلا أن هذه التعليمة الموجهة للمحلفين حذفت بمقتضى القانون الصادر تاريخ 25 نوفمبر 1941 على أساس أنها عديمة الفائدة وغير ملائمة، ولكن المشرع الفرنسي لم يكن يهدف من وراء إلغاء هذه التعليمة إلى إلغاء مبدأ الاقتناع الشخصي القاضي الجزائي الذي استقر القضاء على تأكيده والدليل على ذلك أنه أعاد تجسيد هذه التعليمة بصياغة جديدة وذلك في نص المادة 353 من قانون الإجراءات الجزائية الفرنسي.

[1] زيد مسعود، الاقتناع الشخصي للقاضي الجزائي، المؤسسة الوطنية للكتاب، الجزائر، 1989، ص 36.
[2] بو عامر محمد زكي، الإثبات في المواد الجنائية، الفنية للطباعة والنشر الإسكندرية 2010، ص ص 135، 136.
[3] زيد مسعود، مرجع سابق الذكر، ص 37.

2- الأساس القانوني لمبدأ الاقتناع الشخصي للقاضي الجزائي في القانون الجزائري

جاء المشرع الجزائري بنصوص واضحة وصريحة تجمد مبدأ الاقتناع الشخصي للقاضي الجزائي، فقد كرسه في المادة 307 من ق ... ج" التي تنص على ما يلي : يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة: " إن القانون لا يطلب من القضاة أن يقدموا حسابا على الوسائل التي قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا في إخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم، أوجه الدفاع عنها ولم يضع القانون لهم سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم إقناع شخصي ؟".

كما كرس مبدأ الاقتناع القضائي صراحة في المادة 212 من ق...ج التي جاء في فحواها أنه من الجائز إثبات الجرائم بأي طريقة في الإثبات الجنائي، كما أن للقاضي أن يصدر حكمه بناء على اقتناعه الخاص، بالإضافة إلى أن المحكمة العليا تحرص على ضرورة مراعاة إعمال مبدأ الاقتناع الشخصي للقاضي الجزائي أمام محكمة الجنايات، وهو الأمر الذي أكدته من خلال العديد من قراراتها.

الفرع الثاني: الضوابط التي تحكم اقتناع القاضي بالدليل الالكتروني

بينا فيما سبق بأن تقدير قيمة الدليل الجنائي بما فيه الدليل الرقمي يعود إلى قناعة القاضي الذي يتمتع بسلطة واسعة في تقديره للأدلة، حيث المشرع ترك له الحرية في هذا المجال ويظهر ذلك من خلال سلطته التقديرية، فالأصل أن القاضي يتحرى عن الحقيقة بكافة الأدلة دون إلزامه بقيمة مسبقة الدليل ما، غير أن المشرع لم يترك حرية القاضي مطلقة بل وضع لها ضوابط فهي بمثابة صمام أمان إزاء انحراف القاضي عند ممارسته سلطته.[1]

فقد كان من الضروري وضع ضوابط وقيود يتعين أن تمارس سلطة القاضي في نطاقها، حتى لا تنحرف عن الغرض الذي يبتغيه المشرع، ولذلك حددت أغلب التشريعات الأدلة التي تقبل في إثبات بعض الجرائم بنصوص خاصة كجريمة الزنا، كما تدخل المشرع أحيانا للإلزام القاضي الجنائي بإتباع طرق إثبات خاصة في بعض المسائل مراعاة لطبيعة هذه المسائل من جهة، وحتى لا يكون في نظرها اما القاضي الجنائي هروب من الإجراءات المتبعة في مثلها أمام القضاء المختص أي الغير الجنائي من جهة أخرى.[2]

[1] رشيدة بوبكر، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري والمقارن، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت، 2012، ص ص 507- 508.

[2] زيد مسعود، مرجع سابق الذكر، ص ص 131- 132.

أولا: الضوابط المتعلقة بمصدر الاقتناع الدليل الرقمي نفسه

تقيد الضوابط المشتقة من الدليل الرقمي نفسه سلطة القاضي في تقديره له، واهم هذه الضوابط تتعلق بضرورة تأسيس الاقتناع القضائي على أدلة رقمية صحيحة مقبولة، والى ضرورة مناقشة الدليل الرقمي في الجلسة مع ضرورة وجود أصل الدليل الرقمي في أوراق الدعوى، وهذا كالاتي:

1- تأسيس اقتناع القاضي الجزائي على أدلة رقمية صحيحة: إن القاضي الجزائي ليس حرا في تقدير الدليل الرقمي أيا كان بل هو حر في تقدير الدليل الرقمي المقبول في الدعوى ولكي يكون الدليل صحيحا لا بد من توفر شروط محددة ولو انه متفق على أهمها ضمنيا مع اختلاف في بعض هذه الشروط من تشريع إلى آخر.

فالمنظمة الدولية لدليل الحاسوب وضعت المعايير المطلوبة في الدليل الرقمي وتمت المصادقة عليها خلال المؤتمر الدولي للبحث المعلوماتي والجريمة التقنية المنعقد في نوفمبر عام 1999، وهذه المعايير هي:

- ✓ عدم تغير الدليل أثناء ضبطه.
- ✓ أن تتم عملية الضبط من قبل شخص مؤهل في المعلوماتية الشرعية.
- ✓ جميع النشاطات المتعلقة بالضبط والوصول والتخزين ونقل الدليل الرقمي، يجب أن تكون موثقة ومحفوظة بغرض التدقيق.
- ✓ أن يكون الشخص الذي بحوزته الدليل الرقمي مسئولا عن جميع الإجراءات المتعلقة بهذا الدليل
- ✓ أن تكون الجهات المسؤولية عن ضبط وتخزين ونقل الدليل الرقمي والوصول إليه مسؤولية عن تطبيق هذه المبادئ.

أما المشرع الجزائري فانه لم يحدد صراحة شروط قبول الدليل الرقمي، إلا أنه وبعد الاطلاع على نص المادة 06 من القانون 09-04 السالف الذكر يتبين بان المشرع أكد على ضرورة السهر على سلامة المعطيات في المنظومة المعلوماتية أثناء التفتيش عنها وحجزها وكذا عدم المساس بها في حالة إعادة تشكيل هذه المعطيات لاستعمالها في التحقيق ما يوضح النظرة التشريعية الهادفة نحو حماية الأدلة في صورتها الحقيقية وبمفهوم المخالفة فان تعرضها لأي إتلاف سيؤدي حتما إلى فقدان مشروعيتها ومصداقيتها كوسيلة إثبات[1].

[1] مدربل كريم، الاثبات الرقمي في المسائل الجزائية، مذكرة ماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم والسياسية، جامعة أكلي محند أولحاج، البويرة، 2019، ص79.

2- أن يكون الدليل الرقمي قد طرح في جلسة المناقشة

إن أهم الضوابط في الإجراءات الجزائية انه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح للمناقشة في الجلسة وهو ما يطلق عليه تسمية وضعية الدليل ومعنى ذلك أن يكون الدليل أصل ثابت في أوراق الدعوى وان تمنح للخصوم فرصة الاطلاع عليه ومناقشته[1].

لقد كرس مبدأ ضرورة مناقشة الأدلة في الجلسة في اغلب التشريعات الإجرائية فهو يعد ضمانة للمتهم، فلا يجوز للقاضي الجزائي الاستناد في حكمه إلى أي دليل لم يطرح للمناقشة و التمحيص، ولقد كرس المشرع الجزائري على هذا المبدأ ضمن الفقرة الثانية من المادة 212 ق...ج.ج التي نصت على أنه: " ...لا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه[2]"، ويترتب على الإخلال بهذا الشرط بطلان الحكم المبني على دليل لم يطرح للمناقشة، أو لم تتح للخصوم فرصة إبداء الرأي فيه.

وهذا يعني أن الأدلة الرقمية المتحصلة لإثبات الجرائم المعلوماتية سواء كانت مطبوعة أم اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية أو مصورات، فلمية كلها ستكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال البيئة الإلكترونية يجب أن يعرض في جلسة المحكمة ليس من خلال ملف الدعوى في التحقيق الابتدائي وإنما يعرض بصفة مباشرة أمام القاضي.[3]

وعليه يترتب من شرط مناقشة الدليل الرقمي أن يكون اقتناع القاضي أثناء إصدار الحكم مبني على عقيدته وليس على اقتناع غيره، فلا يجوز أن يبني اقتناعه استنادا إلى معلوماته الشخصية أو رأي غيره، لأن القناعة المتولدة لدى القاضي هي جزء من مناقشة الأدلة والتي عن طريقها تتضح قوة أو ضعف الأدلة، فيبني القاضي قناعته من خلال الأخذ بها أو باستبعادها.[4]

وبغية تمكين المحكمة وأطراف الخصومة من مناقشة الدليل الرقمي يجب تهيئة قاعة المحكمة بالأجهزة والوسائل المناسبة لعرض الأدلة الرقمية، وأن يكون القضاة والمدعي العام وأطراف الخصومة على دراية بالمسائل الفنية ذات الصلة، نظرا لما يتطلبه هذا النوع من الأدلة من الإلمام بالتكنولوجيا

---

[1] عائشة بن قارة، مرجع سابق الذكر، ص 272.

[2] نظر المادة 2 / 212 من الأمر 66 -155متضمن ق...ج.ج، معدل و متمم، السالف الذكر

[3] مدربل كريم، مرجع سابق الذكر، ص 80.

[4] معمش زهية، غائم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية 2012-2013، ص 74

المتخصصة التي تتميز بالدقة والتعقيد، ويمكن استدعاء الشهود والخبراء الفنيين لمناقشتهم في كيفية تحصيل هذه الأدلة ومدى مصداقيتها.

ثانيا- الضوابط التي يخضع لها اقتناع القاضي

بالإضافة إلى الضوابط التي تخضع لها أدلة الرقمية، هناك ضوابط أخرى متعلقة باقتناع القاضي وسلطته التقديرية وذلك أثناء إصدار حكمه، إذ يجب أن يكون النطق بحكمه مبنيا على الجزم واليقين وأن يبنى اقتناعه من الأدلة التي أعتمد عليها بعيدا عن الغموض والإبهام، أي بناء الاقتناع على الجزم واليقين.

إن القاعدة العامة في الإثبات الجزائي أن الأحكام تبنى على الجزم واليقين ولا تبنى على الظن والاحتمال وأن المحكمة ملزمة في حالة وجود شك أن تحكم ببراءة المتهم طبقا للقاعدة القائلة بأن: الشك يفسر لصالح المتهم باعتبارها إحدى النتائج الايجابية لقرينة البراءة[1].

وقد كرس دستور 1996 هذا المبدأ في المادة 45 بنصها على كل شخص يعتبر بريئا حتى تثبت جهة قضائية نظامية إدانته مع كل الضمانات التي يتطلبها القانون، لذلك قضي بأن الأحكام الجزائية تبنى على الجزم واليقين لا على الشك والافتراضات.

وإذا كان القاضي الجنائي يستطيع الوصول إلى اليقين بالمعرفة الحسية أو العقلية عن طريق التحليل والاستنتاج، فإن الجزم بوقوع الجريمة المعلوماتية ونسبتها إلى المتهم المعلوماتي تحتاج من القاضي نوع آخر من المعرفة وهي المعرفة العلمية بالأمور المعلوماتية خصوصا أن القاضي الجنائي يلعب دورا إيجابيا في الإثبات، ويؤدي الجهل في هذه الأمور إلى التشكيك في قيمة الدليل الرقمي، وبالتالي يقضي إلى الحكم بالبراءة ويستفيد من هذا الشك المتهم المعلوماتي مما يؤدي إلى إفلات المجرمين من تطبيق العدالة والقانون، ومن ثم يترتب على ثبوت التهمة بلوغ الاقتناع بالإدانة درجة اليقين من طرف القاضي الجنائي لأن الاقتناع ثمرة اليقين.

المطلب الثاني: تأثير الدليل الرقمي على قناعة القاضي

نظرا لتطور العلمي الذي عرفه المجال الجنائي ومع بروز أدلة علمية حديثة، من بينها نجد الدليل الرقمي الذي يعد كأفضل دليل الإثبات الجرائم الالكترونية وذلك يعود إلى نقص الثقافة العلمية، والأخذ به يجب توافر شروط مصداقيته، وكذا الاستعانة بأهل الخبرة والفصل في النزاعات في حالة ما استعصى عليه الأمر، ولهذا سنتطرق في هذا المطلب إلى مصداقية الدليل الرسمي، كذا القيمة العلمية الدليل الرقمي وتأثيره على قناعة القاضي.

[1] مدربل كريم، مرجع سابق الذكر، ص 82.

الفرع الأول: مصداقية الدليل الرقمي في الاثبات

إذا كان لدليل الرقمي في الإثبات قيمة الآليات من الناحية العلمية، يجب توافر شروط مصداقيته، ولكن هذا لا يمكن أن بسيط عن موضوع الشك من حيث سلامة العبث به من جهة، وكذا صحة الإجراءات المتبعة في الحصول عليه من جهة أخرى.

أولا: يقينية الدليل الرقمي

اليقين هو عبارة عن حالة ذهنية أو عقلية تؤكد وجود الحقيقة، ويتم الوصول الى ذلك عن طريق ما نستخلصه من وسائل الإدراك المختلفة للقاضي ما يقدم اليه من وقائع الدعوى، وما ينطبع في ذهنه من تخيلات ذات درجة عالية، لذلك عندما يصل القاضي إلى اليقين فإنه يصبح في المرحلة مقتنعا بالحقيقة.

ويصل القاضي إلى يقينية المخرجات المقدمة تكرها عن طريق المعرفة الحسية التي تدركها الحواس من خلال معاينتها لهذه المخرجات وعن طريق المعرفة العقلية التي يتم كمن خلالها استخلاص واستقراء الحقيقة التي تهدف إليها، ويجب أن يصدر حكمه استنادا اليها.[1]

ونظرا لطبيعة التقنية التي يتميز بها الدليل الرقمي الا انه هناك قواعد محددة، تم وضعها من طرف المختصين التي تحكم يقينيتها ومن بينها استعمال الوسائل الفنية تكون من طبيعة هذا الدليل تكمن في فحص سلامة وصحة الإجراءات المتبعة للحصول عليه.

أ- تقييم الدليل من حيث سلامة العبث به:

للتأكد من سلامة العبث بالدليل الرقمي يجب أن تتبع عدة طرق منها:

- علم الكمبيوتر يلعب دورا مهما في تقديم المعلومات الفنية التي تساهم في فهم مضمون الدليل الرقمي، وهذا النوع من العلوم تتم الاستعانة به في الكشف عن مدى تلاعب بمضمون هذا الدليل، وفكرة التحليل التناظري الرقمي تبدوا من الوسائل المهمة للكشف عن مدى مصداقية الدليل، ومن خلالها يتم التأكد من عدم إمكانية حصول العبث في النسخة المستخرجة أم لا.[2]

- وهناك نوع من الأدلة الالكترونية والتي تسمى بالأدلة المحايدة، وهر من الأدلة التي لا علاقة بموضوع الجريمة، إلا أنه يساعد من التأكد من سلامة الدليل الرقمي، يجعله يقيني ولا مجال الشك فيه حتى تتم مراجعة المتهم به هذا من ناحية، ومن ناحية أخرى ضمان حقوق المتهم المعلوماتي.

[1] رشيدة بوبكر، مرجع سابق الذكر، ص 517.
[2] حمري سميرة عاشور رزيقة، مرجع سابق، ص 87.

- في حالة عدم حصول الدليل على نسخة الأصلية، أو أن الدليل وقع في حالة عبث، وقد وقع على النسخة الأصلية، فيمكن التأكد من سلامة الدليل الرقي من العبث وذلك من خلال استخدام عمليات حسابية خاصة بالخوارزميات[1].

ب- تقيم الدليل الرقمي من حيث القيمة الفنية:

من بين الإجراءات الفنية التي يمكن الاعتماد عليها التأكد من ساقية التقليل الرقي في الإثبات.

1- التأكد من صحة ودقة الأدوات المستخدمة في استخلاص الدليل الجنائي الرقمي

يتم التأكد من صحة الأدوات المستخدمة في استخلاص الدليل الرقمي بالتحقيق من مدى قدرة هذه الأدوات على عرض كافة البيانات المتعلقة بالدليل الرقمي، وكذلك خضوعها الأدوات الاختيار، فمن خلاله يمكن أن تتأكد من أن الأدلة لا تعرض بيانات إضافية جديدة[2].

ومن خلال هذا الاختيارين تتأكد من الأدلة المستخدمة عرضت على البيانات المتعلقة بالدليل الرقمي، وبالتالي لم يضف اليه أي بيان جديد ويعطي نتائج مقدمة عن طريق جهاز الكمبيوتر مصداقية في الدليل على الواقع.

2- الاعتماد على الأدوات التي أثبتت الدراسات العلمية كفاءتها في تقديم افضل

لقد بينت الدراسات العلمية في مجال تقنية المعلومات على الطريقة الواجب اتباعها في الحصول على الدليل الرقمي وفي المقابل أوضحت الدراسات الأدوات المشكوك في كفاءتها وهذا ساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات[3].

ثانيا: مناقشة الدليل

تتم مناقشة الدليل على مبدأ تقوية المرافعات، وهذا طبقا لنص المادة 212 ق.ج التي تنص على أنه لا يسوع القاضي أن بيتي قراره إلا على الأدلة المقدمة له في المرافعات والتي حصلت المناقشة فيها حضوريا أمامه.[4]

من خلال هذه نجد أن القاضي يعتمد في الحكم على الاجتهاد، ولا يعتمد على رأي الغير إلا إذا كان ذلك من الخبراء المتخصصين، هذا قد تطرقا اليه في المطلب الأول من هذا المبحث[5].

---

[1] كحيل خير الدين إثبات الجريمة الالكترونية، مذكرة الماستر تخصص قانون جنائي، مسيلة 2015، ص 136.
[2] حمري سميرة عاشور رزيقة، مرجع سابق ص. 87. 81
[3] كحيل خير الدين، مرجع سابق الذكر، ص 136.
[4] كحيل خير الدين، مرجع سابق الذكر، ص 137.
[5] نور محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد 11، جامعة باتنة، 2017 ص919.

الفرع الثاني: القيمة العلمية على الدليل الرقمي وتأثيرها على قناعة القاضي

يعرف الدليل العلمي بانه ذلك الدليل التي تقام عليه تجارب علمية لإثبات أو نفي واقعة تثار فيها الشك، وقيمه يتطلب دراية خاصة لا يملكها القاضي في حكمه، وتكوينه القانوني المحضي والدليل الرقمي باعتباره تعليقا من تطبيقات الدليل العلمي لا يمكن للقاضي أن ينازع في قيمته الألبانية وتلك الامتيازات بقوة الاستدلالية من الناحية العلمية.

فتقدير القاضي برأي الخبير، فنجد أن الدليل الرقي يعتبر من الأدلة العلمية التي لا يمكن للقاضي أن ينازع في القيمة وذلك لتمتعه بقوة استدلالية، وهنالك بحجة قاطعة في الدلالة عن الوقائع التي الوضعية التي تتضمنه الأكلة، وكما يمكن القلب من مشكلة الشك في المصداقية الدليل من خلال إخضاعه التجارب تمكن منه التأكد من صحته ، و أنه لا يمكن الخلط بين الشك الذي يشوب الدليل بسبب إمكانية العين به، وكذا لوجود خطأ في الحصول عليه، وكذلك القيمة الاقتناعية به، والقاضي لا يمكن أن يفصل فيها باعتبارها مسألة فنية و رأي هنا يعود إلى الخبير، فإذا سلم الدليل من العبث و توافره فيه كل الشروط ، فإن على القاضي القبول بهذا الدليل، لذلك يرى هذا الاتجاه أن رفض القاضي الرأي الخبير فيكون تعارض مع رأيه و نفسه هو عليه فإن الدليل العلمي و منه الدليل الرقمي أصبح يقيد حرية القاضي في تقدير الأدلة، ويلزمه على الحكم حتى ولو لم مقتنعا بصحة الواقعة المطروحة أمامه.[1]

[1] سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، (رسالة ماجستير)، جامعة الحاج لخضر - باتنة - كلية الحقوق والعلوم السياسية الجزائر، 2013، ص218.

خاتمة

خاتمة |

بعد أن فرغنا من دراستنا لموضوع الإثبات الجنائي في مجال الجرائم الالكترونية فقد اتضح لنا بأن الثورة الصناعية غيرت في الكثير من المفاهيم التي كانت تسير مختلف مجالات الحياة بحيث أدت إلى ظهور العديد من العمليات التي تساعد أفراد المجتمع على تلبية حاجياتهم بسرعة وبدقة دون أي إرهاق، إلا أن هذه الثورة ادت إلى ظهور نوع جديد من الإجراء الا وهو الإجراء الكتروني والذي يعد من أخطر الجرائم في وقتنا الحالي وهذا راجع لصعوبة إثباته ويعود ذلك لكون أن الأدلة الرقمية خفية وغير مرئية، فالإثبات الجنائي في هذه الجرائم يتطلب من السلطات المختصة في البحث والتحري بأن يكونوا ملمين بالتدابير والإجراءات اللازمة لتأمين مسرح الجريمة، كما أنهم ملزمين بضبط وتحريز الآثار الجنائية الرقمية ونقلها بالطريقة العلمية الصحيحة وهذا يتطلب وجود علاقة ترابطية بين هذه السلطات والخبراء حتى يتسنى لهم القيام بعملية نقل الأدلة إلى المخبر وتحليلها وتقديمها في شكل مقروء يثبت أو ينفي إدانة المتهم، فإن تمت هذه العملية بنجاح تؤدي حتما إلى اقتناع القاضي بالحكم الصادر عنهم فهو يجعل الحقيقة العلمية حقيقة قضائية.

ومن هنا يتبين بأن الدليل الالكتروني فرض نفسه في مجال الإثبات الجنائي فهو يتمتع بقوة ثبوتية وحجية كافية في هذا المجال، ولذلك فإن القضاء الجنائي ملزم بمواكبة التطور التكنولوجي لأن الاعتماد على الإجراءات التقليدية في الحصول على الدليل الالكتروني واستخلاصه تصعب على السلطات المختصة القيام بهذه المهمة وهذا ما يؤكد بأن أجهزة التحقيق العدالة في حاجة في التدريب الفني والتقني في هذه الجرائم.

النتائج المتوصل إليها:

وعليه ومن خلال دراستنا لهذا الموضوع توصلنا إلى جملة من النتائج تتمثل فيما يلي:

- قصور أغلب التشريعات من الناحية الإجرائية ويتضح ذلك في كون أن الكثير منها يعتمد على النصوص التقليدية لحماية الحريات الشخصية وحرمة الحياة الخاصة بالرغم من أنها مقتصرة على حماية هذه الحريات من وسائل الاتصال التقليدية فقط.

- إن حجية الأدلة الجنائية في مجال الإثبات الجنائي مقيدة بمجموعة من الشروط المتعلقة بإجراءات التحقيق المخصصة لاستخلاص الأدلة الالكترونية بحيث يفرض على السلطات المختصة بأن تقوم بالحصول عليها بطريقة مشروعة.

- إن القاضي الجنائي يتمتع بالدور الإيجابي في تقدير القيمة القانونية للأدلة الالكترونية مثلها مثل باقي الأدلة.

خاتمة |

التوصيات:

وعلى ضوء هذه النتائج نخلص إلى التوصيات التالية:

- التوعية الدائمة بمخاطر الجرائم الالكترونية.

- العمل على تحقيق التعاون الدولي لمواجهة الإجرام المعلوماتي وذلك عن طريق الدخول في اتفاقيات ومعاهدات.

- الحرص على تدريب رجال البحث والتحري والخبراء والقضاة على التعامل مع الجرائم الالكترونية من الناحيتين الفنية والعلمية.

- العمل على تكريس قواعد قانونية جديدة تتناسب مع طبيعة الجرائم الالكترونية.

قائمة المراجع |

القوانين:

- قانون رقم 09-04 المؤرخ في 5 أوت 2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الجزائر، الجريدة الرسمية، العدد 47، الصادرة في 2009.
- قانون 66-155 مؤرخ في 08 يونيو سنة 1966 يتضمن قانون الإجراءات الجزائية معدل ومتمم بالأمر رقم 11-02 مؤرخ في 23 فبراير 2011.

الكتب:

- زيد مسعود، الاقتناع الشخصي للقاضي الجزائي، المؤسسة الوطنية للكتاب، الجزائر، 1989.
- محمد رمضان بازة، قانون العلويات الليبي جرائم الاعتداء على الأموال بط. القسم الخاص، الجزء الثاني، منشورات جامعة ناصر، طرابلس ليبيا، 1992.
- هشام محمد فريد رستم، قانون المطويات ومخاطر تقنية المعلومات نط مكتبة الآلات الحديثة: أسيوط مصر، 1994.
- هلالي عبد الاله، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة 1997.
- علي القهوجي، الحماية الجنائية لبرنامج الحاسب الآلي، الدار الجامعية للنشر: بيروت، 1999.
- يونس خالد عرب، العالم الالكتروني الوسائل والمحتوى والمزايا والسلبيات، منشورات اتحاد المصاريف العربية: الأردن، 2001.
- جميل عبد الباقي الصغير، الأنترنت والقانون الجنائي الاحكام الموضوعية للجرائم المتعلقة بالأنترنت، الطبعة الأولى، دار النهضة العربية، مصر، 2001.
- عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية. دار الفكر الجامعي، الاسكندرية مصر. 2004.
- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنت الجرائم الالكترونية الدراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت لبنان، 2007.
- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي، ط1، الاسكندرية 2010.
- أبو عامر محمد زكي، الإثبات في المواد الجنائية، الفنية للطباعة والنشر، الإسكندرية، 2010.
- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الالكترونية، ط 1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دار الثقافة للنشر والتوزيع، ط1، عمان، 2011.
- رشيدة بوبكر، جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري والمقارن، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت، 2012.
- هدى حامد قشقوش، السياسة الجنائية لمواجهة الجريمة المعلوماتية، دار النهضة العربية، القاهرة، 2012.
- ياسر محمد الكومى، أبو حطب، الحماية الجنائية والأمنية للتوقيع الالكتروني، منشاة المعارف، الإسكندرية، 2014.
- أحمد يوسف الطحطاوي، أدلة الالكترونية ودورها في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2015.
- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي "النظام القانوني لحماية المعلومات، دار الجامعة الجديدة للنشر الإسكندرية، د ن.

المقالات العلمية:

- ابراهيمي جمال، مكافحة الجرائم الالكترونية في التشريع الجزائري، المجلة النقدية للقانون والعلوم السياسية، المجلد 2، العدد 2، جامعة مولود معمري تيزي وزو الجزائر، 1997.
- علي حمودة، الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الانبات الجنائي، الجزء الأول، مجلة الأكاديمية شرطة دبي، العدد 1، 2003
- محمد أمين البشري، التحقيق في جرائم الحاسب والانترنت، المجلة العربية للدراسات الأمنية والتدريب، عدد 30، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.
- نور محمودي، حجية الدليل الرقمي في إثبات الجريمة المعلوماتية، مجلة الباحث للدراسات الأكاديمية، العدد 11، جامعة باتنة، 2017.

الأطروحات والمذكرات:

الدكتوراه:

- منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات، رسالة الدكتوراه في الحقوق، القاهرة، 2007.

- تومي يحي، جرائم الاعتداء ضد الافراد باستخدام تكنولوجيا الاعلام والاتصال، أطروحة دكتوراه، جامعة الجزائر 1، الجزائر، 2018.

الماجيستر:

- بوشو ليلى، قبول الدليل العلمي أمام القضاء الجنائي، مذكرة من أجل نيل شهادة الماجستير، الجزائر، 2011
- ابراهيم طه الزايد، نطاق المسؤولية الجزائية عن جرائم الذم والقدح والتحقير المرتكبة من خلال المواقع الالكترونية، مذكرة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، 2011.
- عبد الله بن عبد العزيز بن عبد الله الخثعمي، التفتيش في الجرائم المعلوماتية في النظام السعودي، رسالة ماجستير، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011.
- بن بلاغة عقيلة، حجية أدلة الإثبات الجنائية، مذكرة لنيل شهادة الماجستير في القانون فرع القانون الجنائي، جامعة الجزائر، 2011.
- طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة من أجل الحصول على شهادة الماجستير في القانون الجنائي، جامعة الجزائر، كلية الحقوق، 2012.
- سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، (رسالة ماجستير)، جامعة الحاج لخضر باتنة، كلية الحقوق والعلوم السياسية، الجزائر، 2013.
- زهير الحاج الطاهر، اليات الوقاية من الجريمة المعلوماتية، مذكرة الحصول على شهادة الماجستير قانون جنائي، كلية الحقوق، جامعة الجزائر 2013.

الماستر:

- مدربل كريم، الاثبات الرقمي في المسائل الجزائية، مذكرة ماستر، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم والسياسية، جامعة أكلي محند أولحاج، البويرة، 2019.
- هلال أمنة، الإثبات الجنائي بالدليل الإلكتروني مذكرة لنيل شهادة الماستر، جامعة محمد خيضر بسكرة، 2014.
- معمش زهية، غائم نسيمة، الإثبات الجنائي في الجرائم المعلوماتية مذكرة تخرج لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة بجاية 2013.

❖ كحيل خير الدين، إثبات الجريمة الالكترونية، مذكرة لنيل شهادة الماستر تخصص قانون جنائي، جامعة مسيلة، 2015.

المواقع الالكترونية:

– خنفوسي عبد العزيز " تجميد مبدأ حرية الإثبات الجزائي في القانون الجنائي الجزائري"، مقال منشور في الموقع الالكتروني: http://tit.com/images/no_image_card.pn

شكر وعرفان	
إهداء	
مقدمة	أ- د
الفصل الاول: اجراءات تحصيل الدليل الالكتروني في الجريمة الالكترونية	
تمهيد	
المبحث الأول: الإطار المفاهيمي للجريمة الالكترونية	
المطلب الأول: مفهوم الجريمة الالكترونية	
الفرع الأول: تعريف الجريمة الالكترونية	
أولا: التعريف الضيق للجريمة الالكترونية	
ثانيا: التعريف الموسع للجريمة الالكترونية	
ثالثا: تعريف الجريمة الالكترونية في التشريع الجزائري	
الفرع الثاني: خصائص الجريمة الالكترونية	
المطلب الثاني: أساليب الجريمة الالكترونية	
المبحث الثاني: إجراءات تحصيل الدليل الالكتروني	
المطلب الأول: الاجراءات التقليدية للحصول الدليل الالكتروني	
الفرع الأول: المعاينة والتفتيش في الجريمة الالكترونية	
أولا: المعاينة في الجريمة الالكترونية	
ثانيا: التفتيش في الجريمة الالكترونية	
الفرع الأول: الخبرة والضبط في الجريمة الالكترونية	
أولا: الخبرة في الجريمة الالكترونية	
ثانيا: الضبط في الجريمة الالكترونية	
المطلب الثاني: الإجراءات المستحدثة للحصول على الدليل الالكتروني	
الفرع الأول: التسرب الالكتروني	
الفرع الثاني: المراقبة واعتراض المراسلات	
أولا: المراقبة الالكترونية	
ثانيا: اعتراض المراسلات	
الفرع الثالث: حفظ وإفشاء المعطيات	

الفرع الرابع: معوقات اثبات الجريمة الالكترونية	
الفصل الثاني: القيمة الثبوتية للدليل الالكتروني امام القضاء	
تمهيد	
المبحث الأول: حجية الدليل الالكتروني أمام القضاء الجنائي	
المطلب الأول: مشروعية الدليل الالكتروني	
الفرع الاول: مشروعية الدليل في الوجود	
أولا: نظام الاثبات المقيد	
ثانيا: الثبات الحر	
ثالثا: الثبات المختلط	
الفرع الثاني: مشروعية في التحصيل	
المطلب الثاني: موقف المشرع الجزائري من انظمة الاثبات	
المبحث الثاني: سلطة القاضي الجزائي في تقدير الدليل الإلكتروني	
المطلب الأول: مبدا اقتناع القاضي بالدليل	
الفرع الأول: مضمون مبدا الاقتناع الشخصي للقاضي	
الفرع الثاني: الضوابط التي تحكم اقتناع القاضي بالدليل	
المطلب الثاني: تأثير الدليل على قناعة القاضي	
الفرع الأول: مصداقية الدليل في الإثبات	
الفرع الثاني: القيمة العلمية على الدليل وتأثيرها على قناعة القاضي	
خاتمة	
قائمة المراجع	
الفهرس	