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

كلية الحقـــوق والعلـــــوم السياسية
قسم الحقوق
رقم: 68

ميدان: الحقـــوق والعلـــــوم السياسية
فرع: حقوق
تخصص: قانون جنائي والعلوم الجنائية

مذكرة مقدمة لنيل شهادة الماستر أكاديمـــي

إعداد الطالب(ة): بشير حماني

تحت عنوان

خصوصية التحقيق
في الجريمة الإلكترونية

لجنة المناقشة:

د/ الطيب بلواضح	جامعة محمد بوضياف المسيلة	رئيســـا
د/ محمد مقيرش	جامعة محمد بوضياف المسيلة	مشرفا ومقررا
د/ نور الدين بن حميدوش	جامعة محمد بوضياف المسيلة	مناقشا

السنة الجامعية: 2019/2018


بسم الله الرحمن الرحيم
١٤٢٠

الإهداء

إلى من أوصاني بهما ربي برا وإحسانا والدي أمي وأبي

رحمهما الله

إلى من كان لهم فضل رعايتي أعمامي

الشريف وموسى حفظهما الله

إلى رفيقة دربي زوجتي العزيزة

إلى رياحين قلبي بنتي ريان وولديا محمد إلياس وعبد الرؤوف

إلى كل أهلي وأقاربي

شكر وتقدير

يشرفني أن أتقدم بأسمى آيات الشكر والعرفان إلى

أستاذي الفاضل الدكتور مقيرش محمد

الذي كان له فضل

الإشراف على هذا البحث،

كما لا يفوتني أن أخلص بالشكر

إلى كل الطاقم البيداغوجي الذي أشرف على تدريسي.

وكل من أعانني على إنجاز هذه الدراسة

ولو بالكلمة الطيبة

قائمة المختصرات

- ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري.
- ق.ع.ج.: قانون العقوبات الجزائري.
- ج. ر.ج.ج: الجريدة الرسمية للجمهورية الجزائرية.
- ف: فقرة.
- ط: الطبعة.
- ص: صفحة.
- ب ص: بدون صفحة.

مقدمـــــة

أضحى العالم مجتمع معلوماتي كبير فالبشرية حاليا تشهد ما ينعت بالثورة المعلوماتية الصناعية، فهي التي حولت العالم إلى ما أضحى إليه اليوم من مجتمع معلوماتي كبير، تتدفق المعلومات بين أرجائه في يسر وسرعة من خلال شبكات كثيفة ومترابطة من الحسابات ووسائل الاتصال - المحلية والإقليمية والدولية - ويزداد فيه الاعتماد على الكمبيوتر لتخزين واسترجاع ومعالجة المعلومات وأداء الخدمات الحيوية في شتى ميادين الحياة. وقد أدى تقدم وانتشار النظم المعلوماتية وتزايد الاعتماد عليها في مجالات الحياة إلى تزايد فرص ارتكاب الجرائم الإلكترونية (المعلوماتية)، خاصة في ظل تبني بعض الدول ومنها الجزائر لمشروع الحكومة الإلكترونية [1] الذي يهدف إلى تقديم جميع الخدمات إلى المواطنين إلكترونيا عن طريق استخدام الأنظمة المعلوماتية.

فالخطورة التي تتميز بها هذه الجرائم المستحدثة هي أنها سهلة الارتكاب نتيجة للاستخدام السلبي للتقنية المعلوماتية بما توفره من تسهيلات، وأن آثارها ليست محصورة في النطاق الإقليمي لدولة بعينها، فضلا على أن مرتكبيها يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الآلية للمعطيات والإلمام بالمهارات والمعارف التقنية، ليس هذا فحسب بل إنها تستهدف محلا من طبيعة خاصة ونعني بذلك المعلومات التي يحتوي عليها نظام المعالجة الآلية، والذي هو عبارة عن إشارات ونبضات إلكترونية تنساب عبر أجزاء نظم المعالجة الآلية وشبكات الاتصال العالمية بصورة آلية، الأمر الذي بات يثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة (أجهزة العدالة الجنائية بجميع مستوياتها وعلى اختلاف أدوارها) وبالذات فيما يخص إثبات هذه الجرائم وآلية مباشرة إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمهم للعدالة.

فبقدر ما أسعدت هذه التقنيات الحديثة الإنسانية بتوفيرها للراحة والمساهمة في الرفع من المستوى المعرفي والاقتصادي لمختلف شعوب العالم فإن المخاطر التي جلبتها بات أثرها ملموسا ومحسوسا، فإساءة استخدام شبكة الإنترنت مهد الطريق للمجرم الإلكتروني أو المعلوماتي من إشباع رغباته الإجرامية، بسبب طابعها الخاص المتمثل في صعوبة التعرف عليه وصعوبة إثباتها، ومن هنا ظهرت إلى الوجود أنواع جديدة من الجرائم تختلف تماما عن الجرائم التقليدية ومنها: جرائم اختراق المواقع والأنظمة المعلوماتية، جرائم التجسس والتنصت باستخدام الإنترنت، جرائم التهديد والسرقة والاحتيال بالإنترنت، جرائم الآداب العامة، جرائم المساس بالأديان، وانتهاك الحريات الخاصة، جرائم تبييض الأموال والاتجار بالمخدرات عبر الإنترنت وغيرها كثيرا وهي في تطوير وتغيير سريع.

[1] - الحكومة الإلكترونية هو نظام حديث تتبناه الحكومات باستخدام الشبكة العنكبوتية العالمية في ربط مؤسساتها بعضها ببعض، وربط مختلف خدماتها بالمؤسسات الخاصة، والجمهور عموما، ووضع المعلومة في متناول الأفراد وذلك لخلق علاقة شفافة تتصف بالسرعة والدقة تهدف للارتقاء بجودة الأداء.

إن إدراك ماهية الجرائم الإلكترونية والطبيعة الموضوعية لهذه الجرائم واستظهار موضوعها وخصائصها ومخاطرها وسمات مرتكبيها ودوافعهم، يتخذ أهمية لسلامة التعامل مع هذه الظاهرة ونطاق مخاطرها الاقتصادية والأمنية والاجتماعية والثقافية.

فإذا كانت الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين معتادة على التعامل مع الجريمة بصورتها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثار مادية في مسرح الجريمة من بصمات أو آثار أقدام أو بقع دم أو محررات مزورة. ..، فإن المشكلات الإجرائية التي ستواجه هذه الجهات عند تعاملها مع الجريمة المعلوماتية، تبدأ من طبيعة البيئة الافتراضية للتقنية التي ترتكب فيها، فهي لا تخلف أي آثار مادية محسوسة، كما أن هذه الجريمة تتم في الخفاء، فكثيرا ما يعمد المجرم المعلوماتي إلى إخفاء نشاطه الإجرامي عن طريق تلاعبه بالبيانات والذي غالبا ما يتحقق في غفلة من المجنى عليه، فضلا عن سهولة تدمير الدليل ومحوه من مسرح الجريمة مما يعقد أمر كشفها وتحديد مرتكبها.

كما أن الجانب الإجرائي الخاص بمواجهتها يعرف نوعا من الصعوبات والإشكالات العملية، خاصة أثناء مرحلة البحث والتحري أو ما يطلق عليها بمرحلة جمع الاستدلالات، ومرحلة التحقيق أو أثناء إجراءات المحاكمة، ونظرا لم تتميز به أدلة هاته الجرائم عن كونها غير مرئية وليست مادية، مما لا يتم في أغلب الأحيان التبليغ عنها، أي كثيرا ما تبقى في الكتمان، كما أن مسرح الجريمة الذي ترتكب فيه هذه الجرائم يختلف عن ذلك الذي ترتكب فيه الجرائم التقليدية.

ومن المشاكل الإجرائية التي تواجه تلك الفئة، كيفية التفتيش والضبط والمعاينة في العالم الافتراضي، وكيفية التعامل مع الشكاوى والبلاغات التي غالبا ما تسجل ضد مجهول في هذا العالم الافتراضي، وهل هاته الإجراءات التقليدية كفيلة بالبحث والتنقيب عن الجريمة والمجرم الإلكتروني وضبط الدليل الذي يثبت تورطه؟ وما هي الصعوبات التي يجابها التحقيق في هذا النوع من الجرائم؟ لنصل إلى ضرورات إجرائية فرضها عالم الرقمنة والتقنية العالية وحنكة ودهاء المجرم في هذا المجال، تمثلت هذه الضرورة في إيجاد إجراءات جديدة تتماشى وطبيعة الإجرام المرتكب، مع ضرورة مراعاة مدى احترام حقوق الإنسان والحريات العامة والضمانات الممنوحة للمشتبه فيهم والمكفولة دستوريا وقانونيا أثناء إعمال هذه القواعد الإجرائية

وهو العامل الذي كان حاسما لتدخل المشرع بنصوص قانونية إجرائية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، ليمكن من خلالها استنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم ووسائل ارتكابها، مما أدى إلى ظهور نوع جديد من الأدلة يمكن الاعتماد عليه في إثبات هذه الجرائم من ذات الطبيعة التقنية التي تتميز بها البيئة محل الجريمة المعلوماتية. وقد كان ذلك بأن قام المشرع الجزائري بتعديل قانون الإجراءات الجزائية بموجب القانون 06 - 22 المؤرخ في 20 ديسمبر 2006،

بالإضافة إلى إصداره للقانون 09 - 04 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيات الإعلام والاتصال ومكافحتها، ومن خلالهما أوجد المشرع طرقا إجرائية تتفق والطبيعة التقنية للجريمة المعلوماتية.

ولعل الصعوبات التي يثيرها موضوع الدراسة تكمن في صبغته التقنية والإجرائية فلا يكفي في معالجة الموضوع أن يكون الباحث متخصص في القانون بل يجب أن يكون على دراية بالجوانب الفنية للحاسب الآلي، وترجع الصعوبة أيضا في قلة المراجع المتوفرة حول الجرائم الإلكترونية ومحدوديتها خاصة منها المتخصصة في القواعد الإجرائية لمواجهتها وفي الإثبات الإلكتروني، وندرة التطبيقات القضائية في هذا المجال، نظرا لحداثة هذا الموضوع نسبيا على الساحة القانونية لاتصاله بجانب تقني فني يتمثل بالنظام المعلوماتي بشقيه المادي والمعنوي، أضف إلى ذلك أن الجرائم الإلكترونية بصفة عامة لا يمكن حصرها، فتكنولوجيا المعلومات متطورة ومتغيرة مما يؤثر بدوره على الجريمة الإلكترونية، كما تشكل معنوية أو لا مادية الدليل حاجزا كبيرا أمام إثبات الجريمة المعلوماتية والبحث عن الأدلة وكذا التعرف على المجرمين، نظرا لسهولة تطاير ومحو الدليل في مدة وجيزة أو تشفيره، مما يخلق معه صعوبات جمة تعترض عملية الإثبات في مجال المعلوماتية

في نهاية بحثي أخلص إلى معالجة بعض المسائل المتعلقة بالدليل الإلكتروني من حيث قيمته القانونية ومدى حجيته في الإثبات، ومدى اقتناع القاضي الجزائي به، أين أستوضح مسألة نظام الإثبات الذي يعتمده القاضي الجزائي الجزائري، لأصل إلى التعرف عن أثر تبني القاضي الجزائي لنظام الإثبات الجزائي.

إشكالية البحث:

من خلال ما تم عرضه بصورة ملخصة لأهم المسائل المراد التطرق إليها، تقودني هاته الدراسة إلى طرح الإشكالية الرئيسية التي مفادها ما مدى فعالية القواعد الإجرائية الجزائية المنتهجة، التي أوجدها المشرع الجزائي الجزائري في ضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس، في ظل التشريعات الجزائية الحديثة، وهل هي كفيلة باحتواء متغيرات هذا النمط المتجدد والمتطور؟

وإذ أنا بصدد البحث في هذه الإشكالية الجوهرية صادفتني تساؤلات يعتبر البحث فيها أمرا ضروريا للإجابة عن جوهر موضوع الدراسة والتي منها:

* ما هي الجريمة الإلكترونية وسماتها العامة؟

* ما هي الصعوبات والمعوقات التي قد تواجه جهات البحث والتحري والتحقيق في استخلاص الدليل الرقمي؟

* إلى أي مدى يمكن الاعتماد على الإجراءات التقليدية الحديثة في استخلاص الدليل الإلكتروني في الأوساط الافتراضية؟

* ما مدى حجية المخرجات الإلكترونية في الإثبات نظرا لطبيعتها الخاصة بالمقارنة بوسائل الإثبات التقليدية؟

* كيف تعامل المشرع مع هذا الدليل الرقمي في مجال الإثبات الجزائي من حيث كونه دليلا علميا وأثر هذه الخاصية على مبدأ الاقتناع الشخصي للقاضي الجزائي؟

* هل تنصرف السلطة التقديرية التي يتمتع بها القاضي الجزائي الجزائري في إثبات الجرائم الإلكترونية إلى الأدلة المستخرجة من الوسائل الإلكترونية أو ما يسمى بالأدلة الإلكترونية الرقمية؟

أهداف البحث:

* التعرف على الجريمة الإلكترونية وبيان أركانها.

* التعرف على طرق إثبات الجريمة الإلكترونية وحجية الدليل الإلكتروني أمام القضاء الجزائي.

* التعرف على موقف المشرع الجزائي الجزائري من الدليل الإلكتروني.

* التعرف على طرق التحقيق في هذا النوع من الجرائم، ذلك أن حداثة الجرائم المعلوماتية وما تتسم به من خصائص سوف يجد معه المحقق نفسه في حيرة أمامها وكيفية التعامل معها وأسلوب التحقيق فيها، إذ لشك أن إجراءات التحقيق وجمع الأدلة بخصوص هذه الجرائم يختلف عما هو الحال عليه في الجرائم التقليدية.

* التعرف على أثر تبني القاضي الجزائي لنظم الإثبات الجزائي.

منهج البحث المعتمد في هذه الدراسة:

اعتمدت في بحثي المنهج الوصفي كأصل، بالإضافة إلى منهج أخر تكميلي وهو المنهج التحليلي.

فالمنهج الوصفي يظهر من خلال قيامي بوصف ظاهرة الجريمة المعلوماتية وتحديد بعض المفاهيم التي تقوم عليها، وكذا وصف المفاهيم الخاصة بالإجراءات المنتهجة في استخلاص الدليل الإلكتروني من خلال الرجوع إلى المراجع القانونية العامة والمتخصصة والرسائل والدراسات والاتفاقيات الدولية ذات الصلة.

المنهج التحليلي حاولت في هذا البحث تحليل بعض المفاهيم والغوص في جزئياتها وطرحها بشكل من التفصيل والتشريح لما بدا لي من أهميتها، مثلما كان الحال في إجراء تفتيش المنظومة المعلوماتية.

أسباب اختيار البحث:

لقد وقع اختياري على دراسة موضوع خصوصية التحقيق في الجريمة الإلكترونية بالرغم مما يكتنفه من صعوبات، إيمانا مني بأهمية هذا الموضوع للوقوف على هذا النمط المستحدث من الجرائم الذي بدأ يغزو مجتمعاتنا مع زيادة استخدام الأنظمة المعلوماتية مناحي الحياة كلها، والوقوف على حقيقة التعامل مع الجريمة المعلوماتية من الناحية الإجرائية.

خطة البحث:

واتساقا مع ما سبق، ومن أجل معالجة الإشكالية المطروحة، ولاستكمال الإجراءات المنهجية المتبعة في هذا البحث بدا لي قد يكون من الصواب أن يسير تصميمه في الخطوات الثلاث الآتية:

أن أتناول في المبحث التمهيدي ماهية الجريمة الإلكترونية وسماتها، أين قسمته إلى مطلبين: المطلب الأول تكلمت فيه عن مفهوم الجريمة الإلكترونية، أركانها وخصائصها، والثاني مراحل تطور الجريمة الإلكترونية، تصنيفاتها ومواجهتها.

وفي الفصل الأول من البحث، تعرضت فيه بالدراسة إلى إجراءات التحقيق في الجرائم الإلكترونية ومعوقاته، حيث تناولت في المبحث الأول إجراءات التحقيق في الجرائم الإلكترونية، والآخر معوقات (صعوبات) التحقيق في الجرائم الإلكترونية.

أما الفصل الثاني، استرسلت في كيفية استخلاص الدليل الإلكتروني وقيمته الثبوتية، بحيث عالجت في المبحث الأول ماهية الدليل الإلكتروني والقواعد الإجرائية لاستخلاصه، ثم عرجت على القيمة الثبوتية للدليل الإلكتروني وحجيته في إثبات الجريمة الإلكترونية في المبحث الثاني منه.

لأتوصلت في أخر دراستي لعدد من النتائج والاقتراحات، تم إدراجها في خاتمة بحثتي.

المبحث التمهيدي

ماهية الجريمة الإلكترونية وسماتها

الجريمة الإلكترونية، جريمة حديثة نسبيا، لارتباطها بتكنولوجيا المعلومات المتطورة، فقد وجدت تعاريف مختلفة لها، كما أنها تتسم بمجموعة من الخصائص والسمات التي تميزها عن غيرها من الجرائم الأخرى، وأن هذه الجريمة ترتكب من قبل أفراد من ذوي الاختصاص في مجال تقنية المعلومات، أو على الأقل لديه حد أدنى من المعرفة والقدرة على استعمال جهاز الحاسب والتعامل مع شبكة الإنترنت [1].

في هذا المبحث أتطرق إلى مفهوم الجريمة الإلكترونية، أركانها وخصائصها وذلك في المطلب الأول منه، لأعرج من خلال المطلب الثاني إلى مراحل تطور الجريمة الإلكترونية، تصنيفاتها ومواجهتها.

[1] - نهلا عبد القادر المومني - الجرائم المعلوماتية - دار الثقافة للنشر والتوزيع الأردن - طبعة 2010 - ص - 47.

المطلب الأول: مفهوم الجريمة الإلكترونية، أركانها وخصائصها.

عصر الأنترنت أو عصر السموات المفتوحة أو عصر التكنولوجيا الرقمية أو المعلوماتية كل هذه الأوصاف تعبر عن مدى ضخامة القفزات العلمية الهائلة التي تحققت ومدى تنوع الإنجازات التي طرحت ثمارها بشكل ملحوظ في حياتنا في الآونة الأخيرة، إلا أن هذا الوجه المشرق لتقنية المعلومات أخل في جانبه المظلم وولد معه عالم رهيب من الإجرام المعلوماتي أستغل لتحقيق مصالح ومآرب تتنوع وتتعدد.

فنتناول في الفرع الأول من هذا المطلب مفهوم الجريمة الإلكترونية وفي الفرع الثاني نتعرف على أركانها وخصائصها.

الفرع الأول: مفهوم الجريمة الإلكترونية

أتناول في بحر هذا المطلب من خلال الفرع الأول منه أهم التعريفات التي أسندت على موضوع الجريمة، وفي الفرع الثاني أهم التعريفات التي أسندت على وسيلة الجريمة، لنعرج في الفرع الثالث من ذات المطلب على تفرد الجريمة الإلكترونية.

أولا: أهم التعريفات التي أسندت على موضوع الجريمة

تعددت التعريفات الخاصة بالجريمة الإلكترونية واختلفت الاتجاهات في هذا الأمر بين موسع لمفهوم الجريمة المعلوماتية وبين مضيق لها، وبدورنا نتطرق إلى أهم التعاريف التي وضعت، وهناك من أسند تعريفها على موضوع الجريمة والبعض أسندها على وسيلة الجريمة، وهو الأمر الذي أتطرق من خلاله إلى تعريف الجريمة الإلكترونية.

أو هي " كل جريمة أو سلوك غير مشروع يستخدم بالحاسب الآلي، أو محاولة نسخ أو حذف أو إتلاف لبرامج الحاسب الآلي، أو أي جريمة يكون لتنفيذها صلة بالقواعد والعلوم المعلوماتية أو أي سلوك غير مشروع متعلق بالمعالجة الآلية للبيانات"[1].

تعرف الجرائم المعلوماتية أو الرقمية بأنها " كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات" [2].

وعرفها البعض على أنها " مجموعة من الأفعال غير المشروعة التي تتعلق بالمعالجة الإلكترونية للمعلومات أو نقلها ".

[1] - نايل نبيل عمر- الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية - دار الجامعة الجديدة - مصر - طبعة 2012 ص 23.

[2] - أنيس حسيب السيد المحلاوي،الخبرة القضائية في الجرائم المعلوماتية والرقمية، دراسة مقارنة، دار الفكر الجامعي، الطبعة 2016 - ص 40

ويعرفها البعض بأنها " فعل أو أفعال غير مشروعة تتم بواسطة أو تستهدف النظم البرمجية أو النظم المعالجة الإلكترونية للحاسب الآلي أو الشبكات الحاسوبية أو شبكة الإنترنت وما على شاكلتها "وعلى ذلك فتتنوع الجرائم الإلكترونية وتتعدد لدرجة تصعب على الحصر، ما بين التزوير والتزييف الرقمي المعلوماتي، تدمير وإتلاف البرامج والبيانات والمعلومات والسطو على البيانات والمعلومات، والاحتيال الرقمي، والتجسس. ..إلخ.

و عرفت منظمة التعاون الاقتصادي والتنمية والخاص باستبيان الغش المعلوماتي عام 1982 والذي أوردته بلجيكا في تقريرها الجرائم المعلوماتية بأنها " كل فعل أو امتناع من شأنه الاعتداء على الأمور المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل تقنية المعلومات ".

ثانيا: أهم التعريفات التي أسندت على وسيلة الجريمة

على حسب هذا المعيار تعرف الجريمة الإلكترونية على أنها " كل سلوك غير مشروع يرتبط بإساءة استخدام الحاسب الآلي ويؤدي إلى تحقيق أغراض غير مشروعة "

و على أنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية"

كما تعرف بأنها " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكذلك تعرف بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا ".

وإنها " كل فعل أو امتناع من شانه الاعتداء على الأمواج المادية او المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية "

و قد عرفته المذكرة التفسيرية في اتفاقية بودابست في القسم الأول منها في العنوان الأول يلي ذلك العنوان من 2- 4 وهي التي يستخدم الحاسب الآلي بها كأداة اعتداء وليس محلا للاعتداء بذاته، وهي جرائم الغش المعلوماتي وجرائم المحتوى وأعني بها الجرائم التي تستهدف شريحة معينة من الأشخاص كعرض المواد الإباحية والمواد المتعلقة بالسلوك، مختتمة بجرائم التعدي على الملكية الفكرية وهي جرائم التعرض على المصنفات الموجودة على الإنترنت([1]).

أما إذا ما تم التعرض للتعريف الأمني لجرائم الحاسب لوجدنا أنها كل جريمة أو سلوك غير مشروع يستخدم بالحاسب الآلي، أو محاولة نسخ أو حذف أو إتلاف لبرامج الحاسب الآلي، أو أي جريمة يكون لتنفيذها صلة بالقواعد والعلوم المعلوماتية أو أي سلوك غير مشروع متعلق بالمعالجة الآلية للبيانات.

[1] - نايل نبيل عمر، المرجع السابق، ص 22 - 23

ثالثا: تفرد الجريمة الإلكترونية

إن الجرائم الإلكترونية تنفرد بخصائص تميزها عن باقي الجرائم، وذلك لارتباطها الآلي وبأسلوب ارتكابها، ولفهم أكثر هذا الجانب نتطرق إلى دوافع ارتكاب الجريمة الإلكترونية ومن ثم سنستخلص هذه الميزة الخاصة بها والتي تجعلها تتفرد وتتميز عن غيرها من الجرائم

و هي كالآتي:

* دافع مادي، أي تحقيق الثراء، فالربح المتحصل من الجريمة المعلوماتية يساوي أضعاف الربح المتحصل في مختلف الجرائم التقليدية، كالسرقة، التخريب والإتلاف.

* دافع عقلي والذي يعني إثبات التميز العلمي، لأن مختلف البرامج العلمية لها من الصعوبة في اقتحامها أو تخريبها وتثير التحدي في كيفية إتلافها.

* دافع البحث العلمي، وإن كان هذا الدافع يصعب إستعابه كدافع إجرامي إلا أن شرحه المبسط له يكشف عن غموض يكتنفه، فالشركات أو الباحثين العلميين قد يتجهوا للمتابعة الغير المشروعة للمعلومات للوصول إلى ما يوفر لهم البيانات الكافية لأبحاثهم، وهذا الدافع يجمع معه مجموعة من الجرائم الأخرى التي سنتناولها في دراستنا كجريمة السرقة الإلكترونية أو الإتلاف للمعلومات والتي تكون موجهة لبرامج الحماية الإلكترونية الموضوعة للدفاع عن الحاسب الآلي.

* إن الجريمة الإلكترونية، بحسب اتفاقية بودابست هي تبدأ بالولوج غير القانوني سواء كان على الحاسب الآلي أو على جزء منه، وبأي غرض كان، وتقرر المذكرة التفسيرية أن الهدف من تحديد أركان الجريمة المعلوماتية هو حماية أمن وسرية وسلامة البيانات المخزنة على الحاسب الآلي للحد من تكاليف إصلاح هذا الاعتداء ومشاكله [1].

الفرع الثاني: أركان الجريمة الإلكترونية، خصائصها وصعوباتها

أسترسل في بحر هذا المطلب لأركان الجريمة الإلكترونية في الفرع الأول منه، وللخصائص التي تتميز بها في الفرع الثاني، ثم في الفرع الثالث صعوباتها.

أولا: أركان الجريمة الإلكترونية

أركان الجريمة الإلكترونية مثلها مثل الجريمة العادية لها ركن شرعي ومادي ومعنوي.

[1] - أ / ناير نبيل عمر المرجع السابق ص 25،22

1 - الركن الشرعي

معناه اعتراف المشرع والنص على تجريم الفعل المرتكب وهو ما نصت عنه المادة الأولى من قانون العقوبات بقولها " لا جريمة ولا عقوبة أو تدبير أمن بغير قانون " بالنسبة للتشريع الجزائري فقد أحدث في قانون العقوبات في القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات([1]).

2 - الركن المادي

يتكون الركن المادي للجريمة الإلكترونية من السلوك الإجرامي والنتيجة والعلاقة السببية، علما أنه يمكن تحقق الركن المادي دون تحقق النتيجة، كالتبليغ عن الجريمة قبل تحقيق نتيجتها، (مثلا: إنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة إلا أنه لا مناص من معاقبة الفاعل)

يتخذ الركن المادي في هذه الجريمة عدة صور، بحسب كل فعل إيجابي مرتكب، (مثلا: جريمة الغش المعلوماتي: الركن المادي فيها هو تغيير الحقيقة في التسجيلات إلكترونية أو المحررات الإلكترونية.

3 - الركن المعنوي

يتكون الركن المعنوي للجريمة الإلكترونية من عنصريها العلم وإرادة([2]).

– العلم: هو إدراك الفاعل للأمور.

– أما الإرادة: فهي اتجاه السلوك الإجرامي لتحقيق النتيجة. طبقا للمبادئ العامة المعروفة في قانون العقوبات، قد يكون القصد الجنائي عاما وخاصا، القصد الجنائي العام: هو الهدف المباشر للسلوك الإجرامي وينحصر في حدود ارتكاب الفعل. أما القصد الجنائي الخاص: هو ما يتطلب توافره في بعض الجرائم دون الأخرى فلا يكتفي الفاعل بارتكابه الجريمة، بل يذهب إلى التأكد من تحقيق النتيجة (مثلا: في جريمة القتل لا يكتفي الجاني بالفعل بل يتأكد من إزهاق روح المجني عليه). وعليه ما هو القصد الجنائي الذي يجب توافره في الجريمة الإلكترونية؟

الأصل إن الفاعل في الجريمة الإلكترونية يوجه سلوكه ألإجرامي نحو ارتكاب فعل غير مشروع أوغير مسموح به مع علمه وقاصدا ذلك ومهما يكن لا يستطيع انتفاء علمه كركن للقصد الجنائي العام.

[1]-أنظر قانون العقوبات الجزائري، القسم السابع مكرر، المعنون بـ "المساس بأنظمة المعالجة الآلية للمعطيات"، إعتبارا من المادة 394 مكرر إلى غاية المادة 394 مكرر 08.

[2]- محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، بدون رقم الطبعة، دار النهضة العربية، القاهرة 1992. ص4 و13

إذن فالقصد الجنائي العام متوافر في جميع الجرائم الإلكترونية دون أي استثناء ولكن هذا لا يمنع أن بعض الجرائم الإلكترونية تتوافر فيها القصد الجنائي الخاص، مثلا: جرائم تشويه السمعة عبر الإنترنيت، وجرائم نشر الفيروسات عبر الشبكة. وفي كل الأحوال يرجع الأمر للسلطة التقديرية للقاضي.

ثانيا: خصائص الجريمة الإلكترونية

للجريمة الإلكترونية مجموعة من الخصائص هي كالآتي:

* سرعة التنفيذ والتنفيذ عن بعد.

* سهولة إخفاء الجريمة.

* سهولة ارتكابها بعيد عن الرقابة الأمنية.

* عالمية الجريمة.

* قمة الذكاء في ارتكابه

* متعدية الحدود أي عابرة للحدود.

* أسلوب ارتكابها، فهي جرائم هادئة بطبيعتها لا تحتاج إلى العنف.

* تتم عادة بتعاون أكثر من شخص.

* جرائم ناعمة: فهي لا تحتاج إلى مجهود عضلي في ارتكابها كالقتل، السرقة، وغيرها، بل تعتمد على المجهود الذهني المحكم، والتفكير العلمي المدروس القائم عن معرفة تقنية ممتازة بالحاسب الآلي، والتعامل السليم بالشبكة،

* عدم التبليغ عند وقوع الجريمة بواسطة الإنترنت حيث نجد ان بعض المجني عليهم يمتنعون عن إبلاغ السلطات المختصة خشية على السمعة والمكانة واهتزاز الثقة.

* علاوة عن ذلك فهناك خصائص فرعية للجرائم الإلكترونية منها أنها لا تترك أثر بعد ارتكابها، صعوبة الاحتفاظ الفني بأثارها إن وجدت، تحتاج إلى خبرة فنية.. إلخ [1].

[1] - أمير فرج يوسف - الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت - مكتبة الوفاء القانونية - الإسكندرية -الطبعة الأولى 2011 ص 18.

ثالثا: صعوبات الجرائم الإلكترونية

إن أهم الصعوبات التي تتميز بها الجرائم الإلكترونية ما يلي [1]:

* صعوبة التحكم في تحديد حجم الضرر الناتج عنها.

* مرتكبي الجرائم الإلكترونية من بين فئات متعددة نجعل التنبؤ بالمشتبه بهم أمرا صعبا.

* الضخامة البالغة للبيانات الرقمية المتعين فحصها أثناء التحريات.

* داركنت: الشبكة السوداء واستعمال الهوية المخفية. darkent

* استعمال خدمات إخفاء الهوية مما يسمح القيام بالجريمة دون الوصول إلى هوية الفاعل.

* استعمال بروتوكولات تشفير معقدة مما يؤدي إلى صعوبة قراءة البيانات.

* دلائل الإثبات الرقمية في معظم القضايا تكون ضمن خوادم خارج التراب الوطني serveur

* المعاملة المتصلة بالجريمة السبريانية معقدة وسريعة التطور.

* الحاجة الكبيرة إلى كفاءات وأدوات وتقنيات متخصصة.

* ضعف التشريع الدولي في مجال مكافحة الجريمة المعلوماتية مما أدى إلى صعوبة التنسيق بين الدول ويرجع ذلك إلى القيود المتصلة بالتحقيق عبر الحدود.

* أدلة الإدانة في هذه الجرائم غير كافية ويرجع ذلك إلى عدة عوامل تتمثل في عدم وجود أي أثر كتابي إذ يتم نقل المعلومات بالنبضات الإلكترونية [2].

المطلب الثاني: مراحل تطور الجريمة الإلكترونية، تصنيفها ومواجهتها

عرفت الجرائم الإلكترونية تطورا لا يستهان به، وهي كثيرة حيث لم يوضع لها معايير محددة من أجل تصنيفها مما أدى إلى صعوبة إثباتها، وهذا راجع إلى التطور المستمر للشبكة والخدمات التي تقدمها، وعليه خصصنا هذا المطلب لمراحل تطور الجرائم الإلكترونية من خلال الفرع الأول، وتصنيف الجرائم الإلكترونية في الفرع الثاني، والمواجهة التشريعية للجرائم الإلكترونية في الفرع الثالث.

[1] - محاضرة بعنوان (الجريمة السبريانية كنوع من الجرائم المستحدثة) مديرية الشرطة القضائية، 2018

[2] - أنيس حسيب السيد المحلاوي . الخبرة القضائية في الجرائم المعلوماتية والرقمية - دراسة مقارنة - دار الفكر الجامعي- الطبعة 2016. ص 51

الفرع الأول: مراحل تطور الجريمة الإلكترونية

مر تطور الجرائم الإلكترونية بمرحلتين، مرحلة ظهور الكمبيوتر وربطه بالشبكة وهو ما نتناوله في الفرع الأول من هذا المطلب، ثم نعرج على المرحلة الثانية من تطور الجريمة الإلكترونية والمتعلقة بظهور الفيروسات الإلكترونية في الفرع الثاني.

أولا: مرحلة ظهور الكمبيوتر وربطه بالشبكة

ظهر استخدام الكمبيوتر وربطه بالشبكة في الستينيات إلى السبعينيات، أين ظهرت أول معالجة لجرائم الكمبيوتر في شكل مقالات صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي، وشكلت موضوع التساؤل إذا ما كانت هذه الجرائم مجرد حالة عابرة أم ظاهرة جرمية مستجدة؟ وهل هي جرائم بالمعنى القانوني أم مجرد سلوكيات غير أخلاقية في مجال المعلوماتية؟، فبقيت محصورة في إطار السلوك اللاأخلاقي دون النطاق القانوني ومع توسع الدراسات تدريجيا وخلال السبعينات بدأ الحديث عنها كظاهرة إجرامية جديدة.

ثانيا: مرحلة ظهور الفيروسات

في بداية الثمانينات، تأكد مفهوم جديد لجرائم الكمبيوتر والإنترنت حيث ارتبطت هذه الأخيرة بعمليات اقتحام نظام الكمبيوتر عن بعد وأنشطة نشر وزرع الفيروسات الإلكترونية التي تقوم بعملية تدمير كلي للملفات أو البرامج، وشاع اصطلاح "الهاكرز " المعبر عن مقتحمي النظم وكذا المجرم المعلوماتي المتفوق.

شهدت فترة التسعينات تناميا هائلا في حقل الجرائم الإلكترونية وتغييرا في نطاقها ومفهومها وكان ذلك بفعل ما أحدثته شبكة الأنترنت من تسهيلات لعمليات دخول الأنظمة واقتحام شبكة المعلومات ظهرت أنماط جديدة وخطيرة في ذات الوقت[1].

بحيث نمت الإنترنت بشكل مذهل خلال هذه الفترة، بعد ما كانت مجرد شبكة أكاديمية صغيرة وتحولت إلى بيئة متكاملة للاستثمار والعمل والإنتاج والإعلام والحصول على المعلومات، وفي البداية لم يكن ثمة اهتمام بمسائل الأمن بقدر ما كان الاهتمام ببناء الشبكة وتوسيع نشاطها، دون مراعاة تحديات أمن المعلومات، فالاهتمام الأساسي ارتكز على الربط والدخول ولم يكن الأمن من بين الموضوعات الهامة في بناء الشبكة. وهذه الثغرة التي شجعت تنامي الجريمة الإلكترونية وتسببت في أضرار بالغة، وهو ما أدى إلى لفت النظر الى حاجة شبكة الإنترنت إلى توفير معايير من الأمن، وبدأ التفكير

[1] - فضيلة عاقلي، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس يومي 24-2017/03/25. الموقع الإلكتروني JILRC. COM، بدون صفحة.

مليا في الثغرات ونقاط الضعف. وعليه قد يكون الكمبيوتر هدفا للجريمة، وغايته المعلومات المخزنة والسيطرة على النظام دون التصريح والسرقة والاعتداء على الملكية الفكرية. .. إلخ.

كما قد يكون الكمبيوتر محلا للجريمة، كحالة استغلال الكمبيوتر للإستلاء على أموال الغير بإجراء تحويلات غير شرعية. كما أن الكمبيوتر قد يعد أداة للجريمة، كحالة تخزين البرامج المنسوخة أو في حالة استخدامه لنشر المواد غير قانونية.

الفرع الثاني: تصنيف الجرائم الإلكترونية

إن الجرائم الإلكترونية جرائم متعددة ومتنوعة، ويستعصى حصرها بسهولة، بحيث توجد عدة تصنيفات لجرائم الحاسب الآلي والإنترنت فهناك من يصنفها بحسب الفئات مثل جرائم ترتكب على نظم الحاسب الآلي، أو بحسب الأسلوب المتبع في الجريمة أو الباعث الدافع لارتكابها، غير أننا يمكن أن نجمل الجرائم التي وردت في أغلب التشريعات كما يلي[1]:

أولا: تصنيف الجرائم الإلكترونية تبعا لنوع المعطيات ومحل الجريمة: وتشمل:

1 - الجرائم الماسة بقيمة معطيات الحاسوب.

2 - الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة كالإطلاع على المراسلات الإلكترونية والإدلاء بالبيانات الكاذبة في إطار المعادلات والعمليات الإلكترونية.

3 - الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (برامج قرصنة البرمجيات).

ثانيا: تصنيف الجرائم تبعا لدور الحاسب الآلي في الجريمة: وتشمل:

1 - الجرائم التي تستهدف عناصر (السرية والسلامة وموفورية المعطيات والنظم) تضم: الدخول غير المصرح به (غير المشروع)، الاعتراض غير القانوني، تدمير المعطيات (صناعة الفيروسات أو نشرها)، إساءة استخدام الأجهزة. الغش أو التغيير في مواصفات وخصائص تقنية المعلومات.. إلخ.

2 - الجرائم المرتبطة بالحاسب الآلي وتظم: التزوير الرقمي المعلوماتي، الاحتيال الرقمي المعلوماتي.

3 - الجرائم المرتبطة بالمحتوى أو المضمون وتضم: الجرائم المتعلقة بالأفعال الإباحية والأخلاقية والإخلال بالنظام العام (الجرائم المتعلقة بأمن الدولة وسلامتها الداخلية والخارجية)، إنشاء أو نشر مواقع بقصد ترويج أفكار وبرامج مخالفة للنظام العام والآداب، انتهاك المعتقدات الدينية أو حرمة الحياة الخاصة، الإساءة إلى السمعة، والمخدرات وغسيل الأموال... إلخ.

4- الجرائم المرتبطة بالإخلال بحق المؤلف وقرصنة البرمجيات والإرهاب المعلوماتي.

[1] - أنيس حسيب السيد المحلاوي . المرجع السابق ص43

ثالثا: تنصيف الجرائم تبعا لمساسها بالأشخاص والأموال:

1 - طائفة الجرائم التي تستهدف الأشخاص وتظم: الجرائم غير الجنسية التي تستهدف الأشخاص، طائفة الجرائم الجنسية التي تستهدف الأشخاص، كالقتل بالحاسب الآلي.

2 - طائفة جرائم الأموال - عدا السرقة - أو الملكية المتضمنة أنشطة الاختراق والإتلاف.

3 - جرائم الاحتيال والسرقة وخيانة الأمانة كالاعتداء على الأموال الإلكترونية سواء أكان في إطار التجارة الإلكترونية أو غيرها مثل الدخول لمواقع البنوك والدخول لحسابات العملاء وإدخال بيانات أو مسح بيانات بغرض اختلاس الأموال أو تحويلها لآخر[1].

4 - جرائم التزوير مثل تزوير أو تقليد التوقيع الإلكتروني.

5 - جرائم المقامرة والجرائم الأخرى ضد الأخلاق والآداب.

6 - جرائم الحاسب الآلي ضد الحكومة[2].

مما لا شك فيه إننا بأمس الحاجة إلي التشدد في مواجهة منتهكي حقوق الملكية الفكرية خاصة وأن القوانين ذات العلاقة لم تجرم الأفعال التي تتم بإساءة استخدام تقنية المعلوماتية هذا من ناحية ومن ناحية أخري أن قانون حماية المؤلف والحقوق المجاورة الوطني لا زال قاصرا في مواجهة هذه الانتهاكات.

[1] - محمد طارق عبد الرؤوف الخن - جريمة الاحتيال عبر الإنترنت (الأحكام الموضوعية والأحكام الإجرائية) - منشورات الحلبي الحقوقية - لبنان طبعة 2011 ص.

[2] - عرفت الأستاذة عفيفي كامل عفيفي في مؤلفها- جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون - دراسة مقارنة -منشورات الحلبي الحقوقية - طبعة 2003 ص 22. على أن " الحاسوب هو آلة حسابية تستقبل البيانات ثم تقوم عن طريق الاستعانة ببرنامج معين بعملية تشغيل هذه البيانات للوصول إلى النتائج المطلوبة

- كما أن الحاسوب هو عبارة عن مجموعة الأجهزة الإلكترونية تقوم بصورة أوتوماتيكية باستقبال البيانات وتخزينها ومعالجتها واستخراج النتائج تحت سيطرة تعليمات مخزنة فيها.

- ويطلق على مجموعة الأجهزة التي تشكل الكيان المادي لنظام الحاسوب لفظ hard ware أي المعدات ويطلق على مجموعة الأوامر أو التعليمات لفظ soft ware أي البرمجيات وهذه المعدات والبرمجيات تستخدم من قبل الأشخاص لتحقيق أهداف خاصة بهم.

الفرع الثالث: المواجهة التشريعية للجرائم الإلكترونية

نستعرض في هاته النقطة القوانين العامة والخاصة التي أخصها المشرع الجزائري لتنظيم الجريمة الإلكترونية، ثم نتطرق إلى مشكلات إثباتها.

أولا: القوانين العامة المنظمة للجريمة الإلكترونية والعقوبات المقررة لها

1: القوانين العامة

أ - الدستور: كفل دستور الجزائر لسنة 1996 [1] وكذا التعديل الطارئ عليه بموجب القانون المعدل له سنة 2016 حماية الحقوق الأساسية والحريات الفردية، وعلى أن تضمن الدولة عدم انتهاك حرمة الإنسان. وقد تم تكريس هذه المبادئ الدستورية في التطبيق بواسطة نصوص تشريعية أوردها قانون العقوبات وقانون الإجراءات الجزائية وقوانين خاصة أخرى والتي تحظر كل مساس بهذه الحقوق. ومن أهم المبادئ الدستورية العامة نذكر:

المادة 38: الحرّيّات الأساسيّة وحقوق الإنسان والمواطن مضمونة

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

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

ب- **قانون العقوبات**:[2] لقد تطرق المشرع الجزائري إلى تجريم الأفعال الماسة بأنظمة الحاسب الآلي وذلك نتيجة تأثره بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام مما دفع المشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون رقم 04 - 15 المؤرخ في 10 نوفمبر 2004 المتمم لأمر رقم 66-15 المتضمن قانون العقوبات تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى 394 المادة مكرر7.

[1] - القانون رقم 16 - 01 المؤرخ في 06 مارس 2016 المتضمن تعديل دستوري لدستور 1996 الصادر بالجريدة الرسمية رقم 76 بتاريخ 07 مارس 2016.

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

وفي عام 2006 أدخل المشرع الجزائري تعديل آخر على قانون العقوبات بموجب قانون- رقم 06 - 23 المؤرخ في 20 ديسمبر 2006 حيث مس هذا التعديل القسم السابع مكرر والخاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وقد تم تشديد العقوبة المقررة لهذه الأفعال فقط دون المساس بالنصوص، الواردة في هذا القسم من القانون 04 - 15 وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل التكنولوجيا المعلومات وانتشار الأنترنت كوسيلة لنقل المعلومات.

ب/1- أنواع الجرائم الإلكترونية في قانون العقوبات الجزائري والعقوبات المقرر لها

طبقا لقانون العقوبات الجزائري المعدل والمتمم والذي استحدث فيه المشرع قسما خاصا في القسم السابع مكرر من الفصل الثالث الخاص بالجنايات والجنح ضد الأموال تحت عنوان أنظمة المعالجة الآلية للمعطيات، وعلى هذا الأساس يمكن تصنيف الجرائم الإلكترونية كالآتي([1]):

* الغش أو الشروع فيه، في كل أو جزء من المنظومة للمعالجة الآلية للمعطيات

* حذف أو تغيير لمعطيات المنظمة.

*إدخال أو تعديل في نظام المعطيات.

* تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار.

* حيازة أو إفشاء أو نشر أو استعمال المعطيات.

* تكوين جمعية أشرار.

من خلال المواد القانونية السابقة والتي تمثل الركن الشرعي للجريمة الإلكترونية في التشريع الجزائري يمكن تكييف هذه الأفعال المجرمة بأنها جرائم ضد أموال الغير والمضرة بالمجتمع وهي تعتبر من ضمن جرائم الاختلاس وخيانة الأمانة والنصب غير السرقة لاعتبار أن السرقة فعل الاستيلاء على مال الغير ماديا.

ب/2 - العقوبات المقررة للجريمة الإلكترونية

طبقا لقانون العقوبات وبناء على المواد 12،11 و13 من الاتفاقية الدولية للإجرام المعلوماتي فإن العقوبات المقررة للإجرام المعلوماتي يجب أن تكون رادعة وتتضمن عقوبات سالبة للحرية والتي تتمثل في عقوبات أصلية وعقوبات تكميلية تطبق على الشخص الطبيعي، والشخص المعنوي.

1- أنظر المواد من 394 مكرر وما يليها من قانون رقم 04 - 15 المؤرخ في 10 نوفمبر 2004،المعدل والمتمم لأمر رقم 66 - 15 المتضمن قانون العقوبات .

ب/2/أ - العقوبات المطبقة على الشخص الطبيعي

ب/2/أ/1 - العقوبات الأصلية: عقوبة الحبس تتراوح مدتها من شهرين إلى ثلاثة سنوات [1]، حسب الفعل المرتكب والغرامة تتراوح قيمتها من خمسين ألف دج إلي واحد مليون دج، حسب الفعل المرتكب: الدخول والبقاء بالغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك (الجريمة البسيطة)،الدخول والبقاء بالغش (الجريمة المشددة)

وتضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة، الاعتداء العمدي على المعطيات، إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام.

ب/2/أ/2 - العقوبات التكميلية: خص المشرع عقوبة المصادرة لهذا النوع من الجرائم تشمل الأجهزة والبرامج والوسائل المستخدمة في ارتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية، وإغلاق المواقع والأمر يتعلق بالمواقع (les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية، وإغلاق المحل أو مكان الاستغلال غذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الإلكتروني الذي ترتكب منه الجرائم شرط توافر عناصر العلم لدى مالكها وهو ما نصت عنه المادة 394 مكرر 06.

ب/2/أ/3 - عقوبة الشروع في الجريمة: جاءت به المادة 11 من الاتفاقية الدولية للإجرام المعلوماتي واعتمده المشرع الجزائري في قانون العقوبات، بالنسبة للجرائم الماسة بالأنظمة المعلوماتية ،بحيث توسع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية ،إذ أصبح الشروع بموجب نص المادة 394 مكرر 07 منه معاقب عليه بنفس عقوبة المقررة على الجنحة ذاتها.

ب/2/أ/4 - الظروف المشددة: نص قانون العقوبات في المواد 394 مكرر و394 مكرر3 على الظروف تشدد بها عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول والبقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة، أو إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات العامة.

ب/2/ب - العقوبات المطبقة على الشخص المعنوي

تبعا لنص المادة 394 مكرر 4 من ق ع ج يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها ،كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه.

وبالتالي عقوبة الشخص المعنوي تتمثل في الغرامة التي تعادل خمس مرات الحد الأقصى المقررللشخص الطبيعي.

[1] - أنظر المواد من 394 مكرر إلى المادة 394 مكرر 08 من ق ع ج

علما أن نص المادة 18 مكرر من القانون 04 - 15 المتضمن قانون العقوبات تحدد المسؤولية الجزائية للشخص المعنوي والعقوبات المقررة.

ب/2/ج - عقوبة الاتفاق الجنائي (الاشتراك)

تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية، وعقوبة الاشتراك في الاتفاق تكون نفس عقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم تكون العقوبة هي عقوبة الجريمة الأشد[1].

ج: قانون الإجراءات الجزائية الجزائري

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

كما نص على التفتيش في المادة 45 الفقرة 7 من نفس القانون المعدلة حيث أعتبر إن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم الإلكترونية. ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة 6 وكذا على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5 ،كما أن قانون الإجراءات الجزائية نص على أنه لا يجوز ضبطها إلا في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة. غير أنه طبقا لقانون الإجراءات المعدل والمتمم في الفصل الرابع تحت عنوان" في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور ". نصت المادة (65 مكرر5 ف 3) على أنه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص أن يأذن بالاعتراض ووضع ترتيبات تقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة. أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة التقليدية.

[1] - فضيلة عاقلي - المرجع السابق ب ص

[2] - الأمر رقم 66 - 155 المؤرخ في 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم، بالقانون رقم17-07 المؤرخ في 27 مارس 2017، الجريدة الرسمية، رقم 20 بتاريخ 29 مارس 2017.

ثانيا: القوانين الخاصة للتصدي للجرائم الإلكترونية

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

2: قانون التأمينات[2]: تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي،في نصوص قانونية عديدة تخص البطاقة الإلكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني،وكذا للجزاءات المقررة في حالة الاستعمال غير المشروع أو من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الإلكترونية للمؤمن له اجتماعيا أو في المفتاح الإلكتروني لهيكل العلاج أو في المفتاح الإلكتروني لمهن الصحة للبطاقة الإلكترونية حسب المادة 93 مكرر2.

3: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

جاء هذا القانون منظما للجرائم المتصلة بتكنولوجيا الإعلام والاتصال وكل ما يتعلق بالمنظومة المعلوماتية، والمعطيات المعلوماتية، ومقدمو الخدمات، والمعطيات المتعلقة بتسيير

الاتصالات الإلكترونية. من مراقبة وتفتيش المنظومات المعلوماتية عند الضرورة،و حجز المعطيات المعلوماتية، وحفظ المعطيات المتعلقة بحركة السير. على الالتزامات الخاصة بمقدمي خدمة الإنترنت، وأخيرا على إنشاء مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3].

[1] - القانون رقم 03 - 2000 المؤرخ في 05 / 08 / 200 المتضمن القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الصادر في الجريدة الرسمية العدد 48 المؤرخة في 05 غشت 2000.

[2] - قانون رقم 08 - 01 المؤرخ في 23 يناير 2008 يتمم القانون رقم 83 - 11 المؤرخ في 02 يوليو 1983 والمتعلق بالتأمينات الاجتماعية والصادر بالجريدة الرسمية رقم 04 بتاريخ 27 يناير 2008.

[3] - المرسوم رقم 90 - 04 المؤرخ في 16 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47 بتاريخ 05 غشت 2009

ثالثا: مشكلة إثبات الجريمة الإلكترونية

الجريمة الإلكترونية ظاهرة إجرامية مستجدة تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها وأنماط السلوك الإجرامي المجسدة للركن المادي لكل جريمة على حدى، مع تطور أنماطها يوما بعد يوم وما أتاحته الشبكة من فرص جديدة لارتكابها، مما جعل إثباتها من العقبات التي يعمل الخبراء على كسرها من أجل إيجاد وسائل إثبات ناجعة على أساس أنها تتطلب خبرة فنية عالية واعتماد أسلوب واضح في التحقيق ومن الأسباب التي تصعب اكتشاف وإثبات الجائم الإلكترونية نذكر مايلي:

1 - تمتاز الجرائم المعلوماتية بصعوبة الاكتشاف وإثباتها وذلك نظرا لعدم ترك الجاني آثار تدل على إجرامه، فالجرائم التي تتم بواسطة إدخال الرموز والأرقام، هي رموز دقيقة ويصعب اكتشافها وإثباتها لهذا عادة ما يتم اكتشافها بالصدفة.

2- فالجريمة المعلوماتية لا تترك آثارا ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية، يتم فيها نقل المعلومات وتناولها بواسطة نبضات إلكترونية غير مرئية.

3- كذلك وسيلة التنفيذ فيها تتسم في أغلب الحالات بالطابع التقني الذي يضفي عليها الكثير من التعقيد ومن ثم فإنها تحتاج إلى خبرة فنية يصعب على المحقق التقليدي التعامل معها، لأنها تتطلب إلماما خاصا بتقنيات الكمبيوتر ونظم المعلومات.

4- يصعب العثور على دليل مادي للجريمة وذلك راجع إلى استخدام الجاني وسائل فنية وتقنية معقدة لا يستغرق إلا ثواني معدودة يتم فيها محو الدليل والتلاعب به.

5- تتطلب خبرة وتحكما في التكنولوجيا المعلوماتية عند متابعتها، ولذلك لا يستطيع رجال الضبطية القضائية التعامل باحترافية ومهارة أثناء البحث والتحري، لابد أن يكون المحقق متخصص حتى لا يتسبب في إتلاف الدليل الإلكتروني.

6- عدم وجود تعاون دولي، فكما بينا سابقا قد يتم السلوك الإجرامي في بلد معين ولكن النتيجة تحدث في بلد أخر ليس بالضرورة أن ينتج هذا السلوك أثاره في بلد المجرمين.

7- اختلاف النظم القانونية، وبالتالي عدم الاتفاق على الفعل المجرم، فما هو محظور في الجزائر من الناحية الأخلاقية مباح في غيرها من الدول.

8- التطور السريع للجريمة والمعالجة البطيئة لقضايا ،استفادة المجرم من هذه العقبات للعبث ولهذه الأسباب وكذا الطبيعة الخاصة التي تتسم بها الجريمة أدى ببعض التشريعات الى تبنى الخبرة والمعاينة كأسلوبين للإثبات والتحقيق وكشف الجريمة والتخريب والاستمرار في الجريمة[1].

[1] - فضيلة عاقلي - المرجع السابق، ب ص

الفصل الأول

إجراءات التحقيق في الجريمة الإلكترونية ومعوقاته

إن للتحقيق أهمية في إثبات وقوع الجرائم وإقامة الدليل على مرتكبيها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل عليه اسمه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة.

حيث أوكل المشرع الجزائي الجزائري لأجهزة مهمة البحث والتحري عن الجرائم الإلكترونية، هاته الأخيرة وفي سبيل التحقيق في الجرائم الإلكترونية وملاحقة مرتكبيها جنائيا تعرف العديد من المعوقات والعقبات التي من شانها أن تعرقل الوصول إلى الكشف عن الجريمة وإثباتها، بل قد تؤدي إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وفي أدائه، وتنعكس أيضا على المجرم نفسه، فيشعر بأن الجهات الأمنية غير قادرة على كشف أمره والتصدي له.

وهو ما أحاول أن أستوضحه بنوع من التفصيل في هذا الفصل، حيث أتطرق إلى إجراءات التحقيق في الجرائم الإلكترونية في المبحث الأول منه، أما المبحث الثاني أتناول فيه معوقات (صعوبات) التحقيق في الجرائم الإلكترونية.

المبحث الأول: إجراءات التحقيق في الجرائم الإلكترونية

التحقيق الجنائي في الجرائم الإلكترونية هو نشاط قانوني يتعلق بإجراءات ضبط الجرائم والبحث عن مرتكبيها وجمع الاستدلالات التي يتطلبها التحقيق والدعوى الجنائية، فهو الضبط القضائي للجاني والدليل على إدانته أو براءته، ودور المحقق يتلخص في تلقي البلاغ وجمع الاستلالات ضد مرتكب الجريمة لجهات التحقيق القضائي بأدلة الإدانة.

فإجراءات التحقيق القضائي تمر بثلاث مراحل هي:

1 - مرحلة جمع الاستدلالات بواسطة مأموري الضبطية القضائية المختصين بالبحث في الجرائم الإلكترونية.

2 - مرحلة التحقيق الابتدائي بمعرفة النيابة العامة أو قاضي التحقيق لتحريك الدعوى العمومية أو حفظ التحقيقات لعدم كفاية الأدلة.

3 - مرحلة التحقيق النهائي والتي تكون خلال مرحلة المحاكمة[1].

إلا أن إجراءات التحقيق تعرف في بعض الأحيان معوقات وصعوبات نظرا لوقوع الجريمة الإلكترونية ضمن بيئة رقمية كامنة في أجهزة الحاسب الآلي والخوادم (serveur) والشبكات بمختلف أنواعها، مما يجعل عملية الحصول عل الدليل الإلكتروني ليس بالهين، الأمر الذي يترك معه أجهزة البحث والتحري ترفع تحدي في تطبيق القواعد الإجرائية لأجل استخلاص الدليل. وعليه أستعرض في المطلب الأول ماهية التحقيق في الجرائم الإلكترونية، وفي المطلب الثاني الأجهزة المكلفة بالبحث والتحري عن الجريمة الإلكترونية.

المطلب الأول: ماهية التحقيق في الجريمة الإلكترونية

إن التحقيق كما يدل اسمه عليه هو استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة. وكما تم التنويه عنه أن الدعوى الجزائية تمر بمرحلتين، مرحلة التحقيق ومرحلة المحاكمة، وتمر عملية التحقيق بمرحلتين أيضا، مرحلة التحقيق الأولي ومرحلة التحقيق الابتدائي. فالمرحلة الأولى وهي مرحلة جمع الاستدلالات التي يباشرها أعضاء الضبط القضائي، والمرحلة الثانية تدخل في اختصاص قاضي التحقيق[2]

[1] - مصطفى محمد موسى - التحقيق الجنائي في الجرائم الإلكترونية - مطابع الشرطة - القاهرة - الطبعة الأولى 2009 ص 165

[2] - سعيداني نعيم، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، تخصص علوم جنائية، جامعة الحاج لخضر- باتنة، السنة الجامعية 2012- 2013 ص 102

الفرع الأول: تعريف التحقيق:

تعريف التحقيق في الجريمة الإلكترونية لا يختلف عنه في الجرائم الأخرى، وعليه أتطرق إلى تعريفه لغة وقانونا، ثم إلى تعريف المحقق الذي يشرف على إجراءات التحقيق.

أولا: لغة: التحقيق مأخوذ من حقق يحقق تحقيقا، حقق الظن بالله صدقه، الأمر أحكمه - مع فلان - في قضيته: أخذ رأيه فيها.

ثانيا: تعريف التحقيق اصطلاحا: عرف التحقيق بمعناه العام أنه: اتخاذ جميع الإجراءات والوسائل المشروعة التي توصل إلى كشف الحقيقة وظهورها

وعرف التحقيق على أنه مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة، كذلك هو مجموعة الإجراءات التي تباشرها سلطات التحقيق بالشكل المحدد قانونا، بغية تمحيص الأدلة والكشف عن الحقيقة قبل مرحلة المحاكمة [1].

وكذلك عرف التحقيق بأنه " مجموعة من الإجراءات التي تباشرها السلطة المختصة بالتحقيق طبقا للشروط والأوضاع المحددة قانونا بهدف التنقيب عن الأدلة وتقديرها والكشف عن الحقيقة في شأن جريمة ارتكبت لتقرير لزوم محاكمة المدعي عليه أو عدم لزومها.

وهناك من قسم التحقيق إلى [2]:

1 - التحقيق الجنائي العملي: يقصد به جميع إجراءات التحقيق التي يباشرها المحقق الجنائي عند وقوع جريمة أو حادث، توصلا إلى معرفة الحقيقة وقواعد أساسها التجارب العملية التي وصل إليها المحققون في تحقيق القضايا الهامة.

2 - التحقيق الجنائي الفني: ويرتكز على الأبحاث العلمية والتجارب الفنية التي يمكن تطبيقها لاكتشاف حقيقة الحوادث الجنائية والاهتداء إلى مرتكبيها.

وقد عرف أيضا بأنه " التحري والتدقيق في البحث تلمسا لمعرفة الجاني في جناية ارتكبت أو شرع في ارتكابها.

[1] - عمر بن إبراهيم بن حماد العمر، إجراءات الشهادة في مرحلتي الاستدلال والتحقيق الابتدائي في ضوء نظام الإجراءات السعودي، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية،2007 ،ص 22.

[2] - غسان مدحت الخيري، الطب العدلي والتحري الجنائي، دار الراية، المملكة الأردنية، ط1، 2013، ص17.

الفرع الثاني: تعريف المحقق وخصائصه الفنية

أولا: تعريف المحقق

ذهب جانب من الفقه إلى تعريف المحقق بأنه: كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية، وتحقيقها ويسهم بدوره في كشف غموضها وصولا إلى معرفة حقيقة الحادث وكشف مرتكبه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة [1]

كما عرف البعض المحقق أو الباحث الجنائي بأنه " الشخص الذي يتولى ويتكلف بالتحقيق والتحري والبحث وجمع الأدلة لكشف غموض الحوادث ويتحدد دوره بالعمل على منع الجريمة قبل وقوعها أو اكتشافها بعد وقوعها، وضبط مرتكبيها والأدوات التي استعملت فيها "[2]

وعرف المحقق بأنه ذلك الشخص الذي عهد إليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل إلى علمه من جرائم بهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة [3]

أما المشرع الجزائري فقد وضع تعريفا لقاضي التحقيق في المادة 68 من قانون الإجراءات الجزائية حيث جاء في نصها ما يلي " يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة بالتحري عن أدلة الاتهام وأدلة النفي [4]

إن الجريمة الإلكترونية تنبع من التطور الفني الإلكتروني وهذا للاستخدام السيئ لبعض العاملين على أجهزة الحاسوب، مما أضاف أعباء جديدة على أجهزة التحقيق، لما يتطلبه التصدي لهذه الجرائم من قدرات فنية لم يألفها المحققون ولم يتعودوا عليها، مما أدى إلى ضرورة توفير الإمكانيات والمهارات المطلوبة في هذا المجال، وعليه فالتركيز هنا سوف ينصب على الخصائص الفنية التي تتسم بالحداثة والناتجة عن التطور الإنساني في مجال تقنية المعلومات والأنظمة الإلكترونية.

ثانيا: الخصائص الفنية للمحقق: ويمكن ذكر الخصائص الفنية للمحقق كما يلي: [5]

أ - أن يكون هدف المحقق دائما هو الوصول إلى الحقيقة: الشرط المتطلب لنجاح المحقق في أداء رسالته إيمانه بها، وأن يكون هدفه الحقيقي الوصول إلى الحقيقة، لا العدول عنها، وهذا ليس بالأمر الهين ذلك

---

[1] - خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي ،الإسكندرية، ط1، 2009، ص 86

[2] - غسان مدحت الخيري، الطب العدلي والتحري الجنائي، دار الراية، المملكة الأردنية، ط1، 2013، ص1

[3] - خالد ممدوح إبراهيم، المرجع السابق، ص 86

[4] - الأمر رقم 66- 155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو1966 الذي يتضمن قانون الإجراءات الجزائية المعدل والمتمم.

[5] - بختي فاطمة الزهراء - إجراءات التحقيق في الجريمة الإلكترونية - مذكرة لنيل شهادة الماستر- جامعة محمد بوضياف المسيلة، السنة الجامعية 2013 - 2014 ص 43.

أن أساس العدالة من صفات الله تعالى فإن آمن بها المحقق حينها لن يخل بواجباته مهما لاقى من الصعوبات، وعلى المحقق أن يضل مدركا بأنه في حالة صراع دائم بينه وبين المجرم الإلكتروني فالأول ينشد للحقيقة والثاني يجتهد في تضليل العدالة وطمس الحقائق والأدلة.

ب- أن يكون لدى المحقق موهبة فن التحقيق: إن التحقيق الفني هو إبداع، والتمكن من القدرة على التحليل ورفع الستار عن الحقيقة والغموض عن أي أمر، أو أي قضية كانت.

أما فيما يتعلق بفن التحقيق في الجريمة الإلكترونية ليس قدرة المحقق على استجلاء مدى توافر أركان الجريمة المعروضة وعناصرها، إنما هو قدرته أيضا على مناقشة الشهود

لاستجلاء أقوالهم مما يكون قد شابها غموض، ففي التحقيق في الجريمة الإلكترونية، لا يجب أن يكون المحقق مجرد آلة ميكانيكية تسجل فقط الأسئلة والأجوبة بل عليه توجيه الأسئلة للمتهم والشهود.

ج - أن يكون المحقق سريع التصرف في إجراءات التحقيق: إن سرعة إنجاز التحقيق تحافظ على أدلة الجريمة وآثارها، دون أن تمس أو تمحى، ويمنع من ضياعها، فالتأخير في إجراءات التحقيق قد يترتب عليه تعريض أدلة الجريمة ومعالمها لخطر الضياع، فالسرعة في إجراء التحقيق الجنائي من الواجبات الضرورية لمساس ذلك بسلطة الدولة.

وكذا حقوق الناس وحرياتهم، فسرعة التحقيق تؤدي إلى كشف حقيقة الجريمة دون أن يتمكن الجناة من طمس آثارها وأدلتها.

د- قوة الملاحظة وسرعة البديهة: ويقصد بها المعرفة الدقيقة لحقيقة أمر أدركته أحد الحواس عما يحيط به من ظروف، كما يجب عليه معرفة الجوانب الفنية والتقنية لأجهزة الحاسب والإنترنيت التي تتعلق بالجريمة.

و- حياد المحقق أثناء إجراء التحقيق: يعتبر من أهم خصائص التحقيق، فيجب أن يقوم بالتحقيق شخص غير متحيز يعنى بما يفيد الدفاع عنايته بأدلة الاتهام، ولا تتحقق الحيدة التامة للمحقق إلا إذا استقلت سلطة التحقيق عن كل من سلطة الاتهام من ناحية وسلطة الحكم من ناحية أخرى، فلا يجوز للنيابة المنوط بها توجيه الاتهام أن تحقق بعدل.

ي- المساواة في معاملة الحضور: القاعدة العامة بالنسبة للمحقق يلتزم بها هي المساواة في المعاملة، حتى بالنسبة للمتهم الماثل أمامه فينبغي على المحقق المساواة بين المتهم والمجني عليه عند المثول أمامه.

هـ- الهدوء وضبط النفس: يوجد في الحياة كثيرا من ذوي النشاط الإجرامي يعملون على استفزاز المحقق

لتشتيت أفكاره أو بدفعه للتعدي عليهم حتى يمكنهم تبرير اعتراضهم بارتكاب الواقعة وإبطالها بادعاء أنه وليد إكراه، لذا يتوجب على المحقق بالإضافة إلى الهدوء إتباع الإجراءات الصحيحة والمشروعة من أجل

سرعة المحافظة على الأدلة الإلكترونية، التي تدل على وقوع الجريمة الإلكترونية بتخزينها في الأقراص المعدة لذلك ومنع حذفها.

كما يجب أن تتوافر في المحقق بعض الأمور ليقوم بعمله على أحسن وجه[1]:

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

- وصول الإخبارات والبلاغات عن الجرائم الواقعة على الحاسوب والإنترنت من الفنيين الذين يعملون على هذه الأجهزة.

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

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

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

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

الفرع الرابع: خصائص التحقيق في الجريمة الإلكترونية

الجرائم التي ترتكب بواسطة الحاسوب تنشأ في الخفاء وينصب الاعتداء فيها على معطيات الحاسوب المخزنة والمعلومات المنقولة عبر نظم وشبكات المعلومات، وعليه فالتعامل مع مسرح الجريمة الإلكترونية والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق، وقبل التطرق إلى خصائص التحقيق في الجريمة الإلكترونية تجدر الإشارة لخصائص التحقيق عامة وهي كالأتي:

1 - **السرية**: يقصد بسرية الإجراءات عدم الاطلاع عليها، ويقصد بسرية التحقيق عدم علانيتها بالنسبة للغير، وهم غير أطراف الدعوى العمومية فسرية التحقيق إذا تعني إجراء التحقيق في جو من الكتمان بالنسبة للجمهور [2] حيث أن حضور إجراءات التحقيق غير مسموح به للجمهور وذلك لحماية المتهم من الشهر الذي قد يصيبه بسبب التحقيق الذي قد ينتهي بإصدار قرار أن لا وجه لإقامة الدعوى ولحماية

[1] - خالد عياد الحلبي - إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت - دار الثقافة للنشر والتوزيع عمان، الطبعة الأولى 2011 ص183 و184.

[2] - عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، الطبعة الثانية 2011 ص 336

الأدلة من العبث[1].

وقد اختلف في مسالة علانية التحقيق أو سريته فظهر اتجاهان:[2]

أ- **الاتجاه المؤيد للعلنية:** وقرر هذا الاتجاه علانية التحقيق بالنسبة لعامة الناس ولأطراف الخصومة الجزائية ووكلائهم، ومثال ذلك قانون التحقيق الجنايات المصري السابق، فجعل الأصل علانية التحقيق والسرية هي الاستثناء لإحقاق الحق وللآداب ولظهور الحقيقة، كما أخذ به القانون البحريني 1966 والقانون السوداني. 1984

ب - **الاتجاه المؤيد للسرية:** بخلاف الرأي الأول، جعل التحقيق سري بالنسبة للعامة والخصوم على حد سواء، بمن فيهم المدعى عليه وقد اعتمد هذا الاتجاه القانون الفرنسي القديم والحالي الذي أخذ بسرية إجراءات التحقيق كأصل وعلانيته كاستثناء بالنسبة للخصوم، نفس الشيء بالنسبة للمشرع الجزائري فقد نص في المادة 11 من قانون الإجراءات الجزائية على أنه " تكون إجراءات التحري والتحقيق سرية، ما لم ينص القانون على خلاف ذلك ودون إضرار بحق الدفاع".

2- التدوين: لقد أوجب المشرع المختص بالتحقيق اصطحاب كاتب معه يرافقه في جميع إجراءاته ويدون المحاضر ويصادقان معا على جميع صفحات المحاضر، بحيث يجري تدوين جميع إجراءات التحقيق وإثباتها كتابة في محضر رسمي يعد لذلك، حتى يكون حجة في الإثبات.

المطلب الثاني: الأجهزة المكلفة بالبحث والتحري عن الجريمة الإلكترونية

لقد تولد عن ظهور الأنترنت إجرام من نوع مميز، أصبح يهدد دول العالم بأكملها بون استثناء، حيث شهدت السنوات الأخيرة تزايدا كبيرا في كم تلك الجرائم بشتى أنواعها، سواء تلك المتعلقة بالجرائم الجنسية أو جرائم السب والقذف أو جرائم السرقة أو الاحتيال.

وأمام هذا التزايد المستمر والمتضاعف لهذا الإجرام، قررت الدول تجهيز أجهزة لمكافحته، سواء على المستوى الوطني أو الدولي، وهو ما دعت إليه الاتفاقية الأوربية لجرائم الأنترنت وكذلك المؤتمر المنعقد في السربون/ باريس في 2005/01/19 الذي كان موضوعه الشرطة والأنترنت[3].

---

[1] - عمر إبراهيم بن حمادة العمر، المرجع السابق ص 110.

[2] - بختي فاطمة الزهر ء المرجع السابق ص 42.

[3] - نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي الإسكندرية الطبعة الأولى ص105

الفرع الأول: الأجهزة المختصة بالبحث والتحري عن الجريمة الإلكترونية على المستوى الداخلي

لقد ظهرت العديد من الأجهزة والهيئات المختصة في مجال الجريمة المعلوماتية في إطار مكافحتها والبحث والتحري عنها وعن مرتكبيها سواء على المستوى الوطني أم على صعيد الدول الأجنبية.

إنه بالنظر إلى الطبيعة التقنية التي تتميز بها الجريمة المعلوماتية ذهبت أغلب الأنظمة القانونية الإجرائية في التشريعات المقارنة إلى أن تعهد بمسألة البحث والتحري عن هذا النوع من الجرائم لأجهزة متخصصة، لها من الكفاءة والتدريب والوسائل البشرية والمادية ما يؤهلها للتعامل مع هذا النوع المستحدث من الإجرام. وسوف نحاول أن نلقي الضوء على هذه الأجهزة الموجودة في بعض الدول ثم نعرج على الوضع في بلادنا[1].

أولا: الأجهزة المختصة في الدول الأجنبية:

كانت الدول المتقدمة سباقة بإحداث هذه الأجهزة إذ أن مكافحة الجرائم المعلوماتية مرتبط بمدى تقدم الدول من الناحية التقنية وبمدى توفر الإمكانات المادية اللازمة لإنشاء هذه الأجهزة ونذكر على سبيل المثال في هذا الصدد الدول التالية:

1 / الولايات المتحدة الأمريكية: قامت الولايات المتحدة الأمريكية بإنشاء عدة أجهزة لمكافحة الجريمة المعلوماتية ومنها:

أ - **شرطة الواب webpolice:** وتعتبر نقطة مراقبة على الأنترنت إضافة إلى أنها تتلقى الشكاوى من مستخدمي الشبكة وملاحقة الجناة والقراصنة، والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة.

ب - **مركز تلقي شكاوى جرائم الأنترنيت IC3:** والذي تم إنشاؤه من طرف مكتب التحقيقات الفدرالي **FBI** في سنة 2000. ثم في عام 2003 تم دمج مركز شكاوى الاحتيال عبر الإنترنيت المعروف بـ IFCC مع هذا المركز. ويعمل مركز IC3 بصورة تشاركية مع مكتب التحقيقات الفدرالي والمركز الوطني لجرائم الياقات البيضاء NWC، ويقوم هذا المركز بتلقي الشكاوى عبر موقعه على الإنترنيت أين يقوم الشاكي بملء استمارة إلكترونية ثم يقوم المختصون في هذا المركز بتحليل الشكاوى وربطها بالشكاوى الأخرى المستلمة من قبل.

ج - **قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية**: ويختص هذا القسم بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها.

د - **نيابة جرائم الحاسوب والاتصالات CTC**: وتتألف من مجموعة من قضاة النيابة العامة ممن تلقوا تدريبات مكثفة على نظم المعالجة الآلية للبيانات وتم منحهم صلاحيات واسعة في مجال الجرائم

[1] - سعيداني نعيم المرجع السابق ص 103

المعلوماتية والعدوان على حقوق الملكية الفكرية.

و- **المركز الوطني لحماية البنية التحتية**: التابع للمباحث الفدرالية الأمريكية وقد حدد هذا المركز البنى التحتية التي تعتبر هدفا للهجومات والاعتداءات عبر الإنترنيت وعلى رأسها شبكات الاتصالات.

وإضافة إلى هذه الأجهزة يوجد أيضا في الولايات المتحدة الأمريكية وحدة متخصصة بمكافحة الإجرام المعلوماتي تابعة لقسم العدالة الأمريكي تتكون من خبراء في نظام الحوسبة والإنترنيت ومن مستشارين قانونيين([1]).

2 / بريطانيا: قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة المتخصصين في البحث والتحري عن الجرائم المعلوماتية وتضم هذه الوحدة نحو ثمانين عنصرا على درجة عالية من الكفاءة في المجال التقني، وقد بدأت هذه الوحدة نشاطها عام 2001

3 / فرنسا: قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم المعلوماتية ونذكر من هذه الأجهزة:

أ - القسم الوطني لقمع جرائم المساس بالأموال والأشخاص: ويتكون هذا القسم من محققين مختصين في التحقيق بجرائم العالم الافتراضي وقد بدأ هذا القسم مهامه عام 1997.

ب - المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات: ويعد هذا المكتب سلاح الدولة الفرنسية في مكافحة الجرائم المعلوماتية، وقد تم إنشاؤه في 2000/05/15.

4 / الصين: قامت السلطات في هذا البلد بإنشاء وحدة متخصصة على مستوى جهاز الشرطة تعرف باسم" **القوة المضادة للهكرة** " وهي تختص برقابة المعلومات التي يسمح لمواطنيها الدخول إليها عبر الإنترنيت([2]).

وأما على **مستوى الدول العربية** فنجدها لم تقف مكتوفة الأيدي أمام خطر الجرائم المعلوماتية، فقد قامت بعض الدول منها بإنشاء أجهزة متخصصة لمكافحة هذه الجرائم ونذكر على سبيل المثال:

5/ مصر: قامت وزارة الداخلية في مصر بإنشاء عدة أجهزة أوكلت لها مهمة ضبط ما يقع من جرائم من خلال الشبكة المعلوماتية نعرض لها على النحو التالي:

أ - **إدارة مكافحة جرائم الحسابات وشبكات المعلومات:** أنشئت هذه الإدارة بموجب قرار وزاري وهي تابعة للإدارة العامة للمعلومات والتوثيق وتخضع للإشراف المباشر لمدير الإدارة العامة وتشرف عليها فنيا مصلحة الأمن العام التابعة لوزارة الداخلية، وتضم ثلاث أقسام رئيسية: هي قسم العمليات، قسم

[1]- نبيلة هبة محمد هروال، الجوانب الإجرائية لجرائم الأنترنات في مرحلة جمع الإستدلالات للطبعة الأولى، دار الفكر الجامعي الإسكندرية،2007 ص 108.

[2]- سعيداني نعيم المرجع السابق ص 106

التأمين وقسم البحوث والمساعدات الفنية. وتعتبر هذه الإدارة من أكبر الإدارات تعاملا مع الجرائم المعلوماتية، فهي تتكون من ضباط متخصصين في مجال تكنولوجيا الحسابات والشبكات وتختص بمكافحة جرائم الإنترنيت على مختلف أنواعها[1].

ب - **قسم مكافحة جرائم الحاسبات وشبكات المعلومات**: وقد أنشئ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة، ويتبع إدارة المعلومات والحاسب الآلي، ويخضع من حيث الإشراف الفني لإدارة مكافحة جرائم الحاسبات وشبكات المعلومات، ويختص بعمليات تأمين ورقابة نظم وشبكات المعلومات، لمنع وقوع أية جرائم عليها، باستخدام الأساليب والتقنيات العلمية الحديثة، ورصد ومكافحة وضبط الجرائم التي تقع باستخدام الحاسبات على نظم وشبكات المعلومات وقواعد البيانات.

ثانيا: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الوطني: أما الوضع في بلادنا فإنه وبالنظر إلى الخصوصية التي تتميز بها الجريمة المعلوماتية كان الأمر محتما لتوفير كوادر وأجهزة متخصصة تعنى بعملية البحث والتحري عن الجريمة المعلوماتية وكان ذلك إما على مستوى جهاز الشرطة أو الدرك الوطني.

ولعل ابرز الهيئات المختصة في مجال مكافحة الجرائم الإلكترونية على المستوى الوطني تتمثل في الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، إضافة لتلك الوحدات التابعة للمديرية العامة للأمن الوطني، وكذلك تلك التابعة لقيادة الدرك الوطني.

1: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[2]:

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

أ- التعريف بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

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

ب - مهام الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

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

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

[1]- نبيلة هبة هروال، المرجع السابق، ص141

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

- مساعدة السلطة القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات.

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

ج - اختصاصات الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال:

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

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

- تنشيط وتنسيق عمليات الوقاية عن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

- مساعدة السلطة القضائية ومصالح الشرطة القضائية في مجال مكافحة الجرائم المعلوماتية من خلال مدها بالمعلومات والخبرات القضائية.

- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماسة بأمن الدولة وذلك تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

- تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.

- السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلو مات والتعاون على المستوى الدولي في مجال اختصاصها.

- تطوير التعاون مع المؤسسات والهيئات الوطنية المعنية بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال

- المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام والاتصال.

- المساهمة في تحديث المعايير القانونية في مجال اختصاصها.

2 - الهيئات القضائية الجزائية المتخصصة.

أنشئت بموجب القانون 04 - 14 المؤرخ في 2004/11/10 المعدل والمتمم لقانون الإجراءات الجزائية[2] تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 32،37،و40 من

[1] - المرسوم الرئاسي رقم 15- 261 مؤرخ في 08 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، بتاريخ 08 أكتوبر 2015

[2]- القانون رقم 04 - 14 المؤرخ في 10 نوفمبر 2004، يعدل ويتمم الأمر رقم 66 - 155 المؤرخ في 08 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، الصادر بالجريدة الرسمية رقم 71 بتاريخ 10 نوفمبر 2004.

ق.إ.ج.ج. تتمتع بمباشرة مهامها في دائرة الاختصاص الإقليمي الموسع طبقا للمرسوم التنفيذي رقم 06 - 348 المؤرخ في 2006/01/05. بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09 - 04.

3: الوحدات التابعة للمديرية العامة للأمن الوطني والدرك الوطني:

توجد لدى المديرية العامة للأمن الوطني والدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن والنظام العام مجموعة من الوحدات نكرها منها([1]):

أ - الوحدات التابعة للمديرية العامة الأمن الوطني

تضع المديرية العامة للأمن الوطني في إطار تجسيد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديها لأجل التصدي لكل أنواع الجرائم وبالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة والخاصة المرتبطة باستعمال هذا النوع من التكنولوجيات.

حيث أنشأت المديرية العامة للأمن الوطني مصلحة مركزية لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال على المستوى المركزي وفرق على المستوى المحلي، إضافة إلى المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران، تحتوي هذه المخابر على فروع تقنية من بينها خلية الإعلام الآلي. تتمثل مهامها هاته الفرق فيما يلي:

* مساعدة مصالح الشرطة القضائية الموجودة على المستوى المحلي في مجال التحريات التقنية.

* المشاركة في تأمين وحماية الأنظمة المعلوماتية والفضاء السيبرياني الوطني.

* التعاون والمشاركة في التحقيقات والتحريات ذات البعد الوطني والدولي في مجال مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

* استقبال شكاوى المواطنين في مجال الجرائم المتواجد في الفضاء السيبرياني.

* البحث والتحري في الجرائم المعلوماتية تحت إشراف الجهات القضائية

* توعية وتحسيس المواطنين بأخطار الإنترنت وخصوصا على الأطفال.

[1] - فضيلة عاقلي - المرجع السابق، ب ص

ب - الوحدات التابعة للدرك الوطني

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

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

يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني[1] قسم الإعلام والإلكترونيك الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، وإنجاز المقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد رايس والتابع لمديرية الأمن العمومي للدرك الوطني[2].

الفرع الثاني: الأجهزة المختصة بالبحث والتحري عن الجريمة المعلوماتية على المستوى الدولي والإقليمي:

سبق وأن أسلفنا الذكر بأن الجرائم المعلوماتية تتميز بأنها عابرة للحدود الوطنية يمكن أن يتعدى أثرها عدة دول، لذلك كان لابد من وجود تعاون دولي من أجل مكافحة هذا النوع من الإجرام. ومن أساليب التعاون الدولي التعاون الأمني الذي يمكن أن يحقق أهدافه لا قبل للشرطة الإقليمية بتحقيقها، ومن أبرز هذه الأجهزة في مجال مكافحة الجرائم المعلوماتية على هذا الصعيد نذكر ما يلي[3]:

أولا: على المستوى الدولي:

تعد المنظمة الدولية للشرطة الجنائية الأنتربول[4] من أهم الأجهزة على المستوى الدولي لمكافحة الإجرام بصفة عامة ومنها الجرائم المعلوماتية، وتهدف هذه المنظمة الدولية إلى تشجيع التعاون بين

---

[1] - مرسوم رئاسي 04 - 183 مؤرخ 26 يونيو 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد القانوني الأساسي.

[2] - يوسف جفال - التحقيق في الجريمة الإلكترونية - مذكرة ماستر، جامعة محمد بوضياف، المسيلة قسم الحقوق، السنة الجامعية 2016 - 2017 ص 21.

- سعيداني نعيم، المرجع السابق ص 107 3

[4] - المنظمة الدولية للشرطة الجنائية الأنتربول: مقرها في باريس، وضع ميثاق هذه المنظمة في الفترة 7- 1956/06/13 وإعتبرنافذا إعتبارا من1956/06/13 م.

أجهزة الشرطة في الدول الأطراف على نحو فعال من أجل مكافحة الجريمة ذات الطابع العالمي بما في ذلك الإجرام المرتبط بالمعلوماتية.وتستخدم هذه المنظمة لتحقيق أهدافها وسيلتين([1]):

1: تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.

2: التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

وتعمل المنظمة الدولية للشرطة الجنائية في مجال الجرائم المعلوماتية بوضع قائمة اسمية لضباط متخصصين يمكن الاستعانة بهم في مجال البحث والتحري في قضايا الجرائم المعلوماتية، كما توفر هذه المنظمة للدول الأطراف المعلومات اللازمة عن الطرق العملية في مجال الجريمة المعلوماتية من خلال خلق فرق عمل وورشات تكوين. ولقد أنشأت هذه المنظمة وحدة متخصصة في مكافحة الجرائم المعلوماتية تقوم بتزويد أجهزة الشرطة التابعة للدول الأعضاء بإرشادات حول التحقيق في هذا النوع من الإجرام وكيفية التدريب على مكافحته.

ثانيا: الأجهزة على المستوى الإقليمي:

أ / الشرطة الأوروبية أو الأوروبول: وهو جهاز على مستوى الاتحاد الأوروبي تم إنشاؤه في لكسنبورغ عام 1992 ومقره في مدينة لاهاي بهولندا ليكون حلقة وصل بين أجهزة الشرطة الوطنية للدول الأعضاء في مجال الجرائم الإرهابية والمخدرات والجريمة المنظمة وكذا الإجرام المعلوماتي.ويهدف هذا الجهاز إلى تسهيل تبادل المعلومات بين أجهزة الشرطة لمختلف الدول الأعضاء، وكذا تجميع وتحليل المعلومات بغرض المساعدة في التحقيقات المفتوحة في أي دولة عضو بخصوص جريمة من الجرائم المذكورة ومنها الجريمة المعلوماتية.

وبمبادرة من الشرطة القضائية الفرنسية تم إنشاء جهاز على مستوى الأوروبول أطلق عليه اسم Repporting online System Internet Crime (ICROS) في سنة 2010 بغرض التنسيق أكثر في مجال مكافحة الجريمة المعلوماتية على مستوى الدول الأعضاء.

ب / **الأوروجيست:**Eurojust وهو جهاز يعمل على المستوى الأوروبي إلى جانب الأوروبول في مجال مكافحة جميع أنواع الجرائم، تم إنشاؤه عام 2002 وينعقد اختصاصه عندما تمس الجريمة دولتين على الأقل من الدول الأعضاء في الاتحاد الأوروبي أو دولة عضو مع دولة أخرى من غير الإتحاد الأوروبي. ويعد الأروجيست وحدة للتعاون القضائي، مهمتها الأساسية هي التنسيق بين السلطات القضائية المكلفة بالتحقيقات ولها من الصلاحيات ما يؤهلها لفتح تحقيقات ومباشرة متابعات جزائية.

[1]- سعيداني نعيم، المرجع السابق، ص 107 و108

المبحث الثاني: معوقات (صعوبات) التحقيق في الجريمة الإلكترونية

يتسم التحقيق في الجرائم المعلوماتية بالعديد من المعوقات والصعوبات، فنظرا لوقوع الجريمة المعلوماتية ضمن بيئة رقمية، أدت إلى ظهور نوع من التحدي للأجهزة المختصة بالبحث والتحري في تطبيق القواعد الإجرائية التي نظمت مسألة استخلاص الدليل الرقمي، وتضعف قيمتها في مكافحة هذا النوع من الجرائم وتؤثر على عملية التحقيق وتؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وفي أدائه وفي أجهزة التحقيق، وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها على المجرم نفسه حيث يشعر أن الجهات الأمنية غير قادرة على اكتشاف أمره وأن خبرة القائمين على مكافحة الجريمة والتحقيق فيها لا تجاري خبرته، الأمر الذي يعطيه ثقة أكبر في ارتكاب المزيد من هذه الجرائم[1].

ولقد كانت هذه التحديات إحدى المسائل الهامة التي ناقشتها المؤتمرات الدولية ولعل أهمها مؤتمر الأنتربول السادس لجرائم تقنية المعلومات الذي شهدته القاهرة في الفترة ما بين 13 - 2015/04/15[2]

المطلب الأول: المعوقات المتعلقة بجهات التحقيق وإجراءات الحصول على الدليل الإلكتروني

من أهم المعوقات أو الصعوبات التي قد تواجه التحقيق في الجريمة المعلوماتية معوقات تتعلق بجهات التحقيق وإجراءات الحصول على الدليل، وهو ما نستعرضه كما يلي:

الفرع الأول: المعوقات المتعلقة بجهات التحقيق

تتعلق هذه المعوقات بالعامل البشري القائم بالتحقيق في الجريمة المعلوماتية، فإذا كانت السلطات القائمة بالتحقيق من رجال الضبطية القضائية وقضاة بما لها من خلفية قانونية تلعب دورا كبيرا في التحري عن الجرائم والبحث عن مرتكبيها في إطار الجرائم التقليدية فإن وظيفتها في مكافحة الجرائم المعلوماتية لا ترق إلى نفس الدرجة، ذلك أن الطبيعة الخاصة للبيئة الإلكترونية التي تتعامل معها فضلا عن خصوصية الدليل الرقمي ينعكس على عمل الجهات المكلفة بالبحث والتحري.حيث يتطلب الكشف عن هذه الجرائم اكتساب جهات التحقيق مهارات خاصة على نحو يساعدهم على مواجهة التقنيات المعلوماتية، إذ يرى المتخصصون في مكافحة الجرائم المعلوماتية أن الأنظمة المعلوماتية وما يقع عليها من جرائم تعد تحديا هائلا لأجهزة العدالة الجنائية ذلك أن رجل الأمن غير المتخصص والذي إنحصرت معلوماته في جرائم قانون العقوبات بصورته التقليدية من قتل وضرب وسرقة لن يكون قادرا على التعامل مع الجريمة المعلوماتية والتي تقع بطريقة تقنية عالية[3].

---

[1] - خالد عياد الحلبي - المرجع السابق ص 220.

[2] - سعيداني نعيم المرجع السابق ص 186.

[3] - عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي، الإسكندرية الطبعة الأولى2006 ص 68

فنقص المهارة الفنية في استخدام الكومبيوتر والإنترنت وعدم توفر المعرفة بأساليب ارتكاب الجريمة المعلوماتية وقلة الخبرة في مجال التحقيق والتحري عن جرائم العالم الافتراضي والمعرفة باللغة الإنجليزية، عوامل من شأنها أن تضعف دور الأجهزة المختصة بالتحقيق في الجرائم وكشف النقاب عنها، وليس هذا فحسب فإن من المسائل التي تشكل عقبة أمام سلطات التحقيق مسألة كيفية التعامل والحفاظ على الأدلة الرقمية التي مكمنها الحواسيب والخوادم والمضيفات والشبكات.

لأجل ذلك بدأت بعض الأجهزة الأمنية والقضائية في استقطاب المختصين في الكومبيوتر ليكونوا ضمن كوادرها، وتدريب رجال الضبطية والقضاة على استخدام الحواسيب وتكنولوجيا المعلومات، وعلى الرغم من ذلك فقد تكون تلك الأجهزة غير قادرة على مواكبة التطور السريع في مجال تكنولوجيا المعلوماتية لعدة أسباب أهمها:

- الميزانيات المالية المرصودة لاستقطاب النخبة المتميزة في المجال المعلوماتي خاصة وأن الشركات ومؤسسات القطاع الخاص تبذل المستحيل من أجل ضم هذه النخبة إليها.

- عدم تفرغ أجهزة الشرطة والقضاء للجرائم الإلكترونية وحدها، بل تغطيتها لمجالات متنوعة أخرى.

- إزاء ذلك يرى البعض أنه من المستحسن أن تنشأ وحدات تحقيق خاصة بالجرائم الإلكترونية، توكل لها مهمة التحقيق في هذا النوع من الجرائم لا سيما مع وجود شركات عالمية متخصصة في تحقيق الجرائم المعلوماتية حققت النجاح في كثير من الحالات.

وفي هذا الصدد ألزمت الاتفاقية الأوربية لجرائم تقنية المعلومات الدول الأطراف بضرورة تبني الإجراءات التشريعية أو أية إجراءات أخرى ترى أنها ضرورية وفقا لقانونها الداخلي من أجل إنشاء وتأسيس سلطات مختصة في مجال التنقيبات والإجراءات الجنائية النوعية في مجال الجريمة المعلوماتية ([1]).

وقد بادرت مختلف الدول الأعضاء إلى إنشاء وحدات متخصصة في مجال البحث والتحري عن الجريمة المعلوماتية داخل الأجهزة الحكومية كالجزائر التي قامت بإنشاء هاته الوحدات المتخصصة في هذا الإطار كمصالح الضبطية القضائية التابعة للشرطة أو الدرك والمعهد الوطني للأدلة الجنائية وعلم الإجرام ومركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية تابع أيضا لقيادة الدرك ومخابر الشرطة العلمية التابعة لمديرية الشرطة القضائية، والفروع التقنية التي تضمها هذه المخابر، خلية الإعلام الآلي والتي تختص بالتحقيق في كل ما يتصل بالجرائم المعلوماتية بناء على تسخيرات أو إنابات قضائية. والهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[1] - عبد الفتاح بيومي حجازي، المرجع السابق، ص 69.

وفي إطار محاولة التغلب على المعوقات والصعوبات التي تواجه جهات التحقيق في مجال الجريمة المعلوماتية فإنه من غير الكافي أن يتم إنشاء أجهزة فنية متخصصة، بل لابد من إتباع ذلك بتوفير إستراتيجية تدريبية وتكوين متعمق في ميدان تكنولوجيات الإعلام والاتصال العاملين في مجال العدالة الجزائية بصفة عامة.

الفرع الثاني: المعوقات المتعلقة بإجراءات الحصول على الدليل الإلكتروني

إذا كان من السهل على جهات التحري والتحقيق أن تتحرى عن الجرائم التقليدية عن طريق المشاهدة أو التتبع أو سماع الشهود، فإنه قد يصعب عليها ذلك بهذه الطرق بالنسبة للجرائم المعلوماتية التي ترتكب بالوسائل الإلكترونية، وهذا راجع إلى الطبيعة الرقمية التي يتكون منها الدليل التقني سواء من حيث كونه غير مرئي في شكل نبضات مغناطيسية أو كهربائية لا يدركها الرجل العادي بالحواس الطبيعية، أو من حيث تواجده في العالم الافتراضي على الكيفية المعنوية غير الملموسة ضمن مكون رقمي في شكل مختلط وذلك نتيجة لعدم إمكانية وجود فرز ذاتي في إطار التخزين الرقمي، وما يترتب على هذه الخاصية الأخيرة صعوبة في جمع المعلومات الجنائية التي تفيد البحث والتحقيق الجنائي، ذلك لأنها عادة ما تكون مختلطة بغيرها من المعلومات العادية لمستخدمي الحواسيب غير المشتبه فيها وهو أمر قد يشكل تهديدا لخصوصية هؤلاء نظرا لإمكانية امتداد آثار تفتيش النظام المعلوماتي إليهم[1].

فضلا عن ذلك فإن المجرم المعلوماتي غالبا ما يضرب سياجا أمنيا على أفعاله غير المشروعة قبل ارتكابه لها[2]، فيزيد بذلك من صعوبة تطبيق القواعد الإجرائية التي يتوقع حدوثها للبحث عن الأدلة التقنية التي تدينه وذلك بالعمل على ترميز أو تشفير المعلومات المخزنة إلكترونيا والمنقولة عبر شبكات الاتصال، بحيث يستحيل على غيره الإطلاع عليها ويصبح بذلك الدليل الرقمي مرمزا أو مشفرا وبالتالي يكون عائقا أمام سلطات البحث والتحقيق أثناء تطبيقها للقواعد الإجرائية المقررة لاستخلاصه.

ومن الصعوبات التي تعيق التحقيق في مجال الجريمة المعلوماتية والمرتبطة بالدليل الرقمي هي سهولة محو هذا الدليل أو تدميره في زمن قصير جدا، فارتباط الجريمة المعلوماتية بالبيئة التقنية انعكس على طبيعة الدليل المترتب عنها من حيث أن أمر طمسه ومحو آثاره من قبل الفاعل أمرا في غاية السهولة، إذ بإمكان المستخدم الذي يتحكم في المعلومات أن يستعمل نظاما معلوماتيا من أجل محو

[1] - سعيداني نعيم المرجع السابق ص 189.

[2] - خالد ممدوح ابراهيم المرجع السابق ص75.

تلك المعلومات التي تعد موضوعا للتنقيب الجنائي وبالتالي تدمير كل الأدلة. فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها بحيث لا تتمكن السلطات من كشف الجريمة، وإذا ما علمت فإنها لا تستطيع إقامة الدليل ضده، لذلك فإن التحفظ على المعطيات يعتبر إجراء أوليا أو تمهيديا، الهدف منه هو الاحتفاظ بالمعطيات قبل فقدانها. وقد يكون ذلك بالتعاون مع الجهات التي تقدم الخدمة بإلزامهم بطريقة أو بأخرى على حفظ المعطيات المعلوماتية المخزنة بما في ذلك المعطيات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي.

وفي هذا الإطار نجد أن المشرع الجزائري قد ألزم في المادة 10 من القانون 09 - 04 مقدمي الخدمات بحفظ المعطيات المتعلقة بحركة السير والتي حددها في المادة 11 من نفس القانون ووضعها تحت تصرف السلطات المكلفة بالتحريات القضائية.

المطلب الثاني: المعوقات المتعلقة بالجهات المتضررة وصعوبة تحديد الجاني

بالإضافة إلى المعوقات المتعلقة بجهات التحقيق وإجراءات الحصول على الدليل، فهناك معوقات أخرى تتعلق بالجهات المتضررة والقدرة على تحديد الجاني[1].

الفرع الأول: معوقات التحقيق المتعلقة بالجهات المتضررة

قد يكون للجهات المتضررة من الجريمة المعلوماتية يد في إعاقة التحقيق والوصول إلى الدليل لإثبات الجريمة. فالتقنية المستخدمة في نظم المعلومات تعد مجال استثمار وتسابق بين الشركات مما يدفعها في مقابل تحقيق الربح إلى تبسيط الإجراءات وتسهيل استخدام البرامج وملحقاتها وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة في مقابل إهمال الجانب الأمني، وقد وصل الحد ببعض مستخدمي شبكات الإنترنت عبر مزودي الخدمة في خضم التنافس التجاري إلى درجة عدم مطالبة المشتركين بتحديد هوياتهم عند الاشتراك في خدمة الإنترنت مما يحول دون معرفة هوية المستخدم في حالة البحث والتحري عنها من طرف الجهات للتحقيق، ومن ناحية أخرى فإن كثيرا من الجهات التي تتعرض أنظمتها المعلوماتية للاعتداء تعمد إلى عدم الكشف والتبليغ عن ذلك لدى السلطات المختصة تجنبا للإضرار بسمعتها أو خوفا من أن الكشف عن أسلوب ارتكاب الجريمة قد يؤدي إلى تكرار وقوعها بتقليدها من طرف الآخرين.

فذاتية الجريمة المعلوماتية من حيث كونها مجهولة ومستترة تتم في بيئة تقنية لا تترك وراءها أي أثر خارجي تحول دون اكتشافها من طرف المجنى عليه، وإذا ما تصادف واكتشفها فإنه يعمد في أغلب

[1]- سعيداني نعيم، المرجع السابق، ص 191.

الأحيان إلى التستر عليها والصمت بدل إبلاغ الشرطة للتحقيق بشأنها ومعرفة مرتكبها وهو ما ينجم عنه عدم التعاون مع السلطات المختصة لمكافحة هذا النمط الإجرامي.

لأجل ذلك فقد طرحت العديد من الاقتراحات لحمل المجنى عليهم في الجريمة المعلوماتية على التبليغ والتعاون مع السلطات بأن تفرض النصوص القانونية المتعلقة بجرائم المعلوماتية التزاما على عاتق موظفي الجهات المجنى عليها بالإبلاغ عما يصلهم من أخبار عن وقوع تلك الجرائم مع تقدير الجزاء عن الإخلال بهذا الالتزام[1].

الفرع الثاني: صعوبة تحديد هوية الجاني

إن الوصول إلى الدليل الرقمي تعترضه عقبة أخرى تكمن في أن الجناة المتمرسين يجتهدون في إخفاء هوياتهم للحيلولة دون تعقبهم أو كشف أمرهم، بحيث تظل أنشطتهم مجهولة بمنأى عن علم السلطات المعنية بمكافحة الجريمة. ومن الأمثلة التي تساق على ذلك استخدام الجاني حاسبا آخر غير حاسبه الشخصي كاستخدام الحواسيب الموجودة في الأماكن العامة أو اللجوء إلى مقاهي الإنترنت على اعتبار أن جل هذه المقاهي لا تقوم بتسجيل أسماء مرتاديها أو التحقق من هوياتهم لا سيما إذا علمنا أن شبكة الإنترنت تتيح لمستخدميها استعمال الخط الواحد من أكثر من شخص في آن واحد معا، ما يجعل المراقبة والتعقب للمشتبه فيه أمرا ينطوي على الصعوبة وغير ميسور في كثير من الأحيان وربما تتعقد المسألة أكثر عند استخدام الإنترنت اللاسلكي.

وتعد مسألة صعوبة تحديد هوية مرتكب الجريمة المعلوماتية من إحدى المشاكل التي تطرح للكفاح ضد الإجرام المعلوماتي، وإن كان يمكن معرفة النظام أي هوية الحاسوب والخادم والمضيف والشبكات الذي ارتكبت من خلاله [2].

لكن القول أن مسألة عدم معرفة شخصية وهوية الفاعل الذي يتستر وراءها مرسل الرسالة غير المشروعة هو أمر نسبي إذ لا يوجد تجهيل بالمعنى الصحيح بالنسبة لشبكة المعلومات، حيث يترك الفاعل آثارا أثناء تنقله في طرقات شبكات المعلومات تسمح للمحققين من الوصول إليه، والأمر هنا متروك لفطنة رجال الضبطية القضائية من خلال الاستناد إلى فكرة الدلائل الكافية وما ينبثق عنها من شبهات.

المطلب الثالث: ضمانات المشتبه فيه أثناء إجراءات الحصول على الدليل الإلكتروني

لقد كفلت الدساتير الحماية للحياة الخاصة ومنها الدستور الجزائري،لا سيما في المواد 39، 40، 45، 47 و48 منه وذلك من خلال منع الغير من الإطلاع عليها بقصد توفير نوع من الاستقرار والأمن للمواطن حتى يتمكن من أداء دوره الاجتماعي. وقد كفلت العدالة الجزائية ضمان الحرية الشخصية

[1] - خالد ممدوح ابراهيم، المرجع السابق، ص 67

[2] - سعيداني نعيم، المرجع السابق، ص 193

عن طريق إعطاء الإجراءات الجزائية مصداقيتها في دولة القانون التي تقوم فيها سلطاتها وأجهزتها على احترام سيادة القانون، هاته الإجراءات الجزائية تتولى حماية الحرية الشخصية في جميع صورها وأشكالها في كافة مراحل الدعوى. ويتفق فقهاء القانون الجنائي على أن قانون الإجراءات الجزائية يعتبر من القوانين المنظمة للحرية الشخصية للمشتبه فيه وللمتهم، لذلك يعتبر هذا القانون المرآة التي تعكس مدى احترام حريات وحقوق الأفراد في أي دولة، كما أن قواعد هذا القانون تحاول التوفيق بين مصلحتين متعارضتين هما مصلحة الدولة التي تهدف إلى المصلحة العامة وذلك عن طريق الوصول إلى الكشف عن الحقيقة بغرض إحقاق الدولة لحقها في العقاب، ومصلحة الفرد عن طريق ضمان حقوقه وحريته [1].

تعد طرق وأساليب جمع الدليل لإثبات الجريمة المعلوماتية من الإجراءات التي من شأنها المساس بحق خصوصية المتهم المكفولة دستوريا، لذلك فقد قيدت التشريعات الإجرائية عند سماحها بذلك سلطات التحري والتحقيق بشروط وشكليات تمثل في حقيقة أمرها ضمانات للمشتبه فيه.

الفرع الأول: ضمانات المشتبه فيه عند إجراء التفتيش وضبط المراسلات الإلكترونية

أن إجراء التفتيش يمس بحقوق الأفراد سواء في حريتهم الشخصية أم في حرمة مساكنهم أم مراسلاتهم أم في حياتهم الخاصة، وقد أجيز لضرورة الوصول إلى الحقيقة إجراؤه. فقانون الإجراءات الجزائية الجزائري وضع العديد من الضمانات الخاصة بالمشتبه فيه عند تقرير مثل هذا الإجراء، تمتد هذه الضمانات لتشمل حقوق وحريات المشتبه فيه عند تفتيش نظم الحاسوب والإنترنت

أولا: الضمانات العامة للمشتبه فيه في مواجهة التفتيش وضبط الأدلة

إن الشروط والشكليات التي قيد بها القانون سلطة التحري والتحقيق عند إجراء التفتيش تمثل ضمانات للمشتبه فيه أو للمتهم ومن ذلك:

- السائد في القانون أن إجراء التفتيش لا يقع إلا في حالة وقوع جريمة، ومن ثمة يصدر الإذن بالتفتيش.
- ضرورة تحقيق فائدة مرجوة من إجراء التفتيش، ذلك أن الغرض من هذا الإجراء هو احتمال الحصول على أشياء تفيد في كشف الحقيقة، وتحقق الفائدة المرجوة من التفتيش تعني أن تقوم قرائن وأمارات على وجود أشياء تتعلق بالجريمة في المكان المراد تفتيشه، وهذا ما يفهم من نص المادة 44 من قانون الإجراءات الجزائية بقولها " لا يجوز لضباط الشرطة القضائية الانتقال إلى مساكن الأشخاص الذين يظهر أنهم ساهموا في الجناية وأنهم يحوزون أشياء لها علاقة بالجريمة لإجراء التفتيش....." وكذا نص المادة 81 من نفس القانون بقولها أنه " يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة.

[1] - سعيداني نعيم، المرجع السابق ص 195.

- لا يتم التفتيش إلا بناء على إذن مسبق من السلطة القضائية المختصة وهو شرط نصت عليها المادة 47 ف 03 من دستور 2016 ([1]) بقولها أنه " لا تفتيش إلا بأمر مكتوب صادر من السلطة القضائية المختصة" وهو ما تؤكده بعد ذلك المادة 44 من قانون الإجراءات الجزائية.

- تحديد ميعاد معين لإجراء التفتيش وهو ما حددته المادة 47 من قانون الإجراءات الجزائية لا يكون التفتيش قبل الخامسة صباحا ولا بعد الساعة الثامنة مساء.

- حضور المشتبه فيه أو المتهم أثناء إجراء التفتيش أو من ينوب عنه عند إجراء عملية التفتيش، وهذا حتى يكون على بينة ودراية بما ضبط أو اكتشف، وكضمانة لهذه الحقوق فإن الشرع في حالة رفض المشبه فيه الحضور أو في حالة عدم قدرته على ذلك اشترط حضور من ينوب عنه.

- المحافظة على الأسرار عند التفتيش وهو ما نصت عليه المادة 45 من قانون الإجراءات الجزائية بنصها "....غير أنه يجب عند تفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر" وأعقب الشرع على ذلك بالتجريم والعقاب في المادة 46 لكل شخص يفشي مستندا ناتجا من التفتيش. وفي هذا ضمانة للمشتبه فيه حيث تحفظ أسراره من إطلاع غير المحقق عليها ولو كانوا من مساعديه أو أشخاص آخرين لا صفة لهم قانونا في الإطلاع عليها.

وفيما يتعلق بضبط الأدلة المتحصل عليها بسبب التفتيش فإن المشرع أحاط هذه العملية بضمانات وشروط منها:

- أوجب المشرع على ضابط الشرطة القضائية الذي وجد أشياء تفيد في مجريات التحريات وأراد ضبطها أن يعرضها على المراد تفتيشه للتعرف عليها وعلى طبيعتها والمحافظة عليها، وذلك عملا بنص المادة 84 من قانون الإجراءات الجزائية أنه "... ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة.

ولا يجوز فتح هذه الأحراز إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعاؤهما قانونا كما يستدعي أيضا كل من ضبطت لديه هذه الأشياء لحضور هذا الإجراء ولا يجوز لقاضي التحقيق أن يضبط غير الأشياء النافعة في إظهار الحقيقة أو التي قد يضر إفشاؤها بسير التحقيق ويجوز لمن يعنيهم الأمر الحصول على نفقتهم، وفي أقصر وقت على نسخة أو صورة فوتوغرافية لهذه الوثائق التي بقيت مضبوطة إذا لم تحل دون مقتضيات التحقيق".

ثانيا: ضمانات المشتبه فيه في مجال تفتيش نظم الحاسوب وضبط المعطيات

إن إجراءات التفتيش في إطار عملية البحث والتحري عن الدليل في الجريمة الإلكترونية هي كذلك تمنح ضمانات للمشتبه فيه، وهاته الضمانات قد تتقلص بالنظر إلى الخصائص التي تتميز بها

[1] - قانون رقم: 16 - 01 المؤرخ في 06 مارس 2016 ، يتضمن التعديل الدستوري، الصادر بالجريدة الرسمية رقم 14 المؤرخة في 07 مارس 2016

الجرائم الإلكترونية عن غيرها من الجرائم الأخرى كسرعة تنفيذها ومحو آثارها وبعدها المتخطي للحدود الوطنية ويبدو ذلك من خلال ما يلي([1]):

- أن القانون 09 - 04 أجاز اللجوء إلى إجراء التفتيش في الجرائم المعلوماتية حتى ولو لم تقع جريمة بعد لكن ونظرا لخطورة هذا الإجراء على الحق في الخصوصية فإن الشرع قد حصر نطاقه في حالات محددة على سبيل الحصر طبقا لنص المادة 03 من القانون 09 - 04.

- اشترطت المادة 05 ف 02 من القانون 09 - 04 الدخول إلى المنظومة المعلوماتية بغرض تفتيشها بضرورة أن تكون هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة فعلا في هذه المنظومة محل التفتيش، كما يفهم من نص المادة 06 من القانون 09 - 04 أنه إذا كان ليس من الضروري حجز كل المنظومة المعلوماتية فإن السلطة التي تباشر التفتيش تقوم فقط بنسخ المعطيات التي تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وهذا ما يعد ضمانة أخرى.

نظرا لطابع السرعة التي تتميز بها الجرائم الإلكترونية وكذا محو آثارها من جهة طابعها الدولي من جهة أخرى مما يعني ارتكابها من عدة دول في نفس الوقت وأن الوقت في بعضها قد يكون ليلا بينما في دول أخرى يكون نهارا، الأمر الذي ساهم المشرع في التنازل صراحة عن شرط ميعاد التفتيش، فأجاز إجراؤه في أي ساعة من ساعات الليل والنهار عملا بنص المادة 47 فقرة 03 من ق إ ج ج.

- أن المشرع الجزائري لا يشترط حضور المشتبه فيه أو من ينوب عنه أثناء عملية التفتيش في الجريمة المعلوماتية وهو ما نص عليه صراحة في المادة 45 ف 5 ق إ ج ج بقولها أنه لا تطبيق الأحكام المنصوص عليها في هذه المادة إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

- عملا بنص المادتين 08 و09 من القانون رقم 09 - 04 يمكن للسلطة التي تباشر التفتيش أن تأمرباتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي تشكل محتواها جريمة، ولا يجوز استعمال المعلومات المتحصل عليها إلا في الحدود الضرورية للتحريات والتحقيقات القضائية.

- أوجب المشرع بموجب المادة 06 فقرة 01 من قانون 09 - 04 بضرورة المحافظة على المضبوطات المخزنة عن طريق نسخها على دعامة تخزين إلكترونية تكون قابلة للوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

- كما أوجب الشرع أيضا على السلطة التي تقوم بضبط المعطيات العمل على سلامة المعطيات في المنظومة المعلوماتية محل التفتيش وأنه إذا ما استعملت تقنيات لإعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال فإن ذلك يجب ألا يؤدي إلى المساس بمحتواها.

[1]- سعيداني نعيم، المرجع السابق، ص 199

الفرع الثاني: ضمانات المشتبه فيه أثناء إجراء اعتراض المراسلات والمراقبة الإلكترونية

مما لا شك فيه أن مراقبة الاتصالات الخاصة وكذا اعتراض المراسلات يمس بحق الإنسان في الخصوصية ويعد اعتداء صارخا على الحياة الخاصة، ذلك الحق الذي حظي بحماية دستورية في مختلف التشريعات الحديثة، لما لخصوصية الأفراد من أهمية قصوى على كيان الفرد والمجتمع معا والحق في الخصوصية وما يتفرع عنه من حرية المراسلات وسرية الأحاديث الخاصة أضحى في الوقت الراهن تحت تهديد وسائل تقنية حديثة اخترقت الحجب ونفذت من خلال السياج المنيع الذي يحيط بالحياة الخاصة. ولقد كفلت القوانين للفرد حقه في خصوصية مراسلاته بغض النظر عن وسيلة إرسالها سواء كانت مرسلة بواسطة البريد العادي أم بواسطة الإنترنت (البريد الإلكتروني Email) وسواء كانت هذه الرسالة مغلقة أم مفتوحة مشفرة أم غير مشفرة، طالما أن من الواضح قصد المرسل عدم رغبته في إطلاع الغير عليها بدون تمييز، وبالتالي فإن حرمة المراسلات مستمدة من الحق في الحياة الخاصة لأنها تعتبر مستودعا للسر فلا يجوز المساس بها إلا بموافقة من يتعلق الخطاب بحياته الخاصة[1].

إن المشرع الجزائري بموجب القانون 06 - 23 المؤرخ في 2006/12/20 المعدل والمتمم للأمر رقم 66 - 156 المؤرخ في 08 يونيو 1966 والمتضمن قانون العقوبات أضاف المادة 303 مكرر يعاقب بالحبس لكل من يتعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث أو سرية، بالإضافة إلى المادة 127 من القانون 2000 - 03 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية ([2]) التي تنص كذلك على معاقبة كل شخص سواء كان مرخصا له بتقديم خدمة المواصلات السلكية واللاسلكية أو كان عاملا لدى متعاملي الشبكات العمومية للمواصلات السلكية واللاسلكية أو أي شخص آخر غير هؤلاء يقوم بأي طريقة كانت بانتهاك سرية المراسلات الصادرة أو المرسلة أو المستقبلة عن طريق المواصلات السلكية أو اللاسلكية.

وإذا كان المشرع قد أباح وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع محتواها وكذا اعتراض المراسلات السلكية واللاسلكية، فإنه قد أحاط هذه الإجراءات بمجموعة من الضمانات التي تعد ضرورية لحماية حق الإنسان في سرية اتصالاته. وهذا ما يمكن أن نجمله في ما يلي:

أولا: ضمانات المشتبه فيه عند اعتراض المراسلات

- لا يجوز لأعضاء الضبطية القضائية إجراء اعتراض للمراسلات السلكية أو اللاسلكية إلا بموجب إذن مكتوب من السلطة المختصة وكيل الجمهورية في حالة التحقيق الابتدائي، أو قاضي التحقيق إذا ما

[1] - سعيداني نعيم المرجع السابق ص 201

[2]- القانون 2000 - 03 المؤرخ في 05 غشت 2000، يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الصادر بالجريدة الرسمية رقم 48 المؤرخة في 05 غشت 2000.

أفتتح تحقيق قضائي، عملا بأحكام المادة 65 مكرر5 من ق إ ج ج.

- ضرورة تضمن الإذن بالاعتراض وصفا للمراسلات التي يجب اعتراضها والمدة التي يجب أن تستغرقها التدابير اللازمة في هاته العملية والمحددة بموجب المادة 65 مكرر 7 بأربعة أشهر.

- عملا بنص المادة 65 مكرر 9 ق إ ج ج يلزم على ضابط الشرطة المأذون له أن يحرر محضرا عن كل عملية اعتراض ويذكر تاريخ وساعة بداية هذه العمليات والانتهاء منها.

- ألزم المشرع بنص المادة 65 مكرر 10 من قانون الإجراءات الجزائية ضابط الشرطة القضائية أن ينسخ فقط المراسلات والمحادثات التي تكون مفيدة في إظهار الحقيقة[1].

ثانيا: ضمانات المشتبه فيه أثناء مراقبة الاتصالات

حدد المشرع في نص المادة 04 من نفس القانون صراحة الحالات التي يجوز فيها اللجوء إلى هذا الإجراء إذا كان الغرض منه الوقاية فقط دون أن تكون هناك جريمة قد وقعت أصلا وذلك كوسيلة لإجهاض المشروعات الإجرامية التي يكون الهدف منها النيل من المصالح الكبرى للدولة ويكون من الصعب معالجة آثارها إذا تحققت فعلا، مقدرا خطورة وجسامة هذه الأفعال والتي منها الأفعال الموصوفة بالجرائم الإرهابية والجرائم الماسة بأمن الدولة أو الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني. أما في إطار التحريات والتحقيقات القضائية فإنه لا يتم اللجوء إلى إجراء المراقبة الإلكترونية للاتصالات إلا في الحالة التي يكون فيها من الصعب الوصول الى نتيجة تهم هذه التحقيقات دون اللجوء إلى هذا الإجراء.

في هذا الصدد نص المشرع في المادة الثالثة من القانون 09 - 04 باشتراط القيام بإجراء المراقبة الإلكترونية للاتصالات في إطار احترام الأحكام القانونية التي تضمن سرية المراسلات والاتصالات حينما نصت: " مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات. .. يمكن وضع ترتيبات لمراقبة الاتصالات. .. "

اشترط في المادة الرابعة الفقرة السادسة من القانون09 - 04 أنه لا يجوز إجراء عمليات المراقبة إلا بإذن مكتوب من السلطة القضائية[2].

[1] - إرجع إلى نص المادة 65 مكرر ق إ ج ج.

[2] - تكلم المشرع عن تحديد مدة المراقبة في حالة واحدة فقط تتعلق بالمراقبة الإلكترونية التي يقوم بها ضباط الشرطة القضائية المنتمين إلى الهيئة الوطنية للوقاية من الجرائم المتحصلة بتكنولوجيات الإعلام والإتصال بخصوص تحريهم للوقاية من أفعال موصوفة بجرائم الإرهاب والجرائم الماسة بأمن الدولة وهي ستة أشهر قابلة للتجديد.

الفصل الثاني

استخلاص الدليل الإلكتروني وقيمته الثبوتية

نتيجة للتطور العلمي وثورة المعلومات والأعمال الإلكترونية، فإن الدليل التقليدي أصبح لا يتفق بشكل كامل مع طبيعة الوسط الذي ارتكبت فيه الجريمة حتى يستطيع القاضي أن يتبني القناعة الكاملة في الإثبات، ولهذا ظهرت طائفة جديدة من الأدلة تتفق مع طبيعة الوسط الذي ارتكبت فيه الجريمة وهو الدليل الإلكتروني الذي أجبر العاملين في ميدان القانون وخاصة ميدان القضاء إلى إعادة التصنيف التقليدي لمختلف طرق الإثبات التي لم تعد مواكبة ومسايرة للثورة التكنولوجية وهذا بالنظر لخصائص ومميزات الأدلة الإلكترونية، حيث أصبح بموجبه القاضي أن يبني قناعته ويصدر قراره.

و عليه سأحاول من خلال هذا الفصل تحليل وتأصيل المفهوم القانوني للدليل الإلكتروني في المبحث الأول، ونميط اللثام في المبحث الثاني على إشكالية مدى تبني القاضي الجزائي لنظام الإثبات الإلكتروني بعد مناقشة القيمة القانونية له والحجية التي يكتسبها من إجراءات استخلاصه.

المبحث الأول: ماهية الدليل الإلكتروني والقواعد الإجرائية لاستخلاصه

تستند عملية الإثبات الجنائي في الجرائم الإلكترونية على الدليل الإلكتروني باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم الحديثة العهد[1]، فيترى ماهو الدليل الإلكتروني؟ وهو ما نجيب عنه في المطلب الأول من هذا المبحث، وماهي القاعد الإجرائية المعتمدة في استخلاصه؟ وهو ما نسترسل فيه بشيء من التفصيل في المطلب الثاني.

المطلب الأول: ماهية الدليل الإلكتروني

يجب أن يتم استعمال الدليل الإلكتروني بنوع من الحيطة خاصة مع التذبذب في استخدام المصطلحات القانونية وفي التعبير عنها، والتي تتأرجح بين الدليل المعلوماتي preuve informatique، دليل رقمي preuve numérique، دليل تكنولوجيا المعلومات IT evidence

الفرع الأول: تعريف الدليل الإلكتروني

عرف الدليل الإلكتروني بأنه " الدليل الذي يجد أساسه له في العالم الافتراضي ويقود إلى الجريمة، فهو كل بيانات يمكن إعدادها أو تخزينها بشكل إلكتروني بحيث تمكن الحاسوب من إنجاز مهمة ما "[2]

الدليل الإلكتروني هو الدليل المأخوذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم، كما يمتد مفهومه إلى المعطيات اللصيقة بهاته الأخيرة، (إسم الملف، المجلد، تاريخ ووقت إنشاء الملف، آخر مرة تمت فيها عملية الكتابة وآخر مرة تمت فيها عملية الدخول...إلخ)[3].

وعرف كذلك بأنه " معلومات يقبلها العقل والمنطق ويعتمدها العلم، يتم الحصول عليها بإجراءات علمية وقانونية بترجمة المعلومات والبيانات المخزنة في الحاسوب وملحقاته وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق والمحاكمة لإثبات حقيقة فعل أي شيء أو شخص له علاقة بجريمة "[4].

---

[1] - خالد عياد الحلبي - المرجع السابق، ص 229.

2 - مناصرة يوسف - الدليل الإلكتروني في القانون الجزائي - منشورات دار الخلدونية - الجزائر - طبعة 2018 ،ص29 - 31.

[3] - خالد عياد الحلبي المرجع السابق ص 230

[4] - مصطفى محمد موسى - المرجع السابق، ص 213.

كما عرفته المنظمة العالمية لدليل الكمبيوتر IOCE في أكتوبر 2001 بأنه المعلومات القيمة المحتملة والمخزنة أو المنقولة في صورة رقمية.

وكان قد عرفته في مارس 2000 بأنه المعلومات المخزنة أو المقولة والتي يمكن الاعتماد عليها أمام المحكمة.

والدليل الإلكتروني [1] مثله مثل الدليل الكتابي فهو يعبر عن فكر وقول بالكتابة الرقمية بالمعنى الواسع، التي لا تشمل الكتابة التقليدية على الورق فحسب وإنما تشمل أيضا الكتابة التي تتم عن طريق وسائل الاتصال الحديثة مهما كانت الدعامة المستخدمة في تثبيتها. ولهذا نجد بعض الاتفاقيات الدولية قد تبنت هذا المفهوم الواسع للكتابة وكذلك بعض التشريعات المقارنة.

للدليل الإلكتروني أنواع ثلاثة، الأول مخرجات ذات طبيعة ورقية تسجل فيها المعلومات على الورق ويستخدم في ذلك الطابعات والراسم في طباعة الرسومات بدرجات وضوح مختلفة على الورق، النوع الثاني مخرجات ذات طبيعة إلكترونية تستخدم في تخزين المعلومات بدل الوثائق الورقية كالأشرطة المغناطيسية والأوراق المغناطيسية، والنوع الثالث مخرجات مرئية معوضة بواسطة شاشة الحاسب الآلي ذاته ويتمثل هذا النوع في عرض المعطيات المعالجة آليا بواسطة الحاسب الآلي على الشاشة الخاصة به [2]

الفرع الثاني: خصائص ومميزات الدليل الإلكتروني

قياسا على ما أوردناه في خصائص المعطيات الرقمية التي يقتبس منها الدليل الرقمي خصائصه، فهو أولا دليل غير ملموس وثانيا هو دليل من قبيل الأدلة الفنية أو العلمية المستمدة من الآلة machine

IOCE = International Organization on Computer Evidence

[1] - منصور عمر المعايطة - الأدلة الجنائية والتحقيق الجنائي لرجال القضاء والادعاء العام والمحامين وأفراد الضابطة العدلية - دار الثقافة للنشر والتوزيع عمان الطبعة الأولى 2009 ص 27 - حيث يعرف الدليل الإلكتروني كالتالي:

الدليل من الناحية اللغوية بأنه هو ما يستدل له في اللغة دله الطريق، كما يقال أدل بمعنى أمل وكما يقصد به الثقة فيقال فلان يدل فلان بمعنى يثق به. أما الدليل شرعا فهو ما يلزم من العلم به العلم بشيء أخر.

والمشرع الجزائري لم يعرف الدليل وإنما ترك ذلك للفقه والقضاء. ويعرف الدليل بأنه الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه

وقد جاءت كلمة الدليل في القرآن الكريم في قوله تعالى (ألم تر إلى ربك كيف مد الظل ولو شاء لجعله ساكنا ثم جعلنا الشمس عليه دليلا) (الفرقان 45)، ويستخدم لفظ الدليل في الإصلاح الشرعي بمعنى البينة، والتي تعني بدورها الحجة والبرهان. فمن المتفق عليه لدى الفقهاء أن البينة اسم لكل ما يبين الحق ويظهره وقد عرف قضاة المحكمة العليا الدليل على أنه هو البينة أو الحجة التي يستمد منها القاضي البرهان على اقتناعه بالحكم الذي يصدره، قد يكون الدليل مباشرا كالاعتراف وشهادة الشهود وتقرير الخبرة أو غير مباشر كالقرائن قرارات صادرة عن الغرفة الجنائية الأولى، القرار الأول يوم 26 جوان 1984 في الطعن رقم 34186 والثاني 8 نوفمبر 1983 في الطعن رقم 33185 والثالث يوم 4 يناير 1988 في الطعن رقم 30093 وقرار صادر يوم 5 أفريل 1988 في الطعن رقم 47646 - يوسف مناصرة - المرجع السابق ص 30).

[2] - مناصرة يوسف المرجع السابق ص 33

والخصيصة الثالثة أن فهم مضمون الدليل الرقمي يعتمد على استعمال أجهزة تجميع وتحليل محتواه ليكون دليل إثباتها.

والدليل الرقمي غير مادي لأنه يتكون من معطيات ومعلومات ذات هيئة رقمية غير ملموسة وإخراجه في شكل مادي ملموس يتطلب الاستعانة بأجهزة الإعلام الآلي وملحقاته واستخدام أنظمة البرمجة، إذ أنه يتميز بالسرعة والسهولة وصعوبة محوه أو تخريبه وإن حاول المجرم محو الدليل الرقمي، فإن هذه المحاولة بذاتها تسجل عليه كدليل كما أن الطبيعة الفنية للدليل الرقمي تكمن في إخضاعه لبعض البرامج والتطبيقات للتعرف على ما إذا كان قد تعرض للغش والتحريف. ووفق لما سبق، يتميز الدليل الإلكتروني بجملة من المميزات لعل أهمها:

- يتكون الدليل الإلكتروني من بيانات ومعلومات ذات صفة إلكترونية غير ملموسة ولا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بالحاسوب والأجهزة الإلكترونية باستخدام برامج إلكترونية خاصة بذلك.

- يستطاع من استخدام الدليل الإلكتروني في رصد المعلومات عن الجاني وتحليلها، حيث إن الدليل الإلكتروني يمكن من تسجيل تحركات الفرد وسلوكياته ولذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل التقليدي[1]

- نقص مخاطر إتلاف الدليل الأصلي عن طريق استخدام عملية نسخ الدليل الرقمي من أجهزة الكمبيوتر، حيث تتطابق طريقة النسخ مع طريقة الإنشاء.

- سهولة تحديد ما إذا كان الدليل الرقمي، قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل، باستخدام التطبيقات والبرامج الصحيحة.

- صعوبة محو أو العبث بالدليل، حتى في حالة إصدار أمر بحذفه من جهاز الكمبيوتر، فيمكن للدليل الرقمي أن يعاد استخراجه من خلال برامج الاسترجاع.

- يسجل جهاز الكمبيوتر جميع العمليات التي ترد فيه وعليه فنشاط المجرم المعلوماتي لمحو الدليل، يتم تسجيلها ويمكن استخلاصها لاحقا لاستخدامها كدليل إدانة ضده بالرجوع مثلا لسجلات التدقيق LOG

- تمكين المحققين من استغلال الأدلة على مستوى عالمي بالنظر لرقعة مسرح الجريمة المعلوماتية في إطار تبادل المعلومات بين الدول بسرعة عالية وبمناطق مختلفة من العالم، مما يساهم في الاستدلال على الفاعلين أو أفعالهم بسرعة مقبولة.

- قابليته للهجرة والنقل والحفظ في مواقع تخزين متشعبة بالشبكة المعلوماتية.

[1] - خالد عياد الحلبي المرجع السابق ص233

- ينبأ الدليل الإلكتروني عن عادات وسلوكيات المجرم المعلوماتي ويمكن من إجراء دراسة تحليلية لشخصيته وإعداد ما يعرف بـ: profilage خاصة مع تفشي استغلال المواقع الاجتماعية، مما يسهل الوصول نتائج سريعة في التحريات الجزائية[1].

- إمتيازه بالسعة التخزينية العالية، فآلة الفيديو الرقمية يمكنها تخزين مئات الصور ودسك صغير يمكنه تخزين مكتبة صغيرة...وهكذا[2]

المطلب الثاني: القواعد الإجرائية لاستخلاص الدليل الإلكتروني في الأوساط الافتراضية

إن التطور التقني الذي لحق نظام المعالجة الآلية، فضلا عن الطبيعة الخاصة للدليل الرقمي، أدى إلى تغيير الكثير من المفاهيم السائدة حول إجراءات وطرق الحصول عليها، وهو الأمر الذي فرض معه ضرورة إعادة تقييم مناهج بعض الإجراءات المتبعة في استخلاص الدليل الإلكتروني في الأوساط الافتراضية في قانون الإجراءات الجزائية، والتي ثبتت عدم كفايتها نظرا للميزات التي تتسم بها، الأمر الذي فرض معه ضرورة استحداث قواعد إجرائية أخرى تتلاءم مع طبيعة البيئة التقنية، تستند هاته الأخيرة على طرق ومناهج بحث متخصصة ومتطورة، قائمة على أساليب وتجارب علمية صحيحة ومؤكدة، أو على الأقل خاضعة للمعايير الدولية في استخلاصها من البيئة الإلكترونية، لأن هذا النوع من

العالم تنتهجه فئة ذكية - إلى حد ما - من أصناف المجرمين، الأمر الذي يفرض معه أن تكون الهيئات المختصة بالبحث والتحري على مستوى من الذكاء الذي يتمتع به المجرمين في تقصي الدليل وتقفي الأثر le depistage، أخذين في الحسبان عاملي سرعة التنفيذ والكفاءة في الأداء، وعلى درجة من المعرفة العملية المعمقة ومهارة فنية فائقة، وهذه الأخيرة تتطلب إجراءات خاصة وتكوين عالمي لهاته الفئة من

المحققين ضمن مجالات تطبيق محددة[3].

فتطو ر الإثبات ووسائله أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم، وهو الأمر الذي سوف نعالجه من حيث بحث القواعد الإجرائية التقليدية، وإبراز إلى أي مدى يمكن الاستناد إليها في الحصول على الدليل الرقمي، ثم نعرج إلى القواعد الإجرائية الحديثة في استخلاص الدليل الإلكتروني

فبمناسبة تطرقنا للقواعد الإجرائية لاستخلاص الدليل الإلكتروني، تستوقفنا ضرورة حتمية وجب مناقشتها، قبل الخوض في هاته الإجراءات، وهي كيفية اتصال المحقق بالجريمة، لينطلق بعدها في إجراءات التنقيب المتمثلة في البحث والتحري عن الجريمة المرتكبة، معتمدا في ذلك على جملة القواعد الإجرائية التي سنتطرق لها لاحقا.

---

[1] - مناصرة يوسف المرجع السابق ص36 .

[2] - مصطفى محمد موسى المرجع السابق ص218.

[3] - مصطفى محمد موسى المرجع السابق ص74 .

يصل إلى علم المحققين وقوع الجرائم إما بتلقي البلاغات من طرف عامة الناس أو الشكاوى من الأطراف المضرورة، إلا أنه يثار تساؤل حول ما إذا كانت هناك جهات مختصة لتلقي البلاغات والشكاوى بشأن الجريمة الإلكترونية، أم أنها تقدم أمام الجهات المختصة بتلقي البلاغات والشكاوى في الجرائم العادية؟

1 / تلقي البلاغات والشكاوى حول الجريمة الإلكترونية

بمجرد التبليغ عن وقوع الجريمة الإلكترونية، فإنها تتخذ عدة إجراءات للتأكد من وقوعها وكشف مرتكبها، فمعرفة المحققين لوقوع جريمة ما يتم وفق طريقتين:[1]

أ - البلاغات في الجريمة الإلكترونية: الذي هو إخبار السلطات المختصة عن وقوع جريمة، أو أنها على وشك الوقوع، أو أن هناك اتفاقا جنائيا أو أدلة أو قرائن، أو عزما على ارتكابها أو وجود شك أو خوفا من أنها ارتكبت.

كيفية التبليغ في الجريمة الإلكترونية: قد يكون البلاغ واجب في بعض الجرائم وقد يكون اختياري في البعض الأخر، واستنادا إلى نص المادتين "32 من ق.ع و91 من ق ا ج " يتم التبليغ بمختلف الوسائل التي توصل المعلومات إلى الجهات المختصة بالتحقيق فقد يكون التبليغ كتابيا، أو شفويا ومن أي

شخص سواء كان متضررا أو غير متضرر وهذا ما يطلق عليه مصطلح البلاغ المادي وقد يقدم بواسطة البريد أو التلفون أو الصحف وهذا ما يصطلح عليه البلاغ المعنوي، وقد يتم عن طريق الإنترنت وهذا ما يسمى بالبلاغ الرقمي وذلك إما عن طريق إرسال رسالة الإلكترونية إلى عنوان البريد الإلكتروني للجهات المختصة بالتحقيق كإبلاغها عن وجود صفحات أو مواقع غير مشروعة بإرسال رسالة الإلكترونية مثلا، تتضمن التبليغ عن وجود موقع منشور فيه صور الاستغلال الجنسي للأطفال.

ب - الشكوى في الجريمة الإلكترونية:

قد يترتب على الجريمة ضرر خاص قد يصيب احد الأفراد ماديا أو معنويا فينشأ له حق في تحريك الدعوى العمومية بتقديم شكوى أمام الجهة المختصة بالتحقيق[2] حيث نص المشرع الجزائري في المادة 72 من ق ا ج على " يجوز لكل شخص متضرر من جناية أو جنحة أن يدعي مدنيا بأن يتقدم بشكواه أمام قاضي التحقيق المختص" وقد عرفت الشكوى بأنها البلاغ أو الإخطار الذي يقدمه المجني عليه أو وكيله الخاص إلى السلطات المختصة طالبا تحريك الدعوى العمومية بشأن جرائم معينة، ولا

[1] - بختي فاطمة الزهراء، المرجع السابق، ص 54

[2] - محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، ط2 ،2009 ،ص28.

يوجب القانون للشكوى شكلا معينا وإنما يقتصر فيها المعني بالأمر على ذكر اسمه وسنه عنوانه وموجز الوقائع، وإعطاء كافة المعلومات الخاصة بمرتكب الجريمة إذا كان معلوما[1].

2 / الاستجواب وسماع الشهود في الجريمة الإلكترونية

يستدعى أشخاص للإدلاء بأقوالهم، قد يكونون مشتبه فيهم وهذا ما يطلق عليه الاستجواب، وقد يكون هؤلاء أشخاص خارجين عن الخصومة إلا أنهم يؤثرون على مسار القضية من خلال شهادتهم.

أ - الاستجواب في الجريمة الإلكترونية: الاستجواب هو مناقشة المتهم بالتهمة والوقائع المنسوبة إليه ومواجهته بالأدلة القائمة ضده، والمتهم حر في الإجابة عن الأسئلة الموجهة إليه ولا يعد امتناعه قرينة ضده، وهو وسيلة تمحيص للتهمة أو لنفيها عنه، والاستجواب ذو طبيعة مزدوجة، فهو أداة اتهام ووسيلة دفاع في آن واحد [2]، وينقسم الاستجواب إلى [3]:

أ/1 - الاستجواب عند الحضور الأول في الجريمة الإلكترونية: وهو أن يمثل المتهم أمام المحقق لأول مرة وذلك حتى يتحقق من هويته ويحيطه علما بكل الوقائع المنسوبة إليه وينبهه بأنه حر في الإدلاء بأقواله أو عدم الإدلاء بها، كما يجب على المحقق أن يخير المتهم في أن له الحق في توكيل محام وإن كان غير قادر ماديا يجوز للمحقق أن يعين له محام من تلقاء نفسه، كما يجب على المتهم إذا ما طرأ تغيير على عنوانه أن يخطر المحقق.

أ/2 - الاستجواب في الموضوع في الجريمة الإلكترونية: ويعني الاستجواب مواجهة المتهم بالتهمة والوقائع المنسوبة إليه ومناقشته فيهما مناقشة تفصيلية ومواجهته بالأدلة القائمة ضده ومطالبته بإبداء رأيه فيها ويكون إجباري كما هو الشأن بالنسبة للجنايات أو اختياري في الجنح.

أ/3 - الاستجواب الإجمالي في الجريمة الإلكترونية: يهدف إلى تلخيص الوقائع وإبراز الأدلة التي سبق جمعها خلال كافة مراحل التحقيق والإشارة إلى الاستعلامات التي وردت في شأن وحياة وسلوك وشخصية والسوابق العدلية للمتهم، ويختم بطرح السؤال التالي: هذا هو استجوابك الأخير فهل لديك ما تدلي به للدفاع عن نفسك؟ ويحتوي الملف الجنائي على الوثائق التالية: شهادة الميلاد المتهم، صحيفة السوابق العدلية، تقرير البحث الاجتماعي ويقصد بهذا الأخير ندب خبير لإجراء بحث اجتماعي عن حياة المتهم، وسلوكه وأخلاقه في المحيط الذي كان يعيش فيه وكذا محيط مهنته، وكل ما يتعلق بحياته

[1] - نبيلة هبة هروال - الجوانب الإجرائية لجرائم الإنترنت، في مرحلة جمع الاستدلالات، دراسة مقارنة، دار الفكر الجامعي الإسكندرية، الطبعة الأولى 2007 ص 189

[2] - فرج علواني هليل، المرجع السابق، لتحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، الإسكندرية، 2006ص 645

[3] - محمد حزيط، قاضي التحقيق، المرجع السابق، ص 59.

الاجتماعية، وكذا شهادة جيرانه سواء قام به المحقق بنفسه أو عن طريق إنابة قضائية لأحد ضباط الشرطة القضائية[1].

ب/ سماع الشهود في الجريمة الإلكترونية: سماع الشهود هو إجراء من إجراءات التحقيق، يهدف لجمع الأدلة المتعلقة بالجريمة بحيث يستدعى أشخاص ليست لهم علاقة بالجريمة إلا أن وجودهم ضروري للكشف عن الجرائم والقبض عن مرتكبيها، وتخلف الشاهد عن الحضور للإدلاء بشهادته يعرضه للمسائلة الجنائية، وعليه سأتطرق أولا لتعريف الشهادة ثم الشهادة في الجريمة الإلكترونية.

يختلف الشاهد في الجريمة الإلكترونية عن الشاهد في الجرائم العادية لما يتميز به من صفة خاصة تمنحه إياها طبيعة عمله وخبرته في مجال المعلوماتية وقد عرف الشاهد الإلكتروني بأنه: "الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي الذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات ويمكن القول أن الشاهد الإلكتروني هو كل من:

ب1/ مشغلو الحاسب الآلي: هو ذلك الشخص المسؤول عن تشغيل الجهاز والمعدات المتصلة به حيث تكون لديه الخبرة في مجال الحاسب الآلي عن طريق استخدام البيانات واستخراجها كما تكون لديه الخبرة الواسعة في الكتابة السريعة عن طريق لوحة المفاتيح.

ب2/ خبراء البرمجة: هم الأشخاص المتخصصون في كتابة أوامر البرامج وينقسمون إلى فئتين: الأولى هم مخططو برامج التطبيقات والثانية هم مخططو برامج النظم [2].

ج/ المحللون: هم الأشخاص الذين يحللون الخطوات، ويقومون بتجميع البيانات الخاصة بنظام معين، ودراسة هذه البيانات ثم تحليل النظام- تقسيمه - إلى وحدات منفصلة واستنتاج العلاقة الوظيفية بين هذه الوحدات، كما يتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات، واستنتاج الأماكن التي يمكن هيمنتها بواسطة الحاسوب[3].

د/ مهندسو الصيانة والاتصالات: هم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب ومكوناته وشبكات الاتصال المتعلقة به.

هـ/ مديرو النظم: هم الذين توكل لهم أعمال الإدارة في النظم المعلوماتية[4].

---

[1] - محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، ط3، 2008، ص 108،109 .

[2]- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة ط1، 2009،ص612.

[3]- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة ط1، 2009 ص 613.

[4] - خالد ممدوح إبراهيم، المرجع السابق، ص264

الفرع الأول: القواعد الإجرائية التقليدية في استخلاص الدليل الإلكتروني

إن المشرع الإجرائي أوجد قواعد إجرائية معينة لاستخلاص الدليل الإلكتروني في الجرائم الإلكترونية، أهمها المعاينة، الخبرة، التفتيش وضبط الأشياء ومما لا شك فيه أيضا أن هذه القواعد عامة النطاق تنظم استخلاص الدليل في جميع الجرائم، تقليدية كانت أم مستحدثة إلا أنها بحاجة إلى تطوير لكي تتناسب مع طبيعتها الخاصة وطبيعة الدليل الذي يصلح لإثباتها.

أولا: التفتيش في الوسط الإلكتروني

لم يورد المشرع الجزائري تعريفا خاصا ودقيقا للتفتيش بقدر ما أعتبره إجراء من إجراءات التحقيق وإحاطته بضوابط صارمة نظرا لأهميته في كشف الأدلة وخطورته فيما قد يترتب عنه من مساس بحرية الأشخاص وبكرامتهم ومما يؤكد ذلك اهتمام الدستور الجزائري بهذه النقطة في المادة 47 منه بالقول " فلا تفتيش إلا بمقتضى القانون وفي إطار احترامه، ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة "

فالتفتيش هو إجراء من إجراءات التحقيق " غايته ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد في كشف الحقيقة في شأنها " والتفتيش المتعارف عليه في القواعد الإجرائية نوعان تفتيش المساكن وتفتيش الأشخاص كما نص على ذلك قانون الإجراءات الجزائية في المواد 44 و64 منه والتفتيش المنصب على المنظومة المعلوماتية وهو يختلف من حيث الشروط الشكلية والموضوعية وكذا موضوع التفتيش.

1- تفتيش المنظومة المعلوماتية:

نص قانون 09 - 04 في المادة 05 منه على أنه يجوز للسلطات القضائية المختصة وكذا ضابط الشرطة القضائية الدخول بغرض التفتيش ولو عن بعد إلى[1]:

- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

- منظومة معلوماتية.

يلاحظ بأن التفتيش في الوضعيات المشار إليها يأخذ منحنيين فهو إما أن يكون عملا من أعمالا التحقيق تقوم به السلطات القضائية المختصة وإما يكون من أعمال الاستدلال يقوم به ضباط الشرطة القضائية بناء على أمر تصدره السلطة المختصة وفي كلتا الحالتين فإن المستهدف هنا هو جهاز الكمبيوتر بمكوناته المادية والمعنوية. فالمكونات المادية هي مجموعة وحدات متصلة ببعضها كوحدات الإدخال وحدة الذاكرة الخاصة بالتخزين وهي وحدة المعالجة المركزية ووحدة الذاكرة ووحدة التحكم ووحدة الذاكرة المساعدة ووحدة الإخراج والمتمثلة في أجهزة الشاشة والطابعة ومشغلات الأقراص، أما

[1] - زبيجة زيدان المرجع السابق ص 131.

المكونات المعنوية وتسمى كذلك بالكيانات المنطقية هي مجموعة البرامج والوثائق المتعلقة بتشغيل وحدة معالجة البيانات.

2 - شروط التفتيش: حتى تتسم إجراءات التفتيش بالقانونية وجب مراعاة جملة من الشروط الشكلية والموضوعية:

أ - الشروط الشكلية:

إن التفتيش في مجال المعلوماتية يتوقف أساسا على طبيعة المكان الذي يحتوي أجهزة الكمبيوتر ومكوناته وفيما إذا كان خاصا أم عاما هذا فضلا عن تحديد الإقليم فيما كان وطنيا أم أجنبي

فباستقرائنا لنص المادة 05 المشار إليها أعلاه الناصة على أنه " يجوز للسلطة القضائية المختصة وكذا الشرطة القضائية الدخول بغرض التفتيش لو عن بعد "، يتبين بأن التفتيش يكون بصفة مباشرة بالانتقال إلى مسكن المتهم أو المكان الذي تتواجد فيه الأجهزة المقصودة أو في الأماكن العامة حال حيازة شخص لجهاز حاسوب الآلي أو أحد مكوناته المادية كوسائط التخزين، فالقانون أحال إجراءات التفتيش إلى القواعد العمة في قانون الإجراءات الجزائية.

وفقا لأحكام المادة 44 من ق.إ.ج.ج سيما بعد التعديل بموجب القانون 06 - 22 المؤرخ في 20 ديسمبر 2006 تتم إجراءات التفتيش وفق الخطوات التالية:

- وجود إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق.
- الاستظهار بالإذن قبل دخول المنزل المراد تفتيشه.
- أن يتضمن الإذن بيان وصف الجريمة موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.
- أن يكون التفتيش محدد المدة ونطاقه
- حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.
- في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين الخاضعين لسلطته.
- أن يتم التفتيش بأسلوب آلي إلكتروني من قبل الأجهزة القائمة بالتفتيش وبصورة سريعة[1]
- أن يكون أمر التفتيش مسببا.
- قبل القيام بالتفتيش يجب تجميع فريق التفتيش يتكون من خبراء وفنيين متخصصين بالحاسوب والأنظمة الإلكترونية بالإضافة إلى رجال الضبطية القضائية المكلفين بالمهمة[2].

[1] - جفال يوسف - المرجع السابق، ص 31

[2] - خالد ممدوح إبراهيم المرجع السابق ص 226

ب - الشروط الموضوعية:

- وقوع جريمة إلكترونية سواء جناية أو جنحة.

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

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

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

ثانيا: ضبط الدليل الرقمي

إن النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلة التي يتم الحصول عليها أثناءه، فالضبط إذن هو غاية التفتيش القريبة والأثر المباشر الذي يسفر عنه الإجراء، والأساس القانوني للضبط هو العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق والتي تفيد في كشف الحقيقة ما كان منها ضد المشتبه فيه أو ما كان في مصلحته[1].

ولقد تعودت جهات التحقيق في الجرائم التقليدية أن يقع الضبط على الأشياء المادية فقط بوصفها أدلة مادية للجريمة التي يجري التفتيش بشأنها، لكن في مجال الجرائم المعلوماتية الطبيعية العلمية المعقدة للدليل الرقمي الذي يوجب التفتيش عنه وضبطه لإثبات هذا النوع من الجرائم ليس

كالدليل التقليدي، فالبيئة الافتراضية لا تنتج سكينا أو سلاحا ناريا وإنما تنتج نبضات رقمية تشكل قيمة وجوهر الدليل الرقمي.

1 - أنواع الأدلة محل الضبط في الجرائم المعلوماتية: إن الغاية من التفتيش هو ضبط شيء يتعلق بالجريمة ويفيد التحقيق الجاري بشأنها سواء أكان هذا الشيء أدوات استعملت في ارتكاب الجريمة أو شيئا نتج عنها أو غير ذلك مما يفيد في كشف الحقيقة.

وعلى هذا الأساس فإن من الأشياء التي يتم ضبطها والتحفظ عليها في الجرائم المعلوماتية والتي لها قيمة في إثبات تلك الجرائم ونسبتها إلى المتهم هي:

أ - ضبط جهاز الكومبيوتر وملحقاته: " ذلك أن ضبطه أمر مهم جدا للقول بأن الجريمة الواقعة هي جريمة معلوماتية وأنها مرتبطة بالمكان والشخص الحائز على الجهاز. ولأجهزة الكومبيوتر أنواع مختلفة الأمر الذي يتطلب في ضابط الشرطة القضائية المعرفة الكافية التي تؤهله للتعامل معه والتعرف على مواصفاته بسرعة.

[1] - سعيداني نعيم المرجع السابق ص 158

ب - **ضبط المعدات المستعملة في شبكة الإنترنت** وأهمها المودام Modem وهي الوسيلة التي تمكن أجهزة الكومبيوتر من الاتصال ببعضها البعض عبر خطوط الهاتف.

ج - **وسائط التخزين المتحركة:** كالأقراص المدمجة (أقراص الليزر) والأقراص المرنة والأشرطة المغناطيسية.

د - **ضبط البرمجيات** Softwareفإذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بتثبيت وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.

و- **ضبط البريد الإلكتروني**: والذي يحتوي على برامج متخصصة لكتابة وإرسال واستعراض وتخزين الرسائل الإلكترونية،وهذه الرسائل لا يختلف التعامل معها عن التعامل مع الرسالة الورقية،إذ بمقدور المستخدم أن يطرحها جانبا أو يرد عليها أو ينقلها إلى شخص آخر أو يحفظها في ملف خاص، لذلك فالمحقق الذي يريد ضبط الرسائل الإلكترونية Email boitte الخاص به ثم يشغل برامج البريد الإلكتروني في جهاز حاسوبه ثم مراجعة قائمة الرسائل ليلتقط من بينها الرسالة المطلوبة.

2 - **إجراءات ضبط الدليل الرقمي:** بالرجوع إلى القانون 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نجد أن المشرع وضع طريقتين لضبط الأدلة الرقمية، الأولى وتكون عن طريق نسخ المعطيات محل البحث على دعامة تخزين إلكترونية تكون هذه الأخيرة قابلة لحجزها ووضعها في أحراز حسب ما هو مقرر في قواعد تحريز الدليل المنصوص عليها في قانون الإجراءات الجزائية، والطريقة الثانية تكون باستعمال التقنيات المناسبة لمنع الأشخاص المرخص لهم باستعمال المنظومة المعلوماتية من الوصول إلى المعطيات التي تحويها هذه المنظومة أو القيام بنسخها ويكون ذلك في حالة ما إذا استحال لأسباب تقنية ضبط هذه المعطيات وفق الطريقة الأولى[1].

وإن كان الدليل الرقمي يخضع في ضبطه إلى قواعد تحريز الأدلة الجنائية عموما إلا أنه ونظرا إلى الطبيعة الخاصة له فإن عملية ضبطه وتحريزه تحتاج إلى بعض الإجراءات الخاصة لحمايته فنيا والحفاظ عليه وصيانته من إمكانية العبث به، وهو مانوه عليه المشرع في المادة السادسة الفقرة الثالثة

من القانون 09 - 04 حينما أوجب على السلطات التي تقوم بعملية ضبط الدليل الرقمي أن تسهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، وأن لا يؤدي استعمال الوسائل التقنية في ذلك إلى المساس بمحتوى هذه المعطيات. ومن هذه الإجراءات الخاصة في هذا الإطار نذكر على سبيل المثال:

- الإطلاع على المستندات المبحوث عنها مخول فقط لقاضي التحقيق أو ضابط الشرطة القضائية الذي أنابه عنه.

[1] - سعيداني نعيم المرجع السابق ص 162.

- الاحترام التام لمقتضيات وضرورات التحقيق وعلى الأخص ضمان سر المهنة وحقوق الدفاع[1].

- أخذ نسخة احتياطية عن المعطيات والعمل عليها لضمان عدم المساس بالدليل الأصلي.

- عدم تنفيذ برامج على الحاسوب مسرح الجريمة خوفا من إتلاف الأدلة الموجودة عليه أو محو الذاكرة أو الملفات وعدم السماح للمشتبه به بالتعامل مع الحاسوب.

- ضبط الدعائم الأصلية للمعلومات وعدم الاقتصار على ضبط نسخها.

- عدم ثني القرص لأن ذلك يؤدي إلى تلفه وفقدانه للمعلومات المسجلة عليه

- عدم تعريض الأقراص والأشرطة الممغنطة لدرجات حرارة عالية ولا إلى الرطوبة. وفي هذا الإطار بالذات نجد الهيئة الدولية لدليل الحاسب الآلي IOCE computer on Organzation وضعت عدة ضوابط لعملية ضبط الدليل الرقمي منها ألا تكون الإجراءات المتخذة في تحريز الدليل الرقمي سببا في تغيير طبيعة هذا الدليل وأن تكون جميع الأنشطة المتعلقة بتحريز الوثائق الرقمية أو الدخول إليها أو نقلها موثقة توثيقا كاملا مع المحافظة عليها وتوفيرها للمراجعة، وهو الأمر الذي أوردته كذلك الفقرة الثالثة من المادة 19 من الاتفاقية الأوربية للجريمة المعلوماتية.

ثالثا - الخبرة في إثبات الجرائم الإلكترونية

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

فالخبرة هي الوسيلة التي من خلالها تستطيع سلطة التحقيق والمحكمة تحديد التفسير الفني للأدلة

بالاستعانة بالمعلومات العلمية، فهي في حقيقتها ليست دليلا مستقلا عن الدليل القولي أو المادي، وإنما هي تقييم فني لهذا الدليل، فهي في مجملها تقريرا أو رأي فني صادر عن الخبرة في أمر من الأمور بالجريمة والعنصر المميز للخبرة عن غيرها من إجراءات التحقيق كالمعاينة والشهادة والتفتيش هو الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها في الإثبات، والذي يتطلب معارف علمية أو فنية خاصة لا تتوافر سواء لدى المحقق أو القاضي[2].

1 - تعريف الخبير في الجريمة الإلكترونية: هو الفني المتخصص وصاحب الخبرة في التقنية الإلكترونية وشبكاتها، والذي يكون قد رأى أو سمع أو أدرك بحواسه معلومات هامة لازمة للدخول في نضام المعالجة

[1] - زيبجة زيدان المرجع السابق ص 151

[2] - خالد ممدوح إبراهيم المرجع السابق ص283.

الآلية الرقمية للبيانات، إذا كانت مصلحة التحقيق تقتضي البحث عن الدليل الرقمي الإلكتروني داخله ويتمثل الخبراء الإلكترونيون في ما يلي:

2 - أنواع الخبراء الإلكترونيون:

-المبرمجون.

- المحلل هو الشخص الذي يضع خطوات العمل ويقوم بتجميع بيانات نظام معين.

- مهندس الصيانة والاتصالات.

- مشغل الحاسوب الآلي وشبكاته.

- مدير النظام المعلوماتي.

يجب أن يتوافر لدى خبراء الحاسب الآلي المنتدبين للتحقيق المقدرة الفنية والإمكانيات العلمية والفنية في المسألة موضوع الخبرة ولا يكفي في ذلك حصول الخبير على شهادة علمية، بل يجب مراعاة الخبرة العملية، لأنها هي التي تحقق الكفاءة الفنية. ولذلك لا وجود لخبير معلوماتي لديه الخبرة المتعمقة في سائر أنواع الحسابات وبرمجياتها وشبكاتها، أو لديه القدرة على التعامل مع كل أنواع الجريمة المعلوماتية[1].

3 - أهمية الخبرة في البحث عن الدليل الإلكتروني

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

وتكمن أهمية الخبرة في مجال البحث عن الدليل الإلكتروني في أنها وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل، أو تحديد مدلولها بالاستعانة بالمعلومات العلمية وهي البحث في مسائل مادية أ وفنية يصعب على المحقق أن يبحث فيها، ويعجز عن جمع الأدلة بالوسائل الأخرى للإثبات.

تبرز أهمية الاستعانة بالخبرة في مجال الجرائم الإلكترونية، في أنه عند غيبها تعجز الضبطية القضائية في كشف غموض الجريمة لنقص الكفاءة والتخصص اللازمين للتعامل مع الجوانب التقنية والتكنولوجية التي ارتكبت بواسطتها الجريمة، وهو ما قد يؤدي إلى تدمير الدليل ومحوه بسبب الجهل والإهمال عند التعامل معه. ولعل هذه الأهمية للخبرة في مجال التحقيق في الجريمة الإلكترونية جعل

[1] - عبد الفتاح بيومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والأنترنت، المرجع السابق ص 330

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

رابعا: المعاينة في العالم الافتراضي

تعد المعاينة إجراء من إجراءات التحقيق الابتدائي التي يجوز لسلطات التحقيق اللجوء إليها من تلقاء نفسها كلما أرت في ذلك ضرورة لإجلاء الحقيقة، أو بناء على طلب من الخصوم [1] وهي إجراء بمقتضاه ينتقل المحقق إلى مسرح الجريمة ليشاهد ويفحص بنفسه مكانا أو شخصا أو شيئا له علاقة بالجريمة وهي تجرى بحضور أطراف الدعوى الجزائية، غير أنه يجوز للمحقق إجراؤها في غيابهم نظرا لما تقتضيه من سرعة الانتقال إلى محل الجريمة قبل ضياع أو تعديل الأدلة.

تتم المعاينة في الجرائم الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى مكان وقوع الجريمة، غير أن الانتقال هنا يختلف حسب طبيعة الجريمة الإلكترونية المرتكبة، وإذا كانت الجريمة واقعة على المكونات المادية للأجهزة الإلكترونية كجرائم الاعتداء على الحاسب الآلي أو الأشرطة أو الأقراص الممغنطة، فالانتقال في هذه الحالة يكون ماديا إلى مسرح الجريمة الذي يحوي هذه المكونات لمعاينته والتحفظ على الأشياء التي تعد أدلة مادية تدل على وقوع الجريمة وانتسابها لشخص معين، ثم ضبطها وضعها في أحراز مختومة تقدم للنيابة العامة. أما إذا كانت الجريمة واقعة على المكونات غير المادية للأجهزة الإلكترونية أو بواسطتها، كتلك الواقعة على برامج الحاسب وبياناته بواسطة الأنترنت فيكون الانتقال للمعاينة هنا افتراضيا أو إلكترونيا، ويمكن للمحقق إجراء المعاينة الافتراضية أو الإلكترونية بالولوج والانتقال إلى مسرح الجريمة عبر الانترنت انطلاقا من مكتبه بواسطة الحاسب الموضوع تحت تصرفه، أو من خلال مقهى الانترنت أو إحدى مقرات مزود خدمات الانترنت.

ويلتزم المحقق عادة قبل البدء في المعاينة الإلكترونية بجملة من التدابير الفنية والتحفظية التي تساعده في القيام بمهامه على أحسن وجه هي كالتالي:

- الاستعلام المسبق عن مكان وقوع الجريمة، ونوع وعدد ومواقع الأجهزة الإلكترونية وشبكاتها وسائر ملحقاتها والنهايات الطرفية المتصلة بها المتوقع مداهمتها.

-. توفير الوسائل والإمكانات اللازمة من أجهزة وبرامج وأقراص صلبة ولينة التي يمكن الاستعانة بها في الفحص، التشغيل، الضبط والتأمين وحفظ المعلومات.

[1] - براهيمي جمال المرجع السابق، ص 56

- تأمين التيار الكهربائي بشكل لا يتم التلاعب أو التخريب عن طريق قطع التيار أو تعديل الطاقة الكهربائية.

- التأكد من خلو المحيط الخارجي لمسرح الجريمة الإلكترونية من أية مجالات لقوى مغناطيسية او ممرات اتصالات التي يمكن أن تتسبب في محو البيانات المسجلة أو إتلاف الآثار الأخرى للجريمة.

- التحفظ على محتويات سلة المهملات ومستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة لرفع ومضاهاة ما قد يوجد عليها من بصمات.

- إعداد فريق من المتخصصين وأهل الخبرة في مجال تكنولوجية الإعلام الآلي للاستعانة بهم عند الحاجة.

*** نطاق إعمال المعاينة الإلكترونية**

يعتمد المحقق الجنائي لإجراء المعاينة الإلكترونية بحثا عن الأدلة الرقمية على فحص مجموعة مصادر الدليل في البيئة الإلكترونية التي ارتكبت فيها الجريمة المعلوماتية، والمتمثلة عادة في مكونات أجهزة الحواسيب الخاصة بالجاني والمجني عليه وملحقاتها وكذا أنظمة الاتصال بالأنترنت [1].

1 - معاينة مكونات الحاسب: تعتمد عملية الفحص هنا على طريقتين أساسيتين، الأولى هي الفحص الذاتي من خلال قيام الحاسب ذاته بفحص مكوناته وتقديم تقرير كامل إلى طالب الفحص، ومثل هذه العملية تتطلب من القائم بها معرفة تقنية ومهارة فنية عالية. أما الطريقة الثانية، فهي الفحص بواسطة حاسب آلي آخر أو أجهزة تقنية عالية للبحث في جزئية أو جزئيات عبر الحاسب تشمل عملية فحص مكونات الحاسب الآلي العناصر التالية [2]:

أ - معاينة القرص الصلب، ب - معاينة البرمجيات، ج - معاينة النظام المعلوماتي

2 - معاينة أنظمة الاتصال بشبكة الانترنت: ويقصد بأنظمة اتصال بشبكة الانترنت بالمفهوم الإجرائي، تلك الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة الاتصال بالأنترنت، لذلك فعملية فحص أو معاينة هذه الأنظمة يشمل بالأساس فحص مسار الأنترنت أو ما يعرف ببروتوكول الانترنت، والنظام الأمني للشبكات، وكذا فحص الخادم وتتم عن طريق: فحص مسار الأنترنت وفحص الخادم serveur.

[1]- براهيمي جمال، المرجع السابق، ص 59

[2]- خالد ممدوح إبراهيم ، المرجع السابق، ص 215 .

الفرع الثاني: القواعد الإجرائية الحديثة لاستخلاص الدليل

اعتبارا للطبيعة الخاصة للجرائم الإلكترونية في عناصرها ووسائل وتقنيات ارتكابها، اضطر المشرع الجزائي الجزائري كغيره من الدول إلى إعادة النظر في كثير من المسائل الإجرائية [1]، خاصة فيما يتعلق بمسألة التحري والتحقيق عن الجرائم الإلكترونية والأساليب الإجرائية الواجب انتهاجها في سبيل استخلاص الأدلة الإلكترونية، التي تساهم في بناء مبدأ حجية إثبات هذا النوع من الجرائم، ويساهم في منع إفلات العديد من المجرمين من العقاب. وعلى ضوء ما تقدم، أوجد المشرع قواعد إجرائية جديدة أكثر فعالية تحمل معها طرقا إجرائية مدعمة من قبل التقنية ذاتها، يمكن للجهات المكلفة بالبحث والتحري عن الجريمة الإلكترونية الاعتماد عليها في الكشف عن المجرم المعلوماتي والوصول إلى دليل الإثبات فيها بسرعة وسهولة، وهي الإجراءات التي استحدثها في تعديله لقانون الإجراءات الجزائية الجزائري بالقانون رقم 06 - 22 المؤرخ في 20 ديسمبر 2006، وهي أساليب يعرفها من قبل في المواد من 65 مكرر 05 إلى 65 مكرر 18 منه والمتمثلة في اعتراض المراسلات وتسجيل الكلام المتفوه به والتقاط الصور والتسرب، لأجل مواكبة أشكال الإجرام المستحدث، الذي يمارس من قبل أشخاص محترفون يتفننون في ارتكابه بوسائل تكنولوجية حديثة من حيث التنظيم والتخطيط.

إلا أن هذه الأساليب التي منحها المشرع لضباط لشرطة القضائية في مجال البحث والتحري مقصورة إلا في جرائم محددة حصريا في المادة 65 مكرر 05 من ق إ ج وهي جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال والإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد وهذا بعد إذن مسبق من وكيل الجمهورية أو قاضي التحقيق، والإجراءات التي جاء بها القانون رقم 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الذي أدرج إجراءين آخرين هما المراقبة الإلكترونية في المادة 04 منه، وحفظ المعلومات المتعلقة بحركة السير في المادة 11 منه، وهو ما سوف نتناولها بشيء من التفصيل في المسائل إجرائية الحديثة.

أولا: اعتراض المراسلات السلكية واللاسلكية.

استحدث المشرع الجزائري بموجب القانون رقم 06 - 22 المؤرخ في 2006/12/20 المعدل والمتمم لقانون الإجراءات الجزائية من خلال الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، وقد ضمنه ستة مواد من المادة 65 مكرر5 إلى المادة 65 مكرر 10، وتناول من خلالها المقصود بهذا الإجراء وضمانات استخدامه.

[1] - براهيمي جمال، المرجع السابق، ص 81.

1 - مفهوم إجراء اعتراض المراسلات السلكية واللاسلكية وشروطه القانونية.

ورد في اجتماع لجنة الخبراء للبرلمان الأوروبي بستراسبورغ المؤرخ في 2006/10/06 حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية تعريفا لإجراء اعتراض المراسلات بأنها عملية مراقبة سرية المراسلات السلكية واللاسلكية، وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجرائم[1].

وقد اقتبس المشرع الجزائري هذا التعريف بشيء من التفصيل في المادة 65 مكرر5 من قانون الإجراءات الجزائية، إذ اعتبر عملية مراقبة المراسلات بأنها " اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهذه المراسلات عبارة عن بيانات قابلة للانتهاج والتوزيع، التخزين، الاستقبال والعرض.

فاعتبرت المادة 9 ف 6 من القانون 2000 - 03 المؤرخ في 2000/08/05 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات، أن مادة المراسلة هي كل اتصال مجسد في شكل كتابي يتم عبر مختلف الوسائل المادية التي يتم ترحيلها إلى العنوان المشار إليه من طرف المرسل نفسه أو بطلب منه، لا تعتبر الكتب والمجلات والجرائد واليوميات كمادة مراسلات.

وبالتالي فحسب مفهوم هذه المادة فإن المراسلات الخاصة تصبح محصورة في الرسائل المكتوبة بالمفهوم التقليدي.

وبالرجوع إلى نص المادة 46 من الدستور الجزائري لسنة 2016 التي تنص على أن "سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"، وكذا نص المادة 303 من قانون العقوبات التي تعاقب كل من يفض أو يتلف رسائل أو مراسلات موجهة للغير وذلك بسوء نية وفي غير الحالات المنصوص عليها في المادة 137.

نلاحظ أن المشرع الجزائري حدد المراسلات التي تصلح أن تكون محلا للاعتراض بتلك المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية دون أن يشير إلى طبيعة هذه المراسلات، مما يفتح المجال لمختلف الرسائل المكتوبة، بغض النظر عن شكلها (كتابة، رموز، أشكال، صور) أو الدعامة التي تنصب عليها (ورقية أو رقمية)، أو الوسيلة المستعملة لإرسالها سلكية كانت (كالفاكس، تليغرام) أم لاسلكية (البريد الالكتروني، الهاتف النقال)، باستثناء الكتب والمجلاّت والرسائل والحوليات التي تعد مراسلات خاصة.

وهذا ما يؤكده القانون 09 - 04 في المادة 02 الفقرة "و" في تعريفه للاتصالات الإلكترونية على أنها " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية ".

[1] - براهيمي جمال المرجع السابق ص 88.

وبغض النظر عن طبيعة المراسلات السلكية واللاسلكية فعملية الاعتراض أو المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون علم أو موافقة المعنيين، وذلك لغرض التصنت والتقاط وتثبيت وبث وتسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصفة خاصة أو سرية في أماكن خاصة أو عمومية، ومن ثم استعمالها كدليل لمواجهة المتهم.

ولعل من أهم المراسلات الإلكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض والمراقبة والتي تمثل مصدرا غنيا لأدلة إثبات الجرائم الإلكترونية، المراسلات عبر البريد الإلكتروني، كون هذه التقنية من أكثر الوسائل الحديثة استخداما للاتصال عبر الانترنت ومجالا خصبا للربط بين الأشخاص في مختلف أنحاء العالم بسرعة فائقة ودون حواجز. فهو بمثابة نظام تبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة، أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة، كما يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه بسهولة لأنه محاط بحماية فنية.

ومن هنا، فعملية اعتراض ومراقبة البريد الإلكتروني التي تجري بغرض ضبط المراسلات الإلكترونية تنصب على ثلاثة عناصر أساسية وهي: الأول هو الوارد (IN)، ويتم من خلاله مراقبة ومراجعة قائمة المراسلات الإلكترونية التي وصلت المشتبه فيه. والثاني الصادر (OUT)، وهو عكس الوارد يفيد في الكشف عن قائمة المراسلات التي أرسلت من طرف المشتبه فيه. أما العنصر الثالث فهو الحافظ وسلة المهملات (Trash) الذي يسمح بالاطلاع على المراسلات المحفوظة داخل البريد الإلكتروني الخاص بالمشتبه فيه والمحذوفة منه والتي تحفظ بشكل آلي في سلة المهملات[1].

كون هذه المراسلات تتمتع بالخصوصية حمى المشرع سريتها بسن قوانين تعمل على توفير قدر كبير من الحماية الجزائية لها، إلا أن هذا الأمر ليس على إطلاقه فإذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فإنه يجوز

اعتراض هذه المراسلات وكشف السرية عنها في سبيل البحث عن الدليل، وهو السند الشرعي المبرر لإباحة هذا الإجراء بسبب أنه يتضمن اعتداء جسيما على حرمة الحياة الخاصة وسرية الاتصالات، فيباح استثناء وفي حدود ضيقة وذلك للفائدة المنتظرة منه والتي تتعلق بإظهار الحقيقية وكشف الغموض عن الجريمة وضبط الجناة.

وتجدر الإشارة في هذا الصدد أن المراسلات التي تصلح لإجراء اعتراضها يجب أن تتسم بالخصوصية، ولكي تكون كذلك يلزم أن يتوافر لديها عنصران أساسيان هما[2]:

[1] - براهيمي جمال المرجع السابق ص 91

[2] - سعيداني نعيم المرجع السابق ص 179

عنصر موضوعي ويتعلق بموضوع ومضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي وسري أو خاص فيما تخبر به.

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

وحرصا منه على تحقيق هذا المبتغى، قام المشرع الجزائري بإنشاء هيئة وطنية خاصة بموجب مرسوم رئاسي رقم 15 - 261 ([1]) مؤرخ في 8 أكتوبر 2015، أوكل إليها بالإضافة إلى مهام أخرى، مهمة تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها مع السلطات القضائية ومصالح الشرطة القضائية، بما في ذلك جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريب والمساس بأمن الدولة، تحت سلطة القاضي المختص، وكذا تجميع وتسجيل وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من اجل استعمالها في الإجراءات القضائية. أضف إلى ذلك أنها تتولى تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وتحديد مكان تواجدهم.

2 - الشروط والضمانات المقررة لاعتراض المراسلات السلكية واللاسلكية

إن المشرع الجزائري رغم كونه أعطى لسلطات التحقيق إمكانية اعتراض المراسلات كأسلوب مستحدث للبحث عن الدليل يتماشى مع الأساليب المتطورة التي يلجأ إليها الجناة في تنفيذ جرائمهم وإخفاء أي أثر يدل عليهم، إلا أنه أحاط هذا الإجراء المستحدث بشروط قانونية تعمل على منع التعسف وتصون الحرية الفردية وتتمثل هذه الشروط في [(2)]:

- ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ: طبقا للمادة 65 مكرر 05 من قانون الإجراءات الجزائية فإنه لا يمكن لضابط الشرطة القضائية اللجوء إلى إجراء اعتراض المراسلات إلا بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانة لازمة لمشروعية هذا الإجراء وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقدير فائدة إجراء الاعتراض وجديته وملائمته لسير إجراءات الدعوى من خلال معطيات التحريات التي قامت بها الضبطية القضائية مسبقا.

- وقد نصت المادة 65 مكرر09 على أن عملية تنفيذ إجراء اعتراض المراسلات تتم تحت رقابة السلطة

1- المرسوم الرئاسي، رقم 15-261 المؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 53 ،بتاريخ 08 أكتوبر 2015

2 - سعيداني نعيم، المرجع السابق، ص 180.

القضائية التي أذنت به وذلك من خلال قيام ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص بإعداد محضرا عن كل عملية اعتراض للمراسلات وكذا عن عمليات وضع الترتيبات التقنية لهذا الغرض، ويذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات والانتهاء منه.

- يجب أن يتضمن الإذن باعتراض المراسلات كل العناصر التي تسمح بالتعرف على الاتصالات أو المراسلات المطلوب اعتراضها.

- استوجبت المادة 65 مكرر 7 ق إ ج ج أن لا تتجاوز مدة هذا الإجراء أربعة أشهر قابلة للتجديد حسب تقدير نفس السلطة مصدرة الإذن وفقا لمقتضيات التحري والتحقيق.

ثانيا: التسرب (الاختراق)

يعد التسرب من إجراءات البحث والتحقيق الجديدة التي أرستها معظم تشريعات العالم الحديثة لمواجهة الجرائم الإلكترونية، وقد كانت اتفاقية منظمة الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية سباقة إلى احتواء هذا الإجراء بنصها في المادة على أساليب التحري الخاصة بما فيه التسرب الذي عبرت عنه ب" الأعمال المستترة. " أما المشرع الجزائري فقد تبني بدوره هذا الإجراء، مباشرة عقب تصديق الدولة الجزائرية على اتفاقية منظمة الأمم المتحدة أعلاه بموجب المرسوم الرئاسي رقم 02 - 05 المؤرخ في 2002/02/02 بتحفظ واتفاقية مكافحة الفساد لسنة 2003 بتاريخ 2004/04/19 وقد ورد النص على هذا الأسلوب لأول مرة بالجزائر بمناسبة صدور القانون رقم 06 - 01 المتعلق بالوقاية من الفساد ومكافحته[1] في 2006/02/20، الذي نص في المادة 56 على أنه " من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون يمكن اللجوء إلى التسليم المراقب وإتباع أساليب تحري خاصة، ولكن نظرا للغموض الذي انتاب هذ النص بخصوص المقصود بالاختراق أو التسرب شروطه وآليات مباشرته، والمادة 40 من الأمر 05 - 06 المؤرخ في 23 أوت 2005 المتعلق بمكافحة التهريب المعدل والمتمم[2] إذ نصت المادة 33 منه على إمكانية اللجوء إلى أساليب تحر خاصة[3]، بقي هذا الإجراء جامدا وبدون مفعول إلى أن تم تعديل قانون الإجراءات الجزائية بموجب قانون 06 -22 المؤرخ في 2006/12/20، أين تم تحديد معالم إجراء التسرب من خلال تعريفه وتحديد ضوابطه والآثار المترتبة عنه[4] كالترصد الإلكتروني أو الاختراق على النحو المناسب وبإذن من السلطة القضائية المختصة ".

---

[1] - قانون رقم 06 - 01 المؤرخ في 2006/02/20، يتعلق بالوقاية من الغساد ومكافحته، الصادر بالجريدة الرسمية رقم 14 المؤرخة في 08 مارس 2006.

[2] - الأمر رقم 05 - 06 المؤرخ في 23 أوت 2005 المتعلق بمكافحة التهريب .

[3] - مناصرة يوسف المرجع السابق ص 480.

[4] - براهيمي جمال المرجع السابق ص 83.

1- المقصود بالتسرب

نصت المادة 65 مكرر 12 من قانون 06 - 22 على أنه " 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 لهم أو خاف. .."،فهو أسلوب من أساليب التحريات الخاصة، أين أجاز المشرع لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن به تحت رقابته، إذا اقتضت ضرورة التحقيق أو التحري في الجريمة المتلبس بها ذلك، أو في التحقيق الابتدائي في الجرائم المحددة حصريا في المادة 65 مكرر 05 من ق إ ج المشار إليها أنفا، أين أجاز القانون لضابط أو عون شرطة قضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأعمال التالية:

- اقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم المستعملة في ارتكابها.

- استعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل والتخزين أو الإيداع أو حفظ أو الاتصال (المادة 65 مكرر 14 من ق إ ج ج).

من خلال ما سبق ذكره فأن التسرب عملية معقدة تتطلب أن يدخل العون المكلف بالعملية في اتصال بالأشخاص المشتبه فيهم ويربط معهم علاقات من أجل تحقيق الهدف النهائي من العملية، وتتطلب على الخصوص المشاركة المباشرة في نشاط الخلية الإجرامية التي تسرب إليها.

وعلى هدي ذلك فإن التسرب يرتكز على مبدأين[1] :

* المبدأ العام يستند على تقديم صورة على الوسط المراد التسرب فيه، ويستوجب ذلك معرفة عموميات عن هذا الوسط مع توثيق هذه المعطيات.

* والمبدأ الخاص الذي يستند على تعميق التحري عن هذا الوسط ونشاطاته ومميزاته ووسائله وطبيعة الأشخاص المنتمين إليه، ليتم بعد ذلك دراسة الوظيفة العملياتية في هذا المجال بتوفير الوسائل البشرية والتقنية اللازمة.

أحاط المشرع المسرب كذلك بعدة ضمانات من أجل حمايته وحماية أسرته أثناء عملية التسرب وبعد انقضائها، منها ما ورد في المادة 65 مكرر 16 من ق إ ج ج بأنه " لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين يباشرون عملية التسرب تحت هوية مستعارة في أية مرحلة من مراحل الإجراءات" وما تضمنته كذلك المادة 65 مكرر17 من القانون نفسه بأنه " إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في الرخصة للتسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة 65 مكرر14 أعلاه للوقت الضروري الكافي لتوقيف

[1] - سعيداني نعيم المرجع السابق ص 175.

عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسئولا جزائيا، على أن لا يتجاوز ذلك مدة أربعة (4) أشهر

2 - الضوابط التي تحكم التسرب في الجرائم الإلكترونية

نظرا للخطورة التي يشكلها إجراء التسرب على حرمة الحياة الخاصة للمشتبه فيه، فقد قيده المشرع بجملة من الشروط والضوابط الواجب مراعاتها قبل وأثناء مباشرته وهي كالتالي [1]:

أ - الضوابط الإجرائية

إن قانون الإجراءات الجزائية أوجب لمباشرة إجراء التسرب الإلكتروني في الجرائم الخطرة بمجموعة من الضوابط الإجرائية تتلخص فيما يلي:

- ضرورة الحصول على الإذن القضائي الإجراء وكل ما يجب أن يتضمنه من أحكام، إذ لا يجوز للضابط أو عون الشرطة القضائية الخوض في عملية التسرب من تلقاء نفسه دون الحصول على إذن مسبق من طرف الجهات القضائية المختصة والمتمثلة حسب أحكام المادة 65 مكرر 11 ق إ ج في وكيل الجمهورية قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاحه.

- كما أوجبت المادة 65 مكرر 11 ق إ ج أن تتم عملية التسرب الإلكتروني تحت الرقابة المباشرة للجهة الصادرة للإذن حسب الحالة لتفادي حدوث تجاوزات وتعسف في استعمال هذا الحق.

- لا يكفي أن يصدر الإذن بالتسرب من الجهة المختصة إما وكيل الجمهورية أو قاضي التحقيق فحسب، بل يجب أن يكون هذا الإذن مكتوبا وإلا كان الإجراء باطلا، وهذا ما نصت عليه المادة 65 مكرر 15 بقولها يجب أن يكون الإذن المسلم طبقا للمادة 65 مكرر 11 مكتوبا تحت طائلة البطلان" وذلك لأن الأصل في العمل الإجرائي الكتابة.

- يجب أن يتضمن الإذن مجموعة من الشروط يتوقف على تحديدها صحة الإجراء في حد ذاته كذكر هوية ضابط الشرطة القضائية الذي تتم عملية التسرب تحت مسؤوليته.

- إلزامية تحديد المدة المطلوبة في عملية التسرب والتي يجب ألا تتجاوز أربعة أشهر ويمكن أن تجدد حسب مقتضيات التحري والتحقيق ضمن نفس الشروط الشكلية والزمنية وفقا للمادة 65 مكرر 15 الفقرة 03، ق إ ج ج وفي نفس الوقت أجاز القانون للقاضي الذي أذن بهذا الإجراء أن يأمر في أي وقت يوقفه قبل انقضاء المدة المحددة.عملا بنص المادة 65 مكرر 17 ق إ ج ج.

ب - الضوابط الموضوعية

إلى جانب الضوابط الإجرائية المذكورة أعلاه أحاط المشرع عملية التسرب بضوابط أخرى موضوعية يمكن إيجازها في الضوابط التالية:

[1]- براهيمي جمال، المرجع السابق، ص85.

- بحسب نص المادة 65 مكرر15 ق إ ج، يجب أن يكون الإذن بإجراء التسرب مسببا ومشمولا بالمبر ارت والحجج والأسباب التي جعلت ضابط الشرطة القضائية يلجأ إلى هذه العملية المتمثلة عادة في ضرورة التحقيق والتي تكون ضمن موضوع طلبه الإذن والتي أقنعت الجهات القضائية المختصة بمنحه.
- يجب تحديد نوع الجريمة التي ينصب عليها الإذن بالتسرب والتي يجب ألا تخرج عن نطاق الجرائم السبع التي حددتها المادة 65 مكرر05 ق إ ج على سبيل الحصر وهي: " جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد... ".

ج - طرق التسرب في مجال الجريمة المعلوماتية

يمكن تصور عملية التسرب في نطاق الجرائم المعلوماتية في دخول ضابط أو عون الشرطة القضائية إلى العالم الافتراضي وذلك باختراقه لمواقع معينة وفتح ثغرات إلكترونية فيها، أو اشتراكه في محادثات غرف الدردشة أو حلقات الاتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان فاعلا مثلهم، مستخدما في ذلك أسماء أو صفات هيئات مستعارة ووهمية سعيا منه للاستفادة منهم حول كيفية اقتحام الهاكر للموقع [1].

حيث أجاز القانون لضابط أو لعون الشرطة القضائية أن يرتكب الاعمال التالية:

* إقتناء أو نقل أو حيازة أو تسليم أو إعطاء مواد أو أموال أو منتجات أو وثائق أو معلومات متحصل عليها من إرتكاب الجرائم المسبعملة في إرتكابها.

* إستعمال أو وضع تحت تصرف مرتكبي الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل والتخزين أو الإيداع أو الحفظ أو الاتصال (المادة 65 مكرر 14 من ق.إ.ج)[2].

ثالثا: المراقبة الإلكترونية وحفظ المعطيات

استحدث المشرع الجزائري بموجب المادة الثالثة 03 من القانون 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إجراء المراقبة الإلكترونية حينما أجاز تبعا لمستلزمات التحريات أو التحقيقات القضائية الجارية في إطار هذا النوع من الجرائم اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها.

1 - المقصود بمراقبة الاتصالات الإلكترونية

لم يتطرق المشرع الجزائري إلى تحديد ما المقصود بمراقبة الاتصالات الإلكترونية مكتف في ذلك

[1] - سعيداني نعيم المرجع السابق ص 177

[2] - مناصرة يوسف، المرجع السابق، ص 478

بتحديدمفهوم الاتصالات الإلكترونية فحسب، غير أن الفقه قد تصدى إلى هذه المهمة حيث عرف إجراء المراقبة الإلكترونية على أنه مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات ومعلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض أمني أو لأي غرض آخر.

ومن الواضح أن المشرع الجزائري لم يعتبر هذا الإجراء من ضمن طرق الحصول على الدليل الرقمي فقط، بل أدرجه ضمن التدابير الوقائية من الجرائم التي يمكن أن ترتكب بواسطة المعلوماتية، فإلى جانب إمكانية القيام بإجراء مراقبة الاتصالات الإلكترونية في إطار التحريات والتحقيقات القضائية من أجل الوصول إلى أدلة لم يكن بالإمكان الوصول إليها دون اللجوء إلى هذا الإجراء فإنه يمكن كذلك تطوير هذه التقنية لكي تعمل في بيئة الرقابة لغرض الوقاية من احتمال وقوع جرائم خطيرة بواسطة المعلوماتية من شأنها تهديد كيان الدولة وهو ما قررته المادة الرابعة من القانون 09 - 04 بقولها أنه يمكن القيام بعمليات المراقبة الإلكترونية للاتصالات للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة وكذا في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني[1]

فالمراقبة الإلكترونية هي إجراء تطفلي على الحياة الخاصة [2] فأحاطها قانون 09 - 04 بإجراءات صارمة لضمان وجود توازن معقول بين مصالح العدالة والحقوق الأساسية للإنسان من خلال كفالته لضمانات الإشراف القضائي على عمليات المراقبة في حالة الجرائم الإرهابية أو الماسة بأمن الدولة، وضرورة توضيح في تقرير مسبب من طرف الضبطية القضائية دواعي اللجوء لهذا الإجراء ويبين التقرير طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها وتحديد فترة التتبع المقدرة بستة أشهر قابلة للتجديد.

ولأجل دواعي الأمن والحفاظ على النظام العام أو بغية الوقاية من الجرائم الخطيرة مثل الجرائم الإرهابية والماسة بأمن الدولة، يجيز القانون وضع ترتيبات تقنية وبرامج معلوماتية على مستوى متعاملي الأنترنت من أجل القيام بعمليات الرقابة على الاتصالات الإلكترونية، مع القيام بجمع وتسجيل محتواها في الوقت الحقيقي. فهي عبارة عن مراقبة موجهة ووقتية مأذون بها حصريا من طرف السلطة القضائية في شكل ترخيص مكتوب من الجهة القضائية المختصة.

كما سبق القول فإن المشرع الجزائري قيد اللجوء إلى هاته التقنية بجملة من الإجراءات لصحتها في الجرائم الإرهابية والتخريبية والماسة بأمن الدولة أو الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المنصوص عليها في المرسوم الرئاسي رقم 15 - 261 المتعلق بتحديد تشكيلة سير الهيئة

[1] - سعيداني نعيم المرجع السابق ص 182

[2] - مناصرة يوسف المرجع السابق ص 314

الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، حيث تستلزم المادة 11 منه على أن تتم المراقبة الوقائية للاتصالات الإلكترونية، من أجل الكشف عن الجرائم المتصلة بتكنولوجيات الإعلام والاتصال تحت مراقبة السلطة القضائية[1].

حيث تستلزم المادتين 24 و25 من المرسوم الرئاسي 15 - 216 بتسجيل الاتصالات الإلكترونية التي تكون موضوع مراقبة وتحرر بشأنها محاضر وفقا للشروط والأشكال المنصوص عليها في قانون الإجراءات الجزائية،وتسلم التسجيلات والمحررات إلى السلطات القضائية المختصة وتحفظ السلطات القضائية دون سواها بهذه المعطيات[2].

2 - شروط المراقبة الإلكترونية للاتصالات

أحاط المشرع هذا الإجراء باعتباره وسيلة إجرائية للحصول على الدليل الرقمي في مجال الجريمة المعلوماتية بمجموعة من الشروط أهمها:

- أن يتم تنفيذ هذا الإجراء تحت سلطة القضاء وبإذن منه، وهو ما كرسته المادة الرابعة من القانون المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بنصها على أنه لا يجوز إجراء عمليات المراقبة إلا بإذن من السلطة القضائية المختصة.

- أن تكون هناك ضرورة تتطلب هذا الإجراء وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري أو التحقيق دون اللجوء إلى المراقبة الإلكترونية وهو ما أكد عليه المشرع في الفقرة ج" من المادة الرابعة في القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

رابعا - حجز المعطيات المعلوماتية

نصت المادة 06 من قانون 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على أنه " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتي معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في إحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة التي تجري فيها العملية.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن يؤدي ذلك إلى المساس بمحتوى المعطيات. "

[1] - المرسوم الرئاسي رقم 15 - 216 المؤرخ في 08 أكتوبر 2015 الجريدة الرسمية عدد 53 رقم ص 16

[2] - مناصرة يوسف المرجع السابق ص 438

ما من شك أن الهدف الأساسي لعملية التفتيش للمنظومة المعلوماتية هو وضع اليد على الأدلة المادية التي تساعد على كشف الحقيقة لكن من البديهي القول بأن حجز الأشياء المادية كالمعدات والأوراق والمستندات يعد شيئا سهلا وغير مثير لأية إشكالات في نظر القانون، غير أنه ليس من السهل أيدا توقيع الحجز على منظومة معلوماتية ذلك أن المعلومات هي في الأصل شيء معنوي متعارف عليها بمصطلح الأموال المعنوية، يحميها القانون، فما المقصود بالمعطيات المخزنة وما مدى قابليتها للحجز.

إن المعطيات المخزنة تسمى ببنك المعلومات، فهي مخزنة في ذاكرة الحاسوب، إما أن تكون مرصودة ومثبتة على دعامة أو حوامل كالأقراص أو أشرطة ممغنطة، ففي هذه الحالة الأخيرة يمكن ضبط وحجز الأشياء بسهولة كونها أشياء مادية في حين يختلف الأمر ويصبح من الصعوبة بمكان إذا تعلق بالمعطيات أو المعلومات في حد ذاتها [1].

فطبقا لنص المادة 06 من القانون 09 - 04 عندما يتوصل المحققون أثناء إجراء التفتيش في المنظومة المعلوماتية إلى وجود معطيات او بيانات من شأنها الإفادة في التحقيق وضبط الأدلة للكشف عن الجريمة المعلوماتية ومرتكبيها فإنه يمكن لهم حجز المنظومة المعلوماتية برمتها إذا كان ضروريا لمصلحة التحقيق أو القيام بحجز المعطيات المعنية بالذات بعد نسخها على دعامة مادية أو أي وعاء للبيانات كطبعها على الرق أو ضبطها على الشاشة وذلك لتسهيل قراءتها والتعامل.

فضبط الأدلة عن طريق حجز المعطيات أو البيانات من وجهة نظر المشرع الجزائري كما تلخصه المادة 06 المشار إليها يجري وفقا لمقتضيات قانون الإجراءات الجزائية فدعائم التخزين التي يتم نسخ المعلومات محل البحث عليها يجب أن تكون ذات قابلية للحجز والوضع في أحراز وإضافة إلى الحجز فإن قانون العقوبات نص على تدابير أخرى منها مصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع محل الجريمة كما نصت عليه المادة 394 مكرر 6 من قانون العقوبات.

فالمشرع وفقا للمادة 84 من قانون الإجراءات الجزائية وضع ضوابط فيما يتعلق بحجز الأدلة منها مايلي:

- الإطلاع على المستندات المبحوث عنها، مخول فقط لقاضي التحقيق أو ضابط الشرطة القضائية الذي أنابه عنه.

- الاحترام التام لمقتضيات وضرورات التحقيق وعلى الأخص ضمان احترام سر المهنة وحقوق الدفاع.

إن الأشياء والوثائق المضبوطة يتم وضعها في أحراز مختومة لا يتم فتحها إلا بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا وفضلا عن ذلك يستدعي كل من ضبطت لديه هذه الأشياء وذلك لحضور هذا الإجراء.

[1] - زبيجة زيدان المرجع السابق ص 148

نظرا لما يتطلبه الأمر من تقنيات خاصة فإنه أجاز الاستعانة بذوي الاختصاص سواء عن طريق تسخير من لديهم خبرة في مجال عمل المنظومة المعلوماتية بغية مساعدة الجهة القائمة بتفتيش المنظومة المعلوماتية وتزويدها بكل ما من شأنه تسهيل مهمتها كما هو منصوص عليه في المادة 05 فقرة أخيرة 09 - 04.

أو عن طريق تكليف هؤلاء المختصين باستعمال الوسائل التقنية المناسبة والضرورية للحيلولة دون الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية التي تشكل محل الجريمة أو تحتوي على أدلة لها كل ذلك لمنع تهريبها أو تدمير تلك الأدلة المؤدية لها وهو ما أشير له بنص المواد 07 و08 من قانون 09 - 04.

خامسا: التزامات مقدمي الخدمات

رأى المشرع أنه في سبيل الوصول إلى الأدلة التي تكتنفها صعوبة الحصول عليها في بعض الأحيان، أنه من الضروري إلزام الأطراف المتداخلة في خدمات الأنترنيت بتقديم المساعدات الضرورية للجهات المكلفة بالتفتيش والسلطات القضائية المتخصصة وقد خص القانون 09 - 04 الفصل الرابع منه لهذه النقطة بالذات وهو ما نتطرق له فيما يلي[1]:

1 - مساعدة السلطات

بموجب المرسوم التنفيذي رقم 98 - 257 المؤرخ في 25 / 08 / 1998[2] الذي يحدد شروط وكيفيات استعمال خدمة الأنترنت والذي بموجبه فسح المجال لظهور مزودي الخدمة إلى جانب مركز البحث في الإعلام العلمي والتقني بالجزائر، فإن المادة 10 من القانون 09 - 04 ألزمت بذلك مقدمي الخدمات بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية والتفتيش كما ألزمتهم بكتمان السر بخصوص العمليات التي ينجزونها بطلب من المحققين وما تحصل عن ذلك من معلومات وذلك تحت طائلة العقوبات التي يقررها القانون في حالة إفشاء أسرار التحقيق عملا بنص المادة 09 من القانون 09 - 04.

ومن المعلوم أن مقدمي الخدمات في مجال الإنترنيت لهم دور في تمكين مستخدم الأنترنيت من الدخول إلى الشبكة والإطلاع عما يبحث عنه أو ما يريد معرفته، ومن ثمة فإن مقدم الخدمة بإمكانه مراقبة ومعرفة جميع الخطوات التي يتبعها هذا المستخدم إذ بإمكانه معرفة المواقع التي زارها والمعلومات التي خزنها وكل الاتصالات التي أجراها.

هذا الجانب فإن مزود الخدمة بإمكانه تمكين جهات التحقيق بكل المعلومات التي تساعدها أو التي تبحث عنها بل إنه ملزم بذلك وفقا لنص المادة 10 المشار إليها ثم يوجد أيضا متعهد توصيل

1- أنظر الفصل الرابع المعنون بالتزامات مقدمي الخدمات من قانون 09 - 04، اعتبارا من المادة 10 إلى المادة 12 منه.

2- المرسوم التنفيذي رقم 98 - 257 المؤرخ في 25 غشت 1998، يضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها، الجريدة الرسمية رقم 63المؤرخة في 04 جمادى الأولى عام 1419 هـ، الموافق لـ: 26 غشت 1998.

المعلومات ودوره تقني يتجسد في إيصال المستخدم إلى شبكة الإنترنيت وذلك بربطه بالمواقع التي يريدها وليس له علاقة بالمعلومات أو بمحتواها.

لقد عرفت المادة 01 الفقرة 03 من الاتفاقية الأوربية لمكافحة جرائم المعلوماتية التي تم إقرارها في بودابست لسنة 2001 مزودي الخدمات بأنهم كل شخص طبيعي أو معنوي يقوم بتزويد المستخدمين بالخدمات التي تمكن وتسهل الاتصالات بين أجهزة الكمبيوتر وكذلك كل من يتولى معالجة المعطيات المخزنة نيابة عن مزود الخدمة وقد سار المشرع الجزائري على هذا النحو حين نص في المادة 04 من المرسوم التنفيذي رقم 98 - 257 المؤرخ في 1998/08/25 والمتعلق بضبط شروط وكيفيات إقامة خدمات الإنترنيت واستغلالها لأغراض تجارية للأشخاص المعنويين الخاضعين للقانون الجزائري واشترطت نفس المادة على أن يكون ذلك برأسمال يملكه فقط أشخاص معنويون خاضعون للقانون العام أو طبيعيون من جنسية جزائرية.

2 - حفظ المعلومات أو المعطيات المتعلقة بحركة السير

إن قانون 09 - 04 رتب على عاتق مقدمي الخدمات في مجال الإنترنيت والمتعلق بمساعدة السلطات المكلفة بالتحريات والتحقيقات القضائية، التزاما آخر جاء النص عنه في المادة 11 منه وهو حفظ المعلومات التي من شأنها تمكين جهات التحقيق من التعرف على مستعملي الخدمة وحدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة (1) واحدة من تاريخ التسجيل كما أوجب القانون على هؤلاء واجب التدخل فورا لسحب المعطيات أو المحتويات المخالفة للقانون وتخزينها أو منع للدخول إليها باستعمال وسائل تقنية تحول دون الدخول إليها[1].

* التزامات خاصة منصوص عليها في المادة 12 من القانون 09 - 04 وهي:

- وضع الترتيبات التقنية التي بموجبها يتم حصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجودها وقد نصت المادة 11 على أنه يلتزم مقدمو الخدمة بحفظ:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة (أ) من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه.

[1] - زبيحة زيدان المرجع السابق ص 155

سادسا: المساعدة القضائية الدولية في مجال الجرائم المعلوماتية

أكد قانون 09 - 04 في الفصل السادس بعنوان "التعاون والمساعدة القضائية الدولية"، بالضبط في المادة 16 منه على المساعدة القضائية الدولية المتبادلة، بحيث أنه في إطار التحقيقات والتحريات القضائية التي تمت مباشرتها، وتتبع الجرائم المنصوص عليها في هذا القانون 09- 04 والكشف عن مرتكبيها فإن السلطات الجزائية المختصة بإمكانها تبادل المساعدات القضائية في المستوى الدولي [1] نظرا للطابع الخاص لهذا النوع من الجرائم زما يتطلبه تعقبها من سرعة فإن المشرع أجاز في حالة الاستعجال قبول طلبات المساعدة القضائية الدولية حتى وإن ورد عن طريق وسائل الاتصال السريعة مثل الفاكس أو البريد الإلكتروني شريطة التأكد من صحتها وبهذا الصدد أوجبت المادة 36 ف 02 من القانون 05 - 06 الصادر في 23 أوت 2005 والمتعلق بمكافحة التهريب المعدل بالأمر رقم 06 - 09 المؤرخ في 15 جويلية 2006 على أنه وفي حالة توجيه الطلب إلكترونيا من طرف السلطات الأجنبية يمكن تأكيده بواسطة أي وسيلة تترك أثرا مكتوبا.

- القيود الواردة على المساعدة القضائية الدولية: أحاط المشرع الجزائري المساعدة القضائية بجملة من القيود لعل أهمها:

- أن تتم وفقا للاتفاقيات الدولية التي أبرمت في مجال تبادل المعلومات واتخاذ الإجراءات التحفظية أو تسليم المجرمين في ما هو مرتبط بالجريمة الإلكترونية.

- تخضع لمبدأ التعامل بالمثل وهو المبدأ الذي أكدته أيضا المادة 29 من القانون رقم 05 - 01 الصادر في 06 فيفري 2005 والمتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحته.

- لا تنفذ ولا يمكن الاستجابة لها إذا كان فيها: مساس بالسيادة الوطنية أو ماسة بالنظام العام أو غير محافظة على سرية المعلومة المبلغة لتلك الدولة.

المبحث الثاني: القيمة القانونية للدليل الإلكتروني وحجيته في إثبات الجريمة الإلكترونية

إن مجرد وجود دليل يثبت وقوع الجريمة وينسبها لشخص معين لا يكفي للتعويل عليه لإصدار الحكم بالإدانة، إذ يلزم أن يكون لهذا الدليل قيمة قانونية، وهذه القيمة القانونية للدليل الجنائي تتوقف على مسألتين رئيسيتين الأولى مشروعية الحصول على الدليل، لأن ما يثير مسألة مشروعية الأخذ به هي إمكانية عدم تعبيره عن الحقيقة نظرا لما يمكن أن تخضع له طرق الحصول عليه من التعرض والتزييف والتحريف والعبث، وهو ما يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا من

[1] - الحث على التعاون الدولي جاء في قرار صادر عن المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات حول القواعد الإجرائية في بيئة جرائم الكمبيوتر.

حيث وجوده ومن حيث الحصول عليه والثانية اليقينية في دلالته على الوقائع المراد إثباتها لأن مصداقية أو حجية الدليل الرقمي في تعبيره عن الحقيقة هو ما تصبو إليه الدعوى الجزائية.

وعليه نستعرض في المطلب الأول القيمة القانونية للدليل الإلكتروني، وفي الثاني نتناول حجية الدليل الإلكتروني وأثر تبني القاضي الجزائي الجزائري لنظام الإثبات الإلكتروني.

المطلب الأول: القيمة القانونية للدليل الإلكتروني

حتى يكون للدليل الإلكتروني قيمة قانونية من حيث المشروعية الحجية في إثبات جرائم العالم الافتراضي والاعتداد به من قبل القاضي الجزائي، يلزم علينا التطرق إلى المسائل التالية:

الفرع الأول: مشروعية الأدلة الإلكترونية

إن المشروعية هي المطابقة للقانون، وهي فكرة قانونية تختص بوصف تطبيق القاعدة القانونية، لتقرر بالاستناد إلى أصول تلك القاعدة صحة التطبيق من عدمه، فالمشروعية إذن فكرة قانونية، فهي تدور في صحة تصرفات الأفراد والمؤسسات في نظر السلطة من القانون في تحليله الاجتماعي وهو التعبير عن إرادة القائمين على السلطة[1].

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

لذلك فإنه لصحة الإجراءات التي تقوم بها جهة التحقيق أن لا تخل بمبدأ المشروعية من أجل الحصو ل على دليل صحيح وسليم يستند عليه القضاء في أحكامه والحقيقة أن مشروعية الدليل الإلكتروني هي مشروعية الوجود ومشروعية الحصول[2].

وتعرف المشروعية الإجرائية بأنها " الأصل في المتهم البراءة، ولا يجوز اتخاذ إجراء جنائي قبل المتهم إلا بناء على قانون وتحت إشراف القضاء وفي حدود الضمانات المقررة، بناء على قرينة البراءة " [3] وهو التعريف المتوافق مع المادة 6 ف 2 من الاتفاقية الأوربية لحقوق الإنسان، وهذا المبدأ تم النص عليه في الدستور الجزائري لسنة 2016 حيث جاء في المادة 58 منه " لا إدانة إلا بمقتضى قانون صادر

[1] - مناصرة يوسف المرجع السابق ص 126

[2] - جفال يوسف المرجع السابق ص 45.

[3] - أحمد فتحي سرور، الشرعية والإجراءات الجنائية، دار النهضة العربية، القاهرة، 1977 ص 116.

قبل ارتكاب الفعل المجرم "، وتم تطبيق هذا المبدأ في المادة الأولى من قانون العقوبات [1] وهي أيضا مرتبطة بطريقة وكيفية البحث عن الأدلة فيجب أن تكون محترمة لحقوق الأشخاص وكرامة العدالة.

من هذا كان من اللازم تدعيم هذه القاعدة الدستورية، بقاعدة ثانية تحكم تنظيم الإجراءات تتخذ ضد المتهم، على نحو يضمن احترام الحقوق والحريات الفردية وهذه القاعدة تسمى بالشرعية الإجرائية، أو قاعدة مشروعية الدليل وتعني هذه القاعدة ضرورة اتفاق الإجراء مع القواعد القانونية وهذا ما نصت عليه المادة 59 من الدستور الجزائري " لا يتابع أحد ولا يوقف أو يحتجز ، إلا ضمن الشروط المحددة بالقانون، وطبقا للأشكال التي نص عليها ".

ونتيجة تردد الفقه والقضاء حيال مشروعية الأدلة المتحصلة من الوسائل الإلكترونية كمخرجات الحاسب الآلي بأنواعها المختلفة، خشية أن تكون قد تعرضت للتغيير في فحواها أو لطمس الحقيقة فيها، خاصة أن معظمها يمس مساسا مباشرا بحقوق الأفراد الأساسية وحرياتهم ولهذا وضعت شروط ينبغي توافرها في دليل مقدم أمام القضاء الجنائي كأن يكون الدليل مشروعا أي أن يكون وليد إجراءات صحيحة وأن يكون قد طرح في الجلسة وأن يكون مبنيا على الجزم واليقين.

أولا: مشروعية وجود الدليل الإلكتروني

يقصد بمشروعية الوجود أن يكون الدليل معترفا به، بمعنى أن يكون القانون يجيز للقاضي الاستناد إليه والاستدلال به لتكوين عقيدته وقناعته للحكم بالإدانة أو البراءة، ولعل المعيار الذي يتحدد على أساسه موقف القوانين فيما يتعلق بسلطة القاضي الجزائي في قبول الدليل الإلكترونية، تتمثل في طبيعة نظام الإثبات السائد في الدولة إذ يختلف النظام القانوني في موقفها من حيث الأدلة التي يمكن قبولها في الإثبات.

وفي هذا الإطار، تختلف طريقة الاعتراف بالدليل الإلكتروني وقبوله كدليل إثبات من دولة إلى أخرى بحسب طبيعة نظام الإثبات السائد فيها، والذي لا يمكن أن يخرج عن الفئات الثلاث التالية[2]:

1- 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

[1] - أحسن بوسقيعة، الوجيز في القانون الجزائي العام، دار هومة، الطبعة السابعة عشر سنة 2018 ص 50.

[2] - براهيمي جمال المرجع السابق ص 138

بارتكاب المتهم للجريمة المنسوبة إليه. ومن هنا يتضح جليا بأن نظام الإثبات المقيد يقوم على مبدأين أساسيين، الأول يتمثل في الدور الإيجابي 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، ولكونه الذي يحدد القيمة الاقناعية لكل دليل بأن يضفي الحجية الدامغة على بعض الأدلة، والحجية النسبية على بعضها الآخر، أما المبدأ الثاني، فيتمثل في الدور السلبي للقاضي الجزائي في الإثبات، إذ يلتزم التزاما صارما بما يرسمه له المشرع سلفا من أدلة إثبات على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في كثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام، فيصبح القاضي كالآلة في إطاعته لنصوص القانون.

2 - نظام الإثبات الحر

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 إيجابي 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، وهو في ذلك يتمتع بمطلق الحرية في قبول الدليل أو طرحه جانبا إذا لم يطمئن إليه، ودون أن يكون مطالبا بتسبيب اقتناعه.

ويجد هذا النظام مبرارته في كون الإثبات في المسائل الجزائية لا ينصب إلا على وقائع مادية أو نفسية خاصة بالجريمة ولا ينصب على تصرفات قانونية يتفق معها قيام المشرع سلفا بتحديد وسائل إثباتها ومدى الحجية التي تتمتع بها كل منها، كما أن الإثبات ينصرف إلى وقائع إجرامية غالبا ما يعمد الجناة بقدر المستطاع إلى إزالة ومحو آثارها، الأمر الذي يحتم تحويل القضاء كافة الوسائل المتاحة والممكنة لكشف الجريمة وتقصي الحقيقة[1].

وعلى عكس نظام الإثبات المقيد فان فلسفة هذا النظام ترتكز على مبدأين مختلفان هما: الأول يتمثل في الدور السلبي للمشرع في عملية الإثبات، ومن خلاله يمتنع المشرع عن تحديد الأدلة التي تصلح للإثبات مسبقا، وهو ما يفتح المجال لأن تكون جميع الأدلة مقبولة وفقا لتقدير القاضي وليس المشرع، كما يمتنع عن تحديد القيمة الاقناعية للدليل أو إظهار أي تسلسل بين هذه الأدلة في الحجية أو يرجح

[1] - عفيفي كامل عفيفي، مرجع سابق، ص 380

أي دليل على الآخر، فيقتصر دور المشرع على تحديد الشروط اللازمة لصحة الدليل وطريقة تقديمه، وذلك ضمانا للحرية الفردية وكفالة حسن سير العدالة.

أما المبدأ الثاني، فهو الدور الإيجابي 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، وسلطته الواسعة في اتخاذ جميع التدابير والإجراءات التي يعتقد أنها مفيدة لإظهار هذه الحقيقة كسماع الشهود، وندب الخبراء واستدعائهم ليقدموا إيضاحات عن التقارير المنجزة من طرفهم، كما له أن يأمر باستكمال التحقيق إذا ما كانت عناصر الإثبات التي بين يديه غير كافية أو غير مقنعة.

ومن ناحية أخرى فنظام الإثبات الحر 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، كما له أن ينسق بين الأدلة المطروحة أمامه وإزالة التعارض بينها، واستكمال نقصها، ومن ثم تكوين حكمه على أساس القناعة التي توصل إليها من مناقشة هذه الأدلة.

3 - 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 وخروجه عن جادة الصواب، وذلك بأن حدد له وسائل الإثبات التي يلجأ إليها لتأسيس حكمه. كما تم تلافى ما وجه من انتقادات لنظام الإثبات المقيد، 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 الإثباتية لكل منها سلفا من قبل المشرع، ومن جهة أخرى منح القاضي الجزائي سلطة تقديرية واسعة في موازنة وقبول الأدلة المطروحة أمامه وفقا لاقتناعه الذاتي.

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

1- براهيمي جمال، المرجع السابق، ص 143.

ثانيا: مشروعية الحصول على الدليل الرقمي

يشترط في الدليل الجنائي عموما لقبوله كدليل إثبات أن يتم الحصول عليه بطريقة مشروعة، وذلك يقتضي أن تكون الجهة المختصة بجمع الدليل التزمت بالشروط التي يحددها القانون في هذا الشأن[1]. وعليه فمن الضروري أن يتم رسم ضوابط وأطر معينة يتعين أن تمارس في نطاقها عملية البحث عن الأدلة وتحصيلها والتحقيق فيها، بحيث لا تنحرف عن الغرض الذي يبتغيه المشرع من ورائها وهو الوصول إلى الحقيقة الفعلية في الدعوى.

1 - المقصود بمشروعية الحصول على الدليل الإلكتروني

إنه من المقرر أن الإدانة في أي جريمة لابد وأن تكون مبنية على أدلة مشروعة تم الحصول عليها وفق قواعد الأخلاق والنزاهة واحترام القانون من طرف الجهة المختصة بجمع الدليل الجزائي بما يتضمنه من أدلة مستخرجة من وسائل إلكترونية، ولا يكون مشروعا إلا إذا أجرى التنقيب عنه أو الحصول عليه أو كانت عملية تقديمه إلى القضاء أو إقامته أمامه بالطرق التي رسمها القانون، فمتى تم الحصول على الدليل خارج هذه القواعد القانونية فلا يعتد بقيمته مهما كانت دلالته الحقيقية وذلك لعدم مشروعيته، وعلى هذا الأساس فإن إجراءات جمع الأدلة الرقمية المتحصلة من الوسائل الإلكترونية إذا خالفت القواعد الإجرائية التي تنظم كيفية الحصول عليها فإنها تكون باطلة، وبالتالي بطلان الدليل المستمد منها ولا تصلح لأن تكون أدلة تبنى عليها الإدانة في المواد الجنائية.

ولقد صادقت لجنة الوزراء التابعة للمجلس الأوروبي في 1981/01/28 على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، ومن المحاور المهمة التي تناولتها الاتفاقية ضرورة أن تكون البيانات المضبوطة صحيحة وكاملة ودقيقة ومستمدة بطرق مشروعة وعدم إفشائها أو استعمالها في غير الأغراض المخصصة لها، كما أن للشخص المعني الحق في التعرف والإطلاع على البيانات المسجلة المتعلقة به وتصحيحها وتعديلها ومناقضتها ومحوها إذا كانت باطلة.

ولقد وضعت الدساتير والقوانين الإجرائية نصوصا تتضمن ضوابط لشرعية الإجراءات الماسة بالحرية، ومن ثم مخالفة هذه النصوص في استخلاص الدليل يصبغ هذا الدليل باللامشروعية ويهدر قيمته، فمشروعية الدليل تتطلب صدقه في مضمونه وأن يكون هذا المضمون قد تم الحصول عليه بطرق مشروعة تدل على الأمانة والنزاهة من حيث طرق الحصول عليه[2].

[1] - خالد عياد الحلبي المرجع السابق ص 238

[2] - سعيداني نعيم المرجع السابق ص 210

2- موقف القضاء من الدليل غير المشروع

بالنسبة لدليل الإدانة فإن الأمر يقتضي من أجل كسر قرينة البراءة التي يتمتع بها المتهم أن تكون الأدلة التي يؤسس عليها حكم الإدانة مشروعة، ويستوي في ذلك إن كانت أدلة تقليدية أم مستخلصة من الوسائل الإلكترونية. وأي دليل تم الحصول عليه بطريقة غير مشروعة أو بوسيلة مخالفة للقانون يعتبر غير مقبول في عملية الإثبات لأنه إذا ما سمح بقبول أدلة وليدة عن إجراءات باطلة أدى ذلك إلى إهدار الضمانات التي كفلها القانون لحماية حقوق المواطن وكرامته، وترتيبا على ذلك فإنه لا يجوز للقاضي القبول بدليل رقمي تم الحصول عليه من إجراء التسرب جرى القيام به دون مراعاة الشروط الشكلية والموضوعية للإذن بمباشرة هذا الإجراء، أو كان الدليل متحصلا عليه عن طريق إكراه المتهم المعلوماتي من أجل فك شفرة للدخول إلى النظم المعلوماتية أو كلمة السر اللازمة للدخول إلى ملفات المعلومات المختزنة أو القيام بإجراء التنصت أو المراقبة الإلكترونية عن بعد دون مسوغ قانوني، ويكون الدليل المتحصل عليه وفق الطرق السابقة باطلا وعدم إنتاج الآثار القانونية المترتبة عليه[1]. والقاعدة أن الإجراء الباطل يمتد بطلانه إلى الإجراءات اللاحقة له مباشرة وهو الرأي الراجح الذي أخذ به المشرع الجزائري بنص المادة 191 من قانون الإجراءات الجزائية التي نصت على أنه تنظر غرفة الاتهام في صحة الإجراءات المرفوعة إليها وإذا تكتشف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها.

الفرع الثاني: وجوب مناقشة الدليل الإلكتروني

ينبغي لإعمال حق الإثبات وحق النفي في المادة الجزائية، اتخاذ إجراءات الإثبات في مواجهة الخصوم، وتمكينهم من مناقشة الأدلة المقدمة في الدعوى إذ يجب أن يعلم الخصم بكل دليل يقدم ضده ليتسنى له الرد عليه، وهذا ما يعبر عنه بمبدأ مناقشة الدليل.

ويراد بقاعدة مناقشة الدليل في المواد الجزائية أن القاضي لا يمكن أن يؤسس اقتناعه إلا على أدلة الإثبات التي طرحت في جلسات المحاكمة أمامه وخضعت لحرية مناقشة أطراف الدعوى، وهذا عملا بنص المادة 212 ف 02 من قانون الإجراءات الجزائية الناص على أنه " ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه "، وهو المبدأ الذي أكدته المحكمة العليا في قرارها المؤرخ في 2010/01/07 بقولها " استنادا على المادة 212 من ق إ ج بأنه يمكن القاضي الجزائي عند اقتناعه، إفادة المتهم الغائب بالبراءة " [2] وهذا يعني أن الأدلة المستخرجة من الكمبيوتر أو شبكة الإنترنيت سواء كانت مطبوعة أم معطيات مخزنة في وسائل حفظ وتخزين البيانات، أم اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئية، كلها ستكون لزاما محلا

[1] - سعيداني نعيم المرجع السابق ص 212

[2] - مناصرة يوسف المرجع السابق ص 151

للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة ويقتضي مبدأ الوجاهية، ضرورة حضور كل خصم في الدعوى، وأن يطلع خصمه على ما لديه من أدلة وأن يواجهه بها وأن يناقش كل منهما الأخر وتطبيقا لنفس المبدأ يكون للخصم الحق في طلب التأجيل للإطلاع على المستندات المقدمة من الخصم الأخ والرد عليها، ويعد مبدأ الوجاهية بين أطراف الدعوى من أهم المبادئ التي يجب أن يؤسس القاضي إقتناعه على ضوئها، حيث يتطلب هذا المبدأ طرح الأدلة في الجلسة، وأن تمنح الفرصة أمام أطراف الدعوى العمومية، لمناقشة الأدلة المقدمة من كل طرف وتبيانها، ويرتبط هذا المبدأ بمبدأ وجوب إحترام حقوق الدفاع ضمن المحاكمة العادلة وصيانة قرينة البراءة، الذي يعد أحد المظاهر الأساسية لدولة القانون والنظم الديمقراطية.

فعلى القاضي إذن أن يطرح للمناقشة كل دليل قدم أثناء المحاكمة حتى يكون الخصوم على بينة مما قدم ضدهم من أدلة ومن ثم يبطل الحكم إذا كان مبناه دليلا لم يطرح للمناقشة أو لم تتح للخصوم فرصة إبداء الرأي فيه ومن باب أولى إذا لم يعلموا به أصلا.

ويترتب على ذلك أن القاضي الجزائي ليس ملزما بتسبيب طرحه لبعض الأدلة أو الأخذ ببعضها الأخر، فهو حر في اقتناعه بالدليل الذي يراه طالما فيه شرط ثبوته بالأوراق وطرحه بالجلسة ليتمكن الخصوم من مناقشته، بل للقاضي أن يستعين في اقتناعه بالقرائن التي تعزز الأدلة وتساندها طالما أن هذه الأدلة لها أصل بالأوراق وطرحت بالجلسة.

ويترتب على هذا القيد القانوني أن القاضي لا يحكم في النزاع إلا بناء على الأدلة المقدمة في الدعوى، وليس له أن يستند إلى دليل تحراه بنفسه دون طرحه على الخصوم، فلا يجوز له أن يستمد عقيدته من علمه الشخصي الذي يحصله خارج المحكمة أو أن يبني حكمه على واقعة لم تقدم في الدعوى طبقا للإجراءات المقررة في القانتون، لكن يجوز له أن يستند في قضائه إلى المعلومات العامة المستقاة من خبرة القاضي بالشؤون العامة المفروض إلمام كافة الناس بها فلا تعد من قبيل المعلومات الشخصية، مما تلتزم المحكمة قانونا ببيان الدليل عليه وليس له أيضا أن يعتمد في قضائه على أدلة يستمدها من دعوى أخرى لم يقرر ضمها إلى الدعوى المنظورة أمامه، أو من مذكرة تقدم بها أحد الخصوم في جلسات المرافعة في الدعوى، لأن الاعتماد عليها يكون مناقضا لقاعدة الشفوية والوجاهية التي تسود مرحلة المحاكمة ويجعل بذلك حكم المحكمة كأنه غير مسبب ويكون قد ران عليه القصور الذي يتسع له وجه الطعن مما يعيبه[1].

[1] - مناصرة يوسف المرجع السابق ص 152

المطلب الثاني:حجية الدليل الإلكتروني وأثر تبني القاضي الجزائي الجزائري لنظام الإثبات الإلكتروني

إن طبيعة الجرائم الإلكترونية بعناصرها ووسائل ارتكابها، قد تدفع المشرع الجزائي إلى إعادة النظر في كثير من المسائل الجزائية، خاصة فيما يتعلق بمسألة الإثبات، ذلك أن الدليل الذي يقوى على إثبات هذا النوع من الجرائم لابد أن يكون من طبيعة إلكترونية، وهو الأمر الذي يقودنا إلى الحديث عن مسألة قبول هذا الدليل أمام القضاء ومدى تعبيره عن الحقيقة نظرا لما يمكن أن يخضع له من التزييف والأخطاء، وكذا مصداقيته ومشروعيته فإن الأمر لا يتوقف عند هذا الحد، بل يتجاوزه إلى مسألة تتعلق بمدى خضوع هذا الدليل ذو الأصالة العلمية للسلطة التقديرية للقاضي إعمالا لمبدأ السلطة التقديرية للقاضي الجزائي الذي يشكل جوهر أي حكم.

الفرع الأول: حجية الدليل الإلكتروني في الإثبات الجزائي

يقصد بحجية الدليل الإلكتروني ما يتمتع به من القوة الاستدلالية في كشف الحقيقة وصدق نسبة الفعل الإجرامي إلى شخص معين أو كذبه، لذلك فمجرد الحصول على الدليل وتقديمه إلى القضاء لا يكفي لاعتماده كدليل إدانة [1]، إذ إن الطبيعة الفنية الخاصة للدليل الإلكتروني تمكن من العبث بمضمونه على نحو يحرف الحقيقة دون أن يكون في قدرة الشخص غير المتخصص إدراك ذلك العبث، وعليه ينبغي تقدير الدليل وفحص قيمته في إثبات الواقعة الإجرامية، ومسألة تقييم الدليل هي مسألة موضوعية محضة تدخل في صميم سلطة القاضي التقديرية بحثا عن الحقيقة. فالسائد في الفقه أن سلطة القاضي الجزائي في تقدير الدليل يحكمها مبدأ حرية القاضي في تكوين قناعته، مما يستتبع ذلك حتما نتيجة مهمة ألا وهي " حرية القاضي في تقدير الأدلة "، وعملا بهذا المبدأ فالقاضي الجزائي كما يصح له أن يؤسس اقتناعه على أي دليل، له أن يهدره أيضا.

ومقابل ذلك لا ينبغي أن يفهم من حرية القاضي في الاقتناع التحكم المطلق في الأمور والقضاء كيف ما شاء وفقا لأهوائه ومزاجه الشخصي، إنما هو مطالب بتحري المنطق الدقيق في تفكيره الذي قاده إلى اقتناعه واستلهام عقيدته، وألا يكون تفكيره هذا قد جافى الأصول المسلم بها في الاستدلال القضائي.

إن إثبات الدليل الإلكتروني قد يثير عدة صعوبات، فالقاضي الجزائي بثقافته القانونية وعدم كفاءته الفنية في مجال المعلوماتية لا يمكنه إدراك الحقائق المتعلقة بأصالة الدليل الالكتروني، فضلا عن تمتع هذا الدليل في قوته التدليلية بقيمة إثباتية قد تصل إلى حد اليقين شأنه في ذلك شأن الأدلة العلمية عموما، ناهيك عن الطبيعة الفنية الخاصة بالدليل الالكتروني والتي تمكن من العبث بمضمونه بسهولة على نحو يحرف الحقيقة دون أن يكون بمقدور غير المتخصص إدراك ذلك[2].

---

[1] - خالد عياد الحلبي المرجع السابق ص 246

[2] - براهيمي جمال المرجع السابق ص 151

وبوجود هذه الصعوبات وغيرها يطرح تساءل مهم عن مدى سلطة القاضي الجزائي في تقدير ومناقشة الدليل الإلكتروني في مصداقيته وبالتالي قبوله أو رفضه لعدم اقتناعه به؟

أولا: شروط إ كتساب الدليل الإلكتروني حجية في الإثبات

الدليل الإلكتروني ما هو إلا تطبيق من تطبيقات الدليل العلمي الذي يعبر عن حقيقة ٍ علمية ثابتة، فهو يتمتع بحجية قوية في الإثبات، وذلك بما يتميز به من موضوعية وحياد، ولكونه محكما بقواعد علمية حسابية قاطعة لا تقبل التأويل مما يقوي يقينيته، ويساعد القاضي في التقليل من الأخطاء القضائية، والاقتراب أكثر إلى تحقيق العدالة، والتوصل بدرجة أكبر من الحقيقة. لأن التقنية العلمية قد توفر طرقا دقيقة لجمع الأدلة ذات قوة علمية يصعب إثبات عكسها.

ومع هذا فرغم أن الدليل الإلكتروني بحكم طبيعته العلمية وموضوعيته وحياده يمثل إخبارا صادقا عن الواقع، إلا أن ذلك لا يستبعد أن يكون موضع شك في سلامته من العبث عن طريق التحريف أو التغيير من ناحية، وفي صحة الإجراءات المتبعة للحصول عليه من ناحية أخرى.

وإذا كان الشك في مصداقية الدليل الالكتروني مرتبطا أساسا بعوامل خارجية مستقلة عنه لا بمضمونه، فاكتسابه حجية داحضة في الإثبات وكذا قبوله كدليل تبنى عليه الحقيقة في الدعوى الجزائية يتطلب توافر الشروط التالية:

1 - يقينية الدليل الإلكتروني

يشترط في الأدلة الإلكترونية أن تكون غير قابلة للظن أو الترجيح حتى يشيد عليها الحكم بالإدانة، لأنه لا مجال لدحض قرينة البراءة أو افتراض عكسها إلا عند بلوغ اقتناع القاضي حد الجزم واليقين[1].

ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال التمعن والتدقيق فيما يعرض عليه من وقائع الدعوى وأدلة إلكترونية على اختلاف أشكالها، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التأكيد بالنسبة لها، وهكذا يستطيع القاضي أن يحدد قوتها الاستدلالية على صدق نسبة جريمة من الجرائم الإلكترونية إلى شخص معين من عدمه.

ويعتمد القاضي الجزائي عادة لبلوغ اليقين والجزم في اقتناعه بالأدلة على نوعين من المعرفة، الأولى هي المعرفة الحسية التي تستنبط من الحواس بعد معاينته لهذه المخرجات وفحصها، أما الثانية فهي المعرفة العقلية التي يدركها القاضي عن طريق التحليلات، والاستقراءات والاستنتاجات التي يجريها على المخرجات الإلكترونية وربطها بالملابسات التي أحاطت بها. فإن لم ينته القاضي إلى الجزم بنسبة الجريمة الإلكتروني إلى المتهم تعين عليه القضاء بالبراءة، لأن الشك يفسر لصالح المتهم.

وحتى يتحقق اليقين للأدلة الإلكترونية أكثر ينبغي إخضاعها للتقييم الفني بوسائل فنية من طبيعة هذا الدليل تمّكن من فحصه للتأكد من سلامته من العبث، وكذا صحة الإجراءات المتبعة في

1- براهيمي جمال، المرجع السابق، ص 152.

الحصول عليه، فمثلما يخضع الدليل الإلكتروني لقواعد وإجراءات معينة تحكم طرق الحصول عليه، فإنه يخضع كذلك لقواعد أخرى تحكم على قيمته التدليلية من الناحية العلمية، ولعل من أهم هذه الوسائل مايلي:

2 - تقييم الدليل الإلكتروني في سلامته من العبث:

إن الطبيعة التقنية للدليل الإلكتروني تجعله في الغالب عرضة للشك والظنون في سلامته، وذلك راجع إلى إمكانية تعرضه للعبث والخروج به على نحو يخالف الحقيقة، فقد يقدم هذا الدليل ليعبر عن واقعة معينة صنع خصيصا من أجل التعبير عنها خلافا للحقيقة، وذلك دون أن يكون بمقدور غير المتخصص إدراك ذلك العبث، على نحو يمكن القول معه أن ذلك قد أصبح هو الشأن في النظر لسائر الأدلة التقنية التي تقدم للقضاء، فالتقنية الحديثة تمكن من العبث بالدليل الالكتروني التقني بسهولة ويسر ليظهر وكأنه نسخة أصلية في تعبيرها عن الحقيقة.

ولأجل التأكد من سلامة الدليل الإلكتروني يتم الاستعانة بمجموعة من الآليات التالية[1]:

أ/ تقنية التحليل التناظري الرقمي: وهي تقنية يتم من خلالها مقارنة الدليل الرقمي المقدم للقضاء بالأصل المدرج بالآلة الرقمية، ومن ثمة يتم التأكد من مدى حصول عبث في النسخة المستخرجة أم لا، ويستعان في ذلك بتكنولوجية الإعلام الآلي التي أثبتت دورها الفعال في تقديم المعلومات الفنية التي تساهم في فهم مضمون وكينونة الدليل التقني، وكشف مدى التلاعب بمضمون هذا الدليل.

ب/ استخدام عمليات حسابية خاصة تسمى بالخوارزميات: ويتم اللجوء إلى هذه العملية عادة في حالة عدم الحصول على النسخة الأصلية للدليل الإلكتروني أو في حالة ما إذا كان هناك شك في أن العبث قد مس النسخة الأصلية، فهنا تسمح هذه التقنية بالتأكد من مصداقية الدليل الإلكتروني وسلامته من العبث بالتبديل أو التحريف.

ج/ استخدام الدليل المحايد: وهو نوع من الأدلة الإلكترونية الرقمية المخزنة في البيئة الافتراضية ولا علاقة له بموضوع الجريمة، ولكنه يساهم في التحقق من مدى سلامة الدليل الإلكتروني المقصود في عدم وقوع تعديل أو تغيير في نظام الحاسوب[2].

ولا شك أن الخبرة التقنية تحتل في هذه الحالة دورا مهما في التثبت من سلامة الدليل الرقمي، فإذا كان للخبرة التقنية أهمية كبرى في مجال استخلاص الدليل الرقمي، فإن لها ذات الدور في بحث مصداقية وتقييمه من حيث عدم حصول أي عبث عليه، فنقص الثقافة المعلوماتية للقاضي الجزائي

[1] - براهيمي جمال المرجع السابق ص 154

[2] - خالد عياد الحلبي المرجع السابق ص 249

قد يحتم عليه كواجب قضائي أن يستعين في هذه المسائل بوسائل الخبرة كنهج، ليس من اجل استيفاء الدليل فحسب بل لبحث مصداقيته في مجال معالجة الآلية للمعلومات وتحقيق اليقينية لهذا الدليل[1].

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

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

1 - إخضاع الأدلة المستخدمة لعدة تجارب للتأكد من دقتها في إ عطاء النتائج المبتغاة

ويكون ذلك بإتباع اختبارين أساسيين هما:

أ/ إختبار السلبيات الزائفة: ومفاد هذا الإختبار أن تخضع الأداة المستخدمة في الحصول على الدليل لإختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الإلكتروني، وأنه لا يتم إغفال بيانات مهمة عنه.

ب/ إختبار الإيجابيات الزائفة: ومفادها ذلك أن تخضع الأداة المستخدمة في الحصول على الدليل الإلكتروني لاختبار فني يمكن من التأكد من أن هذه الأداة لا تعرض بيانات إضافية جديدة.

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

تبين الدراسات العلمية في مجال تقنية المعلومات على الطرق السليمة التي يجب إتباعها في الحصول على الدليل الإلكتروني، وفي المقابل أوضحت الدراسات الأدوات المشكوك في كفائتها، وهذا يساهم في تحديد مصداقية المخرجات المستمدة من تلك الأدوات[2].

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

[1] - جفال يوسف المرجع السابق ص 49

[2] - خالد عياد الحلبي المرجع السابق ص 250- 251

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

ثالثا: موقف المشرع الجزائري من الدليل الرقمي في مجال الإثبات الجزائي

إن الإثبات الجنائي هو كل ما يؤدي إلى كشف غموض الجريمة وإقامة الدليل على وقوعها والتأكد من أن المتهم هو مرتكب الجريمة بالفعل ووجود الدليل على ذلك، ويعتبر الدليل الوسيلة القانونية التي يستعين بها القاضي للوصول إلى الحقيقة وكشف الجريمة ونسبتها إلى المتهم[1].

فالواجب الملقى على عاتق القاضي هو أن يقيم الدليل على المتهم، لأنه لا يجوز أن يحاكم المتهم ويدان بمجرد وجود قرائن بل لا بد أن تكون هذه الدلائل مكملة لبقية الأدلة المادية الأخرى كما يجب أن تتسم إجراءات جمع الأدلة بالمشروعية وذلك احتراما للحرية الشخصية للمتهم باعتباره بريئا إلى أن تثبت إدانته بحكم بات مقضي فيه.

نصت المادة 212 من قانون الإجراءات الجزائية على أنه يجوز إثبات الجرائم بأي طريق من طرق الإثبات. .. وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص...." كما نصت المادة 307 من قانون الإجراءات الجزائية أيضا أن " 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 يأمر أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المستندة إلى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: " هل لديكم اقتناع شخصي؟ ".

ومن خلال هذين النصين القانونيين يتضح جليا أن المشرع الجزائري قد تبنى كقاعدة عامة 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 مصرعيه كي يستلهم عقيدته من أي موطن يراه، دون أن يطالبه بتقديم مبرر لذلك. واستثناء نجده أخذ أيضا بنظام الأدلة القانونية أو ما يسمى كذلك بنظام الإثبات المقيد في إثبات بعض الجرائم أين اشترط لإثباتها أدلة

1- براهيمي جمال، المرجع السابق، ص 166.

قانونية محددة مسبقا وعلى سبيل الحصر، كما هو الشأن بخصوص جريمة الزنا المنصوص عليها في المادة 339 من قانون العقوبات[1].

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 من ذات القانون 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 المادة 286 التي منحت لرئيس الجلسة سلطة كاملة في ضبط حسن سير الجلسة وفرض الاحترام الكامل واتخاذ أي إجراء يراه 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 الإلكترونية، خاصة أن قانون رقم 09 - 04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها لم يتضمن أية استثناءات أو أوضاع خاصة بهذا الصدد، مما يوحي بأن الدليل الإلكتروني مقبول مبدئيا في الإثبات الجنائي بصفة عامة، والإثبات في مجال جرائم الاعتداء على النظم المعالجة الآلية بصفة خاصة، ويمثل مظهرا من مظاهر اعتناق المشرع لمبدأ حرية الإثبات والاقتناع.

ولم يكتف المشرع الجزائري بالنصوص المذكورة التي أطلقت حرية قاضي الموضوع في إثبات الجريمة بكافة طرق الإثبات وأعطته سلطة تقديرية واسعة في موازنة الدليل، بل خول كذلك لسلطات تنفيذ القانون الأخرى (الاتهام والتحقيق) الحق في البحث عن الأدلة بكل حرية بما فيها الإلكترونية، وتجميعها عن طريق وضع الترتيبات التقنية اللازمة لذلك[2]، وكذا تمحيصها وصولا إلى الحقيقة التي سوف تبرر وفقها الاتهام وتؤسس عليها الأوامر التي يصدرها أثناء التحقيق، منها ما تضمنته المادة 162 الفقرة الثانية من قانون الإجراءات الجزائية " يمحص قاضي التحقيق الأدلة وما إذا كان يوجد ضد

[1] - براهيمي جمال المرجع السابق ص 167

[2] - نذكر منها المادة 68 الفقرة 1 من القانون الإجراءات الجزائية التي تنص على أن: " يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة، بالتحري عن أدلة الاتهام وأدلة النفي. " والمادة 69 من ذات القانون تنص " يجوز لوكيل الجمهورية سواء في طلبه الافتتاحي لإجراء التحقيق أو بطلب إضافي في أية مرحلة من مراحل التحقيق، أن يطلب من القاضي المحقق كل إجراء يراه لازما لإظهار الحقيقة".

المتهم دلائل مكونة لجريمة من جرائم قانون العقوبات ". إضافة إلى إمكانية الاستعانة بكل شخص مؤهل أو لديه علم وخبرة في الواقعة المراد اتخاذ الإجراء بشأنها[1].

وفي مجال الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وضع المشرع الجزائري على عاتق مقدمي خدمات الأنترنت عددا من الالتزامات لمساعدة السلطات المختصة بالتحري والتحقيق[2]، 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 [3] 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 الإلكترونية الرقمية، والتي لا تقبل بطبيعتها إخضاع القاضي لأية قيود بشأنها، بل بالعكس فهي تفرض أن يترك أمر تقديرها وتمحيصها لمحض إرادة واقتناع القاضي الجزائي.

الفرع الثاني: أثر تبني القاضي الجزائي الجزائري لنظام الإثبات الإلكتروني

وإذا كان الدليل الرقمي ذو الأصالة العلمية هو الأوفر والأنسب في إثبات الجريمة المعلوماتية فما مدى إمكانية إعمال القاضي الجزائي لمبدأ الاقتناع الشخصي حيال هذا الدليل طبقا لأحكام المادة 212 من قانون الإجراءات الجزائية.

أولا: مفهوم الاقتناع الشخصي (الذاتي) للقاضي الجزائي

إن الاقتناع الشخصي للقاضي الجزائي هو عبارة عن نشاط عقلي لا يتدخل المشرع ليبين للقاضي كيفية ممارسته وترجمته إلى واقع منتج ولا يرسم له كيف يشكل معادلاته الذهنية في مجال

---

[1] - وهذا ما أكدته المادة 143 من قانون الإجراءات الجزائية الجزائري في نصها " لجهات التحقيق أو الحكم عندما تعرض لها مسالة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم. .."

[2] - أورد المشرع الجزائري في المادة 10 من القانون رقم 09 - 04 أنه في إطار تطبيق أحكام هذا القانون يتعين على مزود الخدمة تقديم المساعدات للسلطات المكلفة بالتحريات القضائية. ..بوضع المعطيات التي يتعين عليهم حفظها وفقا لأحكام المادة 11 أدناه تحت تصرف هذه السلطات.

[3] - أنظر المادة 11ف3 من القانون رقم 09/04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

تقدير الأدلة ليصل من خلالها إلى الحقيقة[1]. فمنهم من عرفه بأنه الإيمان العميق والركون إلى صحة الوقائع التي تقدمها الأطراف المتنازعة الذي يخلف في نفس القاضي الجزائي أثرا عميقا يجعله يصدر حكمه عن قناعة وجدانية وإحساس كبير بإصابته الحقيقة في حكمه، وعرف فقهاء القانون الجنائي الاقتناع بأنه حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث، أو بمعنى آخر هو حالة ذهنية ذو خاصية ذاتية نتيجة تفاعل ضمير القاضي وأدلة الإثبات المطروحة والتي يثيرها الخصوم إما لإثبات أو إنكار اتهام. كما عرف الاقتناع الشخصي أيضا بأنه حالة ذهنية ذاتية تنجم عن إمعان الفكر في وقائع معروضة من أجل بحثها والوصول بعد ذلك إلى حالة تطرد الشك والاحتمال، ويجد هذا المبدأ مناخه الطبيعي الملائم في ظل مذهب الإثبات الحر الذي لا يضع تقديرا مسبقا لأدلة معينة لا يمكن الوصول بغيرها إلى اليقين. ومن خلال هذا التعريف فإن الإقتناع الشخصي للقاضي الجزائي يتميز بخاصيتين هما[2]:

1- أنه حالة ذهنية مبنية على الاحتمال وأن العبرة ليست بكثرة الأدلة وإنما بما تتركه من أثر في نفسية القاضي، لأن هذا التأثير سيلعب دورا في تحديد مصير الدعوى الجزائية بالإدانة أو البراءة.

2- والخاصية الثانية تتمثل في أن القاضي حرفي أن يأخذ عقيدته أو اقتناعه من أي دليل لكن يجب التأكيد هنا أن حرية الإثبات في المسائل الجزائية ليست خاصية يتميز بها القاضي الجزائي لتتسع سلطته في الإدانة أو البراءة ولكنها، ترجع إلى أن الإثبات في المسائل الجزائية والوصول إلى الدليل مسألة جد صعبة وذلك لاختلاف أساليب ارتكاب الجريمة وأن المجرم عادة ما يسعى إلى إخفاء جريمته، لذلك فالبحث عن الحقيقة من خلال الأدلة الجزائية لا يكون إلا عن طريق منح القاضي الجزائي هامشا عن الحرية لمناقشة الدليل الذي يراه مناسبا في إثبات الجريمة.

ثانيا: وسائل تكوين الاقتناع الشخصي للقاضي الجزائي

إن الجهد الاستنباطي الذي يبذله القاضي من خلال نشاطه العقلي المكون لقناعته والذي ينصرف إلى فرز الحقيقة من الدليل محل تقديره يرتكز فيه القاضي على ثلاث طرق[3]:

1- قبوله جميع الأدلة المطروحة أمامه في الجلسة، ولا يحظر على القاضي قبول دليل أو يفرض عليه دليل محدد، ولا يتقيد إلا بقيد مشروعية إجراءات الحصول على الدليل وطرحه للمناقشة العلنية في الجلسة لأجل مناقشته من قبل أطراف الدعوى بكل حرية،عملا وهذا عملا بنص المادة 212 ف 02 من

[1] - براهيمي جمال المرجع السابق ص 171.

[2] - سعيداني نعيم المرجع السابق ص 226

[3] - براهيمي جمال المرجع السابق ص 173.

ق.إ.ج.ج الناص على أنه " ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه[1]"

2- أن يقوم القاضي بموازنة كل دليل على حدى بمعزل عن باقي الأدلة المطروحة أمامه وله أن يقدر قيمة أي دليل مهما تبلغ قيمته طالما أنه لم يطمئن إليه.

3- أن يقوم القاضي بتنسيق كافة الأدلة المطروحة أمامه من خلال التحقيق والتمحيص والتأكد من أنها متساندة تشد بعضها البعض وهو ما يعرف بتساند الأدلة وليست متعارضة.

ثالثا: الشروط التي ترد على القاضي الجزائي في تكوين اقتناعه

إن الهدف من العملية القضائية التي يجريها القاضي الجزائي هو بلوغ الحقيقة الواقعية للجريمة، فكل نشاط أو جهد ذهني يبذله القاضي من خلال هذه العملية ينبغي من وراءه الوقوف على وقائع وملابسات الجريمة كما حدثت، وإذا استقرت لديه تلك الحقيقة وارتاح ضميره للصورة الذهنية التي تكونت له يكون قد وصل إلى حالة الاقتناع.

ولكي يكون هذا الاقتناع منتجا لآثاره يجب أن يراعى فيه الشروط التالية[2]:

1 - بناء اقتناع القاضي على الجزم واليقين: لكي تكون قناعة القاضي سليمة في تقديرها للأدلة، يجب أن تكون النتيجة التي توصل إليها تتفق مع العقل والمنطق، ومطابقة للنموذج المنصوص عليه في القانون وهو ما يطلق عليه الحقيقة القضائية، والتي يشترط أن تتفق مع الحقيقة الواقعية.

2 - تفسير الشك لصالح المتهم: يجد هذا الشرط مكانه عادة عندما لا يتحقق الشرط الأول أي في الحالة التي لا يبلغ فيها القاضي درجة اليقين والجزم في تقديره لوقائع الجريمة أو انتسابها للمتهم، الأمر الذي يسمح بحلول الشك محل اليقين والظن محل الجزم ففي هذه الحالة يجب على القاضي أن يفسر هذا الشك لمصلحة المتهم ويحكم له بالبراءة[3].

رابعا: سلطة القاضي الجزائي في تقدير الدليل الإلكتروني

إن الأصالة العلمية للدليل الرقمي جعلت من سلطة القاضي في تقدير هذا الدليل محل خلاف فقهي، إذ أن هناك من يرى أن الدليل العلمي ومنه الدليل الرقمي له قوته الثبوتية الملزمة حتى للقاضي، مستندين في رأيهم إلى أن هذا الدليل يتسم بالدقة العلمية التي يبلغ معها إلى درجة اليقين، وهناك من يرى أن مبدأ حرية القاضي في الاقتناع يجب أن يبسط سلطانه على كل الأدلة دون استثناء

[1] - ارجع إلى عنصر القيمة القانونية للدليل الإلكتروني، وجوب مناقشة الدليل، من هذه المذكرة، ص 85 .

[2] - براهيمي جمال المرجع السابق ص 173.

[3] - ارجع إلى عنصر شروط اكتساب الدليل الإلكتروني حجيته في الإثبات ويقينية الدليل الإلكتروني، من هذه المذكرة، ص 79.

حتى على الدليل الرقمي، معتبرين أن إعطاء الدليل الرقمي قوة ثبوتية لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى مذهب الإثبات القانوني (المقيد).[1] والمشرع الجزائري كما سبق بيانه أجاز إثبات الجرائم بأي طريق من طرق الإثبات وهو ما أكده بموجب المادة 212 من قانون الإجراءات الجزائية حيث نص على أنه " يجوز إثبات الجرائم بأي طريق من طرق الإثبات. .. وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص...." ما عدا في الجرائم التي قد يتطلب إثباتها دليلا معينا، ومنح القاضي الجزائي سلطة تقدير الدليل والحرية في تكوين اقتناعه من أي دليل يطمئن إليه، فهل تنصرف هذه السلطة التقديرية التي يتمتع بها القاضي الجزائي إلى الدليل الرقمي المستخرج من الوسائل الإلكترونية؟

بالرجوع إلى القانون رقم 09 - 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نجده خاليا من أية أحكام خاصة تتعلق بحجية مخرجات الإلكترونية في الإثبات، ومن هنا فسكوت المشرع عن هذا الأمر هو تفسير لنيته في إخضاع هذه الأدلة مثلها مثل باقي الأدلة الأخرى للقواعد العامة للإثبات. لقد سبق الذكر أن الجريمة المعلوماتية في القانون الجزائري تشمل الأفعال الماسة بأنظمة المعالجة الآلية للمعطيات وكذا كل جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وهذه الأخيرة قد تنصرف إلى جرائم تقليدية منصوص عليها في قانون العقوبات يمكن حسب طبيعتها أن ترتكب بواسطة منظومة معلوماتية، وهذا يعني أن الإجرام المعلوماتي قد يأخذ وصف الجناية أو الجنحة أو المخالفة حسب وصف الجرم المرتكب بواسطة المنظومة المعلوماتية.وإن كان مبدأ الاقتناع القضائي عام لدى كافة أنواع المحاكم الجزائية سواء كانت محاكم الجنايات أم الجنح أم المخالفات فإن قواعد بيان عناصر تقدير الدليل تختلف حسب اختلاف وصف الفعل المجرم. فإذا كان الفعل من طبيعة جنائية فإن محكمة الجنايات تتمتع بسلطة تقديرية مطلقة في مواجهة الأدلة المعروضة أمامها وتصدر أحكامها دون أن يكون قضاتها مطالبين بتسبيب أحكامهم ولا رقابة لجهات الطعن عليهم. أما إذا أخذ الفعل المجرم وصف الجنحة فإن قاضي الجنح مطالب بعرض وبيان تقديره للدليل المعروض عليه من خلال تسبيب حكمه، والذي يكون محل رقابة من جهات الطعن، لهذا فهو مطالب باحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات والتي قد تأخذ شكل محاضر معدة بمناسبة تفتيش أو اعتراض مراسلات أو شكل تقرير خبرة محرر بمناسبة معاينة وفحص الأدلة المضبوطة من جهاز الإعلام الآلي أو دعامات إلكترونية[2].

فأما ما يتعلق بالمحاضر فإن الشرع اعتبر أنها كقاعدة عامة مجرد استدلالات ما لم ينص القانون على خلاف ذلك، ولا يكون للمحضر أي قوة إثبات إلا إذا كان صحيحا من حيث الشكل، وأنه قد تم إعداده من طرف واضعه أثناء مباشرة أعمال وظيفته، ويكون مضمونه ما يدخل في اختصاصه.

[1] - سعيداني نعيم المرجع السابق ص 228

[2] - براهيمي جمال المرجع السابق ص 176 و178.

إلا أن المحاضر التي يخول القانون لضباط الشرطة القضائية إعدادها بنص خاص لإثبات جنح معينة فإن هذه المحاضر تكون لها حجيتها ما لم يدحضها دليل عكسي.

أما بالنسبة لتقارير الخبرة فإن المحكمة العليا ذهبت للقول أن الخبرة شأنها شأن باقي أدلة الإثبات تخضع للسلطة التقديرية لقاضي الموضوع، وهذا المعنى تؤكده المادة 215 من قانون الإجراءات الجزائية التي تنص على أنه:" لا تعتبر المحاضر والتقارير المثبتة للجنايات أو الجنح إلا مجرد استدلالات مالم ينص القانون على خلاف ذلك"

لكن الطبيعة العلمية والتقنية للجريمة المعلوماتية غالبا ما تفرض على القاضي الاستناد في تكوين اقتناعه على الخبرة الفنية والتقيد بالنتيجة المتوصل إليها الخبير في تقرير خبرته ولا يمكنه طرحها واستبعادها إلا إذا قدر أن ما تحمله من أدلة لا يتوافق مع ظروف وملابسات الواقعة أو تتناقض مع الحقيقة العلمية. فحسب الاجتهاد القضائي أنه أحيانا ما تكون الخبرة وحدها كافية بالنسبة للقاضي عندما يكون مطالبا للفصل في وقائع ذات طابع تقني دون أن يحتاج إلى مناقشتها[1].

وفي الأخير، يمكن القول إن إساءة استخدام التقنية المعلوماتية تعد من الموضوعات التي فرضت نفسها على المستوى الوطني والدولي على حد سواء، وأجبرت التشريع الجزائي على التدخل من أجل مواجهتها بتشريعات حاسمة لمكافحتها ومعاقبة مرتكبيها، إلا أن ذلك يبدو غير كاف لتحقيق هذا الهدف، فعلى المستوى الإجرائي تثير الجريمة المعلوماتية مشكلات عدة بدء من مرحلة الاستدلال حتى صدور الحكم الجزائي، لا سيما فيما يتعلق بإثبات الجريمة المعلوماتية ومدى صلاحية الدليل الرقمي للإثباتها ومدى شرعية الأدلة المتحصل عليها عبر التقنية المعلوماتية وحجيتها أمام القاضي الجزائي.

[1] - قرار المحكمة العليا الغرفة الجنائية مؤرخ في 2002/06/04 نشرة القضاة رقم 58 لسنة 2006 ،ص 255

خاتمـــة

خاتمة

إن عالم الإنترنت ولد إلى جانب مزاياه ظاهرة جديدة وخطيرة أصبحت تهدد أمن الإنسان واستقراره تسمى بالجريمة الإلكترونية أو الجريمة المعلوماتية، أخذت في النمو والتزايد وبشكل مذهل وخطير للغاية وبأنماط جديدة، فالمجرم الإلكتروني يوجد في عالم افتراضي غير ملموس لا يعرف الحدود وهو ذكي ويتسم بقدر عالي من الكفاءة العلمية والتقنية، يتولى الولوج إلى عمق الأنظمة المعلوماتية دون أن يكلف نفسه عناء التنقل، يضاف إلى ذلك أنه من الصعب بمكان ملاحقة هؤلاء المجرمين وضبط الأدلة دون الحديث عما يطرح أمام ذلك تحديات بخصوص الاختصاص القضائي والمحاكمة العادلة، فنحن الآن أمام عولمة الجريمة وبهذا الصدد حاولت بشيء من التفصيل إبراز المواجهة التشريعية والإجرائية لهاته الجرائم العالية.

النتائج:

بعد الدراسة والتمعن في موضع البحث حول خصوصية التحقيق في الجريمة الإلكترونية، ومحاولة الإجابة عن التساؤلات المطروحة خلصت إلى أهم النتائج التي أستعرضها فيما يلي:

نتيجة للسمة التي تتميز بها الجرائم الإلكترونية، امتد تأثير ذلك على الشق الإجرائي للقانون الجزائي حيث أثارت العديد من الانشغالات خاصة وأن نطاق نصوصه لا تجد صعوبة في التحري عن الجريمة التقليدية وإثباتها، مما استلزم معه الأمر أن بادر المشرع إلى إعادة النظر في القواعد الإجرائية التقليدية المتعلقة باستخلاص الدليل كالتفتيش والضبط وجعلها صائغة الاستعمال في مجال البيئة الرقمية الإلكترونية. عن طريق استحداث قواعد إجرائية حديثة تتلاءم مع الطبيعة الخاصة التي يتميز بها هذا النوع من الجرائم، كالمراقبة الإلكترونية واعتراض المراسلات والتسرب الالكتروني، وهو ما أقدم عليه المشرع الجزائري من خلال تعديل قانون الإجراءات الجزائية في عام 2006، وإصداره قانون رقم 09 - 04 المتعلق بالقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

تخضع إجراءات البحث والتحقيق في الجرائم الإلكترونية إلى جهات متخصصة في التعامل مع هذا النوع من الجرائم، تعتمد في تكوينها على مجموعة من المختصين في مجال المعلوماتية وكذلك في مجال التحقيق الجنائي، مما يجعلهم يستطيعون التكفل بمهام البحث والتحقيق في الجرائم الإلكترونية، نظرا لتقديرهم العلمي والمعرفي بالأساليب الإجرامية الإلكترونية، وكذلك القواعد القانونية للتعامل بالشكل الشرعي مع هذا النمط من الجرائم.

يقترن نجاح إجراءات البحث والتحقيق في الجرائم لإلكترونية بمدى براعة وفعالية وجاهزية الجهات المختصة بمباشرة إجراءات تتبع الأدلة الإلكترونية، وتحصيلها وحفظها بغرض عرضها على الجهات المختصة بتقديرها.

على الرغم من أن المشرع الجزائي أحاط الحياة الخاصة بالحماية القانونية، خاصة ما تعلق بالاتصالات الإلكترونية، إلا أنه في سبيل الكشف عن حقيقة الجريمة ومقترفيها أجاز للمحققين اختراق هذه الحماية كلما اقتضت ضرورة التحري والتحقيق ذلك، إلا أنه إشترط لمباشرتها التقيد بمجموعة من الشروط أهمها شرط الالتزام بالنص الإجرائي الملائم، لما قد تنطوي عليه هذه الإجراءات من مساس بالحريات الفردية وإطلاع على مستودع سر الأفراد، كالتصنت الإلكتروني واعتراض البريد الإلكتروني، وحجز للمعطيات والبيانات الشخصية، وكل ذلك حفاظا على سلامة الإجراءات من طائلة البطلان وكذلك حفاظا على حريات الأفراد وكرامتهم.

إن سلطات البحث والتحقيق تواجه مشاكل في ما يتعلق بالقيمة القانونية للأدلة الإلكترونية المتحصل عليها أثناء عملية الإثبات الجنائي، إذ أن عملية استخلاص الدليل الالكتروني سواء بالطرق الإجرائية التقليدية أو المستحدثة ليس بالأمر الهين، بل تعيقها في غالب الأحيان صعوبات تتعلق إما بالطبيعة التكوينية للدليل الإلكتروني أو بالعامل البشري.

إن الدليل الإلكتروني المتحصل عليه من العالم الافتراضي غير الملموس حتى يعتبر ذا قيمة قانونية، يجب أن يتصف بجملة من الشروط، أن يكون مشروعا، وأن تكون له حجيته على الوقائع المراد إثباتها وان يتم الحصول عليه بالطرق القانونية وأن يقدم للمحكمة على الهيئة نفسها التي تم جمعها عليها، بدون أن يطرأ عليه أي تغيير أو تحريف خلال فترة حفظه.

فعملية استخلاص الدليل الإلكتروني تشوبها في كثير من الأحيان صعوبات ومعوقات إما تتعلق بالطبيعة التقنية للدليل أو بالعامل البشري تقتضي معها التعامل بحذر وذكاء شديد.

وقد استخلصت أيضا بأن مسألة قبول الدليل الإلكتروني من عدمه إنما تخضع لمطلق تقدير القاضي الجزائي، الذي يتمتع بدور إجابي في مناقشة وموازنة القيمة القانونية للدليل الإلكتروني قبل أن يطمئن إليه، شأنه في ذلك شأن باقي الأدلة.

كما تم التوصل إلى أنه يجب عدم الخلط بين القيمة العلمية القاطعة للدليل الإلكتروني، التي لا يملك للقاضي الفصل فيها لأنها مسألة فنية بحتة والقول فيها هو قول أهل الاختصاص، وبين الظروف والملابسات التي تحيط بالدليل، والتي يجوز للقاضي أن يحل نفسه فيها محل الخبير ويطرح رأيه وفق أسباب سائغة مقبولة، وله في ذلك أن يرفض هذا الدليل إن لم يقتنع بظروف القضية وملابساتها، إعمالا بنظام الإثبات الحر الذي تبناه المشرع الجزائري في نص المادتين 112 و307 من قانون الإجراءات الجزائية.

الاقتراحات:

وعلى هدي ما توصلت إليه من هذا العمل المتواضع، والذي لا أعتبره بحثا معمقا، وإنما محاولة مني الإلمام بالموضوع، فإنه قد بدا لي أن أقدم جملة من المقترحات آمل أن أكون موفقا في طرحها ومفيدة

* رغم إجتهاد المشرع الجزائري للتصدي لهذه الجريمة، إلا أنه لم يخصها بقانون قائم بذاته للتحكم فيها بصرامة مما يستحسن وضع قانون خاص بالجرائم الإلكترونية بدل تناثر أحكام تجريمها في قانون العقوبات والقوانين الخاصة، كما فعل مع جرائم الفساد أين خص لها قانونا خاصا بها رقم 06 - 01 المتعلق بالوقاية من الفساد ومكافحته، أو قانون 04 - 18 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين بها.

* تكثيف التعاون والتنسيق الدولي بين الدول من أجل تطوير وتوحيد التشريعات الموضوعية والإجرائية التي تعنى بمكافحة الجرائم الإلكترونية عن طريق إبرام اتفاقيات دولية وإقليمية ثنائية ومتعددة الأطراف في هذا المجال، أو الانضمام إلى الاتفاقيات المبرمة في هذا الخصوص كالاتفاقيات الأوربية حول الجريمة الإلكترونية المبرمة في بودابيست عام 2001 مع مراعاة المصلحة الوطنية ومبدأ السيادة.

* نشر الوعي في أوساط المجتمع وتحسيسه بالمخاطر الاقتصادية والاجتماعية والنفسية وغيرها الناجمة عن الاستخدامات غير المشروعة وغير الآمنة للإنترنت وما يترتب عنها من انعكاسات سلبية على حياة الفرد والمجتمع.

* إدخال برامج تعليمية في المنظومة التكوينية، خاصة منها تخصيص مادة " أخلاقيات استخدام الإنترنت " للتحسيس بمخاطر الاستعمال السيء لمواقع التواصل الاجتماعي والتعريف بالجرائم المعلوماتية.

* ضرورة تدريب وتأهيل أفراد الضبطية القضائية وكذا النيابة العامة وقضاة التحقيق على كيفية التعامل مع هذا النوع من الجرائم وبالتعاون مع التقنيين من أصحاب الخبرة.

* ضرورة اهتمام كل الفاعلين في مجال مكافحة هذا النوع من الإجرام الذي يتم في عالم افتراضي، رجال القضاء والمصالح الأمنية والباحثين بالدراسات القانونية التي تعنى بالجوانب الإجرائية.

* احتراما لحقوق الإنسان عامة ولحقوق المواطن خاصة يتحتم وضع آليات للتصدي لمواقع ووسائل اختراق المواقع بمختلف صورها.

* بالنسبة لمسيري مقاهي الإنترنت يستحسن إعادة النظر في تسييرها من قبل المشرع، عن طريق إدراج شروط يلتزم بها مقدم هاته الخدمة، منها إلزام الزبون بملء استمارة معلومات تحدد هويته والتوقيت الذي استعمل فيه الشبكة ورقم الحاسوب مع الاحتفاظ بعناوين المواقع التي زارها في ذاكرة

الحاسوب لمدة معينة، وكذلك الأمر بالنسبة لاستعمال شبكات الإنترنت الموجود في المؤسسات العامة كالجامعات وغيرها.

* اقتراح إضافة فقرة على المادة 05 من قانون 09 - 04 الخاصة بتفتيش المنظومة المعلوماتية، تتضمن عدم اللجوء إلى إجراء عمليات التفتيش في المنظومة الأمنية إلا بإذن مكتوب من قبل السلطة القضائية المختصة.

في الختام، أملي أن يحقق بحثي قدر من العزم منه، وما أنا إلا بشر اجتهد فأخطئ وأصيب، فان أصبت فأجري على الله ون أخطأت فأدعوه ألا يحرمني أجر المجتهدين، ولله الأمر من قبل ومن بعد، والحمد الله رب العالمين.

قائمة المراجع

أولا: النصوص القانونية

1- القوانين

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

2- قانون 2000 - 03 المؤرخ في 5 أوت 2000 محدد القواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الصادر بالجريدة الرسمية رقم 48 المؤرخة في 05 غشت 2000.

3 - قانون رقم 06 - 01 المؤرخ في 2006/02/20، يتعلق بالوقاية من الفساد ومكافحته، الصادر بالجريدة الرسمية رقم 14 المؤرخة في 08 مارس 2006.

3- القانون رقم 90 - 04 المؤرخ في 16 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 47 بتاريخ 05 غشت 2009

2- الأوامر

1- الأمر رقم 66 - 156 المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم، بالقانون رقم14-01 المؤرخ في 4 فبراير 2014 جريدة رسمية، رقم 7، بتاريخ 16 فبراير 2014.

2 - الأمر رقم 66 - 155 المؤرخ في 8 يونيو 1966 ،المتضمن قانون الإجراءات الجزائية المعدل والمتمم، بالأمر رقم17-07 المؤرخ في 27 مارس 2017، الجريدة الرسمية، رقم 20 بتاريخ 29 مارس 2017.

3- المراسيم

1 - مرسوم رئاسي 04 - 183 مؤرخ 26 يونيو 2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد القانوني الأساسي، الجريدة الرسمية رقم 49 بتاريخ 27 جوان 2004.

2- المرسوم الرئاسي، رقم 15-261 المؤرخ في 08 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد 53 ،بتاريخ 08 أكتوبر 2015.

3 - المرسوم التنفيذي رقم 98 - 257 المؤرخ في 25 غشت 1998، يضبط شروط وكيفيات إقامة خدمات الأنترنت واستغلالها، الجريدة الرسمية رقم 63المؤرخة في 04 جمادى الأولى عام 1419 هـ، الموافق لـ: 26 غشت 1998.

ثانيا: الكتب

1 - أحمد فتحي سرور، الشرعية والإجراءات الجنائية، دار النهضة العربية، القاهرة، 1977

2 - أمير فرج يوسف - الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والأنترنت، مكتبة الوفاء القانونية - الإسكندرية -الطبعة الأولى 2011

3 - أنيس حسيب السيد المحلاوي- الخبرة القضائية في الجرائم المعلوماتية والرقمية - دراسة مقارنة - دار الفكر الجامعي- الطبعة 2016.

4 - خالد عياد الحلبي - إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت -دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى 2011.

5 - زيبجة زيدان - الجريمة المعلوماتية في التشريع الجزائري والدولي - دار الهدى العين مليلة، الجزائر سنة الطبع 2011

6 - عبد الرحمان خليفي، محاضرات في قانون إجراءات جزائية، دار الهدى ،الجزائر، 2012.

7 - عبد الفتاح بيومي حجازي - مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والإنترنت، دار الفكر الجامعي الإسكندرية، الطبعة الأولى 2006.

8 - عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دار النهضة العربية، القاهرة الطبعة الأولى 2009.

9 - عفيفي كامل عفيفي - جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون - دراسة مقارنة - منشورات الحلبي الحقوقية - طبعة 2003.

10 - غسان مدحت الخيري، الطب العدلي والتحري الجنائي، دار الراية، المملكة الأردنية، ط1، 2013

11 - فرج علواني هليل، التحقيق الجنائي والتصرف فيه، دار المطبوعات الجامعية، الإسكندرية 2006.

12 - محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، ط2 ،2009

13 - محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومة، الجزائر، ط3، 2008

خالد ممدوح إبراهيم - فن التحقيق الجنائي في الجرائم الإلكترونية - دار الفكر الجامعي - - 6 -4 - 3 2009الإسكندرية - مصر الطبعة الأولى سنة

14- محمد طارق عبد الرؤوف الخن - جريمة الاحتيال عبر الإنترنت (الأحكام الموضوعية والأحكام الإجرائية) - منشورات الحلبي الحقوقية - لبنان طبعة 2011.

15 - محمود أحمد طه - المواجهة التشريعية لجرائم الكمبيوتر والإنترنت دراسة مقارنة - دار الفكر والقانون مصر طبعة 2016-2017.

16 - محمود نجيب حسني، شرح قانون العقوبات – القسم الخاص، بدون رقم الطبعة، دار النهضة العربية، القاهرة 1992

17- مصطفى محمد موسى - التحقيق في الجرائم الإلكترونية -مطابع الشرطة - القاهرة - الطبعة الأولى 2009

18 - مناصرة يوسف - الدليل الإلكتروني في القانون الجزائي - منشورات دار الخلدونية - الجزائر - طبعة 2018

19- مناصرة يوسف - جرائم المساس بأنظمة المعالجة الآلية للمعطيات - منشورات دار الخلدونية - الجزائر - طبعة 2018

20 - منصور عمر المعايطة - الأدلة الجنائية والتحقيق الجنائي لرجال القضاء والادعاء العام والمحامين وأفراد الضابطة العدلية، دار الثقافة عمان الطبعة الأولى 2009.

21 - نبيلة هبة هروال - الجوانب الإجرائية لجرائم الإنترنت، في مرحلة جمع الاستلالات، دراسة مقارنة، دار الفكر الجامعي الإسكندرية، الطبعة الأولى 2007

22- ناير نبيل عمر. الحماية الجنائية للمحل الإلكتروني في الجرائم المعلوماتية . دار الجامعة الجديدة للنشر. مصر. طبعة 2012.

23- نهلا عبد القادر المومني - الجرائم المعلوماتية - دار الثقافة للنشر والتوزيع الأردن - طبعة 2010.

24 - 4 - محاضرة بعنوان (الجريمة السبريانية كنوع من الجرائم المستحدثة) مديرية الشرطة القضائية للأمن الوطني - 2018

ثالثا:المذكرات الجامعية

1 - سعيداني نعيم - آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري - مذكرة لنيل شهادة الماحستير في العلوم القانونية تخصص علوم جنائية -جامعة الحاج لخضر باتنة - السنة الجامعية 2013./2012

2 - بختي فاطمة الزهراء - إجراءات التحقيق في الجريمة الإلكترونية - مذكرة لنيل شهادة الماستر- جامعة محمد بوضياف المسيلة، السنة الجامعية 2013 - 2014.

3 - يوسف جفال - التحقيق في الجريمة الإلكترونية -مذكرة ماستر، جامعة محمد بوضياف، المسيلة قسم الحقوق السنة الجامعية 2016 - 2017.

4 - براهيمي جمال - التحقيق الجنائي في الجرائم الإلكترونية - أطروحة لنيل شهادة الدكتوراه في العلوم القانونية- جامعة معمري ميلود - تيزي وزو -تاريخ المناقشة 27 جوان 2018.

2- رابعا: المراجع الإلكترونية

3- فضيلة عاقلي، أ/محاضرة "أ" جامعة باتنة-1- الجزائر، الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري، كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس يومي 24-25/03/2017. الموقع الإلكتروني http://jilrc.com ، بتاريخ 2019/02/21 على الساعة 14.46.

فهرس المحتويات

فهرس المحتويات

ملخص الدراسة

ملخص

إن الجريمة الإلكترونية تعد من الأنماط الإجرامية الحديثة، فجرتها ثورة تقنية المعلومات والاتصالات عن بعد، مما جعلها تتميز بخصائص مختلفة، بحيث أوجدت بظهورها وبتطورها السريع إشكالات إجرائية أمام الجهات المكلفة بالبحث والتحقيق عنها وعن مقترفيها، نتيجة القصور الذي اعترى النصوص الجزائية الإجرائية، الذي صيغت نصوصه لتنظيم الإجراءات المتعلقة بالجرائم التقليدية، بحيث لا توجد صعوبة في إثباتها أو التحقيق فيها وجمع الأدلة المتعلقة بها، مع خضوعها لمبدأ الاقتناع الشخصي للقاضي الجزائي، الذي له حرية تقدير الدليل ومن ثمة الأخذ به أو إبعاده.

الأمر الذي قادني أمام هذه الوضعية إلى طرح إشكالية الدراسية لأنطلق في البحث عن إجابات لها مفادها " ما مدى فعالية القواعد الإجرائية المنتهجة، التي أوجدها المشرع الجزائي الجزائري في ضبط وإثبات جريمة ارتكبت في عالم افتراضي غير ملموس، وهل هي كفيلة باحتواء متغيرات هذا النمط المتجدد والمتطور؟.

أين عالجت جملة من المسائل في سبيل بناء صورة واضحة عن عنوان مذكرتي " خصوصية التحقيق في الجريمة الإلكترونية " أين تناولت في الفصل الأول ماهية الجريمة الإلكترونية وسماتها، لأستفيض بشكل موسع بعدها في الفصل الثاني عن إجراءات التحقيق واستخلاص الدليل الإلكتروني في الجرائم الإلكترونية، لأجل الوصول إلى إيجابة عن الإشكالية المطروحة.

Résumé

La cybercriminalité est un schéma criminel moderne déclenche par la révolution des techniques qui l'a caractérisée par des caractéristiques différentes de sorte que l'évolution rapide des problèmes de procédure devant les autorités chargées de la recherche et de l'enquête sur les auteurs. À la suite de l'échec des textes pénaux de procédure. Le texte de celui-ci à été rédige pour réglementer les procédures relatives aux crimes classiques, qui n'étaient pas difficiles à prouver ou à enquête et rassembler des preuves. Sous réserve du principe de la conviction personnelle du juge pénal.qui est libre d'apprécier la preuve et la prendre ou de l'enlever.

Ce qui m'a amené à poser le problème de l'étude pour commencer à chercher des réponses à l'efficacité des règles de procédure adoptées par le droit pénal algérien pour contrôles et prouver le crime commis dans un monde virtuel n'est pas tangible et peut contenir les variables de ce modèle renouvelé et en évolution.

Ou j'ai abordé un certain nombre de question afin de crier un image claire du titre de ma note « Ce qui a traité un certain nombre de questions afin de brosser un tableau clair de la "confidentialité de l'enquête sur la criminalité électronique" qui est traité dans le premier chapitre qu'est-ce que la cybercriminalité et ses caractéristiques ? Ou sera développer de manière détaillée dans le deuxième chapitre sur les procédures d'enquête et l'extraire les preuves électroniques dans la cybercriminalité. Pour avoir accès une réponse au problème posé.