جامعة 8 ماي 1945

كلية الحقوق والعلوم السياسية

قسم العلوم القانونية والإدارية **تخصص: قانون الأعمال**

مذكرة لنيل شهادة الماستر في قانون الأعمال

حجية الدليل الالكتروني في الإثبات الجنائي

إعداد الطالبة:

– بشرى عواطة

إشراف الدكتور:

– يزيد بوحليط

تشكيل لجنة المناقشة

الرقم	الأستاذ(ة)	الجامعة	الرتبة العلمية	الصفة
01	د/ يزيد بوحليط	جامعة 8 ماي 1945 قالمة	أستاذ محاضر ب	مشرفا
02	د/رابح بوسنة	جامعة 8 ماي 1945 قالمة	أستاذ محاضر ب	رئيسا
03	د/نبيلة عيساوي	جامعة 8 ماي 1945 قالمة	أستاذ محاضر ب	عضوا مناقشا

السنة الجامعية: 2017–2018

بسم الله الرحمن الرحيم

شكر و تقدير

الحمد والشكر لله، سبحانه الذي وفقني أخيرا وأتم علي نعمته ووهبني القوة والعزيمة، وإذا كان للمرء أن يذكر لكل ذي فضل فضله، فإني أتوجه مقرة بالشكر والعرفان وخالص التقدير والاحترام للدكتور الذي أشرف على هذا العمل "يزيد بوحليط" الذي لم يبخل علي بالتوجيهات والرأي السديد، فكان العماد والأساس لهذا الجهد المتواضع.

كما يشرفني أن أتقدم بخالص الشكر والعرفان لأساتذتي الأجلاء،الأفاضل لجنة المناقشة لتحملهم عناء قراءة هذه المذكرة.

فلهم منا أرقى عبارات الشكر والامتنان والتقدير وجزاهم الله خير الجزاء.

ويملي علينا واجب الاعتراف بالفضل أن أتقدم بالشكر والتقدير إلى أعضاء المكتبة والكلية.

إهداء

الحمد لله رب العالمين والصلاة والسلام على خاتم الأنبياء والمرسلين

أهدي هذا العمل إلى:

من ربتني وأنارت دربي وأعانتني بالصلوات والدعوات، إلى أغلى إنسان في هذا الوجود " أمي الحبيبة " أدامها الله لي

إلى من عمل بكد في سبيلي وأوصلني إلى ما أنا عليه " أبي الكريم " أطال الله في عمره

إلى من عملوا معي بكد بغية إتمام هذا العمل

أخي الغالي "علي"، وخطيبي "نور الإسلام" الذي أكن له كامل الاحترام والتقدير

إلى إخوتي:

توأمي "ياسمين"، مهدية، وردة، سعاد، كريم، سارة

وفي الأخير أرجو من الله تعالى أن يجعل عملي هذا نفعا يستفيد منه جميع الطلبة المقبلين على التخرج

قائمة المختصرات .

باللغة العربية :

(ق.إ.ج.ج): قانون الإجراءات الجزائية الجزائري.

(ق.ع.ج): قانون العقوبات الجزائري.

(ج. ر): الجريدة الرسمية.

(د.س.ن): دون سنة النشر.

(ط): طبعة.

(ع): عدد.

(ق): قانون.

(ص): صفحة.

(الخ): إلى آخره .

(.../...): المادة/الفقرة.

باللغة الفرنسية:

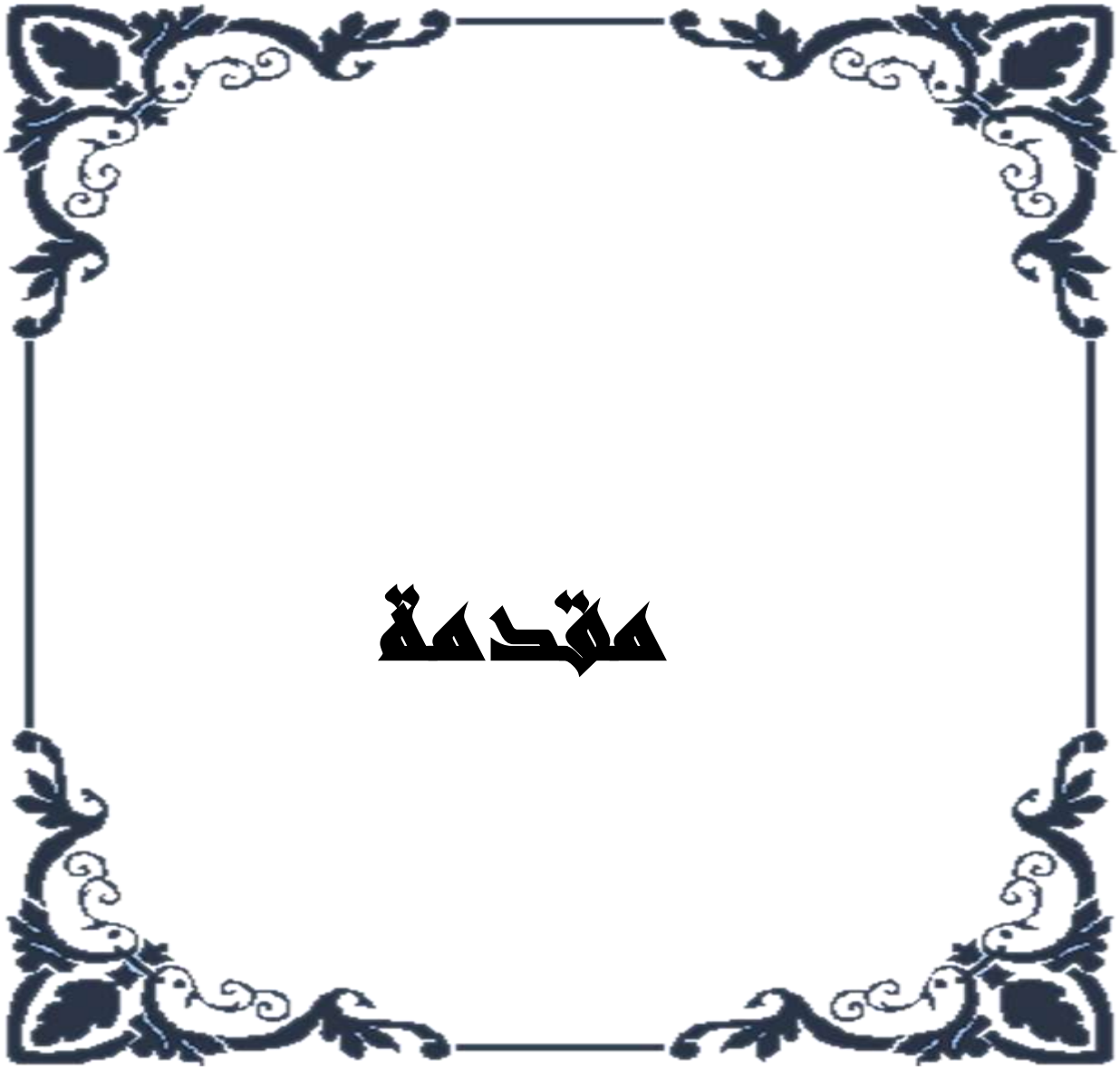
Op.cit.:ouvrage précédemment cité.

pp.: plusieure pages.

p: page.

Art: Article.

cppf: code de procédure pénale francaise



مقدمة

مقدمة

لقد مرت البشرية بمراحل معينة أدت إلى تطورها, حتى وصلت إلى مرحلة الثورة المعلوماتية والتي غيرت حياة الأفراد بشكل كبير في مجالات عدة، نظرا لما تتميز به من سرعة ودقة في تجميع المعلومات وتخزينها ومعالجتها وكذا تبادلها بين الأفراد والشركات والمؤسسات المختلفة سواء كانت داخل الدولة أو بين عدة دول، كما تعتبر أيضا مستودعا للأسرار الخاصة والعملية للأشخاص، خاصة بعدها حدث اندماج بين المعلوماتية والاتصال عن بعد، حيث أصبح الإنسان يعيش في البيئة العالمية للتقنية العالية للمعلومات، أين يعتبر الحاسب الآلي والانترنيت محورا أساسيا لها.

وبقدر ما حققت تكنولوجيا المعلومات أثارا إيجابية من إنجازات و تطورات في المجال الرقمي من خلال الاعتماد عليها في الكثير من قطاعات الحياة، فإنها في الوقت نفسه مهدت إلى ظهور أنواع جديدة من الجرائم المستحدثة، لم يكن للإنسان سابق عهد بها ألا وهي "الجرائم الإكترونية" أو "الجرائم المعلوماتية" تتميز بخصائص فريدة من نوعها وذات طبيعة خاصة تختلف عن الجرائم التقليدية المعروفة.

إن الطبيعة الفنية والتقنية الناجمة عن الجرائم الإلكترونية نتج عنها نوع جديد من الأدلة في مجال الإثبات الجنائي، يطلق عليه الدليل الرقمي أو الدليل الإلكتروني، وهو الأمر الذي أدى إلى تدخل المشرع الجزائري بنصوص قانونية إجرائية تساعد على استنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم ووسائل ارتكابها، ولقد قام المشرع بتعديل قانون الإجراءات الجزائية بموجب القانون 06-22 المؤرخ في 20 ديسمبر 2006 بالإضافة إلى إصدار قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

أهمية الموضوع:

إن دراسة موضوع حجية الدليل الإلكتروني في الإثبات الجنائي له أهمية بالغة، وتتضح هذه الأهمية من خلال أن له صلة وثيقة بطائفة جديدة من الجرائم ظهرت مع التطور التكنولوجي، وتتمثل في الجرائم الإلكترونية، وهو ما استتبع طائفة جديدة من الأدلة، التي تتفق وطبيعة الوسط الذي ترتكب فيه الجريمة الإلكترونية، وهي الأدلة الإلكترونية.

كما تظهر أهمية هذا الموضوع في أنه أصبح لزاما على أجهزة العدالة أن تتعامل مع الدليل الإلكتروني، كدليل مستحدث في مجال الإثبات الجنائي، مما يحتم عليها أن تأخذ به مواكبة للتطور التكنولوجي من جهة، ومكافحة الجرائم الإلكترونية من جهة أخرى.

كذلك تتضح أهمية الموضوع في تقبل الدليل الإلكتروني أمام القضاء الجنائي بغرض التصدي للجرائم الإلكترونية، فالقضاء الجنائي وجد نفسه في مواجهة هذا الدليل المستحدث، بما يفرض تحديات جديدة للقاضي الجنائي.

دوافع اختيار الموضوع:

إن السبب الذي دعانا إلى الولوج في موضوع حجية الدليل الإلكتروني في الإثبات الجنائي، هو نقص الدراسة في الموضوع، باعتبار أنه موضوع مستحدث نسبيا.

كما أنه موضوع فرض نفسه في الوقت الراهن لأنه جاء مصاحبا للتطور التكنولوجي خاصة في نظم المعلومات.

بالإضافة إلى معرفة مدى مواكبة التطور التكنولوجي الحاصل من طرف القضاء الجنائي باعتبار أن هذا التطور تتبعه خطورة المجرمين الذين يستعملون هذه التقنيات الحديثة لأغراض غير مشروعة ومخالفة للقانون.

الإشكالية:

أما عن إشكالية هذا الموضوع، فباعتبار أن صعوبة كشف وضبط الدليل الإلكتروني المستخلص من الجرائم الإلكترونية وما يصاحب إجراءات الحصول عليه من خطوات معقدة، واتساع مسرح الجريمة الذي يتخطى غالبا حدود الدولة الواحدة، وعدم ملائمة القوانين والأنظمة أحيانا لبعض القضايا المطروحة في هذا المجال ونظرا لما قد يثيره قبول الدليل الإلكتروني من مشكلات في الإثبات الجنائي، ذلك أن مستودع هذه الأدلة هو الوسائل الإلكترونية التي يمكن التلاعب فيها.

وعليه ارتأينا أن تكون إشكالية الدراسة كالآتي:

– ما مدى اعتراف المشرع الجزائري بالدليل الإلكتروني في الإثبات الجنائي؟

وتندرج تحت هذه الإشكالية الرئيسية مجموعة من التساؤلات الفرعية الآتية:

– ما المقصود بالجريمة الإلكترونية والدليل الإلكتروني؟

– فيما تتمثل الإجراءات والأساليب القانونية المتبعة للحصول على الدليل الإلكتروني في التحقيق الجنائي؟

– إلى أي مدى يمكن الاعتماد على الدليل الإلكتروني في الإثبات الجنائي؟ وما مدى تأثيره على مبدأ حرية اقتناع القاضي الجنائي؟

إن كل هذا الطرح سواء الإشكالية الرئيسية أو مجموعة التساؤلات الفرعية لا يدل سوى على مدى عمق الموضوع وتشبعه، نظرا لكونه موضوعا يجمع بين مجالين متباعدين نظريا وهما موضوع تكنولوجيا المعلومات ومجال القانون، وهو ما سنحاول تقريبه بالإجابة من خلال أطوار البحث على كل التساؤلات المطروحة مسبقا.

أهداف البحث:

تتلخص أهداف البحث في النقاط الآتية:

– معرفة نوع جديد من الجرائم وهو الجرائم الإلكترونية، ومدى مواكبة القانون للتطور التكنولوجي رغم أنه أقل سرعة في التطور، وكيفية تعامله مع الأدلة الحديثة وبالضبط الدليل الإلكتروني.

– معرفة كيفية تعامل السلطات القضائية مع هذه الأدلة من خلال الإجراءات التي يتم من خلالها الحصول على هذا النوع من الأدلة.

– كما نهدف إلى الكشف عن مدى حجية الدليل الإلكتروني وقوته الثبوتية في مجال الإثبات الجنائي وبيان كيفية تعامل القضاء مع الدليل الإلكتروني للأخذ به كدليل من أدلة الإثبات الجنائي إضافة إلى الأدلة التقليدية.

المنهج المتبع:

استعملنا في دراستنا هذه المنهج الوصفي، في وصف الجريمة المعلوماتية والدليل الإلكتروني الناتج عنها، بالإضافة إلى منهج تحليل المحتوى، بقصد تحليل مضمون النصوص القانونية الموضوعية والإجرائية الخاصة بإحراز الدليل الإلكتروني، مع اعتمادنا في بعض الأحيان على المنهج المقارن لمعرفة موقف المشرع الجزائري في بعض المسائل المقارنة مع التشريعات الأخرى، وذلك للاستفادة من تجارب الدول الأخرى.

الدراسات السابقة:

يعتبر هذا الموضوع من الموضوعات الحديثة، نتج عنه وجود دراسات قليلة تناولت بعض جوانبه حيث اهتمت بالجريمة الإلكترونية دون أن تولي اعتبارا كثيرا للدليل الإلكتروني، أما قلة منهم قد تناول الدليل الإلكتروني لكن دون استفاضة ونأخذ على سبيل المثال منهم:

– نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة الجزائر، 2013.

تطرق إلى الجانب النظري للجريمة المعلوماتية من خلال مناقشة الجوانب القانونية لها، ثم عالج موضوع الدليل الإلكتروني بتحديد تعريفه، وتوضيح خصائصه وأنواعه ومصادر الحصول عليه وإجراءات تحصيله، وبعد ذلك تم التركيز بنوع من الشرح على القواعد الإجرائية المناسبة في عملية استخلاص الدليل الإلكتروني.

– يزيد بوحليط، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر، أطروحة لنيل شهادة دكتوراه العلوم، تخصص قانون خاص، جامعة باجي مختار، عنابة، 2016.

تطرق فيها إلى الجرائم الإلكترونية بمفهومها الواسع، والتي تتم باستعمال تكنولوجيات الإعلام والاتصال، وذلك للتعرف على هذه الجرائم المرتكبة في مجال المعلوماتية، لأنها حتما تختلف في طبيعتها عن الجرائم التقليدية المعروفة، ثم تناول الأحكام الإجرائية في مكافحة هذه الجرائم، وهنا سار إلى تبيان مفهوم الدليل الإلكتروني ومختلف الإجراءات الخاصة لجمع هذا الدليل وحجيته في الإثبات الجنائي.

الصعوبات المتعرضة للبحث:

لا يفوتنا القول أنه تلقينا صعوبات في اختيار موضوع البحث، كون هذا الموضوع – حجية الدليل الإلكتروني في الإثبات الجنائي– حديث لم يسبق بحثه بوضوح وتعمق ولو أن هناك مراجع ومقالات تناولت هذا الموضوع، إلا أنها لم تعالجه من كل جوانبه، كما صادفنا قلة المراجع والبحوث في هذا الموضوع تحديدا وخاصة المراجع الجزائرية، بالإضافة إلى الطابع التقني للموضوع، مصطلحات تقنية شكلت لنا صعوبة خلال انجاز المذكرة، حيث يتطلب هذا الموضوع فهم الباحث للشق التقني للموضوع وما يصاحب ذلك من صعوبات، إضافة إلى الشق القانوني.

التصريح بالخطة:

وعليه وبناء على ما تقدم، ولمعالجة إشكاليتنا الرئيسية ومختلف التساؤلات الفرعية المنبثقة عنه ارتأينا تقسيم الخطة إلى فصلين، معتمدين ذلك على التقسيم الثنائي للخطة.

تطرقنا في الفصل الأول إلى ماهية الجريمة الإلكترونية والدليل الإلكتروني، فقمنا بتقسيمه إلى مبحثين خصصنا الأول منه للحديث عن محل الدليل الإلكتروني (الجريمة الإلكترونية)، وأفردنا الثاني لدراسة الإطار المفاهيمي للدليل الإلكتروني.

وتناولنا في الفصل الثاني إجراءات جمع الدليل الإلكتروني ومدى اقتناع القاضي الجنائي به وقسمناه هو الآخر إلى مبحثين: مبحث تكلما فيه عن الإجراءات الخاصة لجمع الدليل الإلكتروني. وآخر لدراسة مدى اقتناع القاضي الجنائي بالدليل الإلكتروني.

وأنهينا بحثنا بخاتمة ضمناها أهم النتائج والتوصيات المقترحة.

الفصل الأول

ماهية الجريمة الإلكترونية والدليل الإلكتروني

الفصل الأول: ماهية الجريمة الإلكترونية و الدليل الإلكتروني

إن الوسط الذي ترتكب فيه الجريمة الالكترونية يختلف من وسط مادي إلى وسط معنوي أو ما يعرف بالوسط الافتراضي وعلى ضوء ذلك فإن الدليل المناسب لإثبات الجريمة الإلكترونية هو الدليل الالكتروني كما عبرت عنه الاتفاقية الأوروبية لمكافحة الجرائم المعلوماتية، فطبيعة الدليل تتشكل من طبيعة الجريمة التي يولد منها، وبإسقاط هذا على الجريمة الإلكترونية، فإنه يمكن أن تثبت بأدلة تقنية ناتجة عن الوسائل التقنية التي ارتكبت بواسطتها أو من خلالها.

وعلى ضوء ما سبق طرحه سنتطرق في دراستنا إلى محل الدليل الإلكتروني أي الجريمة الإلكترونية في (المبحث الأول)، ثم سنتعرض في (المبحث الثاني) إلى الإطار المفاهيمي للدليل الإلكتروني

المبحث الأول: محل الدليل الإلكتروني (الجريمة الإلكترونية)

إن تزايد سوء استخدام الحاسب الآلي وشبكة الانترنت أدى إلى تنامي معدلات الجريمة المعلوماتية، والتي يطلق عليها أيضا الجريمة الإلكترونية أو جرائم الحاسب الآلي والانترنت أو جرائم التقنية العالية أو جريمة الغش المعلوماتي، أو جرائم تكنولوجيات الإعلام والاتصال أو جرائم إساءة استخدام تكنولوجيا المعلومات والاتصالات وغيرها[1].

من خلال هذا المبحث سنتطرق إلى مفهوم الجريمة الالكترونية في (المطلب الأول)، وأنواعها في (المطلب الثاني)، ثم نتعرف على دوافع ارتكاب هذه الجريمة الالكترونية في (المطلب الثالث).

المطلب الأول: تعريف الجريمة الالكترونية وخصائصها

نظرا للطبيعة الخاصة للجرائم الالكترونية اختلف الفقه في وضع تعريف مانع وجامع لها فأحيانا يكون الحاسوب وسيلة لارتكابها بواسطة الانترنت وأحيانا أخرى يكون هدف لها، سنتناول هذا المطلب تعريف الجريمة الالكترونية في (الفرع الأول) ثم نتطرق إلى خصائص الجريمة الالكترونية في (الفرع الثاني).

الفرع الأول: تعريف الجريمة الالكترونية

استقطب مفهوم الجريمة المعلوماتية اهتمام الفقهاء والقانونيين والمختصين في مجال المعلوماتية من أجل وضع تعريف شامل للجريمة المعلوماتية، فحاول كل منهم حسب اختصاصه وضع تعريف ملائم فمنهم

([1]) اخترنا اصطلاح الجريمة المعلوماتية دون غيره من التسميات الأخرى لكونه مفهوم عام يشمل مختلف التقنيات المستخدمة في التعامل مع المعلومات بما فيها الحاسوب وشبكة الإنترنت .

من عرفها تعريفا ضيقا وقال بأنها " الجرائم المرتبطة بالحاسوب والتي تشكل انتهاكا للقانون الجنائي" ومنهم من قال بأنها " تلك الجريمة التي يستخدم فيها الحاسوب " وهو تعريف واسع جدا[2].

أما من الناحية القانونية فلا يوجد مصطلح قانوني موحد للدلالة على الجرائم الناشئة عن سوء استغلال النظم المعلوماتية أو إساءة استخدامها فهناك من يطلق عليها وصف جريمة الغش المعلوماتي وهناك من يطلق عليها وصف جريمة الاختلاس المعلوماتي، وهناك من يصفها بجرائم الاحتيال المعلوماتي، غير أن المصطلح الأكثر شيوعا هو مصطلح الجريمة المعلوماتية أو الإلكترونية[3].

وقد تعددت التعاريف الواردة بشأن الجريمة المعلوماتية بتعدد النظم والتشريعات والاتجاهات الفقهية، وعليه تناولنا التعريف الفقهي في (الفقرة الأولى)، ثم تطرقنا إلى التعريف القانوني في (الفقرة الثانية).

الفقرة الأولى: التعريف الفقهي

مما يلاحظ في هذا الشأن هو عدم وجود اتفاق سواء على المستوى التشريعي أو الفقهي على استعمال مصطلح معين للدلالة على هذه الظاهرة الجرمية الناشئة في بيئة الكمبيوتر والانترنت، وهو اختلاف رافق مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات والاتصالات، فهناك من يطلق عليها مصطلح جرائم الغش المعلوماتي أو الجرائم المعلوماتية، أو الجرائم الالكترونية، أو جرائم الحاسب الآلي، أو جرائم تقنية المعلومات، أو الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال أو جرائم التكنولوجيا الحديثة، أو جرائم الكمبيوتر والانترنت.

ويرجع السبب في ذلك إلى عدة عوامل منها التطور المستمر واللامتناهي لتكنولوجيا المعلومات والاتصالات، مما نتج عنه جرائم مستحدثة اختلفت التشريعات حول وضع مفاهيم موحدة لها[4]. وقد يكون السبب أيضا ترك المجال أمام المشرع لاحتواء التقنيات المتلاحقة في هذا الميدان، ولعدم حصر قاعدة التجريم في نطاق أفعال معينة تتبدل في المستقبل. ويثير هذا الإشكال العديد من التحديات أهمها صعوبة مواجهتها وتعذر الحلول المناسبة لمكافحتها سواء على المستوى الداخلي أو الدولي[5]. ورغم هذه الصعوبات حاول الفقهاء جاهدين وضع مفهوم لهذه الجرائم المستحدثة أين برز اتجاهان هما:

([2]) عمر بن محمد العتبي، الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية – رسالة مقدمة لأجل نيل شهادة الدكتوراه – قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2010، ص 21.

([3]) تركي بن عبد الرحمان المويشير– بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليته – رسالة مقدمة لأجل نيل شهادة الدكتوراه، قسم العلوم الشرطية، جامعة نايف للعلوم الأمنية، الرياض، السعودية، 2009 ، ص 15.

([4]) Nidal EL chaer .la criminalité informatique devant la justice pénale édition juridique sader . beyrouth . liban .2004.pp.18-19

([5]) خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، مصر، ط1، 2009، ص 73.

) من Merwe**أولا : الاتجاه الضيق لمفهوم الجرائم الالكترونية :** تزعم هذا الاتجاه الفقيه (ميروي خلال وضعه تعريفا مضمونه " أن الجريمة المعلوماتية هي ذلك الفعل غير المشروع الذي يتورط في ارتكابه) بأنها " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف Rosblatالحاسب "[6]، كما عرفها (روز بلات –) فعرفها Solerezأو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه " أما (سولريز بأنها " أي نمط من أنماط الجرائم المعروفة في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات "[7].

الملاحظ أن هذه التعاريف تستند إلى موضوع الجريمة ونمط السلوك محل التجريم، دون أن نأخذ بعين الاعتبار المجرم وهو ما أدى ببعض من الفقهاء إلى وضع تعاريف أخرى ذات طابع موسع تستند إلى الفاعل بدل موضوع الجريمة .

ثانيا :الاتجاه الموسع لمفهوم الجرائم الالكترونية : حاول هذا الاتجاه إعطاء تعريف موسع للجريمة المعلوماتية لهدف تفادي النقص الظاهر على التعاريف السابقة، فعرفت بأنها " كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع للتقنية المعلوماتية بهدف الاعتداء على الأموال المادية أو المعنوية "، كما عرفت بأنها " كل سلوك سلبي كان أم إيجابي يتم بموجبه الاعتداء على البرامج أو المعلومات للاستفادة منها بأي صورة كانت "[8] .

كما عرفت أيضا بأنها " كل عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسوب المادية و المعنوية وشبكات الاتصال الخاصة، باعتبار من المصالح و القيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها "[9].

) أن سوء استخدام الحاسوب Michel & Caredoوفي ذات الاتجاه يرى الفقيهان (ميشال و كريدو – يشمل استخدام الحاسوب كأداة لارتكاب الجريمة، بإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته، كما تمتد هذه الجريمة لتشمل الاعتداءات المادية الماسة بالحاسوب ذاته، أو المعدات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان، وتزييف المكونات المادية والمعنوية للحاسوب بل وسرقة جهاز الحاسوب قي حد ذاته أو مكون من مكوناته[10].

([6]) محمد أمين الشوابكة – جرائم الحاسوب والانترنت (الجريمة المعلوماتية) – دار الثقافة للنشر والتوزيع، عمان، الأردن 2009 ، ص 06.

([7]) محمد سيد سلطان، قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية، دار ناشري للنشر الالكتروني الكويت، سنة 2012 ، ص 62.

([8]) تركي بن عبد الرحمان المويشير، المرجع السابق، ص 17 .

([9]) محمد أمين الشوابكة، المرجع السابق، ص09 .

([10]) محمد علي العريان – الجرائم المعلوماتية – دار الجامعة الجديدة، الإسكندرية، مصر، 2004، ص 45 .

ونستخلص مما سبق أن اختلاف الفقه في وضع تعريف للجريمة المعلوماتية أو الإلكترونية مرده الاختلاف في المعيار المعتمد عليه والزاوية التي ينظر إليها كل اتجاه إلى هاته الجريمة المستحدثة، إلا أنه يمكن إعطاء تعريف ملخص تبعا لهذه الاتجاهات فهي :"سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الكمبيوتر"، فالسلوك يشمل الفعل الايجابي والامتناع عن الفعل وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية ومعاقب عليه قانونا، لأن إسباغ الصفة الإجرامية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرع ومن خلال النص على ذلك، ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة، بيانات ومعلومات معالجة ومخزنة، البرامج بأنواعها الأنظمة المعلوماتية...الخ). وأما الكمبيوتر فهو "النظام التقني بمفهومه المعلومات المستخرجة، والمتبادلة بين الشامل الذي يزاوج بين تقنيات الحوسبة والاتصال بما في ذلك شبكات المعلومات"[11] .

الفقرة الثانية : التعريف القانوني

عرف المشرع الجزائري الجريمة المعلوماتية في نص المادة 02 / أ من القانون رقم09-04 المؤرخ في 05 أوت 2009 والمتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته[12] بالقول بأن" الجرائم المتصلة بتكنولوجيات الإعلام والاتصال هي: جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية".

فمن خلال استعمال المشرع الجزائري لهذا المصطلح " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" للدلالة على الجرائم الالكترونية فهو يزاوج بين تقنية الحوسبة وتقنية الاتصالات الحديثة فالحوسبة تقوم على "استخدام وسائل التقنية لإدارة وتنظيم ومعالجة البيانات"، أما الاتصال فهو قائم على "وسائل تقنية لنقل المعلومات بجميع دلالاتها"[13].

إذن وعملا بالتعاريف المقترحة للجريمة المعلوماتية، فإنه يمكننا اقتراح تعريف خاص يشمل كافة الجوانب المتعلقة بالجريمة هذه فنعرفها بأنها" كل السلوكات المجرمة التي يشكل الحاسوب وشبكات الاتصال الخاصة به وسيلة لارتكابها أو محلا لوقوعها، أي الجرائم التي ترتكب في البيئة الرقمية الالكترونية".

([11]) يونس عرب، صور الجرائم الالكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، يومي 2 و 4 أفريل 2006، ص 7 .

([12]) القانون رقم: 09-04 مؤرخ في: 5 أوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، (ج.ر) رقم 47 المؤرخة في: 2009/08/16.

([13]) يونس عرب، جرائم الكمبيوتر، المرجع السابق، ص 1 .

الفرع الثاني: خصائص الجريمة الالكترونية

إن تعريف الجريمة الالكترونية كما سبق والتطرق إليه، والقاضي بأنها ذلك النشاط الإجرامي المتصل باستعمال تقنية الحاسوب وشبكات الاتصال، يجعل من هذه الجرائم ذات طبيعة خاصة تختلف والمفهوم التقليدي المرتبط بتجريم السلوكات ذات الطبيعة المادية والتي تترك أثرا ملموسا في العالم الخارجي، ذلك لأن هذا النوع من الجرائم يتخذ من العالم الافتراضي ملجأ له بحيث لا تكاد تظهر سلوكات إجرامية نظرا لما تتميز به هذه الجرائم من خصوصيات، تجعل من أمر اكتشافها أمرا غاية في الصعوبة وهي الإشكاليات والمسائل التي سنحاول جاهدين معالجتها في هذا الفرع، من خلال تقسيمه إلى أربع فقرات، تناولنا الجريمة الالكترونية متعدية الحدود أو جريمة عابرة للحدود في (الفقرة الأولى)، وصعوبة اكتشاف الجريمة الإلكترونية في (الفقرة الثانية)،الجريمة الإلكترونية جريمة ناعمة في (الفقرة الثالثة) وأخيرا الجريمة الإلكترونية حديثة في (الفقرة الرابعة).

الفقرة الأولى: الجريمة الالكترونية متعدية الحدود أو جريمة عابرة للحدود

إن ارتباط كل دول العالم بشبكة الاتصالات الدولية، من خلال الأقمار الصناعية، وشبكة الإنترنت الجريمة لا تعترف بمفهوم الحدود الإقليمية للدول جعل أمر عولمة الجريمة أمرا ممكنا وشائعا فأصبحت واكتسحت الساحة العالمية [14].

فأصبح من الممكن أن يرتكب الجاني جريمة في دولة ويكون المجني عليه في دولة أخرى، وقد يترتب الضرر على أماكن متعددة في العالم بسبب الجريمة الواحدة .

ونتيجة للخسائر الكبيرة التي تتسبب فيها هذه الجرائم، تعالت الأصوات الداعية إلى التعاون الدولي المكثف للتصدي لها عن طريق إبرام الاتفاقيات والمعاهدات وتسهيل إجراءات التعاون والمساعدة القضائية بين الدول، فقد تتأثر دول عدة بجريمة إلكترونية واحدة تخلق مشكلات كثيرة مثل: تحديد الدولة صاحبة الاختصاص القضائي وحول القانون الواجب التطبيق وإجراءات الملاحقة القضائية، فعولمة الجريمة المنظمة[15]، تقتضي عولمة مكافحتها أيضا بواسطة التعاون الدولي في صوره المتعددة .

([14]) – عبد العال الدريبي – الجرائم الالكترونية – دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، المركز القومي للإصدارات القانونية، القاهرة، مصر، 2012، ص 55.

([15]) يقصد بالجريمة المنظمة : مشروع إجرامي له نوع من الديمومة يمارس عدة أنشطة إجرامية، ويقوم عليه عدد من الأشخاص متفقون أو متعاونون على استثمار المخطط والحصول على الربح من خلال السوق غير المشروعة، يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، منشورات مركز كردستان للدراسات الإستراتيجية، السليمانية، مصر، 2007، ص 72.

في هذا الشأن سارع المشرع الجزائري إلى التصديق على نصوص الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية [16]، حيث نصت في مادتها الأولى : " تهدف هذه الاتفاقية إلى تعزيز التعاون العربي لمنع ومكافحة الجرائم المنظمة عبر الحدود الوطنية"، كما نصت بموجب المادة (21) منها على "تجريم ارتكاب أو المشاركة في ارتكاب الأفعال التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع لتقنية أنظمة المعلومات"[17]، وتدخل مكافحة الجرائم الالكترونية ضمن هذا الإطار لأنها تتميز بأنها جرائم عابرة للحدود.

وفي السياق نفسه قام المشرع أيضا بالتصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[18] والتي تنص في مادتها الأولى على :" تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها"، والتي ستشكل إضافة جديدة في مجال مكافحة الجرائم الإلكترونية في الجزائر.

الفقرة الثانية: صعوبة اكتشاف الجريمة الالكترونية

تتسم الجرائم الالكترونية (المعلوماتية) بأنها خفية ومستترة في أغلبها لأن الضحية لا يلحظها رغم أنها قد تقع أثناء وجوده على الشبكة لأن الجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة كإرسال الفيروسات والتجسس على البيانات المخزنة ولعل أن ما يزيد من خصوصية صعوبة اكتشافها[19] هي:

أولا: سرعة التنفيذ:

([16]) الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم: 14-251 المؤرخ في: 2014/09/08، (ج.ر) رقم: 56 المؤرخة في: 2014/09/25. .

([17]) تنص المادة (21) من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية على :" تتعهد كل دولة طرف أن تتخذ ما يلزم من تدابير في إطار قانونها الداخلي لتجريم ارتكاب أو المشاركة في ارتكاب الأفعال الآتية التي تقوم بها جماعة إجرامية منظمة في نطاق الاستعمال غير المشروع لتقنية أنظمة المعلومات :

_ الاختراق غير المشروع أو تسهيل الاختراق غير المشروع على نحو كلي أو جزئي لأحد نظم المعلومات _ تعطيل أو تحريف تشغيل أحد نظم المعلومات _ إدخال بيانات بطرق غير مشروعة في أحد نظم المعلومات أو مسح وتعديل أو نسخ أو نشر البيانات التي يحتويها هذا النظام بطريق غير مشروع _ استيراد أو حيازة أو عرض أو ترك أو إتاحة إحدى المعدات أو الأدوات أو برامج تقنية المعلومات بدون سبب مشروع بهدف ارتكاب إحدى الجرائم المنصوص عليها في الفقرات الثلاث السابقة _ أي جريمة من الجرائم التقليدية ترتكب بإحدى وسائل تقنية أنظمة المعلومات" .

([18]) الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ: 21 / 12 /2010، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم : 14 – 252 المؤرخ في: 08 / 09 / 2014 ، (ج ، ر) رقم: 57 المؤرخة في: 28 / 09 / 2014 .

([19]) عبد المؤمن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والمقارن بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16 و17 نوفمبر 2015، كلية الحقوق جامعة بسكرة، الجزائر، ص 08.

لا يتطلب أمر تنفيذ الجريمة الالكترونية أكثر من وقت الضغط على لوحة المفاتيح، و زر الفأرة أو ملامسة الشاشة الرقمية غير أن هذا لا يعني أنها لا تتطلب إعداد مسبقا من خلال توفير المعدات اللازمة والبرامج الضرورية لذلك.

ثانيا: التنفيذ عن بعد:

لا تتطلب الجرائم المعلوماتية في أغلبها وباستثناء جرائم سرقة معدات الحاسوب، وجود الفاعل في مكان الجريمة، فيمكن له إتيان جريمته وهو في مكان بعيد أو في دولة أخرى.

ثالثا: إخفاء معالم الجريمة

عادة ما تكتسي الجرائم المعلوماتية طابعا خفيا فلا يمكن ملاحظة أثارها إلا بعد التدقيق والتمعن من قبل أهل الاختصاص [20].

)المشتركة بين الشرطة الإسبانية ومعهد باندا للأمن المعلوماتي Mariposaوهذا ما كشفت عنه عملية (في 03 مارس 2010، والتي أفضت إلى اكتشاف شبكة عالمية من الحواسيب بلغ عددها ثلاثة عشر(13) مليون حاسوب موزعة على 190 دولة كانت خاضعة للتحكم من قبل مجموعة من المجرمين، في شكل شبكة (BOT)، وقد كانوا يستعملون برنامجا خفيا في شكل فيروس يعرف باسم (Botnet)خاصة خفية تعرف باسم يهدف إلى اعتراض أرقام البطاقات البنكية والأشخاص المرتبطين بالشبكة بما في ذلك عدد كبير من المؤسسات المالية والبنكية، وقد استولى هؤلاء على ما يقارب 800.000 معلومة بنكية خاصة بالأفراد وقدر عدد الشركات التي مسها الاختراق بأكثر من 50% من الشركات على المستوى العالمي وبلغت الخسائر ملايين الدولارات[21].

الفقرة الثالثة: الجريمة الالكترونية جريمة ناعمة

تختلف الجرائم الالكترونية عن الجرائم التقليدية التي تتطلب أحيانا استخدام العنف، كما في جرائم القتل والضرب والجرح والسرقة، وجرائم الإرهاب ...الخ، إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، بل تتطلب مواصفات خاصة كالذكاء و امتلاك الوسائل المناسبة و قدرة على التعامل مع شبكة الانترنت فنقل البيانات من كمبيوتر إلى أخر أو المساس بأنظمة المعالجة الآلية للمعطيات أو الدخول غير مشروع للحاسوب أو القرصنة والسطو الإلكتروني على الأرصدة وبيانات بطاقات الائتمان، لا يتطلب أي عنف سواء مادي أو معنوي ولا يبذل فيه الجاني أي جهد عضلي، فهي جرائم هادئة بطبيعتها [22]، فلا يحتاج المجرم الإلكتروني إلى العنف وإنما يحتاج إلى مهارة وفن ودقة في استعمال تقنية المعلومات مثل: استخدام ما يعرف

) عبد العال الدريبي،الجرائم الالكترونية، المرجع السابق, ص 30.[20](

([21]) Myriam Quéméner . Yves Charpenel. La cybercriminalité. Edition Economica. Paris. France. 2010. p10.

نهلا عبد القادر المومني، جرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الأردن، ط 1، 2008، ص 58.)[22](

بالقنابل المنطقية والفيروسات المعلوماتية...الخ، كما أن معظم هؤلاء من الشباب المثقفين ذوي الاختصاصات العالية في مجال الحاسوب مما يخلق صعوبات إضافية للأجهزة القضائية المتخصصة لملاحقتهم [23].

الفقرة الرابعة: الجريمة الالكترونية من الجرائم الحديثة

إن وجود الجريمة الإلكترونية جاء نتيجة لتطور تكنولوجيا تقنية المعلومات، إذ أن الجريمة الالكترونية لا تقع على أشياء مادية ولا يكون موضوعها إلحاق الضرر بالموجودات الفيزيائية إنما تعتبر البرامج الالكترونية وأنظمة المعلومات والبرامج الحاسوبية وشبكة الانترنت هي مسرح هذه الجرائم، كما أنها جرائم متنوعة عديدة لا يمكن حصرها وإن كانت بعض التشريعات قد أدرجت تسميات لبعض الجرائم الالكترونية، إلا أنه لا يمكن في الواقع حصر هذه الجرائم والسبب في ذلك كما ذكرنا يعود إلى ارتباط هذه الجرائم بتكنولوجيا المعلومات وتطور الاتصالات التي لا يكاد يمر بعض الزمن حتى نسمع بتكنولوجيا حديثة ظهرت للبشرية[24].

المطلب الثاني: أنواع الجرائم المعلوماتية (الالكترونية)

تصنف الجرائم الالكترونية إلى فئات متعددة، تتباين تبعا للأساس المعتمد في ذلك فهناك عدة تقسيمات منها ما تقسم حسب دور الحاسب الآلي في الجريمة إلى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته (فقد يكون النظام المعلوماتي هدفا للاعتداء، أو وسيلة لارتكاب جريمة أخرى)[25] ومنها ما تصنف الجريمة الالكترونية على أساس الغاية من ارتكاب الجريمة التي قد تكون الاعتداء على نظام المعالجة الآلية للمعطيات أو الأموال أو الأشخاص .

وعلى غرار المشرع الجزائري[26]، اهتم المشرع المقارن[27] بتجريم صور الاعتداء الناجمة عن المعالجة الآلية للبيانات، نتيجة ظهور العديد من الصور المستحدثة التي لا تنفك أخطارها في أخذ أبعاد محلية، إقليمية

([23]) نعيم مغبغب، حماية برامج الكمبيوتر، ،منشورات الحلبي الحقوقية، لبنان، ط2، 2009، ص 141.

([24]) عبد الخالق صالح عبد الله مغرب، الأدلة المستخدمة في ارتكاب الجريمة الالكترونية، مجلة العدل، العدد السابع والثلاثون، السنة الرابعة عشر، ص 58.

([25]) أمير فرج يوسف، الجريمة الالكترونية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، مصر،2011، ص 97.

([26]) وذلك بإضافة نوع جديد من الجرائم في القسم السابع مكرر تحت مسمى المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم 04_15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66_155 المتضمن قانون العقوبات، الصادر في الجريدة الرسمية عدد : 71 بتاريخ 12 نوفمبر 2004، ومن ثمة إصدار القانون رقم 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

([27]) فلقد جرم المشرع الفرنسي في قانون العقوبات لسنة 1992، والمعمول به منذ مارس 1994 صور الاعتداء الناجمة عن المعالجة الآلية للبيانات، وكذلك الأمر بالنسبة للمشرع الأمريكي الذي أصدر قوانين عدة في إطار مكافحة الجرائم المرتكبة عبر الإنترنت، منها قانون يتعلق بإساءة استخدام الكمبيوتر (Computer Abuse Act)، وأيضا قانون آداب الاتصالات

وعالمية، وتكبد الدول والأشخاص خسائر لا يستهان بقيمتها، حيث تعذر على النصوص الجزائية التقليدية توفير الحماية القانونية للنظام المعلوماتي، لذلك تم إصدار نصوص عقابية عدة تطبيقا لمبدأ الشرعية الجزائية لمواجهة الجرائم المعلوماتية الماسة بالنظم المعلوماتية والتي سنتطرق إليها في هذا المطلب من خلال (الفرع الأول)، بالإضافة إلى الجرائم المعلوماتية الماسة بالأموال والتي تناولناها في (الفرع الثاني)، وتلك الماسة بالأشخاص في (الفرع الثالث).

الفرع الأول: الجرائم الماسة بالنظم المعلوماتية

عالج المشرع الجزائري[28] العديد من صور الاعتداء على النظام المعلوماتي وقرر لها عقوبات بمقتضى المواد من 394 إلى 394 مكرر 7، وتشمل هذه الجرائم كل فعل أو امتناع عن فعل غير مشروع يقع على نظام المعالجة الآلية للمعطيات[29]، سواء كان ذلك بالتغيير أو التدمير أو إعاقة عملها أو الدخول إليها، أو استعمالها على نحو مخالف للقانون، وسنتناول في هذا الصدد جريمتين، حيث تطرقنا في (الفقرة الأولى) إلى جريمة الدخول والبقاء غير المشروع للنظم المعلوماتية، في حين تناولنا في (الفقرة الثانية) جريمة إتلاف وتعديل المعطيات.

الفقرة الأولى: جريمة الدخول والبقاء غير المشروع في نظام المعلوماتية (جرائم الاختراق)

تعتبر جريمة الدخول و البقاء غير المشروع، أو جرائم الاختراق بشكل عام بأنها:

القدرة على الوصول لهدف معين بطريقة غير مشروعة (بطريقة الغش)، عن طريق ثغرات في نظام الحماية الخاص بالهدف، وهي سمة سيئة يتسم بها المخترق، لقدرته على دخول أنظمة الآخرين دون رغبة منهم ودون علمهم بغض النظر عن الأضرار التي قد تحدثها، وتعد هذه الأنشطة الجريمة الأكثر انتشارا [30]. وقد نص عليها المشرع الجزائري بموجب المادة 394 مكرر من القانون 04-15[31].

(Communication Decency Act) عام 1996 يجرم فيه القذف والسب والتعرض للأخلاق والآداب العامة عبر شبكة الإنترنت، أنظر المرجع نفسه، ص 18.

[28])القانون 04-15 المؤرخ في 10 نوفمبر 2004، المعدل و المتمم للأمر 66-156 المؤرخ في 05 جوان 1966 المتضمن قانون العقوبات والصادر في الجريدة الرسمية عدد 76 بتاريخ 10 نوفمبر 2004.

[29] نشناش مينة، الإطار المفاهيمي للجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني حول الجريمة المعلوماتية، بين الوقاية و المكافحة، يومي 16 و 17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر،2015 ، ص 12.

[30]) خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع عمان، الأردن، 2011، ص 51.

[31] تنص المادة 394 مكرر من (ق.ع.ج) على " يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك...".

الفقرة الثانية: جريمة إتلاف وتعديل المعطيات

قد يعقب جريمة الدخول والبقاء غير المشروع، أفعال أخرى غير مشروعة تتمثل في جريمة إتلاف وتعديل المعطيات، حيث شملت الحماية الجنائية التي تدخل في نظام المعالجة الآلية من كل إدخال أو تعديل أو إزالة بطريق الغش.

) "إضافة معطيات جديدة على الدعامة الخاصة بها، سواء كانت L'intrusionويقصد بـ: الإدخال (خالية أم تحمل معطيات من قبل، ونكون أمام فعل الإدخال في حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة والتزوير"[32] .

- المحو أو الإزالة (L'effacement): يقصد به "إزالة جزء من المعطيات المسجلة داخل النظام وتحطيم تلك الدعامة أو نقل أو تخزين جزء من معطيات في ذاكرة مختلفة".
- التعديل (La Modification): عبارة عن" تغيير المعطيات الموجودة داخل النظام واستبدالها بمعطيات أخرى، سواء تم ذلك بصفة جزئية أو كلية، ويكون عن طريق برامج الفيروسات بصفة عامة "[33] . وقد نص عليها المشرع الجزائري بموجب المادة 394 مكرر 1 من القانون 04-15[34]

الفرع الثاني: الجرائم المعلوماتية الواقعة على الأموال

بعد أن كانت الجريمة المعلوماتية تستهدف النظم المعلوماتية بدافع الفضول أو الانتقام، توسعت الغاية منها لتشمل اكتساب المال بطريق غير مشروع وتحقيق مصلحة مالية عن طريق الاعتداء على المال والمالية عبر شبكة الانترنت واعتماد البنوك والمصارف على المعلوماتي تزامنا مع ازدياد المعاملات التجارية استخدام الأنظمة المعلوماتية ومن بين هذه الجرائم، تناولنا جرائم الاحتيال الالكتروني في (الفقرة الأولى)، والاعتداء على بطاقات الائتمان من خلال (الفقرة الثانية).

ويمكن تعريف المال المعلوماتي المشمول بالحماية القانونية بأنه: " كل مال الكتروني قابل النقل والتملك" أو بأنه: "المال الموجود على الحاسوب سواء في صورة معلومات أو بيانات الكترونية في أي صورة كان عليها سواء كان مخزنا على أقراص صلبة أو دعامات تخزين خارجية، فهو بذلك كل المدخلات الإلكترونية التي لها من قيمة المادية مما يجعلها قابلة للتملك وتكتسي الحماية القانونية " [35].

([32]) أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، الطبعة الثانية، دار هومه، الجزائر،2007، ص 121.

([33]) أمال قارة، الحماية الجزائية للمعلوماتية في التشريع الجزائري، المرجع السابق، ص ص 121- 122.)

([34]) تنص المادة 394 مكرر 1 من قانون العقوبات الجزائري على:" يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبغرامة من 500.000 دج إلى 2.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو زال أو عدل بطريق الغش المعطيات التي يتضمنها".>

([35]) ناير نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، مصر، 2012 ص 32.)

الفقرة الأولى: جرائم الاحتيال المعلوماتي

الاحتيال المعلوماتي أو الغش المعلوماتي أو غش الحاسوب كما يطلق عليها البعض[36]، هي" كل فعل أو مجموعة من الأفعال غير المشروعة والمعتمدة التي ترتكب بهدف الخداع أو التحريف للحصول على شيء ذي قيمة ويكون نظام الحاسوب لازما لارتكابها أو إخفائها".

الفقرة الثانية: جرائم الاعتداء على بطاقات الائتمان

تستخدم بطاقة الائتمان من قبل حاملها كوسيلة وفاء لالتزاماته بدلا من الدفع الفوري بالنقد، وذلك وفقا لشروط البنك مصدر البطاقة، وتختلف أنواع هذه البطاقات ونطاق استخدامها، فمنها ما هو محلي لا يتجاوز حدود الدولة التي صدر فيها ومنها ما يستخدم في كل دول العالم [37].

إن جرائم إساءة استخدام بطاقة الائتمان قد ترتكب من طرف الغير، ويكون ذلك في حالة سرقة بيانات بطاقة الائتمان، أو في حالة استخدام بطاقة الائتمان مزورة و قد ترتكب من قبل حاملها الشرعي لدفع ثمن السلع والخدمات من خلال شبكة الانترنت، رغم علمه بعدم كفاية رصيده في البنك مصدر البطاقة، أو بعد انتهاء مدة صلاحيتها أو إلغائها كل بطاقة ائتمان مدة صلاحية محددة، عادة ما تقدر نسبة يقوم العمل بعد انتهائها بإعادتها إلى بنك لأن بطاقة الائتمان بمثابة محرر يتم تسليمها للعمل لأداء وظيفة معينة، واستخدامها بعد انتهاء صلاحيتها وعدم إعادتها إلى مصدرها بعد جريمة خيانة أمانة[38].

الفرع الثالث: الجرائم الماسة بالأشخاص

إن تسخير البيئة المعلوماتية لارتكاب مختلف صور الاعتداء على نظم المعالجة الآلية للمعطيات وكذا تلك الجرائم الماسة بالأموال، سمح كذلك للمجرم بتحقيق أغلب صور الاعتداء على الأشخاص سواء نجم عنه أذى معنوي أو أدى إلى حدود ضرر مادي، وتعدد صور الجرائم المعلوماتية المتعلقة بالأشخاص، لذا سنأخذ عل سبيل المثال جريمة القذف والتشهير عبر الإنترنت من خلال (الفقرة الأولى) وجرائم الاعتداء على البيانات الشخصية في (الفقرة الثانية).

---

[36]) نهلا عبد القادر المومني، المرجع السابق، ص 188.(

[37](عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الأول، نظام التجارة الالكترونية وحمايتها) مدنيا، دار الفكر الجامعي، الاسكندرية، مصر، 2002، ص 108.

[38](خالد عياد الحلبي، المرجع السابق، ص 125.)

الفقرة الأولى : جريمة القذف والتشهير عبر الإنترنت

تعتبر هذه الجرائم من أكثر الجرائم شيوعا عبر شبكة الإنترنت، أين يعتقد العابثون أن لهم حرية التصرف في نشر وبث رسائل تحمل عبارات ذم وقدح وتحقير لأشخاص مستهدفين بذاتهم أو مجموعة من الأفراد، بصفة غيابية أو وجاهية عبر مختلف الوسائط الإلكترونية[39].

إن غياب نصوص تشريعية تتماشى مع هذه الصورة لجريمة القذف والتشهير، يجعلها تقع تحت أحكام النصوص العقابية لهذه الجريمة بصورها التقليدية، مما يطرح صعوبات في مجال إثباتها، وهو ما ينطبق على المشرع العقابي الجزائري، حيث تبقى المواد من 296 إلى 299 من القانون 06_23 المؤرخ في 20 ديسمبر 2006، مجرد توضيح للفعل المادي لجريمة القذف والسب والتحقير، دون ربطها مع تقنية المعلومات.

عكس المشرع السعودي الذي قام بإيضاح هذا النوع من الجرائم في قانون مكافحة الجرائم المعلوماتية حيث تناول في الفقرة 05 من المادة 03 وذلك تفسيرا لما ورد في نص المادة 14 [40] من الاتفاقية العربية لمكافحة الجرائم المعلوماتية، ويمكن حصر هذه الجرائم في السلوكات التالية :

1 – استهداف شخص معين بذاته بالذم والقدح والتشهير :

حيث يعمد الجاني باستخدام البريد الالكتروني إلى إسناد مادة معينة إلى شخص ما ينال فيها من شرفه أو كرامته ويعرضه إلى بعض الناس واحتقارهم، لا سيما إذا ما عمد الجاني في ذلك على توزيع فحوى الرسالة الالكترونية إلى عدد غير محدد من المتعاملين عبر شبكة الإنترنت.

العالمية في إسناد مادة كتابية أو رسومية أو مرئي من (WEB) كما قد يستعمل الجاني شبكة الويب شأنها الإساءة لشخص معين فتطال شرفه وكرامته وتضعه موضع احتقار وذم من قبل الغير[41]. كما أن غرف قد تستخدم أيضا (TWITER) وتويتر (FACEBOOK)الدردشة والمحادثة ومواقع التواصل الاجتماعي، منها لارتكاب هذه الأفعال التي قد تتم وجاهيا باستعمال تقنيات الاتصال السمعي البصري عن طريق خدمة السكايب مثلا.(SKYPE)

2 – استهداف مجموعة من الأفراد وحث الغير على كراهيتهم:

يكون ذلك بالنسبة لمجموعة من الأفراد لهم نفس الانتماءات الدينية أو العقائدية أو العرقية، وهو الموضوع الذي تناوله البروتوكول الإضافي لاتفاقية الجريمة الالكترونية بشأن تجريم الأفعال ذات الطبيعة العنصرية، التي تحرض على كراهية الأجانب، والتي ترتكب عن طريق أنظمة الكمبيوتر بتاريخ 28

([39]) محمد أمين الشوابكة، المرجع السابق، ص 31 .

([40]) عرفت المادة 14 من الاتفاقية العربية لمكافحة الجرائم المعلوماتية المذكورة سابقا، جريمة الاعتداء على حرمة الحياة الخاصة باعتبارها جريمة معلوماتية بأنها :" الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات".

([41]) محمد أمين الشوابكة، المرجع نفسه، ص 33.

جانفي2008 في ستراسبورغ– فرنسا حيث تضمن الفصل الثاني هذه الجرائم المعلوماتية، والتي تم حصرها في السلوكات التالية:

• نشر المواد التي تتعلق بالعنصرية وكراهية الأجانب عبر أنظمة الكمبيوتر.

• التهديد الذي تحركه دوافع التمييز العنصري وكراهية الأجانب.

• الإهانة التي تحركها دوافع التمييز العنصري وكراهية الأجانب.

• الإنكار أو التقليل أو الموافقة أو تبرير جرائم الإبادة الجماعية وجرائم ضد الإنسانية[42].

تجدر الإشارة إلى أن هذه الصور تكاد تكون نفسها تلك التي جرمتها الفقرة الماد 15/ 4 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية.

إن سرعة وسهولة النشر التي توفرها المعلوماتية زادت من تفشي جرائم القذف والتشهير على نطاق واسع تصعب السيطرة عليه.

الفقرة الثانية: جرائم التعدي على البيانات الشخصية

للإنسان بطبيعته حياة خاصة يحفظها ويهيئ سبل البقاء لها، وتقتضي حرمة هذه الحياة أن يكون له الحق في إضفاء السرية على مظاهرها، لكن التهديد المعلوماتي بهذا الصدد يبرز أساسا في إساءة استخدام المعلومات والبيانات المتعلقة بالأفراد.

ومن صور جرائم التعدي على البيانات الشخصية، انتهاك السرية والخصوصية، وإفشاء البيانات بما يضر بصاحبها، وكذلك الإطلاع على المراسلات الالكترونية، والإدلاء ببيانات كاذبة في إطار العمليات والمعاملات الالكترونية [43].

المطلب الثالث: دوافع ارتكاب الجريمة الإلكترونية

مما لا شك فيه أن السلوك الإنساني أيا كان، شرا أم خيرا له ما يغيره وما يبعث على ارتكابه وهو الذي يطلق عليه الدافع [44]، إلا أن صورة الدافع في قانون العقوبات فكرة تشوبها بعض الغموض وعدم إتفاق من جانب الفقه، ولذلك تعددت الاتجاهات واختلفت فمنهم من أطلق عليه الغاية، ومنهم النية ومنهم الغرض ومنهم الباعث، ولهذه التسميات المختلفة فائدة تذكر كلها تؤدي إلى معنى واحد وهو الدافع. وعليه ارتأينا إلى تقسيم هذا المطلب إلى فرعين، تناولنا في (الفرع الأول) الدوافع الشخصية والسعي إلى تحقيق الربح، وفي (الفرع الثاني) تطرقنا إلى الإثارة والمتعة و التحدي.

([42]) المرجع نفسه، ص 37 .

([43]) نهلا عبد القادر المومني، المرجع السابق، ص ص 173 – 174.

([44]) الدافع عرفه الدكتور محمد مصطفى زيدان بأنه " حالة فسيولوجية وسكيولوجية داخل الفرد تجعله ينزع إلى القيام بأنواع معينة من السلوكات في اتجاه معين، وتهدف الدوافع إلى خفض حالة التوتر لدى الكائن الحي وتخليصه من حالة عدم التوازن..."

الفرع الأول: الدوافع الشخصية والسعي إلى تحقيق الربح

تطرقنا في هذا الفرع إلى الدوافع الشخصية لارتكاب الجريمة الإلكترونية من خلال (الفقرة الأولى)، ثم تناولنا عنصر السعي إلى تحقيق الربح من خلال ارتكاب هذا النوع من الجرائم وذلك في (الفقرة الثانية) .

الفقرة الأولى: الدوافع الشخصية

إن الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر النظام أكثر من شهوة الحصول على الربح، ويميل مرتكبوا جرائم نظم المعلومات إلى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبوا هذه الجرائم لديهم شغف الآلة يحاولون إيجاد_ وغالبا ما يجدون _ الوسيلة إلى تحطيمها بل والتفوق عليها.

ويتزايد شيوع هذا الدافع لدى فئات صغار السن الذين يمضون وقتا طويلا أمام حواسبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الكمبيوتر وشبكات المعلومات وإظهار تفوقهم على وسائل التكنولوجيا، الأمر الذي دفع بالعديد من الفقهاء إلى المناداة بعدم مساءلة مرتكبي جرائم الحاسب الآلي الذي يتمثل باعثهم في إظهار تفوقهم، واعتبار أعمالهم غير منطوية على نوايا آثمة [45].

الفقرة الثانية: السعي إلى تحقيق الربح

يعتبر السعي إلى تحقيق الربح في المرتبة الأولى، من دوافع ارتكاب جرائم الحاسب الآلي، وفي دراسة فإن 13 % من حالات الغش المعلن عنها قد بوشرت من أجل الحصول على المال، ووفقا للدراسات فإن القطاع المالي يعد أكثر القطاعات استهدافا من جرائم الحاسب الآلي، مثال أن البنوك تعتمد وبشكل أساسي على أنظمة التمويل الإلكتروني[46] .

الفرع الثاني : الإثارة والمتعة والتحدي

يدرك القراصنة شيئا عن أساسيات الكمبيوتر وأن هذا الأمر يمكن أن يكون ممتعا، حيث جاء على لسان أحد القراصنة ما يأتي " كانت القرصنة هي النداء الأخير الذي يبعثه دماغي فقد كنت أعود إلى البيت بعد يوم ممل آخر في المدرسة، وأدير تشغيل جهاز الكمبيوتر، وأصبح عضوا في نخبة قراصنة الأنظمة، كان الأمر مختلفا برمته حيث لا وجود لعطف الكبار، وحيث الحكم هو موهبتك فقط، في البدء كنت أسجل أسمي

([45]) http://hrdoegypt.org/wp-content/uploads/2014/12/2_ الجريمة-الإلكترونية-_تقرير.pdf / يوم: 2018/04/05 على الساعة: 13.00 سا.

([46]) التمويل الإلكتروني يعرف بصورة رئيسية على انه خدمات مالية تقدم بواسطة شبكة الإنترنت وبما أن التمويل صناعة كثيفة الاستخدام للمعلومات فانه يتأثر تأثرا بالغا بالانخفاض الشديد الذي شهدته تكلفة توليد المعلومات ومعالجتها ونقلها الذي تحقق بفضل تكنولوجيا المعلومات والاتصال والإنترنت ومن زاوية تطوير البنية الأساسية المالية خصوصا تمويل المشاريع الصغيرة والمتوسطة الحجم. أنظر الرابط التالي :

http://www.alyaum.cm/article/1091233 , يوم : 2018/04/30 على الساعة : 17 سا و 45 د .

الخاصة حيث يقوم الأشخاص الآخرين الذين يفعلون مثلي بالتردد على **Bulletin Borard**في لوحة النشرات هذا الموقع، ثم أتصفح أخبار المجتمع وأتبادل المعلومات مع الآخرين في جميع أنحاء البلاد.

وبعد ذلك أبدأ عملية القرصنة الفعلية، وخلال ساعة واحدة يبدأ عقلي بقطع مليون ميل في الساعة وأنسى جسدي تماما بينما أتنقل من جهاز كمبيوتر إلى آخر محاولا العثور على سبيل للوصول إلى هدفي، لقد كان الأمر يشبه سرعة العمل في متاهة إلى جانب الاكتشاف الكبير لأعداد ضخمة من المعلومات ".

وكان يرافق تزايد سرعة الأدرينالين الإثارة المحظورة بفعل شيْ غير قانوني. وكل خطوة أخطوها كان يمكن أن تسقطني بيد السلطات، كنت على حافة التكنولوجيا واكتشاف ما وراءها، واكتشاف الكهوف الإلكترونية التي لم يكن من المفترض وجودي بها [47].

المبحث الثاني: الإطار المفاهيمي للدليل الإلكتروني

نظرا للطابع الخاص الذي تتميز به الجريمة المعلوماتية، فإن عملية إثباتها تحيط بها الكثير من الصعوبات، ومما لاشك فيه أن كشف هذا النوع من الجرائم يحتاج إلى أدلة ذات طبيعة خاصة، تختلف عن الأدلة التقليدية، بحيث تكون من ذات الطبيعة التقنية الناجمة عن النظم المعلوماتية الناتجة عنها، فما هو إذا الدليل الأنسب لإثبات الجرائم المعلوماتية؟ وما هي صعوبات الحصول عليه؟.

للإجابة على هذا التساؤل سنحدد (مفهوم الدليل الإلكتروني) في (المطلب الأول) ثم (مصادر الحصول على هذا الأخير) في (المطلب الثاني)، و(تقسيمات الدليل الإلكتروني) وذلك في مطلب مستقل (المطلب الثالث) .

المطلب الأول: مفهوم الدليل الإلكتروني

يشمل مفهوم الدليل الإلكتروني على عدة عناصر ينبغي بيانها حتى يتضح هذا المفهوم بشكل جيد، لذلك سنتناول في هذا المطلب تعريف الدليل الإلكتروني في (الفرع الأول) ثم طبيعة الخاصة للدليل الإلكتروني في (الفرع الثاني) وفي الأخير شروط صحة هذا الدليل في (الفرع الثالث).

الفرع الأول: تعريف الدليل الإلكتروني

لتعريف الدليل الإلكتروني، لا بد من دراسة الأصل العام المتمثل في الدليل بصفة عامة، ثم التطرق إلى الفرع المتمثل في الدليل الإلكتروني.

وعليه سنتناول في هذا الفرع معنى الدليل الجنائي في (الفقرة الأولى)، من خلال التكلم عنه لغة وكذا إيراد المعنى الاصطلاحي، ثم سيكون التكلم عن معنى الدليل الإلكتروني من الجاني الفقهي في (الفقرة الثانية).

([47]) دورثي إي، قراصنة أنظمة الكمبيوتر، دينغ ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر، واشنطن ترجمة : آمنة علي يوسف، ديسمبر 1998، ص 11 .

الفقرة الأولى: معنى الدليل الجنائي :

لغة : يعرف على أنه "المرشد"، والدليل هو ما يستدل به، ويقال أدل فأمل والاسم الدالة بتشديد اللام وفلان يدل بفلان أي يثق به[48] . فهو المرشد وما به الإرشاد، وما يستدل به، والدليل الدال والجمع أدلة ودلالات.

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

اصطلاحا : يعرف على أنه :" ما يلزم من العلم به شئ آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة المنشودة"[49] .

وبالنظر إلى غالبية التشريعات نجد أنها لم تعرف الدليل، وإنما اكتفت بتعداد الأدلة ، سواء كان هذا التعداد على سبيل الحصر، أو المثال، إلا أن هناك بعض القوانين التي عرفته مثل قانون أسس الإجراءات الجنائية السوفيتية، إذ عرف الأدلة بأنها : " المعلومات الحقيقية التي على ضوئها يحدد المحقق, أو المحكمة طبقا للطرق المقررة قانونا توافر، أو تلف فعل خطر اجتماعيا وتأثيم الشخص الذي ارتكب الفعل "[50] .

فقد تعددت وجهات نظر القانونيين في معنى الدليل، ومن التعاريف ما جاء به الخبراء الذين عرفوه بأنه " البرهان القائم على المنطق والعقل في إطار من الشرعية الإجرائية لعثات صحة افتراض أو لرفع درجة اليقين الإقناعي في واقعة محل خلاف "[51].

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

الفقرة الثانية : معنى الدليل الإلكتروني : هناك عدة تعريفات من أهمها :

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

([49]) عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، مصر، 2010 ص 51 .

([50]) سامي جلال فقي حسين : الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر 2011، ص 16 .

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

عرفه البعض على أنه :" الدليل المأخوذ من أجهزة الكمبيوتر، ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا، وهو مكون رقمي لتقديم معلومات في أشكال متنوعة مثل : النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ القانون " [52].

وعرفه آخرون على أنه :" كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من إنجاز مهمة ما " [53] .

وأيضا هناك من يعرفه بأنه :" معلومات يقبلها المنطق، والعقل، ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية، وعلمية، بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي، وملحقاتها وشبكات الاتصال، ويمكن استخدامها في أي مرحلة من مراحل التحقيق، أو المحاكمة لإثبات حقيقة فعل أو أي شئ له علاقة بجريمة، أو جان، أو مجني عليه " [54] .

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

) الأدلة الرقمية بأنها: " تشمل جميع البيانات Caseyكما نجد التعريف الذي قال به الأستاذ كيسي (الرقمية التي يمكن أن تثبت أن هنالك جريمة ارتكبت أو توجد علاقة بين الجريمة والجاني أو بين الجريمة والمتضرر منها، والبيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الصور، الصوت و الفيديو"[55].

) IOCE (أما التعريف المقترح للدليل الالكتروني من قبل المنظمة الدولية لأدلة الحاسوب (International Organization Of Computer Evidence) أنه "المعلومات المخزنة أو المثقلة في شكل ثنائي، ويمكن أن تعتمد عليها المحكمة" [56].

من خلال جملة التعاريف السابقة فضلا عن كونها متقاربة يتبين لنا ما يلي:

([52]) ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية مصر، 2006، ص 77 .

([53]) عائشة بن قارة مصطفى، المرجع السابق، ص 53 .

([54]) المرجع نفسه، ص 53 .

([55]) digital evidence encompasses any andall digital data that ran rstablish that a crime has been this digital data is a combination of numbers that represent information of various kinds including trext, images, audio,and vidéo, by eogham casey, Digital Evidence And Computer Crime, Forensic Science Computer And The Internet, Second Edition, Academic Press An Imprint Of Elservier, London; 2004, p 260.

([56]) أحمد مسعود مريم، المرجع السابق، ص 82.)

وقوع تداخل بين تعريف الدليل الالكتروني من جهة ومفهوم برامج الحاسب الآلي من جهة أخرى حيث أن الوظيفة التي يؤديها كل منهما تفرق أحدهما عن الآخر، فدور برنامج الحاسوب يتمثل في تشغيله وتوجيهه إلى حل المشاكل ووضع الخطط المناسبة، أما الدليل الإلكتروني فله دور أساسي في معرفة كيفية حدوث الجريمة المعلوماتية بهدف إثباتها ونسبتها إلى مرتكبها في البيئة الافتراضية غير المحسوسة، إذ يمكن تفتيش الفرص الصلب لمعرفة ما مر به المجرم لتحقيق هدفه الإجرامي.

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

من جهة أخرى نجد أن هذه التعريفات قد حصرت مصادر الأدلة الإلكترونية في أجهزة الحاسب الآلي و ملحقاتها، دون العديد من النظم الأخرى المدمجة بحواسب التي قد تحتوي على العديد من الأدلة الرقمية) و غيرها.Smart Cards) و البطاقات الذكية (Mobile Telephoneكالهواتف المحمولة (

وبالرجوع إلى الملاحظات السابقة نجد أن التعريف الأنسب للدليل الإلكتروني هو الذي يعرف بأنه:

"معلومات مخزنة في أجهزة الحاسوب وملحقاتها أو متنقلة عبر شبكات الاتصال، والتي يتم تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبها"[57].

الفرع الثاني: طبيعة الدليل الإلكتروني

إن الأدلة الجنائية متنوعة، وبالنسبة لطبيعتها فهي لا تخرج عن إما أن تكون ذات طبيعة مادية أو طبيعة معنوية، وفيما يخص الأدلة المادية فالمقصود بها تلك الأدلة التي يمكن إدراكها بالحواس، أي تتميز بطبيعة مادية محسوسة، كوجود الشئ المسروق في حيازة الجاني، أو ضبط الجاني حاملا لسلاح استعمل في ارتكاب الجريمة، بمعنى آخر الأدلة المادية هي تلك التي تخرج عن عناصر مادية معبرة عن نفسها، ولها تأثير في اقتناع القاضي بطريقة مباشرة.

وفيما يخص الأدلة المعنوية فهي عكس الأدلة المادية، أي ليس لها وجود مادي ملموس يعبر عنها، سواء كان هذا الأمر بالقول، أو الإيحاء، أو الكتابة، فهذه الأدلة يطلق عليها تعبير الأدلة الناطقة وهذا راجع إلى أن هذه الأدلة تصل للقاضي عن طريق لسان الغير، كاعتراف المتهم، وشهادة الشهود وبقول آخر هي تلك

---

[57](عائشة بن قارة مصطفى، المرجع السابق، ص 60.)

الأدلة الصادرة من إرادة شخصية، والمتجسدة في أقوال الغير، وتؤثر في اقتناع القاضي بطريقة غير مباشرة[58] .إذا فإن الإشكال المثار هنا هو حول طبيعة الدليل الإلكتروني، سواء كانت مادية أو معنوية.

إن الدليل الإلكتروني بأنواعه هو ذو طبيعة مادية، مهما كان شكله، وسواء كان في شكل مخرجات ورقية، أو غير ورقية، وغيرها، باعتبار أنه حتى وإن كانت غير ذلك فسيتم إخراجها في شكل دعامات، عبارة عن أشرطة ممغنطة، أو أقراص مغناطيسية، إلى غير ذلك، وبالتالي فهي ستصبح ذات طبيعة مادية [59] .

ومنه نقول أن الأدلة الإلكترونية لها طبيعة مادية وهذا الأمر لا يمكن إنكاره، باعتبار أن التطور التكنولوجي في الوقت الحالي يسمح باستخراج مختلف المعلومات من جهاز الحاسوب الآلي أو التقنيات المرتبطة به، في شكل أشياء مادية ملموسة لتصبح دليلا يعتمد عليه في قضية ما وتثبت به .

الفرع الثالث: خصائص الدليل الإلكتروني

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

وهذا ما سنوضحه من خلال تقسيم هذه الخصائص إلى أربع فقرات، حيث تطرقنا إلى أن الدليل الإلكتروني هو دليل علمي غير مرئي وهذا من خلال (الفقرة الأولى)، دليل يصعب التخلص منه في (الفقرة الثانية)، الدليل الإلكتروني قابل للنسخ (الفقرة الثالثة)، صعوبة طمس أو حذف الأدلة الإلكترونية (الفقرة الرابعة) .

الفقرة الأولى: دليل علمي غير مرئي

يتكون هذا الدليل الإلكتروني من بيانات ومعلومات ذات صفة إلكترونية غير ملموسة ولا تدرك بالحواس العادية، بل يتطلب لإدراكها الاستعانة بالبرامج والوسائل الخاصة بذلك[60]، والدليل الإلكتروني كالدليل العلمي يخضع لقاعدة لزوم التجاوب مع الحقيقة كاملة وفق قاعدة (إن القانون مسعاه العدالة، أما العلم فمسعاه

([58]) سامي جلال فقي حسين، المرجع السابق، ص 65 .

([59]) المرجع نفسه، ص65 .

([60]) خالد عياد الحلبي، المرجع السابق، ص 231 .

الحقيقة) إذن فبحكم الطبيعة الخاصة للدليل الإلكتروني فإنه لا يجب أن يخرج عما توصل إليه العلم الرقمي وإلا فقد معناه[61] .

الفقرة الثانية: يصعب التخلص منه

تعتبر هذه الخاصية من أهم خصائص الدليل الرقمي و التي تميزه عن غير من الأدلة التقليدية فيمكن للجاني أن يتخلص بكل سهولة من الأوراق التي تحمل دليل إدانته بحرقها، أو بمسح بصماته من موضعها أو التخلص من الشهود، أما بالنسبة للأدلة الرقمية فإن الحال غير ذلك حيث يمكن استرجاعها بعد محوها أو) وسواء Rescue Box) و(Recover Lost Dataإتلافها وذلك عن طريق العديد من البرامج الخاصة مثل: ( ) وهذا ما يشكل Format) أو قام بإعادة تشكيل القرص عن طريق تقنية (Deleteاستخدام الجاني أمر المحو (على الجاني صعوبة في إخفاء جريمة والتخفي منها عن أعين العدالة والأمن [62].

الفقرة الثالث: قابل للنسخ

تتيح التقنية المعلوماتية استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها القيمة العلمية نفسها، وهذه الخاصية لا تتوافر في الأدلة الجنائية التقليدية، مما يشكل ضمانة فعالة لعدم إتلاف الدليل أو فقده أو تلفه [63].

الفقرة الرابعة : صعوبة طمس أو حذف الأدلة الإلكترونية

الأدلة الإلكترونية يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها مما يؤدي إلى صعوبة التخلص منها وهي من أهم خصائص الدليل الإلكتروني بالمقارنة مع الدليل التقليدي فهناك العديد من البرامج الحاسوبية التي وظيفتها استعادة البيانات التي تم حذفها أو إلغاؤها سواء تم ذلك بالأمر باستخدام الأمر Hard Disk)، أو حتى لو تم عمل إعادة التهيئة أو التشكيل للقرص الصلب(Delete) والبرامج التي تم إتلافها أو إخفاؤها سواء كانت صورا أو رسوما أو كتابات أو غيرها مما يعني (Format) صعوبة إخفاء الجاني لجريمته أو التخفي منها عن أعين الأمن والعدالة طالما وصل علم رجال البحث

([61]) عائشة بن قارة مصطفى، المرجع السابق، ص 62 .

([62]) سامية بلجراف، سلطة القاضي الجنائي في قبول وتقدير الدليل الرقمي، ورقة بحثية مقدمة إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد خيضر، بسكرة، الجزائر، يومي 16 و17 نوفمبر 2015 ص ص 4-5.

([63]) عائشة بن قارة مصطفى، المرجع السابق، ص 64.)

والتحقيق الجنائي بوقوع الجريمة[64]، بل أن محاولة الجاني محو الدليل الإلكتروني بذاتها تسجل عليه كدليل، حيث أن قيامه بذلك يتم تسجيله في ذاكرة الآلة وهو ما يمكن استخراجه واستخدامه كدليل ضده [65] .

ويزيد من صعوبة التخلص من الأدلة الإلكترونية أنه يمكن استخراج نسخ مطابقة للأصل ولها ذات القيمة والحجية الثبوتية، الشئ الذي لا يتوافر في أنواع الأدلة الأخرى (التقليدية) مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد أو التلف أو التغيير عن عمل نسخ طبق الأصل من الدليل[66].

الفرع الرابع : شروط صحة الدليل الإلكتروني

هناك عدة شروط يجب توافرها في الدليل الإلكتروني لقبوله كأساس تقوم عليه الحقيقة في الدعاوى الجنائية سواء كان الحكم الصادر فيها بالبراءة أو الإدانة، وهذه الشروط تم تقسيمها إلى ثلاث فقرات وهي : يجب أن يكون الدليل الإلكتروني غير قابل للشك (الفقرة الأولى)، يجب الحصول على هذا الدليل بصورة مشروعة (الفقرة الثانية)، وفي الأخير يجب أن يكون الدليل الإلكتروني قابلا للمناقشة (الفقرة الثالثة).

الفقرة الأولى : يجب أن يكون الدليل الإلكتروني غير قابل للشك أي يقيني

يشترط في الأدلة المستخرجة من الحاسوب والإنترنت أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا مجال لدحض قرينة البراءة أو افتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم و اليقين[67]، ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الإلكترونية، والمصغرات الفيلمية، وغيرها من الأشكال الإلكترونية، وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات إلكترونية، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه[68] .

([64]) عبد الناصر محمد محمود فرغلي، د-محمد عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث من ضمن أعمال المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، جامعة نايف العربية للعلوم الأمنية، الرياض، 2007، ص 15 .

([65]) طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول للمعلوماتية والقانون المنعقد في الفترة (28-29 /10 /2009) تنظمه أكاديمية الدراسات العليا ، طرابلس، ص 6 .

([66]) عبد الناصر محمد محمود فرغلي، عبيد سيف المسماري، المرجع السابق، ص 15.

([67]) في هذا السياق يشترط قانون البوليس والإثبات البريطاني لسنة 1984 حتى تتحقق يقينية الأدلة الرقمية أن تكون البيانات دقيقة وناتجة عن الحاسوب بصورة سليمة، وقد نصت بعض القوانين في الولايات المتحدة الأمريكية أن النسخ المستخرجة من البيانات التي يحتويها الحاسوب تعد من أفضل الأدلة المتاحة للإثبات وبالتالي يتحقق مبدأ اليقين لهذه الأدلة .

([68]) علي حسن الطوالبه، أستاذ القانون الجنائي المساعد، مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي " دراسة مقارنة "، جامعة العلوم التطبيقية، البحرين، 2009، ص 8 .

الفقرة الثانية : يجب الحصول على الدليل بصورة مشروعة

يعرف بعض الفقه المشروعية بأنها: " التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام فهي تهدف إلى تقرير ضمانة أساسية وجدية لأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة والتطاول عليها في غير الحالات التي رخص فيها القانون بذلك من اجل حماية النظام الاجتماعي تحقيق حماية مماثلة للفرد ذاته [69] .

فطبقا لهذا المبدأ ينبغي على القاضي أن يستقي قناعته في الحكم من خلال أدلة مشروعة، أما الأدلة التي جاءت وليدة إجراءات غير قانونية أو باطلة فلا يجوز الاعتماد عليها، ويجب طرحها نهائيا لأن ما بني على باطل فهو باطل، كما يجب على المحكمة استبعاد كل دليل معيب من بين الأدلة، وإلا كان حكمها باطلا حتى وإن استندت في إصدارها إلى أدلة أخرى مشروعة إلى جانب الدليل الباطل[70].

الفقرة الثالثة : يجب أن يكون الدليل الإلكتروني قابلا للمناقشة

ويعني هذا المبدأ أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى[71]، وهذا يعني أن الأدلة المتحصلة من جرائم الحاسوب والإنترنت سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب، أم كانت بيانات مدرجة في حاملات البيانات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية كل هذه ستكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات، يجب أن يعرض في الجلسة ليس من خلال ملف الدعوى في التحقيق الابتدائي، لكن بصفة مباشرة أمام القاضي، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات [72] .

المطلب الثاني : مصادر الحصول على الدليل الإلكتروني

من أجل تحصيل الدليل الرقمي، تعتمد جهات التحقيق على العديد من المصادر في عمليات البحث والتحري لجمع المعلومات بشأن الجرائم بصفة عامة والجريمة المعلوماتية بصفة خاصة، ومن بين المصادر التي سمح بها القانون هناك ما يعرف بإجراء الإرشاد وهذا ما سنتطرق إليه من خلال (الفرع الأول)، و إجراء الوضع تحت المراقبة الإلكترونية في (الفرع الثاني)، وفي الأخير تناولنا تعاون مقدمي خدمات الإنترنت مع السلطات القضائية في (الفرع الثالث).

([69]) ضياء علي أحمد نعمان، المرجع السابق، ص 312 .

([70]) سامية بلجراف، المرجع السابق، ص 7 .

([71]) قرار محكمة النقض المصرية في 20 / 11 / 1986 – رقم 179 – المبادئ القانونية – ص 943 .

([72]) علي حسن الطوالبه، المرجع السابق، ص 10 .

الفرع الأول: إجراء الإرشاد الجنائي

من بين أهم الأساليب المعتمدة لكشف الجرائم المعلوماتية وتعقب المجرمين، نجد ما هو معروف بإجراء الإرشاد الجنائي، الذي يقوم بمقتضاه ضباط الشرطة القضائية بتجنيد أحد عناصرها لولوج العالم الافتراضي وبالأخص عبر حلقات النقاش وقاعات الدردشة والاتصال المباشر، مستعملين في ذلك أسماء وصفات هيئات وهمية من أجل البحث عن هذه الجرائم وكشف المجرمين [73].

وما يميز هذا الإجراء أنه لا يتطلب بذل جهد مادي كبير، حيث يقوم به ضابط الشرطة القضائية أو يكلف غيره من ذوي الاختصاص، وهذا بعد الحصول على إذن رسمي للقيام بمهام البحث والتحري عن الجرائم وضبط مرتكبيها [74] .

وقد أتاح المشرع الجزائري إمكانية اللجوء إلى هذا الأسلوب تحت إسم " التسرب" من خلال نصوص المواد من 65 مكرر 05 إلى غاية المادة 65 مكرر 18 (ق إ ج ج)، وذلك في العديد من الجرائم بما فيها الجريمة المعلوماتية، بعد الحصول على إذن مسبب من وكيل الجمهورية أو قاضي التحقيق وتحت رقابة الأول لمدة 04 أشهر قابلة للتجديد.

الفرع الثاني: إجراء الوضع تحت المراقبة الإلكترونية

تعتبر المراقبة من بين أهم مصادر البحث والتحري سواء في الجرائم التقليدية أو المستحدثة ومنها الجرائم المعلوماتية، وتسمى حينئذ بالمراقبة الإلكترونية (Cyber surveillance) ، ويقصد بها مراقبة شبكة الاتصالات فتعرف بأنها : " العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع بيانات ومعلومات عن المشتبه سواء أكان شخصا أو مكانا، أو شيئا حسب طبيعته، من أجل تحقيق غرض أمني أو أي غرض آخر، وهي مرتبطة بالزمن " [75] .

أجاز المشرع الجزائري المراقبة الإلكترونية في الجرائم المعلوماتية وهذا عن طريق اعتراض المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية، كما أجاز كل الترتيبات التقنية لها دون علم المعنيين ولا

([73]) في هذا الصدد يقوم المرشد (L`indicateur) بعد حصوله على إذن رسمي بمباشرة مهامه، بالدخول في نقاشات مع الغير عبر الشبكة المعلوماتية، وبمجرد إبراز هذا الشخص لنيته الإجرامية كأن يذكر أنه ينوي الاستيلاء على بطاقات ائتمان بصورة احتيالية، يقوم المرشد باستدراجه من أجل الحصول على كافة المعلومات، ثم يقوم بتوصيلها إلى الضبطية القضائية والتي تقوم بإلقاء القبض على المجرم، عن طريق برمجيات تقودها إلى مسار مزود الإنترنت الذي يستعمله مرتكب الجريمة . أنظر : هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات، دار الفكر الجامعي الجديد، الإسكندرية، مصر، 2007، ص 197 .

([74]) المرجع نفسه، ص 196 .

([75]) نبيلة هبة هروال، المرجع السابق، ص 105.

موافقتهم، بغية الحصول تسجيلات الكلام الصادر عنهم بصفة سرية أو خاصة، وذلك بإذن من وكيل الجمهورية[76] .

وهناك العديد من الأساليب التقنية لإجراء المراقبة الإلكترونية من بينها[77] :

- تقنية برنامج كارنيفور.
- تقنية كشف وجمع الأدلة والقرائن من رسائل البريد الإلكتروني.
- تقنية مراقبة البريد الإلكتروني.
- تقنية تعقب المواقع الإباحة.

سنتطرق لعنصر "إجراء الوضع تحت المراقبة الإلكترونية" بالتفصيل في الفصل الثاني من هذه الدراسة، في المطلب الثاني من المبحث الأول تحت عنوان الإجراءات الحديثة لجمع الدليل الإلكتروني.

الفرع الثالث : تعاون مقدمي خدمات الإنترنت مع السلطات القضائية

يقصد بمزود الخدمة كل شخص يقدم خدمته إلى الجمهور بوجه عام في مجال الاتصالات الإلكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بعقد من العقود[78]، وقد عرف المشرع الجزائري " مقدم الخدمة " بموجب المادة 02/ د في القانون 04/09 بأنه:

1- أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية و/ أو نظام للإثبات.

2- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها.

ونظرا لضلوع الشبكة المعلوماتية في أغلب جرائم العالم الافتراضي، فإن المشرع الجزائري قد فرض على مقدمي خدمات الإنترنت مجموعة من الالتزامات من اجل مساعدة السلطات القضائية في أعمال التحقيق وذلك من خلال القانون رقم 09-04 في فصله الرابع تحت عنوان: " التزامات مقدمي الخدمات "، ومن بين الالتزامات الواردة نجد : الالتزام بمساعدة السلطات و الالتزام بحفظ المعطيات المتعلقة بحركة السير.

([76]) المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

([77]) نبيلة هبة هروال، المرجع السابق، ص ص 201 – 203 .

([78]) شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، 2007، ص 209.

المطلب الثالث: تقسيمات الدليل الإلكتروني

تختلف الجريمة الإلكترونية عن الجريمة التقليدية في كون الأولى تتم في بيئة غير مادية عبر نظام حاسب ألي أو شبكة المعلومات الدولية الانترنت، حيث يمكن للجاني عن طريق نبضات إلكترونية رقمية لا ترى أن يعبث في بيانات الحاسوب أو برامجه، و ذلك في وقت قياسي كما يمكن محوها في زمن قياسي مما يصعب الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الإلكترونية على الدليل المتوافر، إلا أن لهذا الأخير ميزة التنوع فلا يأتي على صورة واحدة، بل يوجد له العديد من الصور والأشكال، وفي هذا الصدد نجد نوعين من التقسيمات للأدلة الإلكترونية بالإضافة إلى تقسيمات أخرى ومنه ارتأينا إلى تقسيم هذا المطلب إلى ثلاث فروع رئيسية، تناولنا في (الفرع الأول) التقسيمات الفقهية للدليل الإلكتروني، في حين خصصنا (الفرع الثاني) للتقسيمات التشريعية للدليل الإلكتروني، أما (الفرع الثالث) تطرقنا من خلاله إلى بعض من التقسيمات الأخرى لهذا الدليل .

الفرع الأول: التقسيمات الفقهية للدليل الإلكتروني

إن فقهاء القانون الجنائي لم يتوسعوا في دراسة الدليل الإلكتروني، ومرد ذلك للحداثة النسبية لهذا الدليل من جهة، وتطوره بصفة دائمة من جهة أخرى، ومن المحاولات الفقهية أنه تم تقسيم الدليل الإلكتروني لأربعة أقسام[79]، والتي قسمناها إلى أربع فقرات كالآتي: الأدلة الإلكترونية المتعلقة بجهاز الكمبيوتر وشبكاته في (الفقرة الأولى)، الأدلة الإلكترونية المتعلقة بالانترنت في (الفقرة الثانية)، الأدلة الإلكترونية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات في (الفقرة الثالثة)، والأدلة الإلكترونية المتعلقة بالشبكة العالمية للمعلومات في (الفقرة الرابعة).

الفقرة الأولى: الأدلة الإلكترونية المتعلقة بجهاز الكمبيوتر و شبكاته

وهي تتماشى مع جرائم الكمبيوتر الواقعة على أجهزة الكمبيوتر بسلوك غير مشروع، سواء كان هذا الأمر على المكونات المادية له[80]، أو المكونات المعنوية[81]، أو قواعد البيانات الرئيسية مثل تخريب مكونات الكمبيوتر كالشاشات.

---

[79] ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 88.)

[80] : هي المكونات الفعلية لجهاز الكمبيوتر التي يمكن مشاهدتها ولمسها. (Hardware)) يقصد بالمكونات المادية للحاسوب (يشتمل ذلك على وحدة النظام وكل شئ متصل بها، مثل الشاشة، لوحة المفاتيح، الفأرة... وغيرها.

[81] : هي التي لا يمكن مشاهدتها ولكن يمكن أن نرى تأثير عملها مثل (Software) يقصد بالمكونات المعنوية للحاسوب)(البرامج.

الفقرة الثانية: الأدلة الإلكترونية المتعلقة بالانترنت

وهي تتطابق مع جرائم الانترنت وهي أيضا سلوك غير مشروع يقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات مثل الدخول غير المشروع لمواقع يمنع الدخول إليها واستخدام عناوين غير دقيقة للدخول لشبكة العالمية للمعلومات وغيرها.

الفقرة الثالثة: الأدلة الإلكترونية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات

وهي متعلقة بالجرائم التي ترتكب باستخدام الكمبيوتر، حيث أنه لا يعتبر استعمال الكمبيوتر أو الشبكة العالمية للمعلومات أو انترنت، في هذه الجرائم من طبيعة الفعل الجرمي، وإنما تعتبر كوسيلة مساعدة لارتكاب الجريمة، مثل غسيل الأموال أو نقل المخدرات من مكان لأخر وغيره، وجهاز الكمبيوتر في هذه الحال يحتفظ بآثار الكترونية قد ترشد للفاعل[82].

الفقرة الرابعة: الأدلة الإلكترونية المتعلقة بالشبكة العالمية للمعلومات

وهي متماشية مع الجرائم المتعلقة بهذه الشبكة، وهي فعل غير مشروع قانونا يقع على أي وثيقة أو نص موجود بالشبكة، مثل قرصنة المعلومات وسرقة بطاقات الائتمان وانتهاك الملكية الفكرية للبرامج وغيرها، فهذا النوع من الجرائم يتطلب الاتصال بالانترنت [83].

الفرع الثاني: التقسيمات التشريعية والقضائية للدليل الالكتروني

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

فهي تعتبر ثاني دولة بعد السويد في إصدار القوانين الخاصة بها التي تجرم عن طريقها نوع مستحدثا من الجرائم وهي الجرائم الالكترونية، كما أنها قامت بإنشاء المنظمة الدولية لأدلة الحاسوب(ICOE) ورافقتها بالفريق العامل على مستوى الأدلة الالكترونية (SWGDE) وهذا بغرض توحيد الجهود التي تقوم بها هذه المنظمة [84].

ومنه سنبرز من خلال ما يلي تقسيمات وزارة العدل الأمريكية للدليل الإلكتروني لسنة 2002 والتي حصرناها في ثلاث فقرات، حيث تطرقنا في (الفقرة الأولى) إلى السجلات المحفوظة في الحاسوب وفي (الفقرة

---

[82] (ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 95.)

[83] (عائشة بن قارة مصطفى، المرجع السابق، ص 73.)

[84] (المرجع نفسه، ص ص 73- 74.)

الثانية)، السجلات المحفوظة جزئيا في الحاسوب، أما في (الفقرة الثالثة) فتناولنا السجلات المحفوظة للإدخال والمنشأة بواسطة الحاسوب.

الفقرة الأولى: السجلات المحفوظة في الحاسوب

عبارة عن وثائق مكتوبة ومحفوظة والمقصودة بالكتابة الإلكترونية أيضا كل الحروف أو الأرقام أو الرموز أو أي علامات أخرى، تثبت على عامة إلكترونية أو رقمية أو ضوئية أو أي وسيلة أخرى وتعطي دلالة قابلة للإدراك[85].

من أمثلتها البريد الإلكتروني الذي عرف على أنه: "طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات"[86] فهو عبارة عن صندوق تتواجد به كل الرسائل المرسلة إلى صاحب البريد والتي سبق له إرسالها و الملفات وغيرها من الأمور التي يحتوي عليها البريد الإلكتروني.

الفقرة الثانية: السجلات المحفوظة جزئيا في الحاسوب

هذا النوع من السجلات يتم إنشاؤها بواسطة الحاسوب، أي هي عبارة عن مخرجات برامج الحاسوب،) بالإضافة لسجلات الهاتف وكذا فواتير أجهزة Log Filesمعنى ذلك أنه لم يتم لمسها من الأشخاص مثل ( ). ATMالسحب الآلي (

الفقرة الثالثة: السجلات المحفوظة للإدخال والمنشأة بواسطة الحاسوب

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

وهذا التقسيم هو نفسه الذي أخذ به القضاء الأمر فسجلات الحاسوب المقبولة أمام القضاء الأمريكي هي التي تكون في شكل نصوص، وهذا إما في هيئة سجلات الحاسوب المتوالدة، أو سجلات الحاسوب المخزنة، ويكمن الفرق بينهما فيما إذا كان الشخص هو المنشى لمحتوى هذه السجلات أو الآلة، فسجلات الحاسوب المخزنة تحتوي على كتابات شخص أو بعض الأشخاص في شكل إلكتروني مثل: البريد الإلكتروني، أما ما يخص سجلات الحاسوب المتوالدة فالكمبيوتر هو الذي يصدرها، فهي عبارة عن مخرجات برامج الحاسوب مثل سجلات الدخول على الإنترنت التي يكون مصدرها مزود خدمة الإنترنت، كما أن هناك نوعا ثالثا من السجلات الذي يجمع بين التدخل الإنساني ومعالجة الكمبيوتر مثلا كأن يدخل متهم معين بيانات ويطلب من الكمبيوتر معالجتها للوصول إلى نتائج يمسح بها هذا البرنامج المستخدم، كالشخص الذي يتهرب

---

[85] (محمد حسين منصور، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، مصر، 2006، ص 272.)

[86] (خالد ممدوح إبراهيم، التقاضي الإلكتروني، دار الفكر الجامعي، الطبعة الأولى،مصر، 2007، ص ص 101- 102.)

من الضرائب فيسجل بيانات غير صحيحة تتعلق بدخله وربحه ويطلب من الكمبيوتر حساب الضريبة المستحقة [87] .

إلا أن ما يؤخذ على هذه التقسيمات أنها لا تشمل الدليل الإلكتروني، فهي حصرته في نوع واحد وهو سجلات الحاسوب المحتواة على نص، رغم أن الدليل الإلكتروني يتعلق بكافة البيانات الإلكترونية التي يمكن تداولها إلكترونيا، كالصور والأصوات والرسوم وغيرها، فنجد في الوقت الراهن بروتوكولات الاتصالات TCP /)والتطبيقات المعلوماتية التي تستعمل في التحقيق فيما يخص الجرائم الإلكترونية، حيث يعتبر نظام من أكثر البروتوكولات المستعملة في شبكات الإنترنت، فهي تعتبر جزءا مهما منه فهي تدل بصفة يقينية (IP عن مصدر الجهاز الذي استخدم في الجريمة، كما تقوم بتحديد الأجهزة التي أصابها الضرر من هذا الفعل الإجرامي [88] .

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

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

الفرع الثالث : تقسيمات أخرى للدليل الإلكتروني

هناك تقسيمات فقهية أخرى للدليل الإلكتروني، فقد أعطى الفقهاء احتمالات عديدة للدليل الإلكتروني وهذا ما سنحاول إيضاحه من خلال تقسيمنا هذا الفرع إلى فقرتين، لمحاولة الإلمام بجميع الأنواع المقترحة للدليل الإلكتروني، حيث تطرقنا في (الفقرة الأولى) إلى تقسيم الدليل الإلكتروني تبعا لمكوناته، أما (الفقرة الثانية) فقد تناولنا فيها تقسيم الأدلة الإلكترونية بحسب مكان وجودها.

الفقرة الأولى : تقسيم الدليل الإلكتروني تبعا لمكوناته

أولا : الأشرطة المغناطيسية

وهذا الشريط هو عبارة عن شريط بلاستيكي مغطى بمادة قابلة للمغنطة ويكون ملفوفا على بكرة مثل التي تستخدم في أجهزة التسجيل الصوتي. يستعمل هذا الشريط في تخزين البرامج والملفات المتتالية أي اللازمة لقراءة البيانات فيها قراءة الشريط من بدايته، والمعلومات الموجودة فيه تنظم على شكل وحدات خاصة.

([87]) عائشة بن قارة مصطفى، المرجع السابق، ص ص 74-76.

([88]) خالد ممدوح إبراهيم، المرجع السابق، ص 76 .

ثانيا : الأقراص المغناطيسية

إن الأقراص المغناطيسية تعد من أفضل وسائط التخزين، التي يمكن استخدامها للتخزين المباشر وهذا راجع لقدرتها الاستيعابية الكبيرة، ولها خاصية مهمة هي إمكانية القراءة أو التسجيل، وكذا إمكانية تغيير أو تعديل أي ملف عليها دون الحاجة إلى إنشاء ملف جديد حيث يتم تعديل التسجيل وهو في موضعه، وهناك عدة أنواع نذكر منها : القرص المرن، القرص الصلب، قرص الخرطوش أو قرص الكارتريدج، المصغرات الفيلمية [89].

الفقرة الثانية : تقسيم الأدلة الإلكترونية بحسب مكان وجودها

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

ثانيا : أجهزة الحسابات : وهي التي تحتوي على ملحقات الحاسوب من شاشات وغير ذلك.

ثالثا : الأقراص المرنة والصلبة : تعتبر من أهم الأدلة لاحتوائها على بيانات وكلمات مرور و صور وتقارير وخطط ارتكاب الجريمة وغيرها.

رابعا : أشرطة تخزين المعلومات : تستخدم لحفظ النسخ الاحتياطية.

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

سادسا : أجهزة المودم : والتي تستخدم في نقل المعلومات, ويمتاز بعضها بإمكانية أن يعمل كجهاز الرد على رسائل الهاتف, ويجب تسجيل الكابلات المتصلة به عند ضبطه.

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

ثامنا : الطابعات والأجهزة الخاصة بتصوير المستندات ك وما قد تحتويه من أوراق مطبوعة و مصورة أو ما هو مخزن في ذاكرتها من معلومات [90] .

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

([89]) سامي جلال فقي حسين، المرجع السابق، ص 75 .

([90]) علي جبار الحسيناوي : جرائم الحاسوب والإنترنت، دار اليازوري العلمية للنشر والتوزيع ، الأردن، 2009، ص143.

خلاصة الفصل

تطرقنا في هذا الفصل إلى الجريمة الإلكترونية باعتبارها مصدر للدليل الإلكتروني من خلال مناقشة تعريف هذه الجريمة وخصائصها، فلا يوجد اتفاق على المستوى التشريعي أو الفقهي على استعمال مصطلح محدد للدلالة على هذه الظاهرة الجرمية، وهذا بسبب طبيعتها الأصلية، فهي تتم في فضاء إلكتروني يتسم بالتغيير والديناميكية والانتشار الجغرافي العابر للحدود.

غير أن المشرع الجزائري وفق في اعتماد مصطلح " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" وعرفها بموجب أحكام المادة (02 / أ) من القانون رقم 09-04 المؤرخ في 5 أوت 2009 والمتضمن لقواعد خاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي يتوافق مع مصطلح " الجرائم الإلكترونية ".

بعد ذلك عالجنا مختلف جوانب الدليل الإلكتروني كأثر ناتج عن الجريمة الإلكترونية من خلال تحديد مفهومه وخصائصه بالإضافة إلى شروط صحة ومصادر الحصول عليه مع إبراز أهم التقسيمات التي جاء بها.

بناء على ما سبق نتسائل عن الإجراءات التقليدية والحديثة لإحراز الدليل الإلكتروني، وعن مدى اقتناع القاضي الجنائي بهذا الدليل.

الفصل الثاني

إجراءات جمع الدليل الإلكتروني ومدى اقتناع القاضي الجنائي به

الفصل الثاني: إجراءات جمع الدليل الإلكتروني ومدى اقتناع القاضي الجنائي به

لقد تناولنا في الفصل الأول مفهوما عاما وشاملا للجريمة الإلكترونية كمصدر للدليل الإلكتروني باعتبارها جريمة فريدة من نوعها حيث أن مسرحها فضاء افتراضي، كما عرفنا الدليل الإلكتروني كأثر ناتج عنها باعتباره الوسيلة الوحيدة أو الرئيسية لإثبات هذه الجرائم، وعليه فإنه يجب علينا أن نبين في هذا الفصل (المبحث الأول)، بينما نخصص (المبحث الثاني) لمسألة مدة الإجراءات الخاصة لجمع الدليل الإلكتروني اقتناع القاضي الجنائي بهذا الدليل.

المبحث الأول: الإجراءات الخاصة بجمع الدليل الإلكتروني

مما لاشك فيه أنه لا يوجد ما يسمى بالجريمة الكاملة مهما حاول الجاني إخفاءها وذلك استنادا إلى قاعدة "لوكارد لتبادل المواد" التي تنص على أنه عند احتكاك جسمين بعضهما ببعض فإنه لابد وأن ينتقل جزء من الجسم الأول إلى الثاني وبالعكس، وبالتالي ينتج عن هذا الاحتكاك ما يعرف بالدليل الإلكتروني، وفي مجال الجريمة الالكترونية لدينا الدليل الالكتروني، وحتى يتحقق هذا الدليل لإثبات هذا النوع المستحدث من الجرائم فإنه لابد من جمع عناصر التحقيق والدعوى، و تقديم هذه العناصر إلى سلطة التحقيق الابتدائي، فإذا أسفر هذا التحقيق عن دليل أو ترجح معها إدانة المته، قدمته إلى المحكمة، ومرحلة المحاكمة هي أهم المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي لإدانة المتهم وإلا قضي ببراءته[91].

إلا أن خصوصية الجريمة الإلكترونية وذاتية الدليل الإلكتروني سيقودان دون شك إلى تغيير كبير إن لم يكن كليا في المفاهيم السائدة حول إجراءات الحصول على هذا الدليل وذلك نتيجة لضآلة دور بعض الإجراءات التقليدية في بيئة تكنولوجيا المعلومات كالمعاينة أو الشهادة مثلا، و بالتالي يقودنا إلى إتباع الإجراءات التقليدية لجمع الدليل الإلكتروني في(المطلب الأول)، ثم يليه الإجراءات الحديثة لجمع هذا الدليل في (المطلب الثاني).

المطلب الأول: الإجراءات التقليدية لجمع الدليل الإلكتروني

نظم المشرع كيفية استنباط الدليل عن طريق إجراءات تتبع وصولا إلى هذه الغاية. وعليه قسمنا هذا التفتيش)الفرع الثاني(المعاينة والخبرة التقنية، وفي)الفرع الأول(المطلب إلى ثلاث فروع أساسية، تناولنا في فقد خصصناه إلى سماع الشهود، وهذه الإجراءات تستخدم بصفة عامة)الفرع الثالث(وضبط الأشياء، أما في

---

[91](، دار الجامعة الجديدة، 2005 ص19.DNAخالد حمد محمد الهادي، الثورة البيولوجية ودورها في الكشف عن الجريمة)

لجمع الدليل في جميع الجرائم التقليدية منها والمستحدثة، إلا أن دورها يكون بين المد في الجرائم الأولى والجزر في الثانية.

الفرع الأول: المعاينة والخبرة التقنية

إن التعامل في الجريمة المعلوماتية يتطلب إجراءات روتينية متفق عليها وذلك من أجل حماية الدليل، غير أن وسائل حفظ الأدلة واستنتاجها تختلف من الجريمة التقليدية إلى الجريمة المعلوماتية الرقمية، ذلك لأن البرامج والبيانات عنصران أساسيان يتحتم على أجهزة تنفيذ القانون وخبراء الأدلة الجنائية جمعها واستخلاصها، وتعد المعاينة والخبرة من بين إجراءات التحقيق، والتي تؤدي للوصول إلى الدليل المستمد من الواقعة الإجرامية، وسوف نتعرض في هذا الفرع لمفهوم الانتقال والمعاينة في (الفقرة الأولى)، وكذا الخبرة التقنية في العالم الافتراضي في (الفقرة الثانية).

الفقرة الأولى: مفهوم الانتقال والمعاينة

لم تحدد أغلب التشريعات المقصود بالانتقال والمعاينة ومنها المشرع الجزائري الأمر الذي دعا بالفقه للتصدي لتعريفهما، حيث يعتبر الانتقال عملا هاما من أعمال التحقيق يتم بقصد جمع الأدلة وفحصها لكشف حقيقة الجريمة ويتطلب ذلك أن ينتقل المحقق من مقر عمله إلى مكان آخر قد يكون مسرح الجريمة لإجراء عمل من أعمال التحقيق، حيث يتم الانتقال بهدف إجراء معاينة أو بهدف القيام بعمل آخر كالتفتيش والضبط وسماع أقوال الشهود في بعض الأحوال[92]، أما فيما يخص المعاينة فهناك عدة تعاريف لها، فيقصد بها: "رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته ومعرفة كل ما يلزم لكشف الحقيقة"[93] في حين عرفها جانب آخر من الفقه تعريف أكثر دقة بأنها: "مشاهدة وإثبات الآثار المادية التي خلفها ارتكاب الجريمة، بهدف المحافظة عليها خوفا من إتلافها أو محوها أو تعديلها"[94].

الأصل في المعاينة أنها إجراء من إجراءات التحقيق، ولهذا في غير حالات التلبس المنصوص عليها في القانون يجب أن تقوم بها سلطة التحقيق بنفسها، أو تنتدب مأمور الضبط للقيام بذلك [95] ويقتضي ذلك تحرير محضر بها عن طريق كاتب، لأنها من الإجراءات التي تستلزم من المحقق تفرغا ذهنيا، وتتبع في شانها أبضا جميع القواعد التي تحكم إجراءات المحاكمة، من إخطار الخصوم بمكان المعاينة وزمانها ليتمكنوا من

---

[92] (خالد ممدوح إبراهيم، المرجع السابق، ص156.)

[93] (عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، دراسة مقارنة منشورات الحلبي الحقوقية، بيروت، لبنان، (د،س، ن)، ص303.)

[94] (علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، ط1 المكتب الجامعي الحديث، مصر، 2012، ص22.)

[95] (محمد علي الجمال، التقاط الدليل المادي من مسرح الجريمة، مجلة الدراسات العليا، العدد الثاني، يناير 2000 ص190.)

الحضور أثناء إجراءها [96]. كما يمكن للمحكمة ان تقوم بإجراء المعاينة إذا ما رأت في ذلك سبيلا في كشف الحقيقة، سواء كان ذلك من تلقاء نفسها أو بناء على طلب الخصوم[97].

هذا فيما يخص بالأحكام العامة للمعاينة، وسنتناول فيما يلي المعاينة في الجريمة الالكترونية ومدى أهميتها مقارنة بالجريمة التقليدية.

للمعاينة أهمية كبيرة في كشف غموض العديد من الجرائم التقليدية، إلا أن دورها في كشف غموض الجرائم الإلكترونية، وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها لمرتكبها ليس بالدرجة نفسها من الأهمية مقارنة بالجريمة الإلكترونية وذلك لأسباب عدة منها:

- أن الجرائم الواقعة على نظم المعلومات أي الجرائم الالكترونية، من النادر ما يتخلف عنها آثار مادية.
- إن عن عدد كبير من الأفراد يكونوا قد ترددوا على مسرح الجريمة خلال الفترة التي تتوسط عادة بين ارتكاب الجريمة واكتشافها، و هذا ما يفتح المجال لحدوث تغيير أو إتلاف أو عبث بالآثار المادية أو محو بعضها، وهو ما يثير الشك على الدليل المستنبط من المعاينة [98].
- استطاعة الجاني من التلاعب في البيانات عن بعد أو محوها عن طريق قيامه بالتدخل من خلال وحدة طرفية، لذلك نص كل من المشرع الجزائري في المادة 43 من قانون الإجراءات الجزائية الجزائري [99]، والمشرع الفرنسي من خلال المادة 55 / 1 من قانون الإجراءات الجنائية الفرنسي[100]، أن تقرر جزاءات جنائية على كل من يقوم بإجراء أي تغيير أو تعديل في المعلومات المسجلة في ذاكرة الحاسوب أو وسائط التخزين أو في بنك المعلومات أو قاعدة البيانات قبل قيام سلطة التحقيق بإجراء المعاينة وذلك حرصا منهما على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي، والملاحظ و إن كانت أحكام هذه النصوص تنصرف إلى أغلب الجرائم التقليدية، إلا أنه يمكن

([96]) جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالانترنت، دار الفكر العربي، القاهرة، 2001، ص27.

([97]) جلال ثروت، نظم الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، 1997، ص456.

([98]) عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2001 ص ص365- 366.

([99]) تنص المادة 43 من قانون الإجراءات الجزائية الجزائري،"يحظر في مكان ارتكاب جناية على كل شخص لا صفة له أن يقوم القضائي، بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق = وإلا عوقب بغرامة 200 إلى 1000دج، غير انه يستثنى من هذا الحظر حالة ما إذا كانت التغيرات أو نزع الأشياء للسلامة و الصحة العمومية أو تستلزمها معالجة المجني عليه.

([100]) Article 55 DU (cppf)

تطبيقها عند معاينة مكونات الحاسوب ذات الطابع المادي على خلاف معاينة المكونات غير المادية لأنها تتطلب إجراءات خاصة [101].

أولا: الانتقال والمعاينة على مسرح الجريمة الإلكترونية

تتم معاينة الجريمة الإلكترونية بالانتقال إلى مسرح الجريمة الإلكترونية وينبغي التعامل مع هذا المسرح على أنه مسرحان هما:

مسرح تقليدي: يقع خارج بيئة الحاسوب ويتكون بشكل رئيسي من المكونات المادية للحاسوب وهو أقرب ما يكون إلى مسرح أي جريمة تقليدية، فقد يترك الجاني آثارا كالبصمات وبعض المتعلقات الشخصية أو وسائط تخزين رقمية .

مسرح افتراضي: يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنت وفي ذاكرة الأقراص الصلبة للحاسوب غير أن الانتقال لا يتم بالضرورة عبر العالم المادي وإنما عبر العالم الافتراضي (cuber space) . وعليه يستطيع ضابط الشرطة القضائية الانتقال إلى العالم الافتراضي لمعاينة الجريمة الإلكترونية كما يأتي [102]:

- يستطيع ضابط الشرطة القضائية الانتقال إلى العالم الافتراضي لمعاينة مسرح الجريمة من خلال حاسوبه الموجود بمكتبه.
- يمكن لضابط الشرطة القضائية اللجوء إلى مقهى الانترنت.
- يمكن لضابط الشرطة القضائية اللجوء على مزود خدمة الانترنت internet server provide الذي يعتبر أفضل مكان يمكن من خلاله إجراء المعاينة [103].

ونتيجة لاختلاف مسرح الجريمة الإلكترونية عن غيره من الجرائم لكون هذا النوع من الجرائم يتميز بوجود الأدلة الإلكترونية ذات الطبيعة غير المرئية، لذلك ينبغي تعاملا خاصا معه ويكون ذلك من خلال إتباع عدة قواعد فنية قبل الانتقال إلى مسرح الجريمة الإلكترونية أبرزها:

- توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد لأجهزة وشبكات الاتصال الخاصة بها قصد تحديد إمكانية التعامل معها فنيا [104].

="dans les lieux ou un crime à été commis, il est interdit, sous peine le l'amende prévue pour les contraventions de la quatriéme classe. à toute personne non habilitée, de modifie avant les premieres opérations de l'enquete judiciaire l'état des lieux et d'y effcttuer des prélévement quelconques…. "

[101] عائشة بن قارة مصطفى، المرجع السابق، ص82.)

[102] نبيلة هبة هروال، المرجع السابق، ص218.)

[103])عمر محمد أبو بكر بن يونس، المرجع السابق، ص895.

[104] هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية، دار الكتب القانونية، القاهرة، مصر، 2015، ص186.)

- إعداد خريطة للموقع المتوقع الإغارة عليه والتأكيد من تأمين وصلاحية الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة [105].
- إعداد فريق متخصص من الخبراء ورجال الأمن والضباط وإعطائهم الوقت الكافي للاستعداد فنيا عن طريق وضع خطة عملية لضبط أدلة الجريمة وقت معاينتها [106].
- الحصول على الاحتياجات الضرورية من أجهزة و برامج للاستعانة بها في الفحص والتشغيل مثل: برامج معالجة الملفات (xtreeprogold)وبرامج النسخ (laplink) وبرامج إنتاج صور مطابقة عن القرص الصلب (encase)، والذي تستخدمه المباحث الفدرالية الأمريكية في التحقيقات الجنائية ويطلق عليه الخبراء (حقيبة الأدلة الرقمية) [107].
- تأمين عدم انقطاع التيار الكهربائي المفاجئ لأن ذلك يتسبب في محو المعلومات من الذاكرة وبالتالي ضياع كافة العمليات التي تم تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة [108].

ثانيا: الإجراءات التي يتعين إتباعها عند إجراء المعاينة

- تصوير الحاسوب والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة بمكانه مع التركيز بوجه خاص على تصوير الأجهزة الخلفية للحاسوب وملحقاته مع مراعاة تسجيل وقت و تاريخ ومكان التقاط كل صورة [109].
- عدم نقل أي مادة معلوماتية من مكان وقوع الجريمة إلا بعد إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي قد تؤدي إلى فقد البيانات المخزنة [110].
- القيام بحفظ المستندات الخاصة بالإدخال وكذا مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة وذلك من أجل رفع مضاهاة البصمات التي قد تكون موجودة عليها[111].

---

[105] نبيلة هبة هروال، المرجع السابق، ص219.

[106] عبد الفتاح بيومي حجازي، المرجع السابق، ص216.

[107] عائشة بن قارة مصطفى، المرجع السابق، ص85.

[108] عبد القتاح بيومي حجازي، المرجع السابق، ص217.

[109] = خالد ممدوح إبراهيم، المرجع السابق، ص172.

[110] عبد العال الدريبي محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، مصر 2012، ص296.

[111] عفيفي كامل عفيفي، المرجع السابق، ص307.

- التحفظ على محتويات سلة المهملات، وكذا القيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطمة المتواجدة فيها [112].
- ربط الأقراص الكومبيوترية التي ربما تحمل الأدلة، مع جهاز يمنع الكتابة أو التسجيل عليها، مما يتيح للمحققين قراءة بياناتها من دون تغييرها.
- قصر مباشرة المعاينة على المحققين الذين تتوافر الكفاءة العملية والخبرة التقنية في مجال المعلوماتية واسترجاع المعلومات، والذين تلقوا تدريبا كافيا على التعامل مع نوعية الآثار والأدلة التي يمكن أن يحتويها مسرح الجريمة الإلكترونية [113].

وعلى ضوء ما تقدم يمكن القول بعدم كفاية المعاينة كإجراء تقليدي للإحاطة بكافة جوانب مسرح الجريمة الإلكترونية نظرا لمميزات الدليل الإلكتروني، فهو غير مرئي كما يسهل على المجرم محوه أو بتعديله بضغطة زر وفي جزء من الثانية وهو جالس وراء حاسوبه، لذا لنجاح المعاينة لابد من توفير فريق متخصص من ضباط الشرطة القضائية لديهم معرفة متميزة بالمعلوماتية عموما وبنظمها خصوصا وكيفية تشغيلها ووسائلها، وتقنيات إساءة استعمالها من قبل مستخدميها. ولا يتأتى ذلك إلا بتكوينهم وتدريبهم وتجديد معارفهم قصد حصولهم على المهارات اللازمة في مجال الكشف عن الجرائم المستحدثة[114].

الفقرة الثانية: الخبرة التقنية في العالم الافتراضي

الخبرة القضائية عموما هي "الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه"[115] فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية والفنية والتي لا تتوافر سواء لدى المحقق أو القاضي، وفي هذا المجال نتطرق أولا إلى دراسة القواعد القانونية التي تحكم الخبرة القضائية بصفة عامة، ثم نتناول ثانيا الجوانب الفنية التي تحكم إنجاز الخبرة التقنية المتعلقة بإثبات الجريمة الإلكترونية.

---

[112] عائشة بن قارة مصطفى، المرجع السابق، ص ص86-87.)

[113] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتب الآلات الحديثة، مصر، 1994.)

[114]) يزيد بوحليط، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر، أطروحة لنيل شهادة دكتوراه العلوم تخصص قانون خاص، جامعة باجي مختار، عنابة، 2016، ص 226.

[115] أمال عثمان، الخبرة في المسالة الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964، ص68 وما بعدها. أنظر) أيضا: عادل حافظ غانم، الخبرة في مجال الإثبات الجنائي، بحث بمجلة الأمن العام، العدد 43، سنة 1968 ص19 و ما بعدها.

أولا: القواعد القانونية التي تحكم الخبرة القضائية

وسنتناول من خلالها مفهوم الخبرة القضائية، طرق اختيار الخبراء، وواجبات الخبير التقني وذلك من خلال النقاط التالية:

1- مفهوم الخبرة القضائية

أ – تعريف الخبرة

يقصد بالخبرة: "مساعدة فنية تقدم للقاضي أو المحقق في مجال الإثبات لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقريرها إلى معرفة فنية أو دراية علمية لا تتوافر لديه" [116].

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

كما يعرف الخبير الإلكتروني بأنه الشخص الذي تكمن له دراية بمسألة من المسائل وله كفاءة فنية وعلمية خاصة [117].

ب- طرق اختيار الخبراء

إذا كانت الاستعانة بالخبير في الجرائم التقليدية أمر بالغ الأهمية في إثبات الجريمة، فإن الاستعانة به في مجال إثبات الجرائم الإلكترونية يعد أمرا متطلبا و ضروريا بسبب التطور التقني السريع في مجال تقنية المعلومات، إذ لا يكشف غموض الجريمة إلا من طرف شخص على درجة كبيرة من العلم والدراية في مجال تخصصه[118]، حيث يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة كما تحدد الأوضاع التي يجري فيها قيد الخبراء أو شطبهم بقرار من وزير العدل [119].

وقد ترك المشرع لقاضي التحقيق حرية ندب خبير واحد أو خبراء متعددين بحسب المادة 147 من قانون الإجراءات الجزائية الجزائري، التي جاء في فحواها بصفة عامة أنه في إمكان القاضي الجنائي أن يندب أكثر من خبير، بغرض حل الدعوى المطروحة أمامه، فقد لا يطمئن القاضي الجنائي لرأي خبير فني وتقني واحد فيلجأ لرأي عدة خبراء.

([116]) صغير يوسف، الجريمة المرتكبة عبر الانترنت، ماجستير، منشورة، جامعة مولود معمري، كلية الحقوق والعلوم السياسية، الجزائر، 2013، ص88.

([117]) عبد الناصر محمد محمود فرغلي، المرجع السابق، ص24.

([118]) David forest et gautier kaufman, **droit de l'informatique gualino éditeur**, extenso édition, France , 2010, p79, 80

([119]) نصت المادة 144 من(ق.إ.ج.ج) على:"يختار الخبراء من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة العامة، وتحدد الأوضاع التي يجري بها قيد الخبراء أو شطب أسمائهم بقرار من وزير العدل..."

وكذلك لم يحدد المشرع طبيعة من يقوم بالخبرة سواء كان شخصا طبيعيا، أو معنويا كمؤسسة متخصصة تعمل في مجال الحاسوب الذين يتم اللجوء إليهم خاصة في مجال الدليل الإلكتروني باعتبار أن هذا النوع من المؤسسات يملك موارد مادية من برامج و أجهزة حديثة وموارد بشرية من مهندسين متخصصين في الحاسوب و الانترنت [120].

ج- واجبات الخبير التقني: له عدة واجبات تتمثل في:

- **حلف اليمين:** أوجب المشرع الجزائري لضمان صحة تقرير الخبير ونيل ثقة أطراف الدعوى، أن يحلف اليمين[121] قبل البدء في انجاز الخبرة .
- **إنجاز الخبير لأعمال الخبرة بنفسه:** لابد على الخبير أن يقوم بأعمال الخبرة بنفسه وفي حدود ما نص عليه أمر أو حكم الندب، وأن يستجيب للطلبات التي يقدمها أطراف الخصومة مثل: سماع أي شخص قادر على إعطاء معلومات فنية[122].
- **الخضوع للرقابة القضائية:** يتعين على الخبير أن يتولى مهمته تحت رقابة القاضي الذي عينه وأن يبقى على اتصال دائم به لأجل إحاطته علما بتطورات الأعمال التي يقوم بها، فالخبير هو مساعد للقاضي ومعاون فني لا أكثر [123].
- **إيداع الخبرة التقنية:** بعد انتهاء الخبير من أعماله التي كلف بها يقوم بإيداع الخبرة التقنية خلال المدة المحددة في أمر أو حكم الندب، وأن يقدم نتائج ما قام به من أبحاث فإن خال ذلك جاز للقاضي استبداله بغيره، كما يمكن أن يتخذ في حق الخبير الذي ثبت وقوع إهمال منه إجراءات تأديبية قد تصل إلى شطب اسمه من جداول الخبراء بقرار من الوزير[124].

([120]) عائشة بن قارة مصطفى، المرجع السابق، ص ص141- 142.

([121]) حيث تنص المادة 145 من قانون الإجراءات الجزائية على: "يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتية بيانها، أقسم بالله العظيم أن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص و أن أبدي رأي بكل نزاهة و استقلال. و لا يجدد هذا القسم ما دام الخبير مقيدا في الجدول..."

([122]) المادة 152 من قانون الإجراءات الجزائية الجزائري المعدل والمتمم.

([123]) Michaud le juge d'instruction et l'expert, R. S. c , 1975,p791.

([124]) حيث تنص المادة 148 من قانون الإجراءات الجزائية على: " كل قرار يصدر بندب خبراء يجب أن تحدد فيه مهلة لإنجاز مهمته ويجوز أن تمتد هذه المهلة بناء على طلب الخبراء إذا اقتضت ذلك أسباب خاصة ويكون ذلك بقرار مسبب يصدره القاضي أو الجهة التي ندبتهم، وإذا لم يودع الخبراء تقاريرهم في الميعاد المحدد لهم جاز في الحال أن يستبدل بهم غيرهم وعليهم إذ ذلك أن يقدموا نتائج ما قاموا به من أبحاث. كما عليهم أيضا أن يردوا في ظرف ثمان وأربعين ساعة جميع الأشياء والأوراق والوثائق التي تكون قد عهد بها إليهم على ذمة إنجاز مهمتهم....ويجوز دائما لقاضي التحقيق أثناء إجراءاته أن يستعين بالخبراء إذا رأى لزوما لذلك".

الفرع الثاني: التفتيش والضبط في البيئة الإلكترونية

يعتبر التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر والغرض منه هو ضبط كل ما يفيد في كشف الحقيقة عن الجريمة التي يجري التحقيق أو جمع الاستدلالات بشأنها، ومعنى ضبطها هو ضعها تحت يد السلطة العامة للتحفظ عليها إلى حين انتهاء الإجراءات في الدعوى الجنائية[125]. ومنه سنتعرف في هذا الفرع على التفتيش في(الفقرة الأولى) والضبط في(الفقرة الثانية).

الفقرة الأولى: التفتيش

يختلف التفتيش في الجرائم المعلوماتية عن التفتيش المعروف في الجرائم التقليدية، ويرجع ذلك لعدة اعتبارات.

أولا: تعريف التفتيش

يجمع الفقه الجنائي على أن التفتيش هو "إجراء من إجراءات التحقيق يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في مكان يتمتع بحرمة، وذلك وفقا للضمانات والقيود القانونية المقررة" [126].

والتفتيش هو "التنقيب في وعاء السر بقصد ضبط ما يفيد من معلومات في كشف الحقيقة، وهو كشف نقاب السرية عما تحويه نظم الحاسوب من خفايا ونوايا إجرامية، وبالتالي إزاحة ستار الكتمان عنها للاستفادة منها في معرفة الحقيقة"، وهذا المعنى لا يتقيد بالكيان المادي للحاسوب والأجهزة الملحقة به بل يشمل كذلك كيانه المنطقي من شبكات أو أنظمة و برمجيات [127].

إذا فالتفتيش ليس غاية في حد ذاته، وإنما وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تسهم في كشف الحقيقة [128].

ثانيا: شروط التفتيش

للتفتيش شروط موضوعية وأخرى شكلية، سنعرضها على النحو التالي:

---

[125] فرج علواني هليل، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، دار المطبوعات الجامعية، مصر، 2006 ص622.

[126] نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2013، ص143.

[127] علي حسن محمد الطوالبة، التفتيش الجنائي في نظم الحاسوب والإنترنت، دراسة مقارنة، عالم الكتب الحديثة، الأردن 2004، ص28.

[128] أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، الإسكندرية، مصر، 2015 ص140.

أ- الشروط الموضوعية للتفتيش: ويمكن تقسيمها إلى شرطين أساسيين هما السبب والمحل.

1- سبب التفتيش في البيئة المعلوماتية: وهو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث[129]، ويتمثل في:

- وقوع جريمة من الجرائم الإلكترونية بالفعل سواء كانت جناية أو جنحة.
- اتهام شخص أو أشخاص معينين بارتكاب جريمة أو المشاركة فيها.
- توافر أمارات قوية أو قرائن على وجود بيانات أو معدات معلوماتية تفيد في كشف الحقيقة لدى المتهم المعلوماتي أو غيره [130].

2- محل التفتيش في البيئة المعلوماتية: ويتمثل محل التفتيش في الجريمة المعلوماتية في المكونات المادية والمعنوية للحاسوب وكذا شبكات الاتصال الخاصة به، ويستوي أن يكون محل التفتيش بحوزة شخص معين أو موجود في مكان ما كالمسكن أو المكتب [131].

ب- الشروط الشكلية للتفتيش

- أن يتم تفتيش النظم المعلوماتية بأسلوب إلكتروني من قبل الأجهزة القائمة بالتحقيق.
- يجب أن يكون الإذن بالتفتيش مسببا حتى تتمكن الجهة القضائية من مراقبة مدى مشروعيتة.
- كما ينبغي في نهاية التفتيش تحرير محضر للتفتيش يثبت فيه ما تم من إجراءات وما أسفر عنه التفتيش من أدلة، ويشترط أن يكون المحضر مكتوبا باللغة الرسمية [132].

ثالثا: مدى قابلية مكونات و شبكات الحاسب الآلي للتفتيش:

كما أن له شبكات saftware ومكونات منطقية hardware يتكون النظام المعلوماتي من مكونات مادية اتصالات بعدية سلكية ولاسلكية سواء على المستوى المحلي أو على المستوى الدولي[133].

أ- تفتيش المكونات المادية للحاسوب:

بخصوص تفتيش المكونات المادية للحاسوب لا توجد صعوبة في ذلك، لأنه يرد على عناصر مادية لا خلاف للقانون فيها، فتطبق بشأنه القواعد التقليدية للتفتيش، لكن مع الأخذ بعين الاعتبار القواعد الخاصة

---

[129] نبيلة هبة هروال، المرجع السابق، ص229.

[130] عبد العال الدريبي و محمد صادق إسماعيل، الجرائم الإلكترونية، دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، مصر 2012، ص305.

[131] خالد عياد الحلبي، المرجع السابق، ص154.

[132] أشرف عبد القادر قنديل، المرجع السابق، ص151.

[133] عائشة بن قارة مصطفى، المرجع السابق، ص88.

بضبط هذه الأجهزة لحساسيتها وإمكانية تعريضها للتلف، كما تطبق على إجراء التفتيش الضمانات المقررة قانونا [134].

ب- تفتيش المكونات المنطقية للحاسوب

ولما كان التفتيش وسيلة للإثبات المادي، لا غاية في حد ذاته، فهو إجراء يسعى إلى ضبط الأدلة المادية المتعلقة بالجريمة لتقديمها إلى المحكمة كدليل إدانة، فإن التساؤل يثور حول إمكانية اعتبار تفتيش المكونات المنطقية للحاسب الآلي نوعا من التفتيش باعتبار أن البيانات الإلكترونية أو البرامج في حد ذاتها ليس لها مظهر مادي محسوس في المحيط الخارجي. وقد انقسم الفقه في هذا الشأن إلى اتجاهين:

- **الاتجاه الأول:** تتجسد فكرة هذا الرأي في عدم إمكانية انسجام وتطابق أحكام التفتيش في القانون الجنائي الإجرائي مع ما قد يتطلبه كشف الحقيقة في الجرائم المعلوماتية. إذ أن التفتيش يقتصر مفهومه على أشياء ذات حيز مادي ملموس.
- **الاتجاه الثاني:** يرى أنصار هذا الاتجاه أن برامج الحاسوب يمكن أن تطبق عليها خصائص وسمات المادة، وهو ما يجعلها تدخل في نطاق الأشياء المادية ويستوي في ذلك أن تكون برامجا أو تطبيقات حاسوبية، مستندين في ذلك إلى أن الكيان المنطقي للحاسوب أو البرنامج يشغل حيزا ماديا في ذاكرة الحاسوب ويمكن قياسه بمقياس معين مثل البايت (byte) و الميغابايت MB [135].

وبخصوص موقف المشرع الجزائري فهو يتضح جليا من خلال القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها حينما أجاز صراحة بموجب نص المادة 5 منه تفتيش المنظومات المعلوماتية[136].

إذا فالمشرع الجزائري قد حسم بذلك الجدل القائم حول مدى قابلية النظام المعلوماتي للتفتيش فيه.

الفقرة الثانية: ضبط الدليل الإلكتروني

إن الأدلة الرقمية المضبوطة أثناء عملية التفتيش لها أهمية كبيرة في إثبات الواقعة الجرمية ونسبتها لمرتكبها من عدمها و بالتالي الحكم عليه بالإدانة أو البراءة.

---

[134] فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و17 نوفمبر، 2015، كلية الحقوق، بسكرة، الجزائر، ص3.

[135] نعيم سعيداني، المرجع السابق، ص146.

[136] طبقا للمادة 5 من القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فإنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، الدخول بغرض التفتيش إلى منظمة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

أولا: مفهوم ضبط الأدلة

سنتناول في هذا العصر تعريف ضبط الدليل وأنواع الأدلة القابلة للضبط .

أ- تعريف ضبط الأدلة

يعتبر ضبط الأشياء أثرا من آثار المعاينة والتفتيش باعتبارهما يؤديان إلى جمع الأدلة المادية وأدوات ارتكاب الجرائم، وبيان مدلولاتها من أجل الاستفادة منها في إثبات الوقائع الجنائية ونسبتها إلى مرتكبه، فضبط الأدلة إذا لا يخرج عن كونه وضع اليد على شئ يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، وقد يرد الضبط على منقولا أو عقارا ويستوي أن يكون الشئ المضبوط مملوكا للمتهم أو لغيره [137].

ب- الأدلة القابلة للضبط

توجد العديد من أدلة الإثبات القابلة للضبط في مجال الجرائم المعلوماتية، ومن أهم هذه الأدلة نذكر ما يلي:

- المخرجات الورقية والمستندات التي تفيد الكشف عن الجريمة.
- أجهزة الحاسوب الآلي وملحقاتها مثل وحدات المعالجة المركزية أجهزة لوحة المفاتيح وغيرها.
- الأقراص المرنة والشرائط الممغنطة والتي قد تحتوي معلومات تفيد في مجريات التحقيق.
- أجهزة المودم وهي الوسائل التي تمكن الحواسيب من الاتصال ببعضها.
- مختلف برامج الحاسوب حيث تعتبر الأدوات الرئيسية التي يستعملها الجاني في تنفيذ جرائمه.
- البطائق الممغنطة وبطائق الائتمان والمواد المستعملة في إعدادها حيث تعتبر من قرائن الإثبات[138].

ثانيا: مدى قابلية جرائم الحاسوب لضبط أدلتها:

ونفرق في ذلك بين حالتين:

أ- ضبط الأدلة المادية للجريمة:

لا يثار أي إشكال بشأن ضبط الأدلة المادية التي تفيد في كشف الحقيقية سواء كانت أجهزة حاسوب أو ملحقاته أو غيرها من الأشياء المنقولة، حيث أنه يمكن تحريزها، أما العقارات التي تحتوي على أجهزة الحاسوب وشبكاته فيتم التحفظ على ما تشتمل عليه من آثار للجريمة المعلوماتية أو أشياء يتعذر نقلها، عن طريق وضع الأختام على هذه الأماكن وتعيين السلطة المختصة حارسا عليها [139].

---

[137] (عبد العال الدريبي، المرجع السابق، ص320 ,)

[138] (ضياء علي أحمد نعمان، المرجع السابق، ص ص374 – 375 .)

[139] (علي حسن محمد طوالبة، المرجع السابق، ص142.)

ب-ضبط المكونات المنطقية للحاسوب:

لقد سمح المشرع الجزائري للمحقق بحجز معطيات الحاسب الآلي، مع إمكانية نسخها إذا لم يكن هنالك داعي لحجز المنظومة المعلوماتية برمتها، بالإضافة إلى ذلك منحه سلطة استعمال الوسائل التقنية لتشكيل أو إعادة تشكيل هذه المعطيات ثم حجزها ووضع الأختام عليها، طبقا لقانون الإجراءات الجزائية وفي حالة تعذر حجز هذه الأدلة لأسباب تقنية يتعين على السلطات المختصة بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات ومنع الإطلاع عليها، وذلك بتكليف أشخاص مؤهلين في هذا المجال[140]، وهو الأمر الذي تناوله المشرع بالنص في المادة 6 من القانون رقم 09-04 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

الفرع الثالث: الشهادة الإلكترونية

في هذا الفرع سنعرف الشهادة بمختلف جوانبها في (الفقرة الأولى)، ثم نحدد مختلف فئات الشاهد المعلوماتي (الفقرة الثانية)، وفي الأخير نتطرق إلى التزام الشاهد المعلوماتي في (الفقرة الثالثة).

الفقرة الأولى: تعريف الشهادة

لم يتطرق المشرع الجزائري إلى تعريف الشهادة وترك ذلك للفقه والاجتهاد القضائي لكنه بالمقابل قام بتنظيمها وتحديد مجالها وشروط قبولها وحجيتها في الإثبات [141].

"تعتبر الشهادة إجراء من إجراءات التحقيق، وهي الأقوال التي يدلي بها غبر الخصوم أمام سلطة التحقيق بشأن جريمة وقعت، سواء تعلقت تلك الأقوال بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها"[142]، ويختلف الشاهد في مجال الجرائم المعلوماتية عن الشاهد في سائر الجرائم.

أولا: الشاهد في الجرائم التقليدية:

"وهو كل شخص تناهت إلى علمه عن طريق حواسه معلومات عن واقعة إجرامية، وعليه الإدلاء للسلطات القضائية بكل ما يفيد في كشف الحقيقة عنها".

---

[140] أمال حابت، الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري، ورقة بحثية مقدمة (لأعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر، ص17.

[141] القسم الرابع من الفصل الأول من الباب الثالث تحت عنوان: سماع الشهود، المواد 88،99 من قانون الإجراءات الجزائية (الجزائري، والتي تتلخص حول استدعاء الشهود وحضورهم وكيفية تلقي إفاداتهم وحلف اليمين والحالات التي لا يجوز فيها سماع الشخص كشاهد ونصاب الشهادة...الخ.

[142] (علي عدنان الفيل، المرجع السابق، ص61 .

ثانيا: الشاهد في الجرائم المعلوماتية:

"وهو ذلك الفني صاحب الخبرة والتخصص في تقنية الحاسب وشبكات الاتصال والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات، إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله"، ويطلق على هذا النوع من الشهود مصطلح "الشاهد المعلوماتي" وذلك تمييزا له عن الشاهد التقليدي [143].

الفقرة الثانية: فئات الشاهد المعلوماتي

يمكن القول أن الشهود في الجرائم المعلوماتية ينحصرون ضمن إحدى الطوائف التالية:

أ- **مشغل الحاسب الآلي:** وهو كل شخص مسؤول عن تشغيل الحاسوب والمعدات المتصلة به ولابد أن تكون لديه خبرة كبيرة وواسعة في هذا الميدان.

ب- **المبرمجون:** وهم الأشخاص المتخصصون في كتابة أوامر البرامج، وهم فئتين الأولى هم مخططوا برامج التطبيقات والثانية هم مخططوا برامج النظم [144].

ت- **المحللون:** فالمحلل هو ذلك الشخص الذي يقوم بتجميع البيانات الخاصة بنظام معين، ثم تقسيمها على وحدات منفصلة بغية استنتاج العلاقة الوظيفية بينها.

ث- **مهندسوا الصيانة والاتصالات:** وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

ج- **مديروا النظم:** الذين توكل لهم أعمال الغدارة في النظم المعلوماتية [145].

الفقرة الثالثة: التزام الشاهد الإلكتروني (المعلوماتي)

يتعين على الشاهد في حال حصوله على معلومات تفيد بارتكاب جريمة أن يعلم بها السلطات يدفعنا لتحديد المختصة على سبيل الإلزام، وهو ما يعبر عنه بالالتزام بالإعلام في الجريمة المعلوماتية، مما السمات الجوهرية لهذا الالتزام وشروطه، ولكن قبل التعرض لذلك سنحاول البحث في مدى إمكانية إجبار الشاهد على تقديم معلومات تتعلق بالجريمة [146].

---

[143] خالد ممدوح إبراهيم المرجع السابق، ص263.)

[144] عبد الفتاح بيومي حجازي، الجزائب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة على ضوء (القواعد العامة للإجراءات الجنائية، ط1، دار النهضة العربية الإسكندرية مصر، 2009، ص ص612 - 613.

[145] علي عدنان الفيل، المرجع السابق، ص63.)

[146] رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين (الوقاية والمكافحة، يومي 16، 17نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر، 2015، ص5.

أولا: مدى التزام الشاهد بتقديم إفادته

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله لكن بالمقابل يثار التساؤل: هل أن الشاهد المعلوماتي ملزم بطبع ملفات البيانات المخزنة في ذاكرة الحاسب؟ أو هل يجوز له الإفصاح عن كلمات المرور السرية والشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج؟.

في هذا الصدد برز هناك اتجاهان نتطرق إليهما كما يأتي:

أ- **الاتجاه الأول:** يرى القائلين بهذا الرأي أنه ليس من واجب الشاهد المعلوماتي أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة، ويميل إلى هذا الاتجاه الفقه الجنائي الألماني، على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب [147].

ب-**الاتجاه الثاني:** على عكس الأول يرى أنصار الاتجاه الثاني، أن من بين الالتزامات التي يتحملها الشاهد القيام بطباعة ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة[148]، وقد أخذ المشرع الجزائري على غرار المشرع الفرنسي بهذا الاتجاه حيث ألزم كل شخص له إطلاع ودراية بعمل المنظومات المعلوماتية، بمساعدة السلطات المختلفة وتزويدها بكافة المعلومات الضرورية لإنجاح مهامها [149].

ثانيا: التزام الشاهد بالإعلان في الجريمة المعلوماتية

ويعني ذلك باختصار أنه في الجرائم المعلوماتية ومتى كان الشاهد حائز المعلومات جوهرية لازمة لاختراق نظام المعالجة الآلية للبيانات بحثا عن أدلة للجريمة داخلها، فإنه يكون مطالبا بإعلام سلطات التحري والتحقيق على سبيل الإلزام وإلا تعرض للعقوبات المقررة للامتناع عن الشهادة [150].

ثالثا: خصائص التزام الشاهد المعلوماتي:

مما سبق ذكره يتبين لنا أن هذا الالتزام له مجموعة من السمات الجوهرية هي:

- التزام الشاهد بالإعلام التزام قانوني.
- الالتزام بالإعلام التزام مستقل له ذاتيته الخاصة.

---

[147] علي عدنان الفيل، المرجع السابق، ص64.

[148] رضا هميسي، المرجع السابق، ص06.

[149] أنظر: الفقرة 4 من المادة 5 من قانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها.

[150] عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية، المرجع السابق، ص ص613 - 614 .

- يعتبر الالتزام بالإعلام التزام وقائي [151].

رابعا: شروط التزام الشاهد المعلوماتي بالإعلام:

تتمثل هذه الشروط في ما يلي:

- وقوع جريمة معلوماتية بالفعل.
- علم الشاهد ومعرفته بالمعلومات المتعلقة بالجريمة.
- أن تقتضي مصلحة التحقيق الحصول على معلومات من قبل الشاهد [152].

المطلب الثاني: الإجراءات الحديثة لجمع الدليل الإلكتروني

تطرقنا في المطلب السابق على الإجراءات التقليدية لجمع الدليل الإلكتروني وبالرجوع إلى الأنظمة القانونية الإجرائية الحالية، يلاحظ أن هناك قصورا بخصوص أساليب التحري التقليدية في استخلاص الدليل الإلكتروني. فالمشرع أجاز استخلاص الدليل عموما وفق ضوابط إجرائية معينة منها: الانتقال والمعاينة، الخبرة ، التفتيش وضبط الأدلة، الشهادة... الخ، كما أن هذه الإجراءات تخص استخلاص الدليل من الجرائم سواء كانت تقليدية أم مستحدثة، والأكيد أن هذه الإجراءات غير كافية لاستيعاب كافة أشكال الجريمة الالكترونية، فهي تحتاج من المشرع تعديلها أو استحداث أخرى جديدة لمواكبة التطورات التقنية المتلاحقة في مجال مكافحة الجريمة الالكترونية، وهذا ما قام به المشرع الجزائري من خلال التعديلات المتتالية لأحكام قانون الإجراءات الجزائية، وذلك بإدراج قواعد إجرائية جزائية جديدة وفي الوقت نفسه أحاطها بجملة من الضمانات بهدف عدم المساس بحرمة الحياة الخاصة للأفراد[153].

وعليه ارتأينا تقسيم هذا المطلب إلى فرعين، نتناول الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب المادة (65 مكرر 5 إلى 65 مكرر 18) في (الفرع الأول) ثم نتطرق بعدها إلى الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب القانون 09-04 في (الفرع الثاني).

الفرع الأول: الإجراءات الحديثة لجمع الدليل الإلكتروني بموجب المادة(65 مكرر 5 إلى 65 مكرر 18) من قانون الإجراءات الجزائية.

قام المشرع الجزائري باستحداث أساليب جديدة في التحري ولو اعتبرها البعض بأنها تمس بالحياة الخاصة للأفراد وانتهاكا لحق كفله الدستور ولأن الضرورات تبيح المحظورات والمصلحة المحمية أولى جعل

---

(151) رضا هميسي، المرجع السابق، ص10.)

(152) المرجع نفسه، ص ص10- 11.)

(153) يزيد بوحليط، المرجع السابق، ص 248.)

المشرع من اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب أهم الأساليب المستخدمة للكشف عن الجرائم الإلكترونية.

ونظرا لأهمية هذه الوسائل ولما تشكله من مساس بحرية الأفراد وانتهاك لخصوصياتهم، ارتأينا إلى تقسيم هذا الفرع إلى ثلاث فقرات، تطرقنا إلى المقصود باعتراض المراسلات والتقاط الصور وتسجيل الأصوات في (الفقرة الأولى)، في حين تناولنا الضوابط التي تحكم اعتراض المراسلات والتقاط الصور وتسجيل الأصوات في (الفقرة الثانية)، وفي الأخير تطرقنا إلى التسرب في (الفقرة الثالثة).

الفقرة الأولى: المقصود باعتراض المراسلات والتقاط الصور وتسجيل الأصوات

من خلال هذه الفقرة، سنتناول مفهوم مفصل لكل إجراء على حدة.

أولا: مفهوم اعتراض المراسلات:

يقصد باعتراض المراسلات على أنه "إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة تأمر به السلطات القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث وتتم بواسطة الوسائل السلكية واللاسلكية" [154].

من جانب آخر نجد المشرع الجزائري لم يعرف بإجراء اعتراض المراسلات، بل اكتفى بوضع بتنظيم لهذه العملية بموجب المادة(65 مكرر 5) من قانون الإجراءات الجزائية التي تنص على: "إذا اقتضت ضروريات التحري في الجريمة الملتبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي:

- اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية.
- وضع الترتيبات التقنية دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو بسرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص..." .

باعتبار المشرع الجزائري لم يتطرق إلى تحديد مفهوم اعتراض المراسلات فهل يقصد بها التنصت الهاتفي أم مجرد الاطلاع عليها؟ أو يمتد إلى أكثر من ذلك من خلال ضبط كل ما له علاقة بوسائل المواصلات السلكية واللاسلكية؟

---

[154] (سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماستر أكاديمي، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2014، ص32.

باستقراء نصوص المواد (100-107) من قانون الإجراءات الجزائية الفرنسي[155]، يتبين أن اعتراض المراسلات تتعلق بتلقي مراسلة مهما كان نوعها بغض النظر عن وسيلة إرسالها وتلقيها سلكية أو غير سلكية أو ورقية[156]، كما عرفت لجنة الخبراء للبرلمان الأوروبي Supportيتم تثبيتها وتسجيلها على دعامة إلكترونية المنعقدة بستراسبورغ بتاريخ 06-10-2006، حول أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية اعتراض المراسلات على أنها: "عملية مراقبة سرية المراسلات السلكية واللاسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم أو مشاركتهم في ارتكاب الجريمة" [157].

ثانيا: مفهوم تسجيل الأصوات

يعرف التسجيل الصوتي بأنه: "النقل المباشر والآلي للموجات الصوتية من مصادره بنبراتها ومميزاتها الفردية وخواصها الذاتية، بما تحمل من عيوب في النطق إلى شريط التسجيل لحفظ الإشارات الكهربائية على هيئة مخطط مغناطسي بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه"[158]. كما تتم هذه العملية باستخدام وسائل تقنية خاصة لها صلة مباشرة بنوعيها السلكية واللاسلكية، والتي من خلالها يتم بث الكلام المتفوه وتثبيته واستغلاله في التحريات، وهو إجراء تحقيقي تأمره به السلطة القضائية خلسة وينتهك سرية الأحاديث الخاصة بغية الحصول على دليل غير مادي للجريمة[159].

إلا أن المشرع الجزائري لم ينص في قانون الإجراءات الجزائية على تعريف التسجيل الصوتي مثل ما لم ينص على تعريف اعتراض المراسلات كما رأينا سابقا، إنما أشار لها في نص المادة (65 مكرر في الفقرة

([155]) Article 100 du (cppf) : "En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou superieur à deux ans d'emprisonnement, le juge d'instruction peut lorsque les necessités de l'information l'exigent, pre scrire l'interception l'enregistrement et la transcription de corespondance émises par la voix des télécommunications. Ces operations sont éffectuées sous son autorité et son controle. La decision d"interception est ecrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d"aucun recours."

([156]) عبد المجيد حجازي، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2012، ص62.

([157]) رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2012، ص442.

([158]) سارة قادري، المرجع السابق، ص34.

([159]) حافظ بن زلاط، التنصت الهاتفي في ظل قانون الإجراءات الجزائية، بحث متوفر على الموقع الرسمي لمجلة (القانون والأعمال) لسنة 2015، على الرابط الآتي: http://www.droitentreprise.org/web/ بتاريخ 2018/04/10، على الساعة: 22.00 سا.

المعنيين من أجل التقاط وتثبيت وبث تسجيل الكلام المتفوه به بصفة 2) "وضع الترتيبات التقنية دون موافقة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية" [160].

وعليه فإن التسجيلات التي يقوم بها الأفراد فيما بينهم لا تعد من قبيل الإجراءات الجنائية نظرا لأنها لم تصدر في شأن دعوى جنائية حركتها السلطات القضائية قصد الوصول إلى الحقيقة، كما لا تعتبر أدلة، واستغلال التسجيل الذي لا يتضمن اعتداء على حق من تم تسجيل صوته أو حديثه، كما هو الشأن في حالة تسجيل الأحاديث الإذاعية أو التلفزيونية أو الصحفية.

ثالثا: مفهوم التقاط الصور:

تعتبر عملية التقاط الصور الفوتوغرافية من الإجراءات الجديدة التي جاء بها المشرع الجزائري لمكافحة الجرائم المستحدثة ومنها الجرائم الإلكترونية، غير أنه ومثل الإجراءات السابقة لم يتطرق إلى تعريف هذا الإجراء، وإنما نص على مجال تطبيقه وتوضيح إجراءات القيام بذلك، يقوم هذا الإجراء أساسا على استخدام الكاميرات، أو أجهزة خاصة لالتقاط صورة للمشتبه فيه على الحالة التي كان عليها وقت التصوير بغرض استخدام هذه الصورة كدليل مادي، على اعتبار أن عدسة الكاميرا أصبحت من الأساليب العالمية والمطلوبة لإثبات الحالة بما تنقله من صور حية لحادثة معينة[161].

لقد شاع اليوم استخدام كاميرات رقمية بغرض المراقبة في الأماكن العامة والخاصة كالبنوك والمطارات وماكينات الصرف الآلي والمحلات والمستشفيات...الخ قصد ضبط الجرائم وإثباتها[162] ويكون الاطلاع على صور هذه الكاميرات في حالات وقوع الجرائم بأمر من المحكمة، ولاشك أن ذلك يثير قضايا تتعلق بالخصوصية الشخصية. لذا يرى جانب من الفقه أن تركيب هذه الكاميرات يكون في الأماكن العامة فقط و بترخيص قانوني [163].

وعليه يربط هذا الإجراء الشخص أو الأشخاص في مكان واحد وفي وقت واحد، خاصة في ظل التطور التكنولوجي الرقمي الذي يسمح بالتصوير ليلا وبجودة عالية من خلال الكاميرا ذات العدسات فائقة

---

[160] عباسي خولة، الوسائل الحديثة للإثبات الجنائي في القانون الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية حقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة، 2013، ص22.

[161] فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط صور والتسرب كالإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة قسنطينة1، الجزائر، العدد 33، جوان 2010.

[162] سارة قادري، المرجع السابق، ص39.

[163] عبد الفتاح بيومي حجازي، الجوانب الإجرائية، المرجع السابق، ص782.

التكبير والتي تستخدم أيضا الأشعة تحت الحمراء بما يمكن ضابط الشرطة القضائية من التقاط الصور الثابتة أو المتحركة للمشتبه فيه خلال جميع مراحل البحث والتحري[164].

الفقرة الثانية: الضوابط التي تحكم اعتراض المراسلات والتقاط الصور وتسجيل الأصوات

حدد المشرع الجزائري من خلال قانون الإجراءات الجزائية شروط للقيام بهذا الإجراءات كونها تشكل انتهاكا لحرمة الحياة الخاصة للأفراد، واعتداء على سرية مراسلاتهم واتصالاتهم.

أولا: الشروط الشكلية:

تتعلق بالضوابط الشكلية بإجرائيين هما:

أ- الحصول على إذن من طرف وكيل الجمهورية: لابد من ضابط الشرطة القضائية الذي يباشر هذا الإجراء في عملية التحري والبحث، أن يكون مستندا في ذلك على إذن من وكيل الجمهورية يخوله اللجوء إلى إجراء التقاط الصور واعتراض المراسلات وتسجيل الأصوات، وكذلك يمكن لضابط الشرطة القضائية أن يحصل على الإذن من طرف قاضي التحقيق المختص إذا كانت القضية معروضة عليه[165]، وفي حالة قيام ضابط الشرطة القضائية بممارسة الإجراء دون إذن، فإن إجراءه الذي قام به يقع تحت طائلة البطلان.

ويشترط في الإذن أن يكون مكتوبا، ويتضمن عمل العناصر التي تسمح بالتعرف على الأشخاص المراد التقاط أو بث أو تسجيل أحاديثهم وكذا الأماكن المقصودة سواء كانت عامة أو خاصة وكذا الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، يسلم الإذن مكتوبا لمدة أقصاها 4 أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق [166].

ب-تحرير محضر عن العملية: باعتبار محاضر الشرطة القضائية لها حجية في الإثبات، وجب على ضابط الشرطة القضائية الذي قام بإجراء اعتراض المراسلات والتقاط الصور وتسجيل الأصوات أن يقوم بتحرير محضر موقع عليه من طرفه، يسرد فيه بالتفصيل العمليات التي قام بها [167].

---

[164] نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة للكتاب، طرابلس لبنان، ط1، 2011، ص154.

[165] أنظر: المادة 65 مكرر 5 من القانون رقم 06-22 المؤرخ في 20-12-2006، المعدل والمتمم لقانون الإجراءات الجزائية، الصادر بالجريدة الرسمية للجمهورية الجزائرية، عدد 84، المؤرخة في 24 ديسمبر 2006.

[166] أنظر: المادة 65 مكرر 5 من القانون رقم: 06-22، المعدل والمتمم لقانون الإجراءات الجزائية.

[167] أنظر: المادة 65 مكرر 9 من القانون رقم: 06-22 المعدل والمتمم لقانون الإجراءات الجزائية.

أما مضمون المراسلات المسجلة والصور الملتقطة، فيقوم ضابط الشرطة بنسخ محتواها في محضر يودع بملف الإجراءات، أما إذا كانت تلك المراسلات أو الاتصالات بلغة أجنبية فيتم تسخير مترجم لترجمتها [168].

تتم عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور بتسخير أعوان مصالح الاتصالات السلكية واللاسلكية سواء العمومية أو الخاصة للتكفل بالجوانب التقنية للعملية، وهذا بموجب نص المادة (65 مكرر 8) [169].

ثانيا: الضوابط الموضوعية:

تتعلق هذه الضوابط بنشوء الحق في اللجوء إلى اعتراض المراسلات والتقاط الصور وتسجيل الأصوات، وتتمثل هذه الضوابط في:

- أن يكون الإجراء من أجل التحري والكشف عن الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.
- غاية المراقبة وضرورتها، عبر المشرع الجزائري عن المصطلح بلفظة: "إذا اقتضت ضرورة التحري في الجريمة الملتبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد..."، وهذا حسب المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري.

يتضح من خلال نص هذه المادة أن اللجوء لهذا الإجراء لا يتم إلا في حالة الضرورة التي تفرض استعمال تلك الوسائل لكشف الجريمة دون غيرها من الوسائل التقليدية.

ح- الجهة المكلفة بهذه العملية:

باعتبارها تمس بحرمة الحياة الخاصة، لا يقوم بها إلا ضابط الشرطة القضائية.

ثالثا: ضوابط التنفيذ:

تتعلق بكيفيات المراقبة ونتائجها والأدلة الناجمة عنها، لذا سمح المشرع من خلال نص المادة (65 مكرر 5 الفقرة 4)، لضابط الشرطة القضائية الدخول إلى المكان المعني دون احترام الشروط الواردة في المادة 47 من قانون الإجراءات الجزائية وذلك باستخدام الترتيبات التقنية، حيث نصت الفقرة الثانية من المادة 65

---

[168] أنظر: المادة 65 مكرر 10 من القانون رقم: 06-22 المعدل والمتمم لقانون الإجراءات الجزائية.

[169] حيث تنص المادة 65 مكرر 8 من قانون الإجراءات الجزائية على: "يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له، ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالعمليات المذكورة في المادة 65 مكرر 5 أعلاه."

مكرر 05 على أن النيابة العامة يمكنها منح الإذن لضابط الشرطة القضائية لوضع الترتيبات التقنية، التي يتم عن طريقها التصنت على المحادثات وتسجيلها والتقاط الصور دون الحاجة إلى موافقة المشتبه فيه [170].

وتكمن تلك الترتيبات في وضع أجهزة التصنت وتسجيل الكلام الذي يتفوه به المشتبه فيه خاصة فيما يتعلق بموضوع الجريمة، إضافة إلى زرع وسائط التقاط الصور والغرض دائما من كل ذلك هو الحصول على أدلة تدين الأشخاص الذين يشتبه فيهم القيام بالجريمة.

وفي حالة اكتشاف جرائم أخرى غير تلك التي يتم التحقيق فيها والواردة في الإذن فيمكن التحري بشأنها ولا يكون ذلك سببا في بطلان الإجراءات وهذا حسب أحكام المادة 65 مكرر 6 من قانون الإجراءات الجزائية الجزائري.

الفقرة الثالثة: التسرب

استحدث المشرع الجزائري إجراء التسرب بموجب المادة 65 مكرر 11 من قانون الإجراءات الجزائية الجزائري التي تنص على: "عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابة حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبنية في المواد أدناه".

وبخلاف إجراءات التحري السابقة الذكر التي لم يعرفها المشرع الجزائري، أورد تعريف التسرب بموجب نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية الجزائري التي تنص على: "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، يسمح لضابط أو عون الشرطة القضائية أن يستعمل لهذا الغرض هوية مستعارة وأن يرتكب عند الضرورة الأفعال المذكورة في المادة 65 مكرر 14 أدناه، ولا يجوز تحت طائلة البطلان، أن تشكل هذه الأفعال تحريضا على ارتكاب الجرائم". كما حدد المشرع نطاق تطبيق التسرب بموجب المادة 65 مكرر 5 سالفة الذكر والتي من بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

يلاحظ من خلال التعريف السابق أن التسرب عملية تتسم بالتعقيد، فهو من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية، وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرب بهدف مراقبة أشخاص مشتبه فيهم وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية وتقديم المتسرب لنفسه على أنه فاعل أو الشريك[171].

---

[170] أنظر: المادة 65 مكرر 5 من قانون الإجراءات الجزائية الجزائري.

[171] سارة قادري، المرجع السابق، ص42.

والتسرب كغيره من الإجراءات الحديثة، له ضوابط وشروط شكلية وأخرى موضوعية حتى يعتد به:

أولا: الضوابط الشكلية: تتعلق بما يلي:

أ- **تحرير التقرير:**

يلزم ضابط الشرطة القضائية المكلف بعملية التنسيق بتحرير تقرير كتابي يتضمن بيان مفصل عن جميع العناصر المتعلقة بالعملية[172]، ويجب أن يذكر في التقرير ووفق الترتيب الزمني جميع المعلومات ذات الصلة كالأفعال التي استدعت حدوث عملية التسرب، وكذا تحديد هوية العناصر المشتبه تورطهم في الجريمة (أسمائهم و ألقابهم)، تحديد الكيفيات التي تم بها مخادعة الجناة، فيجب ذكر جميع العمليات منذ بداية التسرب حتى نهايته.

ب-**الحصول على إذن بالتسرب:**

تنص المادة (65مكرر 11) من (ق.إ.ج) على:"عندما تقتضي ضروريات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر 5) أعلاه، يجوز لوكيل الجمهورية أو لقاضي التحقيق، بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة مباشرة عملية التسرب ضمن الشروط المبينة أدناه"، وعليه فالجهة القضائية المختصة بإصدار الإذن هو وكيل الجمهورية أو قاضي التحقيق، ومنه لا يجوز لضابط أو أعوان الشرطة القضائية القيام به حماية للحقوق المكرسة دستوريا.

كما يجب أن يكون الإذن مكتوبا، وهذا وفق نص المادة (65 مكرر 15) التي تنص على: "يجب أن يكون الإذن المسلم تطبيقا للمادة (65 مكرر 11) أعلاه، مكتوبا... وذلك تحت طائلة البطلان" ذلك أن الأصل في العمل الإجرائي هو الكتابة وفقا لنص المادتين (138-139) من (ق.إ.ج) [173]، كما يشترط ذكر اسم الضابط المشرف، وهو ما نصت عليه المادة(65 مكرر 15) بقولها:"يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه، مكتوبا...وذلك تحت طائلة البطلان، تذكر في الإذن الجريمة التي تبرر اللجوء لهذا الإجراء وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته...".

ج- **مدة التسرب:**

حددتها المادة (65 مكرر 3/15) حيث تنص على:"... ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر..."، غير أنه ومراعاة لمقتضيات التحقيق الابتدائي يمكن تجديد هذه المدة

---

[172] أنظر المادة 65 مكرر 13 من قانون الإجراءات الجزائية الجزائري.

[173] حيث تنص المادة (138) من (ق.إ.ج) على:"يجوز لقاضي التحقيق أن يكلف بطريق الإنابة القضائية أي قاض من قضاة محكمته أو أي ضابط من ضباط الشرطة القضائية المختصة بالعمل في تلك الدائرة أو أي قاض من قضاة التحقيق بالقيام بما يراه لازما من إجراءات التحقيق في الأماكن الخاضعة للجهة القضائية التي يتبعها كل منهم، ويذكر في الإنابة القضائية نوع من الجريمة موضوع المتابعة وتؤرخ وتوقع من القاضي الذي أصدرها وتمهر بختمه...".

ضمن نفس الشروط الشكلية والزمنية السابقة، وحفاظا على حياة العون المتسرب من الخطر إضافة إلى الأشخاص المسخرين، أجازا المشرع للقاضي الذي رخص بعملية التسرب أن يأمر في أي وقت بوقفها قبل انقضاء مدتها، وذلك إذا وصل إلى علمه أن معلومات تفيد باحتمال كشف العملية من طرف المجموعة الإجرامية[174].

د- **إبقاء الإذن بالتسرب خارج ملف الإجراءات إلى غاية الانتهاء من العملية:**

وذلك للحفاظ على السرية المطلوبة لنجاح عملية التي التسرب والتي حصرها المشرع بين القاضي الآمر بها (وكيل الجمهورية أو قاضي التحقيق)، وضابط الشرطة القضائية المشرف على العملية وكذا العون المتسرب.

بعد الانتهاء من عملية التسرب، يجب إيداع رخصة التسرب في ملف الإجراءات وهذا وفقا لنص المادة (65 مكرر 6/15) التي تنص على:"... تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب".

ثانيا: الضوابط الموضوعية:

تتمثل الضوابط الموضوعية لعملية التسرب في شرطين رئيسيين هما:

أ- **التسبيب:**

يعتبر التسبيب أساس العمل القضائي، وعليه يجب على وكيل الجمهورية أو قاضي التحقيق عند إصدار الإذن بالتسرب توضيح الأدلة القانونية والموضوعية بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية[175]، وهذا طبقا لنص المادة (65 مكرر 1/15) التي تنص على:"يجب أن يكون الإذن المسلم تطبيقا للمادة 65 مكرر 11 أعلاه مكتوبا ومسببا وذلك تحت طائلة البطلان...".

ب- **نوع الجريمة:**

وقد حصرتها المادة (65 مكرر 5) من (ق.إ.ج) في سبعة أنواع هي: جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، وجرائم الفساد[176]. وعليه يجب أن تكون الجريمة جناية أو جنحة.

---

[174] عبد المجيد جباري، المرجع السابق، ص60.)

[175] سيدهم سيدي محمد، محاضرة جول التسرب حسب تعديل قانون الإجراءات الجزائية، محكمة فرندة، مجلس القضاء تيارت،) في 20 / 03 / 2008، ص 03.

[176] أحسن بوسقيعة، التحقيق القضائي، دار هومة، ط2، الجزائر،2009، ص 114.)

الفرع الثاني: الإجراءات الحديثة بموجب القانون 09-04.

تطرقنا سابقا إلى بعض الإجراءات التقليدية المتعلقة بجمع الدليل الإلكتروني وخلصنا إلى عدم كفايتها لاستيعاب كافة أشكال هذا النوع المستحدث من الجرائم، مما دفع بالمشرع الجزائري إلى استحداث أساليب بحث وتحري جديدة تتلائم وخطورة هذه الجرائم. ونظرا للطبيعة الخاصة للجرائم الإلكترونية، لم يكتف المشرع باستخدام هذه الأساليب حينما تقع الجريمة، ولكن أيضا قبل وقوعها. وعليه صدر القانون رقم: 09-04 المؤرخ في 5 أوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والذي جاء لتكريس إطار قانوني أكثر ملائمة وانسجاما مع خصوصية وخطورة الجريمة الإلكترونية.

نص هذا القانون على جملة من الإجراءات الهامة، وعليه سنتناول مراقبة الاتصالات الإلكترونية وحالات اللجوء إليها في (الفقرة الأولى)، ثم نتطرق إلى تفتيش المنظومة المعلوماتية في (الفقرة الثانية) ثم حجز المعطيات في (الفقرة الثالثة).

الفقرة الأولى: مراقبة الاتصالات الإلكترونية وحالات اللجوء إليها.

سنحاول التطرق من خلال هذه الفقرة إلى تعريف مراقبة الاتصالات الإلكترونية وحالات اللجوء إليها وشروطها.

أولا: المقصود بمراقبة الاتصالات الإلكترونية.

لم يتطرق المشرع الجزائري شأنه شأن أغلب التشريعات المقارنة إلى تعريف مراقبة الاتصالات الإلكترونية، لكنه بالمقابل أوضح لنا مفهوم الاتصالات الإلكترونية بموجب المادة 2 من القانون رقم: 09-04 سالف الذكر[177] والتي تنص على:"يقصد في مفهوم هذا القانون ما يأتي...:

- الاتصالات الإلكترونية: أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية، وبذلك وسع المشرع الجزائري من مفهوم الاتصالات الإلكترونية والتي تتم بأي وسيلة إلكترونية حديثة كجهاز الفاكس والهاتف النقال...الخ" .

بالرجوع إلى المفهوم الفقهي لمراقبة الاتصالات الإلكترونية الذي يعني:"العمل الذي يقوم به المراقب باستخدام الاتصالات الإلكترونية لجمع معطيات عن المشتبه فيه سواء أكان الخاضع للمراقبة شخصا أو مكانا، أو شيئا ومثال ذلك مراقبة أحد الأشخاص ممن قام باختراق الحاسب الآلي الخاص بالمجني عليه أو القيام بإعداد بريد إلكتروني مستنسخ في مراقبة المشتبه فيه عند إرساله أو استقبال لصور دعارة للأطفال عبر

---

[177](يزيد بوحليط، المرجع السابق، ص ص 303- 304 .)

الانترنت، وإفراغ ما تسفر عنه المراقبة الإلكترونية في تقارير أمنه"[178]. أو هي "مراقبة شبكة الاتصالات"[179].

ثانيا: حالات اللجوء للمراقبة الإلكترونية.

مما لا شك فيه أن مراقبة الأحاديث والاتصالات الخاصة والتي تتم بالوسائل الإلكترونية، تمس بحق الإنسان في الخصوصية المكفول دستوريا في مختلف التشريعات الحديثة، وعليه لم يترك المشرع الجزائري الأمر على إطلاقه استجابة للمواثيق الدولية وحماية لحقوق الإنسان في هذا المجال، حيث نصت المادة (04) من القانون 09-04 سالف الذكر على الحالات التي يجوز فيها مراقبة الاتصالات الالكترونية حيث تنص على:"يمكن القيام بعمليات المراقبة المنصوص عليها في المادة 3 من القانون 09-04 في الحالات الآتية:

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

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

ج- لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

د- في إطار تنفيذ طلبات المساعدة القضائية الدولية.

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

ثالثا: شروط مراقبة الاتصالات الالكترونية.

كما رأينا سلفا، وحفاظا على الحق في سرية المراسلات بكافة أنواعها والمكفولة دستوريا، أحاط المشرع الجزائري إجراء المراقبة الالكترونية تحت طائلة البطلان بشروط قانونيا، تتمثل في النقاط الآتية:

أ- **وجود إذن قضائي:**

أوجب المشرع الجزائري وجود الإذن القضائي الصادر عن السلطة القضائية المختصة وذلك بموجب المادة (05/04) من القانون 09-04 سالف الذكر التي تنص على:"...لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية، عندما يتعلق الأمر بالحالات المنصوص عليها في الفقرة "أ" من هذه المادة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية

---

[178] (ناير نبيل عمر، مرجع سابق، ص149، راجع أيضا: عفيفي كامل عفيفي، مرجع سابق، ص ص474- 475.)

[179] (نعيم سعيداني، المرجع السابق، ص183.)

المنتمين للهيئة المنصوص عليها في المادة 13 أدناه إذنا لمدة ستة (6) أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها"[180].

ب-وجود ضرورة:

يتم اللجوء إلى إجراء مراقبة الاتصالات الالكترونية في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.

الفقرة الثانية: تفتيش المنظومة المعلوماتية.

عرفت المادة (2/02) من القانون رقم: 09-04 سالف الذكر المنظومة المعلوماتية "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"، كما عرف أيضا النظام المعلوماتي على أنه:"جهاز يتكون من مكونات مادية ومكونات منطقية وذلك بغرض المعالجة الآلية للبيانات الرقمية، وهو يشتمل على وسائل الإدخال والإخراج وتخزين البيانات، وهذا قد يكون منفردا أو متصلا بمجموعة من الأجهزة المماثلة عن طريق شبكة".

جعل المشرع الجزائري من إجراء التفتيش مهمة وقائية الغاية منها الحيلولة دون وقوع الجريمة الإلكترونية، وذلك من خلال القيام بعمليات المراقبة المسبقة وفق نص المادة (3) من القانون رقم:09-04 السالف الذكر، التي تنص على:"مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية، وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

من جهة أخرى يهدف التفتيش المنصب على المنظومة المعلوماتية إلى استخلاص الدليل الإلكتروني، قبل قيام المجرم المعلوماتي بتدميره أو إخفائه للإفلات من العقوبة. لكن ما هي الجهة القضائية المختصة بمنح الإذن بالتفتيش؟ هذا ما سنجيب عنه.

- **الجهة القضائية المختصة بذلك:**

بالرجوع إلى المادة (04/أ) من القانون رقم: 09-04 السالف الذكر، يبين لنا المشرع الجهة القضائية المختصة بهذه الحالة في المادة نفسها الفقرة الأخيرة إذ يختص النائب العام لدى مجلس قضاء الجزائر بمنح

---

[180] (تجيز بعض التشريعات الوطنية كالقانون الأمريكي وضع أجهزة لتسجيل الاتصالات الالكترونية في حالة الضرورة دون إذن من النيابة العامة، إذا توفر خطر على الحياة أو خطر جسيم على السلامة الجسمية، خالد ممدوح إبراهيم، فن التحقيق، المرجع السابق، ص 351.

ضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها المنصوص عليها بموجب المادة (13) من القانون نفسه، إذنا لمدة ستة أشهر قابلة للتجديد، وذلك على أساس طبيعة ونوعية الترتيبات التقنية المراد أخذها بخصوص الحالات التي تسمح باللجوء إلى المراقبة الالكترونية[181].

الفقرة الثالثة: حجز المعطيات المعلوماتية.

يظل الهدف الأساس لعملية تفتيش المنظومة المعلوماتية، هو وضع اليد على الأدلة الرقمية لإدانة المجرم الإلكتروني، فإذا كان حجز الأشياء المادية كالمعدات (المكونات المادية للحاسوب) والأوراق والمستندات...الخ، لا يعد مشكلة ويتم وفق القواعد الإجرائية التقليدية، غير أن الأمر يختلف تماما، إذ ليس من السهل توقيع الحجز على المنظومة المعلوماتية التي هي في الأصل شيء معنوي غير ملموس.

وطبقا لنص المادة (06) من القانون رقم:09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها التي تنص على:"عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ 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 المعلوماتية التي يجري بها العملية.

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

أولا: الحجز عن طريق منع الوصول إلى المعطيات.

نص المشرع الجزائري في المادة (7) من القانون رقم:09-04 السالف الذكر "إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة (6) أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الدخول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها...".

والملاحظ أن المشرع لم يحدد الأسباب التقنية المانعة للحجز سواء ما تعلق بالمنظومة المعلوماتية نفسها كاستحالة الدخول لوجود كلمة السر أو نظام حماية يصعب اختراقه، لذلك نص على ضرورة إجراء تدابير

---

[181] (أنظر: المادة (4) من القانون رقم: 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

احترازية من طرف المختصين باستعمال الوسائل التقنية المناسبة القصد منه عدم تمكين المجرم من الوصول للمعطيات المخزنة في المنظومة المعلوماتية[182].

ثانيا: حدود استعمال المعطيات.

تطرقنا فيما سبق إلى أن إجراء مراقبة الاتصالات الالكترونية يمس بحق الأشخاص في سرية مراسلاتهم ومنها المراسلات الالكترونية، وهو حق مكفول دستوريا، لذا نص المشرع الجزائري تحت طائلة العقوبات على حدود استعمال المعلومات المتحصل عليها من عمليات المراقبة، إلا فيما تتطلبه التحريات والتحقيقات القضائية، وهذا بموجب نص المادة (09) من القانون رقم: 09-04 السالف الذكر التي تنص على:"تحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية".

المبحث الثاني: مدى اقتناع القاضي الجنائي بالدليل الالكتروني.

الدليل الالكتروني شأنه شأن باقي الأدلة الأخرى يخضع لنفس القواعد المقررة لباقي الأدلة، سواء كانت هذه القواعد تتعلق بسلطته في قبول الدليل الالكتروني، أو تتعلق بسلطته في تقدير هذا النوع من الدليل، ذلك لأن القاضي لا يقدر إلا الدليل المقبول، ولا يكون مقبولا إلا بعد التيقن من مراعاة الدليل لقاعدة المشروعية والتي لا يمكن من دونها أن يرتب الدليل الالكتروني أي آثار قانونية.

وبالنظر إلى الطبيعة الخاصة التي يتميز بها الدليل الالكتروني، وما قد يصاحب الحصول عليه من خطوات معقدة، فإن قبوله في الإثبات قد يثير العديد من المشكلات، حيث أن مستودع هذه الأدلة هو الوسائل الالكترونية، ولذا التلاعب فيها وتغيير الحقيقة أمر وارد[183]، وهذا ما يجعلنا نتساؤل: كيف نضمن مصداقية الدليل الالكتروني وأنها بالفعل تعبر عن الحقيقة التي تهدف إليها الدعوى الجنائية؟.

وعلى ذلك، ستكون الإجابة على هذا الإشكال من خلال تعرضنا بالدراسة إلى:

- حجية الدليل الالكتروني في ظل أنظمة الإثبات المختلفة وذلك في (المطلب الأول).
- سلطة القاضي الجنائي في تقدير الدليل الالكتروني وهذا من خلال (المطلب الثاني).
- أما (المطلب الثالث) سنخصصه لمدى تأثير مشكلات الدليل الالكتروني على اقتناع القاضي.

---

[182] (زيدان زبيحة، المرجع السابق، ص153.)

[183] (عائشة بن قارة مصطفى، المرجع السابق، ص 114 .)

المطلب الأول: حجية الدليل الالكتروني في ظل أنظمة الإثبات المختلفة.

نتناول هذه المسألة بحسب كل نظام من أنظمة الإثبات، وتنقسم هذه الأنظمة إلى النظام الحر والذي سنتناوله في (الفرع الأول)، النظام المقيد في (الفرع الثاني)، النظام المختلط في (الفرع الثالث) مع التعرض ختاما إلى موقف المشرع الجزائري في (الفرع الرابع) .

الفرع الأول: في ظل نظام الإثبات الحر (النظام اللاتيني).

تأخذ الدول اللاتينية بنظام الإثبات الحر وهو لا يثير صعوبات بشأن حجية الدليل الرقمي، لأن القاضي الجنائي يملك الحرية في تقديره، ومن ثمة الأخذ به من عدمه حيث لا يخضع في ذلك لرقابة المحكمة العليا، وإنما لرقابة موضوعية بخصوص مبررات الأخذ به، وأخذت بذلك العديد من التشريعات مثل: فرنسا وتركيا واليونان والبرازيل وسويسرا [184] ، في حين تشترط بعض الدول أن يكون الدليل الالكتروني مقروءا بعد استخراجه من الحاسوب أو من خلال شاشته.

إن أدلة الحاسوب هي تطبيق من تطبيقات الدليل العلمي بما يتصف به من موضوعية وحياد ومشروعية لإقناع القاضي الجنائي الذي يجب عليه قبل الإقناع به أن يميز بين قيمته العلمية أولا عن طريق الاستعانة بالخبراء والمختصين، وثانيا الظروف والملابسات التي وجد فيها الدليل فيمكن أن يرفضه إذا رأى وجوده لا يتناسب منطقيا مع وقائع القضية [185].

الفرع الثاني: في ظل نظام الإثبات المقيد.

تعتمد حجية الدليل الإلكتروني في ظل هذا النظام على تحديد أدلة الإثبات من قبل المشرع وليس تقديرها من القاضي، فالدول التي تأخذ بهذا النظام مثل: بريطانيا وأمريكا تفرض قيودا على هذه الأدلة حتى يمكن الأخذ بها مثل: اعتماد مبدأ تعاضد الأدلة في التشريع البريطاني[186].

كما يحدد القانون الألماني على سبيل الحصر وسائل الإثبات التي يتعين على القاضي قبولها كسماع أو سؤال المتهم وشهادة الشهود وتقارير الخبراء [187]. في الشأن نفسه يستبعد المشرع الأمريكي الأدلة التي يمكن الحصول عليها بالمخالفة للحقوق الدستورية كالحجز والمصادرة والتفتيش غير المشروع [188].

---

[184](هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، النسر الذهبي، القاهرة، مصر، 2002، ص 43) وما بعدها.

[185](سامي جلال فقي حسين، المرجع السابق، ص ص75- 76.

[186](يقصد بهذا المبدأ: تعزيز دليل بديل آخر، فمثلا الشهادة لا تكفي وحدها في بعض الحالات، حيث يجب توافر دليل آخر معزز لها كشهادة أخرى مستقلة عنها، أو دليل آخر كخبرة أو مستند، فإذا لم يتوافر هذا الدليل المساند حكم القاضي بالبراءة، راجع سامي جلال فقي حسين، المرجع السابق، ص83.

[187](عائشة بن قارة مصطفى، المرجع السابق، ص ص181- 182.

إن دور القاضي في هذا النظام دور سلبي فإذا لم تكن هذه الشروط متوفرة، لا يستطيع الحكم بالإدانة بصرف النظر عن اعتقاده الشخصي حتى لو كان يميل إلى إدانة المتهم [189].

كما تبرز في ظل هذا النظام صعوبات في مجال إثبات الجرائم الإلكترونية، مما يستوجب إدخال تعديلات تتلائم وطبيعة هذه الجرائم، نظرا للطفرة التكنولوجية الحاصلة في مجال المعلوماتية وشبكة الانترنت، حيث لوحظ بعض التغييرات على حدة هذا النظام. بحيث صار يقبل بمبدأ حرية القاضي في تقدير الأدلة، فقاعدة حرية القاضي الجنائي في الاقتناع معترف بها تقريبيا لدى جميع التشريعات القانونية مع اختلاف الصياغة في القوانين ففي النظام اللاتيني تسمى بمبدأ الاقتناع القضائي، أما في النظام الأنجلوسكسوني فتسمى بالأدلة بدون شك معقول، أو الإدانة الخالية في أي شك[190].

الفرع الثالث: في ظل نظام الإثبات المختلط.

يعتبر نظام الإثبات المختلط نظام وسط، أي نظام توفيقي بين نظام الإثبات الحر ونظام الإثبات المقيد، حيث تتراوح أحكامه بين التقييد والإطلاق، كما جاء هذا النظام لتلاقي الانتقادات الموجهة للنظامين السابقين فيجنب تعسف القاضي في نظام الإثبات الحر وخروجه عن جادة الصواب، كما يخفف من الدور السلبي المحض للقاضي في النظام المقيد بأن يمنح له الحرية في تقدير ما يعرض عليه من أدلة [191]، كما قد يكون التوفيق بين النظامين عندما يحدد القانون أدلة معينة للإثبات في بعض الوقائع دون الأخرى، أو يطلب شروطا في بعض الحالات، أو يعطي القاضي الحرية في تقدير الأدلة كالقانون الياباني الذي يحصر طرق الإثبات المقبولة في أقوال المتهم وشهادة الشهود والخبرة المنجزة من طرف الخبراء [192].

لكن بالمقابل أين موقف المشرع الجزائري من كل هذا؟ هذا ما سنعرفه في الفرع الموالي.

الفرع الرابع: موقف المشرع الجزائري.

لم تفرد تشريعات الدول المنتمية للنظام اللاتيني كفرنسا وغيرها من الدول المتأثرة بها ومنها الجزائر، نصوص خاصة بقبول الدليل الإلكتروني، وهذا على أساس استنادها لمبدأ حرية الإثبات في المواد الجنائية تطبيقا لنظام الإثبات الحر. حيث نصت المادة (212) من (ق.إ.ج) على:"يجوز إثبات الجرائم بأي طريق من

---

(188) سامي جلال فقي حسين، المرجع السابق، ص ص81- 83.

(189) هلالي عبد الإله أحمد، المرجع السابق، ص50.

(190) سامي جلال فقي حسين، المرجع السابق، ص84.

(191) اقترح النظام المختلط من طرف الأستاذ: (روبسيير) (robsir) أمام الجمعية التأسيسية الفرنسية سنة 1971، حيث كان هذا الاقتراح مكونا من جزئين: يتمثل الأول في عدم الحكم على المتهم إذا لم تتوفر ضده أدلة حددها القانون، والثاني في عدم الحكم بإدانة المتهم حتى إذا توافرت أدلة قانونية، لكن هذه الأدلة لم تحقق قناعة القاضي. سامي جلال فقي حسين المرجع السابق، ص93.

(192) هلالي عبد الإله أحمد، المرجع السابق، ص59.

طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص، ولا يصوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه"، من جهة أخرى يأتي إدراج المشرع لهذه المادة ضمن الأحكام المشتركة بطرق الإثبات، مما لا يدع للشك في تطبيقها أمام كل الجهات القضائية الجزائية وبالتالي اعتمد المشرع الجزائري نظام الإثبات الحر كأصل ونظام الإثبات المقيد كاستثناء[193].

المطلب الثاني: سلطة القاضي الجنائي في تقدير الدليل الإلكتروني.

يعتبر مبدأ حرية الاقتناع الشخصي للقاضي الجزائي [194] من أهم عناصر الإثبات في الدعوى الجنائية، فالقاضي حر بأن يأخذ بالأدلة التي يراها مناسبة للكشف عن الحقيقة وله أن يتحرى بنفسه صدق الأدلة، كما أنه حر في تقدير جميع الأدلة بما فيها الأدلة الرقمية، وله الحق في أن يستمد اقتناعه وعقيدته من أي مصدر يطمئن إليه.

سنتناول مبدأ الاقتناع القضائي في (الفرع الأول)، ثم نتطرق إلى الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني في (الفرع الثاني).

الفرع الأول: مبدأ الاقتناع القضائي.

بالنسبة لمعنى الاقتناع القضائي فقد اختلفت الاتجاهات الفقهية في تحديد المدلول القانوني للقناعة القضائية، إلا أنها تتفق على أنها تعني بأن القاضي حر في تكوين عقيدته من أي دليل يراه مناسبا ويطمئن إليه، وهذه الأدلة قد تكون من طرف الخصوم أو النيابة العامة أو من القاضي بنفسه والتي عن طريقها تتكون قناعة هذا القاضي، والجدير بالذكر أن هذه الحرية الممنوحة للقاضي الجنائي ليست بهدف توسيع سلطته، وإنما لصعوبة الحصول على الدليل في المواد الجزائية فيما يتعلق بالأدلة العلمية، ومنها الدليل الإلكتروني[195].

وهذا المبدأ تم النص عليه لأول مرة من طرف المشرع الفرنسي الذي أقر بأن القضاة لا يحاسبون على الأدلة التي اقتنعوا بها، كما نص على أن هذا المبدأ يطبق أمام جميع الجهات القضائية الجنائية[196].

---

[193] (يزيد بوحليط، المرجع السابق، ص 288.)

[194] (يتميز الاقتناع الشخصي للقاضي الجزائي بخاصيتين هما:)

الخاصية الأولى: تعبر عن حالة ذهنية مبنية على الاحتمال وأن العبرة ليست بكثرة الأدلة وإنما لما تتركه من أثر في نفسه القاضي سيحدد مصير الدعوى الجزائية إما بالبراءة أو الإدانة.

الخاصية الثانية: تتمثل في أن القاضي حر في أن يأخذ عقيدته أو اقتناعه من أي دليل يراه مناسبا لإظهار الحقيقة، نعيم سعيداني، المرجع السابق، ص226.

[195] (ناير نبيل عمر، المرجع السابق، ص 179.)

[196] (فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، دار الثقافة للنشر والتوزيع، ط1، الأردن، 2006 ص ص 106-107.

أما المشرع الجزائري فقد كرس مبدأ الاقتناع القضائي في المادة 307 من (ق.إ.ج)، وهي مستوحاة من المادة 353 من القانون الفرنسي.

كما أن المشرع الجزائري كرس مبدأ الاقتناع القضائي صراحة في المادة 212 من (ق.إ.ج) التي جاء في فحواها أنه من الجائز إثبات الجرائم بأي طريقة في الإثبات الجنائي، كما أن للقاضي أن يصدر حكمه بناءا على اقتناعه الخاص، بالإضافة إلى أن المحكمة العليا أكدت على ضرورة مراعاة مبدأ الاقتناع القضائي، وتوصي بإعماله أمام المحاكم الجنائية[197].

الفرع الثاني: الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني.

بالرغم من الحرية الكبيرة التي يتمتع بها القاضي في نظام الإثبات الحر، إلا أن هذه الحرية ليست مطلقة بل إن وضع المشرع لها ضوابط وهي بمثابة صمام أمام إزاء انحراف القاضي عند ممارسته لها كي لا تختل الأحكام ولا يصار إلى التحكم[198]، إذا أن القاضي عليه تسبيب الأحكام.

وعلى ذلك فإن دراستنا للضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الإلكتروني نتناولها من جانبين، الأول يتعلق بمصدر الاقتناع أي بالدليل الإلكتروني الذي يتأسس عليه الاقتناع القضائي وهذا من خلال (الفقرة الأولى)، والثاني يتعلق بالاقتناع ذاته والذي نتناوله في (الفقرة الثانية).

الفقرة الأولى: الضوابط المتعلقة بمصدر الاقتناع:

في هذا الشأن يحكم اقتناع القاضي بالأدلة الإلكترونية ضابطان هما:

أولا: شروط قبول الدليل الإلكتروني:

أن القاضي ليس حرا في تقدير أي دليل كان بل هو حر فقط في تقدير الدليل الإلكتروني المقبول في الدعوى، بمعنى الحصول عليه بطريق مشروع، إعمالا بمبدأ الشرعية الإجرائية، وبالتالي يستبعد في مقابل ذلك من المرافعة سائر الأدلة الإلكترونية غير المقبولة، لأنها لا تدخل ضمن عناصر تقديره[199].

ثانيا: شروط وضعية الدليل الإلكتروني:

من القواعد الأساسية في الإجراءات الجنائية أنه لا يجوز للقاضي أن يبني حكمه على أدلة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعبر عنه بوضعية الدليل، ومقتضى ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الاطلاع عليه ومناقشته وكلا الأمرين ينبغي توافرهما. وقد أرسلت هذا الضابط المادة (212 / 2) من قانون الإجراءات الجزائية إذ تنص: "ولا يسوغ للقاضي أن يبني قراره إلا على

---

[197](عائشة بن قارة مصطفى، المرجع السابق، ص ص242- 243.)

[198](فاضل زيدان محمد، المرجع السابق، ص232.)

[199](عائشة بن قارة، المرجع السابق، ص269.)

الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه"[200]. ويترتب على ذلك أنه لا يجوز للقاضي الجنائي اقتناعه على دليل قدمه أحد أطراف الدعوى إلا إذا تم عرضه في جلسة المحاكمة وخضع للمناقشة بحيث يكون معلوما لكافة أطراف الدعوى.

الفقرة الثانية: الضوابط المتعلقة بالاقتناع ذاته.

يتيح مبدأ الإثبات الجنائي حرية كبيرة للقاضي في تقدير عناصر الإثبات بما في ذلك الأدلة الرقمية، وعليه فإن تقدير كفاية أو عدم كفاية الدليل الإلكتروني في إثبات الجريمة الإلكترونية ونسبتها إلى مرتكبيها أمر متروك لمحكمة الموضوع المعروض عليها الدليل، ولا تخضع في ذلك لرقابة محكمة النقض التي يقتصر دورها على مراقبة المنطق القضائي لمحكمة الموضوع عن طريق رقابتها على صحة تسبيب الحكم[201].

وعليه لبلوغ القاضي درجة الاقتناع التام للفصل في القضية، ، لابد له من شروط تتمثل أساسا في:

أولا: بلوغ الاقتناع القضائي درجة اليقين: تقتضي العدالة أن يصدر القاضي حكمه عن اقتناع يقيني بصحة ما ينتهي إليه من وقائع لا مجرد الضن والاحتمال.

ثانيا: توافق الاقتناع مع مقتضيات العقل والمنطق: ومعنى ذلك أن يكون استخلاص محكمة الموضوع لوقائع الدعوى استخلاصا معقولا، وأن معيار معقولية الاقتناع بما في ذلك الأدلة الإلكترونية، هو أن تكون هذه الأدلة مؤدية إلى ما رتبه الحكم عليها من غير تعسف في الاستنتاج ولا تعارض مع مقتضيات العقل والمنطق[202].

المطلب الثالث: مدى تأثير مشكلات الدليل الالكتروني على اقتناع القاضي.

يثير الدليل الإلكتروني العديد من المشكلات، وهذه المشكلات تعود عليه سلبا حيث تقلل من قيمته في مجال الإثبات الجنائي في حالة عدم إيجاد حلول بشأنها، وسنحدد نوعين من المشاكل أولهما موضوعية في (الفرع الأول) وثانيهما إجرائية في (الفرع الثاني).

الفرع الأول: المشكلات الموضوعية للدليل الإلكتروني.

وتتعلق هذه المشكلات غالبا بطبيعة الدليل ذاته، وهذا بسبب الخصائص الفيزيائية التي يتكون منها سواء بسبب تنوعه وهذا ما سنتطرق إليه في (الفقر الأولى)، أو الطبيعة غير المرئية له (الفقر الثاني) أو مشكلة الأصالة (الفقر الثالثة)، أو بسبب ديناميكيته (الفقر الرابعة).

---

[200] (كذلك نصت على هذه القاعدة المادة (427) من (ق.إ.ج) في فقرتها الثانية بقولها:"لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحكمة ونوقشت أمامه في مواجهة الخصوم".

[201] (عائشة بن قارة مصطفى، المرجع السابق، ص606.)

[202] (فوزي عمارة، المرجع السابق، ص 78.)

الفقرة الأولى: الدليل الإلكتروني متنوع:

يشمل كافة أشكال وأنواع البيانات، يمكن أن يظهر عليها كأن يكون بيانات غير مقروءة، وقد يكون بيانات مفهومة، كما يمكن أن يكون صورة ثابتة أو متحركة، أو يكون مخزنا في البريد الإلكتروني يعد هذا المفهوم تعبيرا عن اتساع قاعدة الدليل الرقمي، إذ يمكن لهذه البيانات الرقمية سواء كانت منفردة أو مجتمعة أن تكون دليل براءة أو إدانة هذا المتهم [203]، وهنا تكمن صعوبة البحث والتحري عن الجرائم الالكترونية لاستخلاص الدليل الرقمي الذي يحتاج لأفراد متخصصين في مجال تقنية المعلومات، فضلا عن صعوبة اقتناع القاضي الجزائي به.

الفقرة الثانية: الدليل الإلكتروني دليل غير مرئي:

فهو عبارة عن نبضات إلكترونية، لا تفصح عن شخصية معينة وهذه المشكلة تظهر بصفة جلية مع شبكة الانترنت حيث تسمح لمستخدميها الاتصال بدون الكشف عن أسمائهم الحقيقية فضلا عن ذلك يمكن التلاعب بالدليل الرقمي مما يقطع الصلة بين المجرم وجريمته ويحول دون كشف شخصيته وبالتالي يشكل هذا الدليل عائق أمام رجال التحري والتحقيق.

الفقرة الثالثة: مشكلة الأصالة في الدليل الالكتروني:

إن الأصالة في الدليل الالكتروني لها طابع افتراضي لا يرقى إلى مستوى الأصالة في الدليل المادي التقليدي، فهذه الأخيرة تعبر عن وضعية مادية ملموسة كما هو الشأن في الدليل الورقي...الخ في حين أن الدليل الإلكتروني عبارة عن تعداد غير محدود من الأرقام الثنائية [204] ولقد أثارت الأصالة العديد من المشكلات من حيث مدى الاعتداد بالنسخة التي تشكل دليلا كاملا.

الفقرة الرابعة: صعوبة فهم الدليل المتحصل من الوسائل الإلكترونية:

تثير الطبيعة غير المادية للبيانات المخزنة بالحاسب الآلي العديد من المشاكل في الإثبات الجنائي، وبما أن طبيعة هذه البيانات لا تخلف وراءها آثارا ملموسة، فإن هذا يزيد من صعوبة عمل المحققين، لذا فالأمر يحتاج إلى خبرة فنية ومقدرة على معالجة المعلومات والبيانات.

الفرع الثاني: المشكلات الإجرائية للدليل الإلكتروني:

قسمنا هذا الفرع إلى فقرتين، خصصنا (الفقرة الأولى) إلى ارتفاع تكاليف الحصول على الأدلة الإلكترونية، في حين تطرقنا في (الفقرة الثانية) إلى نقص المعرفة التقنية لدى جهات البحث والتحري.

---

(203) نعيم سعيداني، المرجع السابق، ص124.)

(204) عائشة بن قارة مصطفى، المرجع السابق، ص252.)

الفقرة الأولى: ارتفاع تكاليف الحصول على الأدلة الإلكترونية:

غالبا ما يتم اللجوء إلى الخبرة الرقمية من أجل إثبات الجرائم الإلكترونية، إلا أن إنجاز هذه الخبرة يتطلب مصاريف كبيرة، وهذا راجع للطبيعة الخاصة لهذا النوع من الأدلة. وبالتالي يجب على كل دولة إنشاء وحدات تابعة لأجهزة البحث والتحري متخصصة ومؤهلة وعلى مستوى عال من التدريب على استعمال وسائل تقنية المعلومات لخلق توازن بين وسائل ارتكاب الجرائم الإلكترونية ووسائل الكشف عنها في ظل بيئة افتراضية، وهذا ما أقام به المشرع الجزائري بهدف تحقيق الفعالية وتخفيض التكاليف.

حيث أنشأت المديرية العامة للأمن الوطني بالمخبر المركزي للشرطة العلمية بالجزائر العاصمة خلية للإعلام الآلي، مهمتها البحث والتحري عن الجرائم الإلكترونية، كما تم تدعيم مراكز الأمن الولائي بفرق متخصصة بالتحقيق في هذا المجال [205].

الفقرة الثانية: نقص المعرفة التقنية لدى جهات البحث والتحري:

إن الكشف عن الجريمة الإلكترونية وإثباتها يتطلب اكتساب أفراد هذه الأجهزة مهارات خاصة تمكنهم من مواكبة التطورات الحاصلة في مجال تقنية المعلومات، إذ أن البيئة الإلكترونية تسمح للمجرم ارتكاب جريمته بضغطة زر، فهي تسمح أيضا لجهة البحث والتحري إمكانية كشفه وملاحقته وتوقيع العقاب عليه، سريع جدا، لذلك نجد الكثير من الدول بشرط تحكم هؤلاء في التقنية المعلوماتية خاصة وأنها تتطور بشكل المتقدمة قد اهتمت بتدريب المحققين في الجرائم الإلكترونية[206]

---

[205] أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، الأردن، 2001، ص291.

[206] عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة 2002، ص355.

خلاصة الفصل.

تطرقنا في هذا الفصل إلى بعض الإجراءات التقليدية لجمع الدليل الإلكتروني، كإجراء المعاينة والخبرة، والتفتيش، ومدى انطباق هذه الإجراءات على الجرائم الإلكترونية، حيث تبين أنها غير كافية لإثبات هذا النوع من الجرائم الإلكترونية، مما دفع بالمشرع إلى تعديل قانون الإجراءات الجزائية بموجب القانون رقم: 06-22 المؤرخ في 20 / 12 / 2006 المعدل والمتمم، أين استحدث أساليب خاصة للبحث والتحري عن بعض الجرائم على سبيل الحصر، ومنها الجرائم الإلكترونية، مثل، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب وذلك بموجب المواد من (65 مكرر 5 – 65 مكرر 18).

غير أن المشرع الجزائري لم يكتف بهذا التعديل رغم أهميته البالغة بل اتجه إلى إقرار سياسة جزائية وقائية من الجرائم الإلكترونية، وذلك بموجب القانون رقم: 09 -04 سابق الذكر، أين نص على جملة من الإجراءات الخاصة، مثل: مراقبة الاتصالات الإلكترونية، وتفتيش المنظومة المعلوماتية، وحجز المعطيات المعلوماتية.

ثم تطرقنا إلى مدى قبول واقتناع القاضي الجنائي بالدليل الإلكتروني، حيث تناولنا حجية هذا الدليل على مستوى أنظمة الإثبات الجنائي، الحر، المقيد، المختلط، وحجيته أمام القاضي الجنائي، من خلال إبراز مدى حرية القاضي الجنائي بالأخذ بهذا الدليل الإلكتروني وضوابط هذه الحرية .

الخاتمة

الخاتمة

من خلال الدراسة التي قمنا بها والتي هدفها الرئيسي هو الوصول إلى تحديد مدى حجية الدليل الإلكتروني في الإثبات الجنائي. كان لزاما علينا المرور في الفصل الأول إلى مفهوم الجريمة الإلكترونية باعتبارها مصدر للدليل الإلكتروني وذلك عبر التطرق لمختلف تعريفاتها وأهم خصائصها بالإضافة إلى أنواعها مع إبرازنا لدوافع ارتكاب هذه الجريمة.

ثم تطرقنا إلى الدليل الإلكتروني كأثر ناتج عن هذه الجرائم الإلكترونية والذي يستلزم شروطا معينة حتى يكون صحيحا ومرتبا لآثاره القانونية. وما دفعنا إلى تناول مسألة الجريمة الإلكترونية هو المجرى المنطقي للأمور إذ أنه لا يعقل أن تقوم جهات التحقيق بالبحث عن الدليل لإثباتها الجريمة دون معرفة موضوعية لهذه الجريمة والطبيعة الخاصة للآثار الناتجة عنها وكيفية التعامل معها.

في حين خصصنا الفصل الثاني للإجراءات الخاصة لجمع الدليل الإلكتروني ومدى اقتناع القاضي الجنائي بهذا الدليل، حيث بينا فيه مختلف الإجراءات المتبعة والتي لابد أن تتلائم مع خصوصية هذا النوع من الأدلة، بالإضافة إلى بيان حجية هذا الدليل في مختلف أنظمة الإثبات الجنائي، وفي الأخير انتهينا إلى حرية القاضي الجنائي في الاقتناع بالدليل الإلكتروني.

وبناء على دراستنا لهذا الموضوع توصلنا إلى:

أولا: النتائج:

– نظرا للطبيعة الخاصة للجريمة الإلكتروني، لا يوجد اتفاق على وضع تعريف موحد لها، فهي تتم في فضاء افتراضي يتسم بالتغيير والانتشار الجغرافي العابر لحدود.

– لقد اعتمد المشرع الجزائري مصطلح " الجرائم المتصلة بتكنولوجيات الإعلام والاتصال " وعرفها بموجب أحكام المادة (2 / أ) من القانون رقم: 09 – 04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وعليه وفق المشرع الجزائري في اختياره لهذا المصطلح للدلالة على هذه الجرائم المستحدثة، والذي يتوافق أيضا مع مصطلح " الجرائم الإلكترونية " بالمفهوم المستعمل في بحثنا.

– كما تتميز الجرائم الإلكترونية بخصائص متفردة عن باقي الجرائم، فهي جرائم عابرة للحدود ويصعب على المحققين اكتشافها وإثباته، وتتم بأساليب وأدوات متنوعة، يغلب عليها الطابعان التقني والفني وهذا ما يميزها عن باقي الجرائم التقليدية.

– تتنوع الجرائم الإلكترونية، فهي لم تأتي في صورة واحدة بل تعددت إلى الجرائم التي تمس بالنظم المعلوماتية والجرائم الواقعة على الأموال، والجرائم الماسة بالأشخاص.

– تخلف الجرائم الإلكترونية دليلا من نوع خاص من ذات طبيعة البيئة الرقمية الناشئ عنها، وهو الدليل الإلكتروني، عبارة عن نبضات كهربائية تتم ترجمتها من طرف الأخصائيين في شكل مخرجات ورقية يستدل بها في إثبات واقعة جرمية.

– نظرا لعدم كفاية الإجراءات التقليدية المتعلقة بالبحث والتحري عن الجرائم الإلكترونية، سارع المشرع إلى استحداث أساليب خاصة بموجب المادة (65 مكرر 5 – 65 مكرر 18) من قانون الإجراءات الجزائية، يهدف من وراء ذلك إلى استخلاص الدليل الإلكتروني، الذي تختلف طبيعته عن الدليل التقليدي.

– نص المشرع على إجراءات وقائية بموجب القانون رقم: 09 –04 سابق الذكر، الهدف منها الوقاية من الجريمة الإلكترونية قبل حدوثها مثل، مراقبة الاتصالات الإلكترونية، وتفتيش المنظومة المعلوماتية وحجز المعطيات.

– اعتراف المشرع الجزائري بحجية الدليل الإلكتروني في الإثبات الجنائي.

ومن خلال ما توصلنا إليه من نتائج يمكننا اقتراح مايلي:

ثانيا: التوصيات:

– التكوين الدوري والمستمر لضباط الشرطة القضائية سواء من الناحية القانونية والتقنية بغية إكسابهم للمهارات المطلوبة في التعامل مع الأدلة الإلكترونية.

– توفير الوسائل الحديثة في مجال تكنولوجيات الإعلام و الاتصال للسلطات القضائية المكلفة بالبحث والتحري والعمل على تحديثها دوريا لتتماشى والتطور المستمر لتقنية المعلومات.

وأخيرا وبرغم النقائص المسجلة، أرجو أن أكون قد وفقت في إنجاز هذا العمل ولو بجزء بسيط .

قائمة المراجع:

أولا : المراجع باللغة العربية:

1- المؤلفات:

- ابن منظور : لسان العرب, دار صادر, الطبعة الثالثة, المجلد الحادي عشر, لبنان, 1414ه 1994م.
- أحسن بوسقيعة، التحقيق القضائي، دار هومة، الطبعة الثانية، الجزائر،2009.
- أسامة أحمد المناعسة وآخرون، جرائم الحاسب الآلي والانترنت، دراسة تحليلية مقارنة، دار وائل للنشر والتوزيع، الأردن، 2001.
- أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة الإسكندرية، مصر، 2015.
- أمال قارة, الحماية الجزائية للمعلوماتية في التشريع الجزائري, الطبعة الثانية, دار هومه الجزائر,2007.
- أمير فرج يوسف، الجريمة الالكترونية و الجهود الدولية و المحلية لمكافحة جرائم الكمبيوتر والانترنت، مكتبة الوفاء القانونية، مصر،2011.
- جلال ثروت، نظم الإجراءات الجنائية، دار الجامعة الجديدة للنشر، الإسكندرية، 1997 ص456.
- جميل عبد الباقي الصغير، الجوانب الإجرامية للجرائم المتعلقة بالانترنت، دار الفكر العربي القاهرة، 2001.
- خالد حمد محمد الهادي، الثورة البيولوجية و دورها في الكشف عن الجريمة DNA، دار الجامعة الجديدة، 2005.
- خالد عياد الجلي،إجراءات التحري و التحقيق في جرائم الحاسوب والانترنت،الطبعة الأولى، دار الثقافة للنشر و التوزيع،عمان، الأردن، 2011.
- خالد ممدوح إبراهيم ,الجرائم المعلوماتية,دار الفكر الجامعي,الإسكندرية,مصر,ط1 ,2009.
- خالد ممدوح إبراهيم، التقاضي الإلكتروني، دار الفكر الجامعي، الطبعة الأولى،مصر، 2007.
- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن منشورات الحلبي الحقوقية، بيروت، لبنان، ط1، 2012.
- سامي جلال فقي حسين : الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي, دار الكتب القانونية, مصر, 2011.

- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة 2007.
- عائشة بن قارة مصطفى, حجية الدليل الإلكتروني في مجال الإثبات الجنائي, دار الجامعة الجديدة, مصر, 2010.
- عبد العال الدريبي – الجرائم الالكترونية – دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت – المركز القومي للإصدارات القانونية – القاهرة – مصر – 2012.
- عبد العال الدريبي و محمد صادق إسماعيل، الجرائم الإلكترونية–دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية و الإنترنت، المركز القومي للإصدارات القانونية، الطبعة الأولى، القاهرة، مصر، 2012.
- عبد الفتاح بيومي حجازي، الجزائب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية دراسة مقارنة على ضوء القواعد العامة للإجراءات الجنائية، الطبقة الأولى دار النهضة العربية الإسكندرية مصر، 2009.
- عبد الفتاح بيومي حجازي، النظام القانوني لحماية التجارة الالكترونية، الكتاب الأول، نظام التجارة الالكترونية و حمايتها مدنيا، دار الفكر الجامعي، الاسكندرية، مصر، 2002.
- عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2001.
- عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2002.
- عبد المجيد حجازي، دراسات قانونية في المادة الجزائية على ضوء أهم التعديلات الجديدة، دار هومة للطباعة و النشر و التوزيع، الجزائر، 2012.
- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت، لبنان، دون ذكر سنة النشر.
- علي جبار الحسيناوي : جرائم الحاسوب و الإنترنت, دار اليازوري العلمية للنشر و التوزيع الأردن, 2009.
- علي حسن الطوالبه, أستاذ القانون الجنائي المساعد, مشروعية الدليل الإلكتروني المستمد من التفتيش الجنائي " دراسة مقارنة " ,جامعة العلوم التطبيقية – البحرين ,2009 .

- علي حسن محمد الطوالبة، التفتيش الجنائي في نظم الحاسوب و الإنترنت–دراسة مقارنة– عالم الكتب الحديثة، الأردن، 2004.
- علي عدنان الفيل، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، الطبعة الأولى، المكتب الجامعي الحديث، مصر، 2012.
- فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، دار الثقافة للنشر والتوزيع، الطبعة الأولى، الأردن، 2006.
- فرج علواني هليل، التحقيق الجنائي و التصرف فيه و الأدلة الجنائية، دار المطبوعات الجامعية مصر، 2006.
- محمد أمين الشوابكة – جرائم الحاسوب و الانترنت (الجريمة المعلوماتية) –دار الثقافة للنشر والتوزيع –عمان الاردن –2009.
- محمد حسين منصور، الإثبات التقليدي و الإلكتروني، دار الفكر الجامعي، مصر،2006،ص 272.
- محمد سيد سلطان , قضايا قانونية في امن المعلومات وحماية البيئة الالكترونية – دار ناشري للنشر الالكتروني ,الكويت ,سنة 2012 .
- محمد علي العريان – الجرائم المعلوماتية – دار الجامعة الجديدة – الإسكندرية – مصر – 2004.
- محمد مصطفى زيدان، دراسة سيكيولوجية تربوية لتلميذ التعليم العام، ديوان المطبوعات الجامعية الجزائر.
- ممدوح عبد الحميد عبد المطلب, البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت دار الكتب القانونية, مصر, 2006.
- ناير نبيل عمر، الحماية الجنائية للمحل الالكتروني في جرائم المعلوماتية، دار الجامعة الجديدة مصر، 2012.
- نبيلة هبة هروال, الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات, دار الفكر الجامعي, الإسكندرية, مصر, 2007.
- نصر شومان، التكنولوجيا الجرمية الحديثة وأهميتها في الإثبات الجنائي، شركة المؤسسة الحديثة للكتاب، طرابلس، لبنان،ط1، 2011.
- نعيم مغبغب،حماية برامج الكمبيوتر،منشورات الحلبي الحقوقية،لبنان،ط2، 2009.
- نهلا عبد القادر المومني، جرائم المعلوماتية، دار الثقافة للنشر و التوزيع، عمان، الأردن، ط1 2008.

- هبة حسين محمد زايد، الحماية الجنائية للصفقات الإلكترونية، دار الكتب القانونية، القاهرة مصر، 2015.
- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية–دراسة مقارنة – مكتب الآلات الحديثة، مصر.
- هلالي عبد الإله أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، النسر الذهبي، القاهرة مصر، 2002.
- يوسف كوران , جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي منشورات مركز كردستان للدراسات الاستراتيجية, السليمانية, مصر , 2007.

2 – الرسائل:

أ_ أطروحة الدكتوراه:

- أمال عثمان، الخبرة في المسالة الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1964 ص68 وما بعدها. أنظر أيضا: د/عادل حافظ غانم، الخبرة في مجال الإثبات الجنائي، بحث بمجلة الأمن العام، العدد 43، سنة 1968.
- تركي بن عبد الرحمان الموشير– بناء نموذج أمني لمكافحة الجرائم المعلوماتية وقياس فعاليته – رسالة مقدمة لأجل نيل شهادة الدكتوراه – قسم العلوم الشرطية – جامعة نايف للعلوم الأمنية – الرياض – السعودية –2009.
- عمر بن محمد العتبي، الأمن المعلوماتي ومدى توافقه مع المعايير المحلية والدولية – رسالة مقدمة لأجل نيل شهادة الدكتوراه – قسم العلوم الشرطية – جامعة نايف للعلوم الأمنية – الرياض – السعودية – 2010.
- يزيد بوحليط، السياسة الجنائية في مجال مكافحة الجرائم الإلكترونية في الجزائر، أطروحة لنيل شهادة دكتوراه العلوم، تخصص قانون خاص، جامعة باجي مختار، عنابة، 2016، ص 303–304 .

ب _ المذكرات:

ب1 _ مذكرات الماجستير:

- أحمد مسعود مريم : (آليات مكافحة جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون رقم 09–04)، مذكرة مقدمة لنيل شهادة ماجستير, منشورة, جامعة قاصدي مرباح, كلية الحقوق والعلوم السياسية, قسم الحقوق , الجزائر, 2013.

- نعيم سعيداني، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير، علوم جنائية، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، الجزائر، 2013.
- صغير يوسف، الجريمة المرتكبة عبر الانترنت،مذكرة لنيل شهادة الماجستير، جامعة مولود معمري، كلية الحقوق و العلوم السياسية، الجزائر، 2013.

ب2 _ مذكرات الماستر:

- سارة قادري، أساليب التحري الخاصة في قانون الإجراءات الجزائية، مذكرة ماستر أكاديمي، قسم الحقوق، كلية الحقوق و العلوم السياسية، جامعة قاصدي مرباح، ورقلة، الجزائر، 2014.
- عباسي خولة، الوسائل الحديثة للإثبات الجنائي في القانون الجزائري، مذكرة مكملة من مقتضيات نيل شهادة الماستر في الحقوق تخصص قانون جنائي، كلية حقوق و العلوم السياسية جامعة محمد خيضر، بسكرة، 2013.

3 _ المقالات العلمية:

- جميلة محلق، اعتراض المراسلات، تسجيل الأصوات و التقاط الصور في قانون الإجراءات الجزائية الجزائري، مجلة التواصل في الاقتصاد و الإدارة و القانون، جامعة باجي مختار، عنابة الجزائر، العدد 42، جوان 2015.
- عبد الخالق صالح عبد الله مغرب، الأدلة المستخدمة في ارتكاب الجريمة الالكترونية، مجلة العدل، العدد السابع و الثلاثون، السنة الرابعة عشر.
- فوزي عمارة، اعتراض المراسلات و تسجيل الاصوات و التقاط صور و التسرب كالإجراءات تحقيق قضائي في المواد الجزائية، مجلة العلوم الإنسانية، جامعة قسنطينة1، الجزائر، العدد 33 جوان 2010.
- محمد علي الجمال، التقاط الدليل المادي من مسرح الجريمة، مجلة الدراسات العليا، العدد الثاني يناير 2000.

4 _ الملتقيات:

- أمال حابت، الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الإلكترونية في القانون الجزائري، ورقة بحثية مقدمة لأعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، يومي 16 و 17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر.

- رضا هميسي، أحكام الشاهد في الجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية و المكافحة، يومي 16، 17نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر، 2015.
- سامية بلجراف، سلطة القاضي الجنائي في قبول و تقدير الدليل الرقمي، ورقة بحثة مقدمة إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة، جامعة محمد خيضر بسكرة، الجزائر، يومي 16 و 17 نوفمبر 2015.
- طارق محمد الجملي , الدليل الرقمي في مجال الإثبات الجنائي, ورقة عمل مقدمة للمؤتمر المغاربي الأول للمعلوماتية والقانون المنعقد في الفترة (28-29 /10 /2009) تنظمه أكاديمية الدراسات العليا , طرابلس.
- عبد المؤمن بن صغير، الطبيعة الخاصة للجريمة المرتكبة عبر الانترنت في التشريع الجزائري والمقارن بحث مقدم إلى أعمال الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة 16 و 17 نوفمبر 2015،كلية الحقوق جامعة بسكرة، الجزائر.
- عبد الناصر محمد محمود فرغلي, محمد عبيد سيف المسماري, الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية, بحث من ضمن أعمال المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي, جامعة نايف العربية للعلوم الأمنية, الرياض, 2007 .
- فاروق خلف، الآليات القانونية لمكافحة الجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني للجريمة المعلوماتية بين الوقاية و المكافحة، يومي 16 و 17 نوفمبر، 2015، كلية الحقوق، بسكرة، الجزائر.
- دورثي إي، قراصنة أنظمة الكمبيوتر, دينغ ورقة مقدمة للمؤتمر القومي الثالث عشر لأمن الكمبيوتر, واشنطن, ترجمة : آمنة علي يوسف, ديسمبر 1998.
- نشناش مينة،الإطار المفاهيمي للجريمة المعلوماتية، ورقة بحثية مقدمة لأعمال الملتقى الوطني حول الجريمة المعلوماتية، بين الوقاية و المكافحة، يومي 16 و 17 نوفمبر 2015، كلية الحقوق، جامعة بسكرة، الجزائر،2015 .
- يونس عرب, صور الجرائم الالكترونية واتجاهات تبويبها، ورقة عمل مقدمة ضمن ورشة عمل تطوير التشريعات في مجال مكافحة الجرائم الالكترونية، هيئة تنظيم الاتصالات، مسقط، سلطنة عمان، يومي 2 و 4 أفريل، سنة 2006.

5 _ النصوص الرسمية:

أ _ الإتفاقيات:

- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية, المحررة بالقاهرة بتاريخ : 21 / 12 / 2010, صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم: 14 – 251 المؤر في : 08 / 09 / (ج,ر) رقم :56 المؤرخة في : 25 / 09 / 2014 .
- الإتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ: 21 / 12 /2010 صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم : 14 – 252 المؤرخ في: 08 / 09 / 2014 ، (ج ، ر) رقم: 57 المؤرخة في: 28 / 09 / 2014 .

ب _ القوانين و الأوامر:

ب1 _ القوانين:

- القانون رقم 04_15 المؤر في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66_155المؤرخ في 08 / 06 / 1966، والمتضمن قانون العقوبات, الصادر في الجريدة الرسمية عدد : 71 بتاريخ 10 نوفمبر 2004.
- القانون رقم 06–22 المؤرخ في 20–12–2006، المعدل و المتمم لقانون الإجراءات الجزائية الصادر بالجريدة الرسمية للجمهورية الجزائرية، عدد 84، المؤرخة في 24 ديسمبر 2006.
- القانون رقم: 09–04 مؤرخ في: 5 أوت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها, (ج.ر) رقم 47 المؤرخة في: 2009/08/16.

ب2 _ الأوامر:

- الأمر رقم: 66–155 المؤرخ في: 08 جوان 1966 الذي يتضمن قانون الإجراءات الجزائية الجزائري، (ج.ر) رقم: 48، الصادرة بتاريخ 1966/06/10، المعدل والمتمم.

د – قرارات المحكمة العليا:

- قرار محكمة النقض المصرية في 20 / 11 / 1986 – رقم 179 – المبادئ القانونية.

6 _ المحاضرات:

- سيدهم سيدي محمد، محاضرة حول التسرب حسب تعديل قانون الإجراءات الجزائية، محكمة فرندة، مجلس القضاء تيارت، في 20 / 03 / 2008.

7_ مواقع الإنترنت:

- حافظ بن زلاط، التنصت الهاتفي في ظل قانون الإجراءات الجزائية، بحث متوفر على الموقع الرسمي لمجلة (القانون و الأعمال) لسنة 2015، على الرابط الآتي:

http://www.droitentreprise.org/web/

- مفهوم التمويل الإلكتروني، منشور على الرابط الآتي:

http://www.alyaum.cm/article/1091233

- تقرير الجريمة الإلكترونية، منشور على الرابط الآتي:

([1]) http://hrdoegypt.org/wp-content/uploads/2014/12/2_تقرير-الجريمة-الإلكترونية-_pdf /

ثانيا : المراجع باللغة الأجنبية.

Deuxiémement: Référence en Français

1 - Ouvrages:

codes:

- Code de procédure pénale francais

Les Auteurs:

- . Asimplified guide to digital evidance, nationale forensic science technology centre, florida, 2009.

- David forest et gautier kaufman, **droit de l'informatique gualino éditeur**, extenso édition, France , 2010.
- Eogham asey. Digital Evidence And Computer Crime. Forest Science Computer And The Internet. Second Edition. Academic Press An Imprint Of Elservier. London. 2004.
- Michaud le juge d'instruction et l'expert, R. S. c , 1975
- Myriam Quéméner . Yves Charpenel. La cybercriminalité. Edition Economica. Paris. France. 2010.
- Nidal EL chaer .la criminalité informatique devant la justice pénale édition juridique sader . beyrouth . liban .2004

الملخص:

لا تترك الجرائم المعلوماتية آثارا مادية يمكن إدراكها بالحواس على عكس الجرائم التقليدية الأمر الذي أضحى يشكل تحديا كبيرا من الناحية التقنية والقانونية لإثباتها، وعليه يعد الدليل الإلكتروني الوسيلة المناسبة لذلك، حيث تدخل المشرع الجزائري بنصوص قانونية إجرائية تساعد على استنباط الدليل الذي يتوافق مع الطبيعة الخاصة لهذه الجرائم، فبدأ المشرع بتعديل قانون الإجراءات الجزائية بموجب القانون رقم: 06-22 المؤرخ في 20 ديسمبر 2006، أين نص على أساليب خاصة للبحث والتحري تتلائم وطبيعة هذه الجرائم المستحدثة وذلك بموجب المواد: (65 مكرر 5 – 65 مكرر 18) كاعتراض المراسلات وتسجيل الأصوات... الخ. بالإضافة إلى إصداره للقانون 09 -04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على جملة من الإجراءات الوقائية كمراقبة الاتصالات الإلكترونية، حيث كان هدف المشرع الوقاية من الجريمة قبل حدوثها، وعليه اعترف المشرع الجزائري بحجية الدليل الإلكتروني في الإثبات الجنائي بصفة عامة بموجب المادة (323 مكرر1 من القانون المدني) وأعطاه نفس درجة الدليل التقليدي، وذلك بإتباع إجراءات حديثة تتوافق وتكنولوجيات الإعلام والاتصال لاستخلاص الدليل الإلكتروني، من هذه البيئة الافتراضية والتي تشكل صعوبات بالغة لأجهزة البحث والتحري.