

وزارة التعليم العالي والبحث العلمي

جامعة عباس لغرور خنشلة

كلية الحقوق والعلوم السياسية

نيابة العمادة للدراسات بما بعد التدرج

قسم الحقوق

والبحث العلمي والعلاقات الخارجية

وسائل الإثبات في الجريمة المعلوماتية

مذكرة مكملة لنيل شهادة الماجستير في تخصص: العلوم الجنائية.

إشراف الدكتور:

سعادته العيد

إعداد الطالب:

بحريه هارون

لجنة المناقشة

اللقب والإسم	الرتبة العلمية	الجامعة الأصلية	الصفة
د.مباركي دليلة	أستاذة محاضرة- قسم أ-	جامعة الحاج لخضر باتنة	رئيسا
د.سعادته العيد	أستاذ محاضر- قسم أ-	جامعة عباس لغرور خنشلة	مقررا ومشرفا
أ.د.زواقري الطاهر	أستاذ التعليم العالي	جامعة عباس لغرور خنشلة	عضوا مناقشا
د.قصورى رفيقة	أستاذة محاضرة- قسم أ-	جامعة عباس لغرور خنشلة	عضوا مناقشا

السنة الجامعية: 1434-1435 هـ / 2013-2014م

مقدمة:

إن ثورة المعلومات سمة عصرنا الحالي فنحن نعيش الآن في عصر الحاسوب و الانترنت ولا بد أن تنعكس آثاره على كل من يعيش فيه بمن فيهم رجال القانون، ومع التطور الهائل في ثورة المعلومات و الاستخدام المتزايد للحاسوب و المعالجة الآلية للمعلومات، تجسد في الواقع وبمعدل متزايد العديد من أوجه الاستغلال المتعسف و الأفعال المقترنة بسوء النية لأداة المعالجة الآلية للمعلومات، ما أظهر أنواعا جديدة من الجرائم القائمة على الاستغلال غير المشروع لهذه التكنولوجيا، اصطلحت بالجرائم المعلوماتية و التي أدت إلى ثورة هائلة وانقلاب خطير في النظرية التقليدية للجريمة و الجزاء، إذ وفرت طرقا و وسائل جديدة للأشخاص لارتكاب جرائمهم، دون أن يتركوا أثرا أو يتحملوا جهودا كبيرة، خصوصا باعتماد الغالبية العظمى من هذه الجرائم على إدخال أوامر مختصرة وبسيطة للحاسوب، ليتكفل هو بعد ذلك بالباقي .

ولذلك فإن ظاهرة جرائم المعلوماتية توجب على الجميع التنبيه لأهمية وحجم المخاطر و الخسائر الناجمة عنها باعتبارها تستهدف المعطيات بدلالاتها التقنية الواسعة ، وأصبح متطلباً من أجهزة العدالة الجنائية التي تسعى إلى محاربة الجريمة من خلال الاستعانة بوسائلها المتاحة لديها و التي نظمها التشريع الإجرائي لإثباتها وطرحها أمام القاضي المختص للفصل فيها بحكم عادل يكون عنوانا للحقيقة أن تتعامل مع أشكال مستحدثة للجريمة تتطلب وسائل حديثة متطورة لإثباتها لذا كان من المنطقي أن تكون مسألة قبول ومصداقية وحجية الأدلة الجنائية المستخرجة من الكمبيوتر لإثبات الجريمة المعلوماتية، إحدى المسائل الهامة التي تعرض لها المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات، الذي عقد في ريو دي جانيرو بالبرازيل في الفترة من 4-6 سبتمبر 1994، كما أن هذه المسألة أيضاً كانت محل بحث على المستوى الدولي في فريبورج Warburg بألمانيا لبحث جرائم الكمبيوتر والتي عقدت في الفترة من 5-8 أكتوبر 1992.

كما طرح بتر بتلرز أستاذ بجامعة نيويورك مسألة الذكاء الاصطناعي في الإثبات الجنائي في المؤتمر الدولي الثاني للاتجاهات الحديثة في الإثبات الجنائي المنعقد في أمستردام سنة 1999

كأسلوب مستحدث يمكن أن يكون مقبولا ومؤهلا لمواكبة متغيرات الجريمة المعلوماتية، كما أصدرت الأمم المتحدة مرشداً عاماً حول مكافحة جرائم الكمبيوتر في يناير 2000م، وفي 23 نوفمبر 2001 جرى إبرام اتفاقية دولية خاصة بمكافحة الجريمة الالكترونية في هذه الاتفاقية التي باتت تعرف باتفاقية بودابست ، وهي أول الاتفاقيات الدولية التي اختصت بمكافحة الجريمة المعلوماتية بإشراف المجلس الأوروبي، والتي دخلت حيز النفاذ في 2007/1/1. إذا كان الاهتمام على المستوى الدولي يأخذ منحى إيجابياً كما وكيفا، إلا أن الاهتمام على المستوى العربي لا يزال متردداً في اقتحام هذا المجال بعلمية وإيجابية أكثر ، لتسهم في حل المشكلات القانونية المترتبة على استخدام الكمبيوتر و الشبكات المعلوماتية في ارتكاب الجريمة فالمشرع الجزائري وسعياً منه لمواكبة التطور المستمر للجريمة المعلوماتية ، فإنه ادخل تعديلات على قانون العقوبات تضمنه القانون 15/04، الذي احتوى مجموعة من النصوص تصنف وتعاقب على الجرائم المعلوماتية ، كما انه خص قانون الإجراءات الجزائية بتعديل حملته القانون 22-06، استحدث من خلاله مجموعة من النصوص الإجرائية كوسائل جديدة لمواكبة الجرائم المستحدثة، ليتدعم بالقانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها، الذي جاء بقواعد للوقاية من الجرائم الافتراضية ودعم وسائل مكافحتها من خلال رصدها المبكر وجمع الأدلة عنها، دون أن يكون له قانون مستقل ينظم قواعد الإثبات الجنائي ، في خضم كل ذلك لا يزال موضوع إثبات الجريمة المعلوماتية يطرح صعوبات جمة دفع بالكثير من القانونيين و المختصين إلى البذل في سبيل اقتراح أفضل وأنجع الطرق للتصدي للظاهرة.

أ- أهمية البحث: يتناول الباحث أهمية البحث من زاويتين العلمية و العملية كما يلي:

1- الأهمية العلمية :

تتجلى الأهمية العلمية في ضرورة إجراء أبحاث قانونية تتناول البحث حول مدي مساهمة التشريع الوطني للتطور التقني المصاحب لإثبات الجرائم المعلوماتية مع محاولة الباحث إلقاء الضوء على الموضوع من زاوية الإثبات الجنائي في الجرائم المعلوماتية، لقللة الدراسات العلمية في

هذه الجزئية التي تعتبر بالغة الأهمية من الناحية النظرية ومسايرة لتطور الجريمة المستمر ، مع محاولة إجراء دراسة متكاملة تثري المكتبات الجامعية الوطنية ، وتساعد المشرع في تحيين بعض النصوص بعد إجراء مقاربات وجعلها أكثر انسيابية مع التطور التكنولوجي الحاصل حولنا ، مع إثراء البحث العلمي من خلال وضع لبنة علمية تضاف إلى المجهودات العلمية الدعوية بحيث يستعان بها في دراسات علمية مستقبلية.

2- الأهمية العملية :

تتجلى الأهمية العملية في إلقاء الضوء على وسائل ناجعة تكفل مواجهة الجريمة المعلوماتية من حيث إثباتها، مع تبني أدلة علمية جديدة تكفل لها غطاء قانوني تتماشى مع طبيعة الجريمة بحيث تضمن إثبات الجريمة لتوقيع الجزاء على المجرمين المعلوماتيين.

كما أن للبحث أهمية اجتماعية واقتصادية تتمثل في حماية أنظمة المعلوماتية الخاصة بأفراد المجتمع أو مؤسسات الدولة، ومن منظور اقتصادي حماية الشركات سواء الوطنية أو الأجنبية من الإجرام المعلوماتي، وذلك بصياغة قواعد قانونية أكثر حماية تعزز الثقة في المعاملات المعلوماتية وتخلق نوع من الأمن المعلوماتي ما يعزز المكانة الاقتصادية للمؤسسات المالية ويجلب رؤوس أموال جديدة للاستثمار.

ب- أسباب اختيار الموضوع : تتلخص أسباب اختيار الموضوع إلى أسباب شخصية وأخري موضوعية نجلها في ما يلي:

1- الأسباب الشخصية :

تتمثل الأسباب الشخصية في الرغبة في البحث في مجال الجريمة المعلوماتية بالنظر لطبيعة الجريمة التقنية المتطلبة م عارف علمية إلى جانب التكوين القانوني ، مع وجود ميولات مستمدة من تساؤلات علمية حول كيفية إثبات الجريمة المعلوماتية من الناحية الإجرائية ، خصوصا وان التكنولوجيا الحديثة أدت إلى انقلاب في النظرية التقليدية للجريمة والجزاء ووفرت طرقا ووسائل جديدة للأشخاص لارتكاب جرائمهم، وبالمقابل فرضت على جهات إنفاذ القانون التفكير و البحث

لإيجاد حلول قانونية تناسب الجريمة ، وتتعدى حدود فكر المجرم المعلوماتي ، فالأمر يتطلب من رجال القانون أن يتصدوا للجريمة بالبحث العلمي و الوسائل العلمية الحديثة التي توصل إليها العقل البشري.

2- الأسباب الموضوعية :

تتلخص الأسباب الموضوعية للبحث في تصاعد منحي الجرائم المعلوماتية بشكل كبير نتيجة تزايد استخدام الحواسيب تماشياً مع الاستخدامات المهنية من جهة ، ومع اتساع الشبكات العالمية من جهة أخرى ما جعل هذا الفضاء مكاناً خصباً للتعدي على البيانات و المعطيات الخاصة بالأشخاص و المؤسسات في صور مختلفة للجرائم المعلوماتية، وهو ما يعود بالضرر على الأفراد والدولة ، ولضمان عدم إفلات مرتكبي هذه الجرائم من الجزاء، بات من الضرورة التفكير في وضع منظومة قانونية مهيبة تتماشى مع تطور الجريمة ، فكان لا بد من اختيار زاوية نساهم فيها في بناء هذه المنظومة، لذلك أردنا أن تكون مشاركتنا من باب وسائل الإثبات الجنائي باعتباره حجر الأساس في التصدي للجرائم المعلوماتية.

ت- إشكالية البحث:

إن البحث في الإثبات ووسائله في إطار مدى انقائها مع التقنية الحديثة يبدو غير ذي معني إذا لم يكن مدعماً بتوفيق من قبل التقنية ذاتها، مع كل ما يتم إثباته في هذا الشأن، وهذا القول له أساس من المنطق، سيما حال تلمسنا لنوعية الإشكاليات التي يمكن أن تثيرها الجريمة المعلوماتية في مدى تجاوبها مع الحالة التي يعيشها القانون في النطاق الرقمي، فقد أنتجت حالة الصراع بين المجتمعات و بين الجريمة في ثوبها الجديد نظرة جديدة إلى الإثبات الجنائي تمثلت في سؤال فرض نفسه على دراسات القانون الجنائي ، وهو ما نصيغه كإشكالية للبحث من خلال التساؤل التالي:

ما مدى تجاوب وسائل الإثبات في صورتها التقليدية والحديثة مع إثبات الجريمة المعلوماتية ؟

وهي الإشكالية التي تنفرع منها مجموعة من التساؤلات الفرعية التالية :

- ما هو مفهوم الإثبات الجنائي ؟
- ما هي الجريمة المعلوماتية ؟ ومن هم أطراف الجريمة المعلوماتية؟
- ما هي وسائل الإثبات التقليدية ؟ و إلي أي مدى يمكن الاستعانة بها في إثبات الجريمة المعلوماتية ؟
- ما هو الدليل الرقمي ؟ و ما هي وسائل استخلاصه؟ وما مدى حجيته في الإثبات الجنائي؟

ث- الهدف من البحث :

- يسعى هذا البحث إلى تحقيق عدة أهداف يمكن تلخيصها في العناصر التالية:
- الإجابة على إشكالية البحث و تساؤلاته الفرعية.
 - عرض الآليات القانونية التي تبناها المشرع الجزائري لمواجهة الجريمة المعلوماتية.
 - البحث في مدى مساهمة وسائل الإثبات التقليدية في إثبات الجريمة المعلوماتية.
 - التعريف بالأدلة الرقمية الحديثة ومعرفة كيفية استخلاصها.
 - البحث عن مدى حجية الأدلة الرقمية باعتبارها وسيلة جديدة فرضت نفسها ضمن وسائل الإثبات الجنائي.
 - ما مدى توفيق المشرع في تطوير الآليات القانونية مقارنة بالتشريعات المقارنة في مجال التصدي و الإثبات في الجريمة المعلوماتية.

ج- المنهج المتبع في البحث:

- بغية التوصل إلى إجابة على إشكالية هذه الدراسة وتساؤلاتها الفرعية، اعتمدت على المنهج الوصفي المقترن بآلية التحليل في الدراسة لإعطاء صورة أوضح عن طبيعة الجريمة المعلوماتية وكيفية إثباتها ، وذلك من خلال تحليل النصوص ، و الوقوف على المراد منها نصوصا

وروحاً، مع الاعتماد على المنهج المقارن الذي يناسب طبيعة الدراسة بسبب حداثة الجريمة المعلوماتية وعدم اكتمال نصوصها التشريعية، لذلك استلزم إلقاء الضوء على القوانين المقارنة اللاتينية منها، و الانجلوسكسونية خصوصاً، لإجراء مقاربات تساعد على التحليل و تقييم النصوص القانونية وفقاً لما تتطلبه مقتضيات الدراسة.

ح- الدراسات السابقة:

من خلال بحثي في الموضوع فإنني لم أعر على دراسات متكاملة سابقة تتناول موضوع الإثبات في الجريمة المعلوماتية لأبني عليها دراستي، فكل المذكرات و الرسائل التي عثرت عليها تتناول دراسة الجريمة المعلوماتية في إطارها المفاهيمي بشكلها العام، أو تلك التي تناولت الدليل الرقمي من جانبه التقني المحض، دون الخوض في مجال حجيته في إثبات الجريمة المعلوماتية.

خ- صعوبات البحث:

إن أهم الصعوبات التي صادفتها و أنا بصدد البحث تتمثل في الطبيعة التقنية المحضة للجريمة المعلوماتية مقارنة مع دراستنا النظرية القانونية هذا من جهة، ومن جهة أخرى قلة المراجع التي تناولت موضوع الإثبات المتفق بالإجماع على صعوبته في هذا النوع من الجرائم، يضاف إلى ذلك ندرة و خلو المكتبات الوطنية من المراجع باللغات الأجنبية التي تطرقت لهذا الموضوع.

د- خطة البحث :

للإجابة على إشكالية البحث ارتأيت تناول موضوع "وسائل الإثبات في الجريمة المعلوماتية" وفقاً للتقسيم الثنائي للخطة مستعينا بمبحث تمهيدي كما يلي:

المبحث التمهيدي تناول الإطار المفاهيمي للإثبات الجنائي و الجريمة المعلوماتية، وتضمن ثلاث مطالب تناولت في المطلب الأول مفهوم الإثبات الجنائي، ثم في المطلب الثاني ماهية الجريمة المعلوماتية، أما المطلب الثالث تضمن أطراف الجريمة المعلوماتية.

الفصل الأول خصص لإثبات الجريمة المعلوماتية بالوسائل التقليدية ، وتم تقسيمه إلى مبحثين تناول المبحث الأول إثبات الجريمة المعلوماتية بالوسائل الشخصية ، فيما خصص المبحث الثاني لإثبات الجريمة المعلوماتية بالوسائل المادية و القرائن.

الفصل الثاني تضمن إثبات الجريمة المعلوماتية بالدليل الرقمي ، وتم تقسيمه إلى مبحثين ، المبحث الأول لهاهية الدليل الرقمي، بينما تناول المبحث الثاني حجية الدليل الرقمي في الإثبات الجنائي.

الخاتمة: تضمنت مجموعة من النتائج والاقتراحات.

إن الإثبات في الجريمة المعلوماتية يتطلب وضع له إطار عام يحدد الأساس المفاهيمي موضوع للدراسة ، باعتباره القاعدة التي نستند إليها، لتكون المنطلق في البحث و تحليل الموضوع ومن أجل ذلك تطرح تساؤلات مبدئية حول: مفهوم الإثبات الجنائي بصفة عامة (المطلب الأول) وتتعمق أكثر في البحث عن فهم طبيعة الجريمة المعلوماتية (المطلب الثاني) ومن هم أطرافها؟ (المطلب الثالث)، وهو ما سنحاول الإجابة عنه في هذا المبحث التمهيدي.

المطلب الأول

مفهوم الإثبات الجنائي.

يعتبر الإثبات الجنائي العمود الفقري في الخصومة الجزائية فهو يبدأ من أول مرحلة في الدعوى ويستمر معها إلى غاية صدور الحكم إما بالبراءة أو الإدانة ولتحديد مفهوم الإثبات في إطاره المفاهيمي نعرض على تعريف وسائل الإثبات (الفرع الأول) ثم نحدد أهمية الإثبات (الفرع الثاني) ومن جهة أخرى نبين أنواع أنظمة الإثبات (الفرع الثالث).

الفرع الأول: تعريف وسائل الإثبات.

يتركب مصطلح "وسائل الإثبات" من كلمتين هما الوسائل و الإثبات، لذلك نقسم هذا الفرع إلى عنصرين نتناول في كل واحد منهما التعريف اللغوي و الاصطلاحي لكل مصطلح، لنستتير به ونتحرر من كل قيد ونحن على بساط البحث.

أولاً- تعريف الوسائل:

إن مصطلح الوسائل كثيرا ما يتردد على ألسنة دارسي القانون بشتى فروع و نظرا لكونه حجر زاوية في بحثنا كان لزاما علينا معرفة المعنى اللغوي والاصطلاحي للوسائل كمايلي:

أ-المعنى اللغوي للوسائل: الوسائل جمع وسيلة وتعني الوصلة بضم الواو، الاتصال، ما تصل بين الشئين.وهي ما يتقرب به الإنسان وما يعتمده في أمر ما⁽¹⁾.

(1) عصام نور الدين معجم نور الدين الوسيط عربي عربي، الطبعة الثانية ، دار الكتب العلمية، سنة 2009، بيروت لبنان، ص 1109.

المبحث التمهيدي.....الإطار المفاهيمي للإثبات الجنائي و الجريمة المعلوماتية.

وفي حديث الآذان " اللهم آت محمد الوسيلة" ، هي في الأصل ما يتوصل به إلى الشيء ويتقرب به والمراد به في الحديث القرب من الله تعالى (1).

ويقول تعالى " يا أيها الذين آمنوا اتقوا الله وابتغوا إليه الوسيلة " (2) أي اتبعوا الشيء الذي يوصلكم ويقربكم من الله.

ب-المعنى الاصطلاحي للوسائل: المقصود بالوسائل اصطلاحاً هي كل ما يوصل إلى تحقيق هدف معين (3).

ثانياً- تعريف الإثبات :

نتناول معنى الإثبات من الناحية اللغوية ومن الناحية القانونية كما يلي:

أ-تعريف الإثبات من الناحية اللغوية: الإثبات لغة هو تأكيد الحق بالدليل و الحجة و يقال "لا أحكم بكذا إلا بثبت" بفتح الباء أي بحجة (4)، وهو الحجة والبيينة و أثبت حجته بمعنى أقامها و أوضحها، وأثبته يعني عرفه حق المعرفة (5). والإثبات مشتق من كلمة "ثبت" بمعنى استقر ويقال ثبت الشيء أي أثبته، و التثبيت أي إعطاء أو تلقين الحجة ، والمثبت كلام غير منفي (6).

والإثبات نحوياً ضد النفي كقولنا أتى زيد ف "أتي" فعل مثبت غير منفي الحق، مثبت أكده بالبيينة القاطعة والحجة الدامغة (7)، ويقول تعالى في محكم تنزيله " يثبت الله الذين آمنوا بالقول

(1) ابن منظور أبو الفضل جمال الدين محمد بن مكرم بن منظور الإفريقي المصري، لسان العرب، الطبعة الأولى، دار إحياء التراث بيروت، ص 4838.

(2) سورة المائدة ، الآية 35.

(3) تافرونت الهاشمي، وسائل إثبات الدفاع الشرعي، رسالة مقدمة استكمالاً لنيل درجة الماجستير تخصص الشريعة و القانون لعام جامعة العقيد الحاج لخضر باتنة، السنة الجامعية 2001-2002 ص 44.

(4) محمد بن أبي بكر الرازي، مختار الصحاح، دار الجبل، بيروت، 1987، باب الثاء ، ص 35.

(5) ابن منظور أبو الفضل جمال الدين محمد مكرم بن منظور الإفريقي المصري ، معجم لسان العرب، الطبعة الأولى، دار إحياء التراث، بيروت لبنان، ب. س. ط، ص 468.

(6) فيصل سعيد غريب، التوقيع الالكتروني وحجته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، 2005، ص 9.

(7) عصام نور الدين ، المرجع السابق، ص 42.

الثابت⁽¹⁾، ومن ثمة فالإثبات بالمعنى العام يعني كل ما هو محقق ومستقر و واضح ومعروف تعريفا جيدا ناف للجهالة⁽²⁾.

ب-تعريف الإثبات من الناحية القانونية: لم يجمع فقهاء القانون على تعريف موحد للإثبات ولم يتوصلوا إلى صياغة تعريف موحد له يكون مقبولا من الجميع لذلك اتخذ الإثبات عدة معاني تحصر في ضيق وسعة معناه:

ففي مفهومه الضيق يقصد بالإثبات "كل الوسائل التي تقنع" وفي هذا الصدد فالإثبات يتمثل في "الطرق التي يستعملها الخصم لإقناع القاضي بصحة الواقعة وحقيقة قيام الحق مثل الأوراق المحررة والشهود..الخ"⁽³⁾. و يقصد به كذلك " البرهان المبين للحقيقة " ولذلك عادة ما يقال أن لدي دليل الإثبات، ويؤخذ على هذا التعريف أن كلمة الإثبات لا تفيد في كثير من الأحيان الحقيقة وإنما خلاصة قد تكون مطابقة لحقيقة استنتجها القاضي عن طريق تقدير وسائل الإثبات المتوفرة لديه، وفي مفهوم آخر فإن كلمة الإثبات " تدل على تقديم عناصر القرار للقاضي " ، أما حسب مفهومه الواسع وهو الأكثر استعمالا فإن كلمة الإثبات " تنصرف إلى مجموع الوسائل المستعملة للوصول إلى إظهار الحقيقة حول فعل معين "⁽⁴⁾. وعرف كذلك بأنه " ما يتخذ من قبل سلطات العدالة في مجالي التحقيق و الحكم من إجراءات لكشف الغموض و إظهار الحقيقة في ظل ضمانات الحريات و حماية الحياة الخاصة ومراعاة قرينة البراءة وحقوق الإنسان "⁽⁵⁾.

(1) سورة إبراهيم، الآية 27.

(2) فيصل سعيد غريب، المرجع السابق، ص 9.

(3) الغوثي بن ملحّة قواعد وطرق الإثبات ومباشرتها في النظام القانوني الجزائري، الديوان الوطني للأشغال التربوية، الطبعة الأولى سنة 2001، ص 9.

(4) محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، ديوان المطبوعات الجامعية الجزائر سنة 1999، ص 105.

(5) محمد محمد محمد غنّب ، استخدام التكنولوجيا الحديثة في الإثبات الجنائي ، مطبعة السلام الحديثة مصر، سنة 2007، ص 9.

كما أن الإثبات بمعناه القانوني هو " إقامة الدليل أمام القضاء على واقعة مدعى بها بكافة الطرق و الإجراءات التي حددها القانون"⁽¹⁾، وهو ما أكدته محكمة النقض المصرية⁽²⁾.

وتعني كلمة الإثبات الوسائل التي يتذرع بها أطراف الرابطة الإجرائية للوصول إلى الدليل بالمعاينة أو الخبرة أو الكتابة أو الشهادة أو القرائن وغيرها⁽³⁾.

وخلاصة هذه التعاريف فإن الإثبات يسع الوسائل فكل تعريف للإثبات إلا وتضمن في طياته الوسائل، ومن ثمة فالإثبات مصطلح يشمل الوسائل وهي الطرق والأدوات، وبتعبير آخر فإن وسائل الإثبات هي " الحجج و الأدلة المشروعة التي تؤيد الدعوى و يصل بها القاضي إلى إثبات حق أو نفي ادعاء"⁽⁴⁾.

إن المتمعن في معني الإثبات يجد من الدليل أو الحجة والبرهان جوهره لذلك تعين علينا معرفة ما هو الدليل ؟ وهل أن الإثبات هو الدليل أم أن هناك تمييز بينهما؟ وهو ما سنتطرق إليه في العنصر الموالي.

ثانيا- تعريف الدليل الجنائي وتمييزه عن الإثبات الجنائي:

نتناول في هذا العنصر تعريف الدليل ثم نميزه عن الإثبات الجنائي في عنصر موالي له.

أ- تعريف الدليل: وردت عدة تعريفات للدليل الجنائي فعرف بأنه " الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها"⁽⁵⁾.

(1) مصطفى يوسف ، مشروعية الدليل في المسائل الجنائية في ضوء الفقه و القضاء، دار الجامعة الجديدة للنشر ، الإسكندرية سنة 2011، ص11.

(2) بقولها " الإثبات هو إقامة الدليل أمام القضاء بالطرق التي حددها القانون، فهو قوام الحق الذي يتجرد من قوته ما لم يقم الدليل عليه"، مصطفى يوسف، نفس المرجع، ص12.

(3) نصر الدين مروك، محاضرات في الإثبات الجنائي النظرية العامة للإثبات الجنائي، الطبعة الثالثة ، دار هومة، الجزائر، 2009، الجزء الأول، ص 167.

(4) تافرونت الهاشمي ، المرجع السابق، ص44.

(5) عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن، دار الجامعة الجديدة، مصر، سنة 2010، ص 51.

وأنه " الوسيلة المتحصلة بالطرق المشروعة لتقديمها للقاضي لتحقيق حالة اليقين لديه و الحكم بموجبها " (1).

كما عرف أيضا بأنه " النشاط الإجرائي الحال و المباشر من أجل الحصول على اليقين القضائي وفقا لمبدأ الحقيقة المادية وذلك ببحث أو تأكيد الاتهام أو نفيه " ، بينما يري جانب من الفقه أن التعريف الراجح للدليل هو " الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه ". وعلّة ترجيح هذا التعريف يعود لمرحلة الحكم باعتبارها المرحلة الحاسمة التي تقرر المصير النهائي في الدعوى الجنائية (2).

في حين نجد أن قضاة المحكمة العليا للجزائر يعرفون الدليل بأنه " البينة أو الحجة التي يستمد منها القاضي البرهان على اقتناعه بالحكم الذي يصدره قد يكون الدليل مباشرة كالاقراراف و شهادة الشهود و تقرير الخبرة ، أو غير مباشر كالقرائن" (3).

ب- التمييز بين الدليل و الإثبات الجنائي:

لقد دأب الفقه إلى استخدام كلمة إثبات للتعبير بها عن الدليل و كلمة الدليل للتعبير بها عن الإثبات، بحيث يبدو و كأنهما كلمتان مترادفتان، هذا و بالرغم من الصلة الوثيقة بينهما إلا أنه لا يمكن تصور وجود تطابق كامل بينهما على الإطلاق، ذلك أن كلمة إثبات بالمعنى العام يمكن أن تطلق على كل المراحل التي تربط العملية الإثباتية بدءا من جمع عناصر التحقيق و الدعوى تمهيدا لتقديمها لسلطة التحقيق الابتدائي، بالإضافة إلى ما تتوصل إليه سلطة التحقيق القضائي و انتهاء بتمحيصها أثناء جلسة المحاكمة التي تحكم بناءا على ما تم تقديمه من أدلة، مشكلة قناعتها اليقينية، سواء بالإدانة أو البراءة، ومن ثم شاع القول بان الإثبات هو التنقيب عن الدليل وتقديمه

(1) عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري ، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية (دراسة تطبيقية مقارنة)، بحث مقدم الى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي ، المنعقد بالرياض في 12-14 نوفمبر 2007 ، جامعة نايف العربية للعلوم الأمنية ، ص 12.

(2) نصر الدين مروك، محاضرات في الإثبات الجنائي، أدلة الإثبات الجنائي ، الطبعة الثالثة ، دار هومة، الجزائر، 2009، الجزء الثاني، ص 8.

(3) نصر الدين مروك، نفس المرجع، ص8.

المبحث التمهيدي.....الإطار المفاهيمي للإثبات الجنائي و الجريمة المعلوماتية.

وتقديره لاستخلاص السند القانوني للفصل في الدعوى⁽¹⁾، ويرى الدكتور هلاي عبد اللاه أحمد في خلاصة تقديره للإثبات أن كلمة الإثبات أعم وأشمل من كلمة دليل⁽²⁾.

أما فيما يخص التفرقة بين الدليل و الوسيلة، فانه هناك من يؤكد على ضرورة التفرقة بين مضمون الدليل المتمثل في الواقعة التي تصل إلى القاضي، وبين الوسيلة التي عن طريقها وصلت تلك الواقعة إلى علمه، رغم ذلك فانه هناك من يعتبر الدليل هو نفسه الوسيلة فالدليل هو الوسيلة المبحوث عنها في التحقيقات بغرض إثبات واقعة تهم الجريمة أو ظرف من ظروفها المادية أو الشخصية، وان المقصود بالوسيلة عند اعتبارها دليلا هي الوسيلة العلمية التي تحقق الدليل في حد ذاته، فهي مصدر وجوده، ويؤكد أصحاب هذا الاتجاه بعدم الفصل بين الدليل و الوسيلة⁽³⁾.

الفرع الثاني: الهدف من الإثبات الجنائي.

إن غاية الإثبات من الوجهة المجردة واحدة تهدف بالدرجة الأولى إلى إثبات وتأكيد وجود الحق أو الواقعة المتنازع فيها بالوسيلة المشروعة التي يقرها القانون بصفة عامة، وذلك بغض النظر عن نوع القضاء المناط به الفصل في ثبوت ذلك الحق أو تلك الواقعة الجنائية، فالعملية الإثباتية في صورتها المطلقة لا تختلف باختلاف نوع النزاع أو الحق، أين يسعى فيها كل طرف إلى تأكيد موقفه وتعزيز حقيقة مركزه، ويزول التجرد إذا كان الفرع المختص بنظر الدعوى له سمات ومميزات خاصة كالفرع الجنائي المتميز باستقلال قواعد الإثبات الجنائي، وقد عبر اهرنج عن تلك الأهمية بقوله بان " الإثبات هو فدية الحق"⁽⁴⁾.

(1) نصر الدين مروك، المرجع السابق ، ص9.

(2) جمال نجيمي، إثبات الجريمة على ضوء الاجتهاد القضائي دراسة مقارنة، دار هومة للطباعة والنشر و التوزيع ، الجزائر، سنة 2012 ، ص23.

(3) صالح عبد الحي، الإثبات الجنائي في الجريمة الدولية، مذكرة مكملة لنيل شهادة الماجستير في القانون الجنائي تخص قانون جنائي دولي، المركز الجامعي عباس لغرور خنشلة، السنة الجامعية 2011-2012، ص 89-90.

(4) أحمد ضياء الدين محمد ، مشروعية الدليل في المواد الجنائية دراسة تحليلية مقارنة لنظريتي الإثبات و المشروعية في مجال الإجراءات الجنائية، دار النهضة العربية، مصر، سنة 2010 ، ص139 و 156.

ولعل الهدف الأساسي للإثبات في المواد الجنائية هو إظهار الحقيقة سواء فيما يتعلق بالأفعال المرتكبة أو فيما يتعلق بشخصية المتهم الذي يكون محل متابعة جنائية، تماشيا و مقتضيات السياسة الجنائية الحديثة، كما أن إظهار الحقيقة انشغال رئيسي لدى المشرع الجزائري بحيث تردد ذكر هذه العبارة عدة مرات في نصوص قانون الإجراءات الجنائية، وخصوصا في نص المواد 1/68 و 1/69 و 286 من ق.إ.ج (1).

وتظهر أهمية الإثبات الجنائي في كونه يتعلق بالجريمة نفسها التي تنتمي بدورها إلى الماضي ولم يكن في وسع المحكمة أن تعاينها بنفسها وتتعرف على حقيقتها وتستند إلى ذلك فيما تقضي به من شأنها، ومن ثمة تعين عليها أن تستعين بوسائل تعيد أمامها تفاصيل ما حدث وهذه الوسائل هي أدلة الإثبات (2)، والتي تعتبر الروح الذي يقوم عليه الحكم الجزائي، فالبحث عن الأدلة كما يقول "بوزا"، يعد إحدى المشاكل الأساسية للإجراءات الجنائية، وبدون الدليل لا يتم الإسناد وتطبيق الجزاء (3).

الفرع الثالث: أنواع نظم الإثبات.

انقسمت نظم الإثبات في التشريعات المقارنة إلى عدة نماذج تبعا للسياسات الجنائية المختلفة بسبب اختلاف الأفكار القانونية من مجتمع لآخر، والتي أرست على إثرها قواعد تبلورت صياغتها إلى قوانين إجرائية تتماشى و طبيعة النظام المتبع وتمثل هذه الأنظمة في: نظام الأدلة القانونية (أولا) و نظام الاقتناع الذاتي للقاضي (ثانيا) وحديثا أضيف لهما نظام الأدلة العلمية (ثالثا).

(1) محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، المرجع السابق، ص 107-108.
- تنص المادة 1/68 من ق.إ.ج على أنه " يقوم قاضي التحقيق وفقا للقانون باتخاذ جميع إجراءات التحقيق التي يراها ضرورية للكشف عن الحقيقة".

- تنص المادة 1/69 من ق.إ.ج على أنه "يجوز لوكيل الجمهورية سواء في طلبه الافتتاحي لإجراء التحقيق أو بطلب إضافي في اية مرحلة من مراحل التحقيق أن يطلب من القاضي المحقق كل إجراء يراه لازما لإظهار الحقيقة".
- تنص المادة 286 من ق.إ.ج على أن "ضبط الجلسة وإدارة المرافعات منوطان بالرئيس، وله سلطة تقديرية تسمح له باتخاذ أي إجراء يراه نافعا لإظهار الحقيقة".

(2) مروك نصر الدين، محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي، الجزء الأول، المرجع السابق، ص 172.

(3) العيد سعادن، الإثبات في المواد الجنائية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في ال حقوق تخصص قانون جنائي، جامعة الحاج لخضر باتنة، السنة الجامعية 2005-2006، ص 18.

أولاً- نظام الأدلة القانونية:

ويقصد بنظام الأدلة القانونية ذلك النظام الذي يقيد القاضي بالإدانة وفقاً لشروط قانونية يحددها المشرع سلفاً، وفي هذه الحالة لا يتم الاقتناع بحرية في عملية عقلية إنما يصل إليه القاضي من خلال عملية تتوقف على قواعد محددة يحددها المشرع، ويتم ذلك عن طريق تحديد المشرع سلفاً للأدلة القانونية، وليس للقاضي أن يبحث فيما عدا هذه الأدلة عن مصدر آخر لاقتناعه الشخصي، لكنه متى توافرت هذه الأدلة فلا يكون القاضي سيد الموقف في تقدير قيمتها في الإثبات، بل يتمثل دوره في مجرد التحقق من قيامها ومراقبة توافر هذه الأدلة أو عدم توافرها وعلى ذلك لا يعدو عمل القاضي أن يكون سوي عملية حساب رياضية لا دخل فيها لاقتناعه الشخصي⁽¹⁾.

وساد هذا النظام قبل قيام الثورة الفرنسية، حينها كانت الأدلة مقسمة إلى أدلة كاملة وأدلة شبه كاملة أو إمارات قريبة وأخيراً الأدلة الناقصة، وكان هذا النظام ينطوي على ضمان للأبرياء وحمايتهم ضد تجاوزات نظام الإجراءات التفتيشي الذي كان سائداً والمرتكز على سرية جمع الأدلة دون إتاحة الفرصة للمتهم لمناقشتها، فنظام الأدلة القانونية كان يلزم القاضي أن يحكم ببراءة المتهم إذا لم يجتمع لديه العدد من الأدلة الذي يتطلبه القانون، ولا يسمح بإعدام متهم إلا إذا توافر الدليل الكامل، ولتكلمة دليل غير كامل لا بد من الحصول على اعتراف أياً كانت وسيلة الحصول عليه، أما الأدلة الناقصة فلم تكن تصلح أساساً لأية إدانة بمفردها⁽²⁾.

ثانياً- نظام الاقتناع الذاتي للقاضي:

نظراً للرغبة في حماية الحرية الفردية ضد العيوب التي نتجت عن تطبيق نظام الأدلة القانونية المنتقد وحرصاً على عدم إدانة بريء وعدم إفلات مذنب من سطوة العقاب تغيير نظام

(1) أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية في ضوء التعديلات الحديثة، الطبعة الثامنة (مطورة)، دار النهضة العربية، القاهرة مصر سنة 2012، ص 458.

(2) ممدوح خليل البحر، بحث بعنوان نطاق حرية القاضي الجنائي في تكوين قناعته الوجدانية، مجلة الشريعة و القانون، العدد الحادي و العشرون، الإمارات العربية المتحدة، جوان 2004، ص 329 متاح على الموقع الإلكتروني:

<http://www.sljournal.uaeu.ac.ae/issues/21/docs/6.pdf>

الإثبات الجنائي من نظام الأدلة القانونية إلى نظام حرية الإثبات، حيث أصبح كل دليل مقبول في الإثبات⁽¹⁾. بحيث يسمح هذا النظام بأن يقدر القاضي فيه بحرية قيمة الأدلة أيا كان مصدرها، ولا يمل عليه المشرع أي حجة معينة لإعمالها، وعلى القاضي أن يبحث عن الأدلة اللازمة مهما كان مصدرها ثم يقدرها في حرية تامة، على أن هذا التقدير الحر يجب ألا يصل إلى حد التحكم الكامل، فافتناع القضاة يجب أن يخضع دائما للعقل و المنطق، فلا يمكن ولا يجوز أن يعني مبدأ الاقتناع الذاتي للقاضي أكثر من هذا، ولا يصح أن يكون معناه إطلاق حرية القاضي في أن يحل محل أدلة الإثبات تخميناته ومحض تصوراته الشخصية مهما كانت وجاهتها⁽²⁾.

والمشرع الجزائري اعتنق مبدأ حرية الإثبات في المواد الجزائية، و التي تتم بكافة الطرق القانونية، ويصدر القاضي حكمه وفقا لاقتناعه الخاص (المادة 212 من ق.إ.ج.ج)، ويختلف الإثبات الجزائي عنه في الإثبات المدني، من حيث وسائل الإثبات، وقيمتها الإثباتية إلى نظام الإثبات المعتمد، فالإثبات الجزائي يعتمد على مبدأ حرية الإثبات أو نظام الأدلة المعنوية، بينما يعتمد الإثبات المدني على نظام الأدلة القانونية⁽³⁾.

ثالثا - نظام الأدلة العلمية:

يقوم هذا النظام على الاستعانة بالأساليب الفنية التي كشف عنها العلم الحديث في إثبات الجريمة ونسبتها إلى المتهم، ويعطي الدور الرئيسي في الإثبات "للخبير" ويجعل أهم الأدلة هي القرائن التي تخضع للفحص العلمي الدقيق، ويستخرج منها في صورة قاطعة ما يثبت الإدانة أو البراءة وقد حذب هذا النظام أنصار "المدرسة الوضعية" وتنبؤوا أن يكون نظام المستقبل، وأصبح هذا النظام يطبق إلى جانب نظام الاقتناع القضائي، لكن ما يقولون به هو أن يحل هذا النظام محل الاقتناع القضائي وبصير الخبير هو قاضي الدعوى وهو أمر ليس مرغوبا فيه، بما يعنيه ذلك من حرمان المتهم من ضمانات الحرية الفردية و الكرامة البشرية التي لا يحسن توفيرها غير القاضي

(1) ممدوح خليل البحر، المرجع السابق، ص 330.

(2) أحمد فتحي سرور، المرجع السابق، ص 459.

(3) العيد سعادنه، المرجع السابق، ص 16-17.

بالإضافة إلى أن مباشرة الخبير عمله تفترض تحديد عناصر مهمته ثم تقدير قيمة تقريره وهما وظيفتان قضائيتان والفصل في الدعوى تثير مسائل قانونية من اختصاص القاضي ما يجعل من ضرورة عمل النظامين جنبا إلى جنب⁽¹⁾.

المطلب الثاني

مفهوم الجريمة المعلوماتية.

برزت الجريمة المعلوماتية كنتيجة منطقية للتطور الهائل و المستمر و المتواتر للتكنولوجيا الحديثة، خصوصا مع مسابرة الإجرام للتقدم الفكري للمجتمعات مع عدم اكتمال رؤية شاملة ونهائية للجريمة في منظور التشريعات المقارنة بسبب التفاوت العلمي و التكنولوجي لها ، لذلك كان لزاما على الباحث أن يوليها قدرا من الدراسة و التحليل و التعمق في مفهومها بدءا من معايير تعريفها(الفرع الأول) إلى إبراز خصائصها التي تميزها عن باقي الجرائم (الفرع الثاني)، وصولا إلى تحديد أهم التصنيفات و الصور التي أعطيت لها دون أن ننسى تحديد موقف المشرع الجزائري عن كيفية تناوله لهذه الجريمة (الفرع الثالث).

الفرع الأول : تعريف الجريمة المعلوماتية.

الحقيقة أن الفقه وكذلك القضاء وبعض التشريعات التي تتعلق بمكافحة جرائم المعلوماتية لم تتفق على تعريف موحد أو نموذج موحد لجرائم الحاسب الآلي و الانترنت، ويرجع ذلك إلى الخلاف في شأن تعريف المعلوماتية ومن قبلها تعريف المعلومة ذاتها فالأصل ان المشرع في غالب الأحيان لا يعرف الجريمة لكنه يجد نفسه مضطرا الى ذلك إما لتحديد الأركان العامة و الخاصة للجريمة أو لأن السلوك الإجرامي من الصور المستحدثة للجريمة⁽²⁾.

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، دار النهضة العربية، القاهرة مصر، سنة 2013، الجزء الثاني، ص 843.

(2) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الإنترنت في القانون العربي النموذجي، الطبعة الأولى، 2009، ص 18.

ولقد تناولت المؤلفات الفقهية و القانونية اصطلاحات و مسميات مختلفة بشأن هذه الجريمة فمنها من يسميها جرائم الكمبيوتر و الانترنت ، ومنها من يسميها جرائم تكنولوجيا المعلومات ، وكذا جرائم الهاكرز ، و منهم من يصطلحها بالجرائم الالكترونية ، ومنهم من تناولها تحت مسمي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال كالمشرع الجزائري ، بالإضافة إلى المصطلح الحديث و المتفق عليه في عديد المؤلفات وهو الجرائم المعلوماتية، وهي التسمية المختارة لموضوع دراستنا.

ولعل إطلاق اصطلاح " الجرائم المعلوماتية"⁽¹⁾ على الجرائم المتعلقة بالحاسب باعتبارها أدق ما يمكن إطلاقه على مثل هذه الجرائم على اعتبار أنها تشمل الحاسب وسائر المبتكرات والتقنيات الراهنة و المستقبلية المستخدمة في "التعامل مع المعلومات" وأيضا على أساس آخر أن هذه الجرائم يمكن تصورها من زاويتين بحسب دورها في التجريم، فمن الزاوية الأولى تكون المعلوماتية أداة ووسيلة للغش أو الاعتداء ، ومن الزاوية الثانية تكون موضوعا للاعتداء⁽²⁾.

كما تجدر الإشارة إلى أن اختلاف التعاريف وكثرتها مرده الزاوية التي يتناول منها دراسة الجريمة، ونحن بدورنا نعرض الاتجاهات المختلفة التي تناولت التعاريف كل من زاويته ثم نخلص إلى موقف المشرع الجزائري من هذه التعريفات.

أولا- تعريف الجريمة المعلوماتية المستند إلى معيار واحد:

نتعرف في هذا القسم إلى التعريف المستند إلى وسيلة ارتكاب الجريمة، ثم التعريف المستند إلى موضوع معيار الجريمة، وأخيرا التعريف المستند إلى السمات الشخصية للجاني.

أ- التعريف المستند إلى وسيلة ارتكابها:

(1) يرجع الفضل في اقتراح مصطلح "المعلوماتية" إلى الأستاذ Drefus حيث استخدمه عام 1962 لتمييز المعالجة الآلية للمعطيات، وتبنته الأكاديمية الفرنسية في افريل 1966 وعرفته بأنه " علم المعالجة المنطقية للمعلومات والتي تعتبر بمثابة دعامة للمعارف الإنسانية والاتصالات في المجالات المختلفة وذلك باستخدام معدات آية". فهي علم المعالجة العقلية للمعلومات المقترنة بالحاسب الآلي. انظر عمر أبو الفتوح عبد العظيم أحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، القاهرة، سنة 2010، ص 44-45.

(2) عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة و القانون دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت لبنان، 2003، ص 32.

المبحث التمهيدي.....الإطار المفاهيمي للإثبات الجنائي و الجريمة المعلوماتية.

إن التعريفات التي انطلقت من وسيلة ارتكاب الجريمة يري أصحابها أن جريمة المعلوماتية تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة، إذ يعرفها الأستاذ توم فورستر و الأستاذ اسلي دبال أنها " فعل إجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" ، كما يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها " الجريمة التي تلعب فيها البيانات الكمبيوترية و البرامج المعلوماتية دورا رئيسيا" ، ويعرفها الفقيه تايدمان بأنها " كل أشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب " (1). وانتقد هذا التعريف بسبب عموميته إلى جانب أسباب أخرى(2). ومنهم من عرف الجريمة المعلوماتية بأنها " كل فعل غير مشروع يرد على الكمبيوتر أو يتم باستعماله" (3).

بينما يعرفها الفقيه Merwe على انها " الفعل الغير مشروع الذي يتورط في ارتكابه الحاسب الآلي" (4).

وينتقد هذا التعريف لأنه ينظر للحاسب الآلي كما لو أنه شخص طبيعي يساهم في قيام الجريمة، وهناك تعريف آخر توسع في وسيلة الاستعمال وقيل انه " كل جريمة تتم في محيط الحاسبات الآلية" لكنه تم انتقاده بدوره لأنه ينطوي على توسع كبير في مجال الجريمة المعلوماتية، لأنه يري انه بمجرد مشاركة الحاسب الآلي تقوم الجريمة وتوصف بالمعلوماتية ، في حين ان

(1) نسرين عبد الحميد نبيه، الجريمة المعلوماتية و المجرم المعلوماتي، منشأة المعارف، الإسكندرية، سنة2008، ص 58.

(2) أهم الانتقادات الموجهة الى هذا التعريف يعود للأسباب التالية:

1- أنه تعريف بالغ العمومية والاتساع لأنه يدخل كل الجرائم التقليدية ضمن نطاق الجريمة المعلوماتية استنادا إلى كل سلوك غير مشروع يضر المجتمع، إذ بالرغم من اشتراط ارتباط هذا السلوك بالحاسب الآلي إلا انه لا ينفي شمول كافة الجرائم التقليدية وهو غير مقبول.

2- تعريف غير منطقي لأنه لم يبين أنه خاص ببعض الجرائم التي لا يتصور وقوعها إلا بواسطة الحاسب الآلي، مما يجعله بعيد عن التعريفات العلمية.

3- أن استخدام البيانات و المعلومات و البرامج يضيف على الجريمة المعلوماتية سمتها الخاصة عكس استخدام الحاسب الآلي وحده الذي لا يضيف إلى السلوك غير المشروع أي جديد. انظر، أيمن عبد الله فكري ، جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة للنشر الإسكندرية ،سنة 2007، ص 83 .

(3) شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، سنة 2007، ص12.

(4) سميرة معاشي، مقالة بعنوان ماهية الجريمة المعلوماتية، مجلة المنتدى القانوني ، العدد السابع ، جامعة محمد خيضر بسكرة الجزائر، أبريل 2010، ص276.

هناك من الأفعال المتفق عليها أنها خارج نطاق الجريمة كتلك التي تتعلق بسرقة المكونات المادية أو الغش فيها ،ولا يمكن إسباغ وصف الجريمة المعلوماتية على النشاط لمجرد أن الحاسب أو أيا من مكوناته كانت محلا للجريمة⁽¹⁾.

ولقد وجه لهذه التعريفات المستندة أساسا إلى وسيلة ارتكابها نقدا إذ لا يكاد أي مؤلف أن يخلو منها تقريبا ، ومن بين الفقهاء المنتقدين لهذا الاتجاه نجد كل من : John Taber و Rostoker Michael و Robert Rines من أن تعريف الجريمة يستدعي الرجوع إلى العمل الأساسي المكون لها وليس فحسب الوسائل المستخدمة لتحقيقه، لأن القانون الجنائي يهتم بالفعل و النشاط غير المشروع لا الوسيلة ، ويعزز هذا النقد الأستا ذ: R. E.Andersone بقوله انه " ليس لمجرد أن الحاسب قد استخدم في جريمة أن نعتبرها من الجرائم المعلوماتية "⁽²⁾.

ب- التعريف المستند إلى معيار موضوع الجريمة:

هناك مجموعة من التعريفات استندت إلى موضوع الجريمة والى أنماط السلوك محل التجريم فهي حسب تعريف الأستاذ: Rosblat "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه" ، أما الدكتورة هدى قشقوش تعرفها بأنها "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"⁽³⁾.

فيما حاول كلا من الأستاذين Le Stanc & Vivant أن يقوموا بوضع تعريف يراعي فيه موضوع الجريمة وذلك بوصفها بأنها " مجموعة الأفعال غير المشروعة و المرتبطة بالمعلوماتية و التي يمكن أن تكون جديرة بالعقاب" ، ولم يقتصر الأمر على قيام الفقه بمحاولة وضع التعريفات بل ساهمت الهيئات و المؤسسات المهمة بدراسة الجريمة المعلوماتية ، إذ يعرف خبراء منظمة

(1) أيمن عبد الله فكري، المرجع السابق، ص 85.

(2) نسرين عبد الحميد نبيه، المرجع السابق، ص 58.

(3) خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، الطبعة الأولى، دار الثقافة للنشر و التوزيع عمان الأردن، سنة 2011، ص 28.

التعاون الاقتصادي و التنمية جرائم نظم المعلومات بأنها " كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/أو نقلها" ، وقد امتدح جانب من الفقه هذا التعريف فيما اعتبره آخرون انه ونتيجة لسعته سيتسبب في إرباك الباحثين ويقل النفع به بالنسبة للفقهاء ،كما سيتضمن نطاق التجريم دائرة الأخلاق⁽¹⁾.

إن هذا النقد الموجه لهذا التعريف لم يوضح كيفية إرباك الباحثين ومن أي زاوية وطالما أن هذا التعريف تضمن فقط عبارة الأخلاق فهي غير مؤثرة على المعنى العام للتعريف ذلك انه مجرد وصف للسلوك غير المشروع متعلق أساسا بصفة الجاني.

ت- التعريف المستند إلى السمات الشخصية للجاني :

هذا الاتجاه يري أن الجريمة المعلوماتية تقتضي أن يكون لمرتكبها مهارات ومعارف مكتسبة بالحاسب الآلي وكل مشتملاته،

ومن التعريفات التي تبنت هذا الاتجاه ما جاءت به وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة في دليلها لعام 1979 إذ تعرفها بأنها "أية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها" ، في حين عرفها David Thompson بأنها "أية جريمة يتطلب لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسوب" ⁽²⁾. أيضا يعرفها الفقيه Stien Sckjoberg بأنها "أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه و التحقيق فيه وملاحقته قضائيا"⁽³⁾.

وهناك من يري بأن التعريف وفقا لهذا المعيار يعد أمرا قاصرا لا يحيط بحقيقة الأفعال غير المشروعة ولا يساهم في توضيح مفهوم هذه الجرائم، لأنه يتطلب البحث عن شخصية الجاني وهو ما يتنافى مع القانون الجنائي لأنه موضوعي لا يأخذ بالظروف الشخصية إلا استثناءا، كما انه

(1) وضع هذا التعريف من قبل مجموعة الخبراء المشار إليهم للنقاش في اجتماع باريس الذي عقد عام 1983 ضمن حلقة (الإجرام المرتبط بتقنية المعلومات) يتبنى هذا التعريف الفقيه الألماني Ulrich Sieber. أنظر أيمن عبد الله فكري، المرجع السابق، ص 86-87.

(2) خالد عياد الحلبي، المرجع السابق، ص 30.

(3) سميرة معاشي، المرجع السابق، ص 277.

يضيق من مفهوم الجريمة المعلوماتية خصوصا في الحالات التي تتطلب معرفة تقنيات عالية لارتكابها، ناهيك عن حالات متفق عليها تدخل ضمن دائرة هذه الجرائم لا تتطلب إلماما بتقنية المعلومات مثل حالات إتلاف المعلومات (1).

مما سبق يتضح وأنه هناك اختلاف واضح بشأن تحديد تعريف شامل متفق عليه فمن الفقهاء من استند إلى معيار الوسيلة للتعريف بالجريمة ومنهم من رأي في المعيار العضوي أساسا للتعريف بها وهناك اتجاه ثالث أخذ بمعيار الصفة الشخصية للجاني في حين أن كل هذه التعريفات وجهت لها مجموعة من الانتقادات، فبين هذا وذاك ظهرت تعاريف حاولت الجمع بين هذه المعايير للوصول إلى تعريف شامل وموحد وهو ما سأتناوله في العنصر الموالي.

ثانيا- تعريف الجريمة المعلوماتية المستند إلى عدة معايير:

أمام قصور التعريفات المؤسسة على معيار واحد سواء القائمة على معيار قانوني أو موضوعي أو شخصي، برز عدد من التعريفات التي تركز على أكثر من معيار، فقد جاء في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة و معاقبة المجرمين المنعقد في فيينا سنة 2000 تعريف لجرائم المعلوماتية كما يلي: " يقصد بالجريمة المعلوماتية أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي، و الجريمة تلك تشمل من الناحية المبدئية، جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية " (2).

و بالنظر إلى كثرة التعريفات و الصادرة عن جهات نظر قانونية وأحيانا اجتماعية وفلسفية وضع لها تعريف آخر يتمثل في أن الجريمة المعلوماتية هي " كل فعل وعمل وكل سلوك غير مشروع أو غير أخلاقي أو غير مسموح به صادر عن إرادة جنائية يقوم به شخص ما له دراية و معرفة بتكنولوجيا المعلومات المختلفة (تكنولوجيا التخزين و الاسترجاع وتكنولوجيا الاتصالات الحديثة) ويوجه ضد المصلحة العامة والخاصة وتشتمل تلك الجرائم من الناحية

(1) أيمن عبد الله فكري، المرجع السابق، ص 91.

(2) خالد عياد الحلبي، المرجع السابق، ص 30.

المبدئية جميع الجرائم التي يمكن أن ترتكب فيه أو عبر وسط إلكتروني، ويقرر لها القانون عقوبة أو تدبيراً" (1).

وتجدر الإشارة إلى أن أفضل التعريفات التي تبناها العديد من الفقهاء و الباحثين هو ما جاء به الخبراء المتخصصون من بلجيكا في معرض ردهم على استبيان لمنظمة التعاون الاقتصادي و التنمية OECD بأنها " كل فعل او امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".

و السبب في ذلك أن هذا التعريف واسع يتيح الإحاطة الشاملة بظاهرة جرائم التقنية كما انه ينطوي على إبراز صور الجريمة المعلوماتية و يتيح إمكانية التعامل مع التطورات التقنية المستقبلية وهو ما حدا بجانب من الفقه المصري لتأييد هذا الطرح (2).

أما المشرع الجزائري فقد عرف الجرائم المعلوماتية والتي أوردها تحت تسمية الجرائم المتصلة بتكنولوجيات الإعلام والاتصال في المادة 02/أ من القانون 04/09 المتضمن قواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال بأنها " 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". إن الملاحظ على هذا التعريف انه يتكون من شقين الأول يحيل على جميع أنواع الجرائم الواردة في القسم السابع مكرر 1 من قانون العقوبات بعنوان جرائم المساس بأنظمة المعالجة الآلية للمعطيات والمحددة في المواد من 394 مكرر إلى غاية 394 مكرر 07 ، أما الشق الثاني من التعريف ركز على وسيلة ارتكاب الجرائم من خلال تعريف المنظومة المعلوماتية وكذا المعطيات معلوماتية في ذات المادة(ب،ج) .

وللإشارة فإن مصطلح المعالجة الآلية للمعطيات ليس له أي تعريف رسمي في القرار

المتعلق بإثراء المصطلحات المعلوماتية رغم انه يمثل أساس النظرية العامة للقانون المعلوماتي

(1) جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة ، الطبعة الأولى، دار البداية للنشر و التوزيع سنة 2007 ، ص110.

(2) أنظر أيمن عبد الله فكري، المرجع السابق، ص88-89.

على خلاف مصطلح معالجة آلية الذي استعمل لتنظيم حماية المعلومات الاسمية عن طريق القانون 1978/01/06 الخاص بالمعلومات الاسمية الفرنسي⁽¹⁾.

الفرع الثاني: الطبيعة القانونية للجريمة المعلوماتية وخصائصها.

لطالما شكلت الطبيعة القانونية للجريمة المعلوماتية(أولا) محل خلاف بين الفقهاء بالنظر إلى بيئة وقوعها والتي تتميز بخصائص(ثانيا) تجعلها تتميز عن باقي الجرائم التقليدية فما هو جوهر الخلاف بين الفقهاء ؟ و ما هي أهم الخصائص المميزة لها؟

أولا- الطبيعة القانونية للجريمة المعلوماتية:

في البحث عن الطبيعة القانونية وتصنيفات الجريمة المعلوماتية يتبين لنا أنها تختلف عن أنماط الجرائم العادية ،لأن الاعتداء يقع على البيانات و المعلومات و البرامج والتي تختلف عن الاعتداء على المكونات المادية المحسوسة التي تخضع للمفهوم التقليدي، ذلك أن المعطيات أو المعلومات⁽²⁾ تمثل عنصر معنوي غير محسوس على عكس العناصر المكونة للحاسوب⁽³⁾. وتقع هذه الجريمة في غالب الأحيان في بيئة المعالجة الآلية للبيانات تكون المعلومات محل الاعتداء عبارة عن نبضات إلكترونية ونكون أمام ظاهرة إجرامية ذات طبيعة خاصة لها صلة بما يعرف عند البعض بالقانون الجنائي المعلوماتي⁽⁴⁾.

ومن هذا المنطلق طرح تساؤل عن الوضع القانوني للمعلومة وعن كيفية حمايتها ؟ وفي هذا الشأن ظهر اتجاهين الأول يستبعد صفة المنقول عن المعلومة وبالتالي لا تخضع للنصوص

(1) محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن، دار الجامعة الجديدة، الإسكندرية مصر سنة 2007، ص 25.

(2) "هي مجموع رموز يستخلص منها معني معين في مجال محدد وتتمتع بالتحديد و الابتكار و الاستثنائ و السرية يمكن تبادلها بين الجهات ولها قيمة مالية،وعلى ذلك فهي ذات قيمة اقتصادية كسلعة تباع وتشترى والمعلومات هي أساس المعلوماتية (وتعرف المعلوماتية على انها علم معالجة الآلية للبيانات و المعلومات)".انظر «سميرة معاشي، المرجع السابق، ص 280.

(3) خالد عياد الحلبي، المرجع السابق، ص 54 .

(4) عفيفي كامل عفيفي، المرجع السابق، ص 34.

التقليدية وتحتاج إلى نصوص خاصة للحماية، بينما الاتجاه الثاني أضيف على المعلومة صفة المنقول وأخضعها لحماية النصوص الجنائية التقليدية.

أ- الاتجاه الفقهي المستبعد لصفة المنقول عن المعلومة :

إن هذا الاتجاه تبناه الفقه الفرنسي تحديدا لما اعتبر أن الأموال ذات طبيعة خاصة انطلاقا من أن غياب الكيان المادي للمعلومات لا يجعلها محلا لحق مالي من الحقوق المتعارف عليها في الفقه و التي ترد على كيانات مادية ،وان جاز اعتبارها محلا لحق ملكية أدبية أو فنية أو صناعية والمعلومات التي لا تكون متصلة بطبيعتها بهذه الحقوق تستبعد من طائفة الأموال، أما الاستخدام غير المشروع للمعلومة يعد خطأ رتب عليه الفقه الفرنسي المسؤولية المدنية استنادا إلى نص المادة 1382 من القانون المدني الفرنسي وباعتراف المحكمة بالحق في المعلومات يكون الحق الوارد عليها من نوع الملكية العلمية⁽¹⁾.

وقد صدر للقضاء الفرنسي أحكام في هذا الاتجاه عندما قضت بان البيانات المبرمجة هي من قبيل الأفكار فهي نتاج ذهني ، وبهذا الوصف فإنها لا تصلح أن تكون محلا للسرقة ، كما صدر للقضاء الأمريكي أحكاما تستبعد وقوع جريمة السرقة ممن قام بنسخ برامج من كمبيوتر مملوك للغير وذلك عن بعد ، وقد جاء في تسبيب احد الأحكام انه لا تعتبر الومضات الالكترونية من قبيل الأشياء المحسوسة التي ترد عليها جريمة السرقة⁽²⁾.

ب- الاتجاه الفقهي المسند لصفة المنقول على المعلومة :

يري أصحاب هذا الاتجاه أن المعلومة تعد قيمة في ذاتها ، ولها بالتأكيد مظهر معنوي ولكنها تملك قيمة اقتصادية مؤكدة ، بحيث يمكن عند الاقتضاء أن ترفعها إلى مصاف القيم القابلة لأن تحاز حيازة مشروعة وبذلك فهي مال قابل للتملك أو الاستغلال، على أساس قيمتها الاقتصادية

(1) نسرين عبد الحميد نبيه، المرجع السابق، ص 100-101.

(2) شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 34-35.

المبحث التمهيدي.....الإطار المفاهيمي للإثبات الجنائي و الجريمة المعلوماتية.

وليس على أساس كيانها المادي ، ولذلك فهي تستحق الحماية القانونية ويجب معاملتها معاملة المال⁽¹⁾.

كما قرر جانب من الفقه أن أي قانون يرفض إسباغ صفة المال على شيء له قيمة اقتصادية هو بلا جدال قانون ينفصل تماما عن الواقع، وباعتبار البرامج في جوهرها معلومات معالجة بطريقة ما ولها قيمة اقتصادية فيجب معاملتها على أنها من عداد الأموال محمية من القانون الجنائي تحت موضوع جرائم الاعتداء على الأموال⁽²⁾.

فيما اتجه القضاء في عديد من الدول مثل القضاء البلجيكي إلى اعتبار المعلومات في الكمبيوتر من قبيل الأموال التي تصلح لوقوع جريمة السرقة، وفي نفس الاتجاه ذهبت بعض المحاكم الهولندية ، وقد تبني القضاء الفرنسي نفس الاتجاه عندما قضت محكمة النقض الفرنسية بتوافر خيانة الأمانة بخصوص رقم كارت السحب من البنك على أساس أن أحكام المادة 1/314 من قانون العقوبات تسري على كل مال أيا كانت طبيعته وليس فقط على المال المادي⁽³⁾.

إن كل هذا الجدل دفع إلى الوصول يوما بعد يوم إلى حقيقة مفادها انه وفيما يتعلق بالمعلومات ونظمها وسبل معالجتها آليا فإن الأمر لا ينبغي أن يترك للتفسير الفقهي و القضائي من أجل بسط النصوص القائمة على الاستيلاء على المعلومات على نحو ما فعله الفقه و القضاء في فرنسا وقد شقي في ذلك ، فالأيسر و الأصوب أن يلتفت المشرع إلى هذه المشكلة بتشريع خاص ينص على تجريم صور العدوان المتصورة على المعلومات ونظمها وبرامجها وسبل معالجتها⁽⁴⁾.

ثانيا- خصائص الجريمة المعلوماتية:

(1) سميرة معاشي، المرجع السابق، ص282.

(2) عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، بدون طبعة، دار الكتب القانونية ، سنة 2007، ص26.

(3) شيماء عبد القني محمد عطا الله، المرجع السابق، ص 37.

(4) نسرين عبد الحميد نبيه، المرجع السابق، ص 101.

إن التطرق لخصائص الجريمة المعلوماتية له قيمة كبيرة في هذا البحث ذلك أن التعرف على أهم مميزاتها يزيل اللبس ويساعد على التعمق أكثر في فهم الجريمة مقارنة بالجرائم التقليدية الأخرى بالنظر إلى طبيعة محل الجريمة، إذ تتسم بما يلي:

1- غياب مفهوم عام متفق عليه بين الدول حول نماذج النشاط المكون للجريمة المتعلقة بالنظام المعلوماتي يضاف له عدم الاتفاق على التعريف القانوني للنشاط الإجرامي المتعلق بهذا النوع من الإجرام⁽¹⁾.

2- الجرائم المعلوماتية جرائم عابرة للدول، أي تلك الجرائم التي تقع بين أكثر من دولة بمعنى أنها لا تعترف بالحدود الجغرافية للدول إذ غالبا ما يكون الجاني في بلد ما و المجني عليه في بلد آخر وقد يكون الضرر المحتمل في بلد ثالث وعليه تعد الجرائم المعلوماتية من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية.

3- أنها جرائم صعبة الإثبات حيث يصعب في كثير من الأحيان الحصول على أثر مادي للجريمة المعلوماتية ولعل السبب في ذلك يعود إلى استخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان، كما يتمثل السلوك المكون للركن المادي فيها بعمل سريع قد لا يستغرق أكثر من بضع ثواني علاوة على سهولة محو الدليل و التلاعب به في وقت تفنقر فيه هذه الجرائم إلى الدليل المادي التقليدي.وهي الخاصية التي نحن بصدد دراستها تحليلا في الفصلين المواليين.

4- تعد الجرائم المعلوماتية أقل عنفا من الجرائم التقليدية أي أنها لا تحتاج إلى ادني مجهود بل تحتاج إلى الدراية الذهنية و التفكير العلمي المدروس القائم على تقنيات الحاسب الآلي، فلا يوجد في واقع الأمر شعور بعدم الأمان تجاه المجرمين في مجال المعالجة الآلية للمعلومات باعتبار أن مرتكبيها ليسوا من محترفي الإجرام بصيغته المتعارف عليها.

5- أن الباعث على ارتكاب الجريمة المعلوماتية يختلف عنه بالنسبة للجرائم التقليدية ففي الحالة الأولى يتمثل الباعث في مخالفة النظام العام و الخروج عن القوانين أكثر من استهداف الحصول

(1) أيمن عبد الله فكري، المرجع السابق، ص 92.

على الربح في حين نجد الباعث وراء ارتكاب الطائفة الثانية هو عموماً السعي وراء اكتساب النفع المادي السريع⁽¹⁾.

6- أنها طائفة من الجرائم تتسم بسمات خاصة عن غيرها من الجرائم فهي تستهدف معنويات وليست ماديات محسوسة، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي إن جاز التعبير⁽²⁾.

7- تتم الجريمة المعلوماتية في زمن قياسي إذ لا تستغرق سوى بضع ثواني لإتيانها.

8- تدني نسبة الإبلاغ عن تلك الجرائم من المجني عليهم-خاصة في حالة شركات ومؤسسات الأعمال- لتجنب الإساءة للسمعة⁽³⁾.

9- يتم اكتشاف معظمها إن لم يكن جميعها بالصدفة البحتة و الدليل على ذلك كما يؤكد البعض أنه لم يكتشف إلا نسبة 1% فقط منها و أن 15% منها تم الإبلاغ عنها وإن خمس النسبة الأخيرة هي التي يصدر فيها أحكام بإدانة مرتكبيها⁽⁴⁾.

إن طبيعة وأبعاد هذه الجرائم سيما في ظل تطور أنماطها وكذا تطور استخدام الشبكات وما أتاحه الانترنت من فرص جديدة لارتكابها خلقت أنماطاً مستجدة لها ، مما يشير إلى أنها تتميز بأحكام لا توفرها المبادئ و النظريات القائمة وهما بالتحديد محل الاعتداء في هذه الجرائم و السلوكيات المادية المتعلقة بارتكاب الجريمة ، وهذا ما يدعو إلى وضع تشريعات ونصوص جديدة

(1) محمد على سالم و حسون عبيد هجيج، مقالة بعنوان الجريمة المعلوماتية، منشورة في مجلة جامعة بابل للعلوم الإنسانية ، المجلد 14 العدد 06، العراق، سنة 2007، ص92. متاح على الموقع الإلكتروني: <http://www.iasj.net/iasj.pdf>.

(2) جعفر حسن جاسم الطائي، المرجع السابق، ص141.

(3) تعرض بنك Marchant Bank City في بريطانيا لسرقة 8 مليون جنيه إسترليني من احدي أرصدته إلى رقم في سويسرا وتم ضبط الفاعل متلبساً بسحب المبلغ المسروق ،وبدلاً من محاكمته قام البنك بدفع مليون جنيه له مقابل عدم الإعلام عن جريمته وإعلام البنك عن الآلية التي نجح من خلالها في اختراق نظام الأمن بحاسوب البنك الرئيسي. انظر ، عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، بحث بعنوان الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية (دراسة تطبيقية مقارنة) مقدم الى المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، المنعقد بالرياض في 12-14 نوفمبر 2007 ،جامعة نايف العربية للعلوم الأمنية، ص10.

(4) عفيفي كامل عفيفي، المرجع السابق، ص 35.

تكون قادرة على الإحاطة بمتطلبات ومفردات وخصوصيات هذه الجرائم ، وفي هذا يقول الدكتور محمود نجيب حسني ((ثمة نظريات للقسم الخاص لا صلة بينها وبين تطبيق القسم العام... لقد أنتجت دراسة القسم الخاص نظريات لا تقل من حيث الخصوبة على نظريات القسم العام...))⁽¹⁾.
الفرع الثالث : تصنيف الجرائم المعلوماتية.

منذ ظهور الجرائم المعلوماتية والجهود تتكاثر سواء على الصعيد الإقليمي أو الدولي أو على الصعيد الوطني لتنسيق التعاون للحد من الظاهرة وبلورة نصوص متكاملة تضمن عدم إفلات أي صورة من صور الإجرام والم سراس بالمجال المعلوماتي، إلى هذا الحد هناك عدة تقسيمات للجرائم المعلوماتية بالرغم من عدم الاتفاق على صياغة نظريات متكاملة تتناول بالتعريف والإحاطة الشاملة لأنواع هذه الجرائم ولعل السبب في ذلك يعود بالدرجة الأولى إلى التطور المستمر والمستطرد للجريمة ووسائل ارتكابها ، وفي جميع الأحوال فان أهم التقسيمات الواردة في اغلب التشريعات لم تكن وفقا للتقسيم التقليدي للجريمة بالنظر إلى العقوبة المقررة لها من مخالفات وجنح وجنايات، بل وجدت لها تصنيفات مختلفة وفقا لمعايير جديدة يعود بالدرجة الأولى إلى طبيعة الجريمة ذاتها، ولعل أهم تصنيف يتفق عليه اغلب الدارسين للقانون الجنائي هو التصنيف الذي تضمنته الاتفاقية الدولية لمكافحة الجريمة المعلوماتية بودابست 2001.

أولاً- تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة:

هذا التصنيف هو الذي ترافق مع موجات التشريع في ميدان تقنية المعلومات وهو السائد في مؤلفات الفقيه Ulrich Zebar وتقسم إلى الطوائف التالية⁽²⁾:

أ- الجرائم الماسة بقيمة معطيات الحاسوب وتشمل فئتين أولهما الجرائم الواقعة على ذات المعطيات كجرائم الإتلاف والتشويه للبيانات و المعلومات وبرامج الحاسوب بما في ذلك استخدام

(1) محروس نزار غايب، مقالة بعنوان الجريمة المعلوماتية، منشورة في مجلة التقني، مجلد 24 العراق، سنة 2011 . متاح على الموقع الالكتروني: <http://www.iasj.net/iasj.pdf>.

(2) عماد مجدي عبد الملك ، جرائم الكمبيوتر و الإنترنت، دار المطبوعات الجامعية ، بدون طبعة، الإسكندرية مصر، سنة 2011 ص 47-48، انظر كذلك عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، المرجع السابق، ص 6-7.

المبحث التمهيدي.....الإطار المفاهيمي للإثبات الجنائي و الجريمة المعلوماتية.

وسيلة الفيروسات التقنية، وثانيهما الجرائم الواقعة على ما تمثله المعطيات آليا من أموال أو أصول كجرائم غش الحاسوب للحصول على المال، أو جرائم الاتجار بالمعطيات، وجرائم تزوير المستندات المعالجة آليا واستخدامها.

ب- الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة، وتشمل جرائم الاعتداء على المعطيات السرية، أو المحمية، وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الشخصية .

ت- الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات) التي تشمل نسخ وتقليد البرامج، وإعادة إنتاجها وصنعها دون ترخيص، و الاعتداء على العلامة التجارية وبراءة الاختراع.

وبإمعان النظر في هذه الطوائف نجد أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومتحقق إذ أن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله هو اعتداء في ذات الوقت على امن المعطيات، لكن الغرض المحرك للاعتداء انصب على ما تمثله من قيمة، والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب هو اعتداء على الحقوق المالية والأدبية لكنها تتميز عن الطوائف الاخرى بان محلها هو البرامج فقط.

ثانيا- تصنيف الجرائم تبعا لدور الحاسب الآلي في الجريمة:

إن تقسيم الجرائم المعلوماتية وفقا لذا التصنيف مرده هدف ووسيلة ومحتوي الحاسب الآلي وهو الاتجاه العالمي الجديد في ظل تطور التدابير التشريعية في أوروبا تحديدا، وأفضل ما يعكس هذا التقسيم الاتفاقية الأوروبية لجرائم الكمبيوتر و الانترنت بودابست⁽¹⁾ لعام 2001، ذلك أن

(1) في 23 نوفمبر 2001 وفي مدينة بودابست عاصمة المجر قامت 26 دولة بالتوقيع على تلك الاتفاقية فيما بينها لمكافحة الجريمة المعلوماتية وهي تعد أول معاهدة دولية لمكافحة الجريمة المعلوماتية، وقد كانت تلك الاتفاقية نتاج لتعاون وعمل لجان قانونية وفنية من تلك الدول وتغاضت عن اختلافها في النظم القانونية حتى تتمكن من تنظيم العمل والاستفادة من مجتمع المعلومات وثورة الاتصالات، وأسهمت هذه المعاهدة في تقنين الجهود الدولية المبذولة وهي المعاهدة الأوروبية بشأن حماية البيانات الشخصية وكذلك استندت إلى الميثاق الدولي لحماية الحقوق المدنية والسياسية الصادرة عن الأمم المتحدة 1966، كما تأثرت بمعاهدة التعاون

المبحث التمهيدي.....الإطار المفاهيمي للإثبات الجنائي و الجريمة المعلوماتية.

العمل منذ مطلع عام 2000 يتجه إلى وضع إطار عام للتصنيف وعلى الأقل وضع قائمة الحد الأردني محل التعاون الدولي ويساهم في هذا الجهد إلى جانب دول أوروبا كل من استراليا وكندا وأمريكا وتقسم الجرائم المعلوماتية وفقا لهذه الاتفاقية إلى الطوائف التالية⁽¹⁾:

أ- الجرائم التي تستهدف عناصر السرية و السلامة و موفورية المعطيات والنظم وتظم :

1 +الدخول غير القانوني (غير المصرح به).

2 +الاعتراض غير القانوني.

3 تدمير المعطيات.

4 +اعتراض النظم.

5 +إساءة استخدام الأجهزة.

ب- الجرائم المرتبطة بالكمبيوتر و تظم:

1 +التزوير المرتبط بالكمبيوتر.

2 +الاحتيال المرتبط بالكمبيوتر.

ت- الجرائم المرتبطة بالمحتوي وتظم: طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالأفعال الإباحية و اللا أخلاقية.

ث- الجرائم المرتبطة بالإخلال بحق المؤلف والحقوق المجاورة (قرصنة البرمجيات).

ثالثا - تصنيف الجرائم تبعا لمساسها بالأشخاص و الأموال:

شاع هذا التصنيف في الدراسات و الأبحاث الأمريكية كما يعتبر المعيار المعتمد لتقسيم

جرائم الكمبيوتر و الانترنت في مشروعات القوانين النموذجية التي وضعت من جهات بحثية بقصد

الدولي في مكافحة الجريمة المعلوماتية الصادرة عن الأمم المتحدة ، ومنظمة التعاون الاقتصادي و التنمية OECD ودول الاتحاد الأوروبي، و مجموعة G8 وكذلك التوصية الأوروبية رقم 10/85 و التوصية رقم 2/88 و التوصية رقم 9/89 و التوصية رقم 13/95 ، وتظم هذه الاتفاقية 48 مادة تم توزيعها على أربعة أبواب، انظر أيمن عبد الله فكري، المرجع السابق، ص129-130. (1) عماد مجدي عبد الملك، المرجع السابق، ص50-51.

محاولة إيجاد الانسجام بين قوانين الولايات المتحدة المتصلة بهذا الموضوع، وبرز تقسيم هو الذي تضمنه مشروع القانون النموذجي لجرائم الكمبيوتر و الانترنت الموضوع سنة 1998 و المعد من قبل الفريق البحثي الاكاديمي Model State Computer Crimes Code وتبعاً لهذا التقسيم تصنف الجرائم المعلوماتية على النحو التالي⁽¹⁾:

أ- الجرائم التي تستهدف الأشخاص : وتضم طائفتين رئيسيتين هما :

1- الجرائم غير الجنسية التي تستهدف الأشخاص وتشمل القتل بالكمبيوتر.

2- الجرائم الجنسية : وبإمعان النظر في الأوصاف الواردة ضمن هذه الطائفة نجد أنها تجتمع جميعاً تحت صورة واحدة هي استغلال الانترنت والكمبيوتر لترويج الدعارة أو إثارة الفحش واستغلال الأطفال و القصر في أنشطة جنسية غير مشروعة.

ب- الجرائم التي تستهدف الأموال عدا السرقة أو الملكية المتضمنة أنشطة الاختراق أو الإتلاف.

ت- جرائم الاحتيال و السرقة.

ث- جرائم التزوير: وتشمل تزوير البريد الالكتروني وتزوير الوثائق و السجلات وتزوير الهوية.

ج- جرائم المقامرة والجرائم الاخرى ضد الأخلاق و الآداب.

ح- جرائم الكمبيوتر ضد الحكومة : وتشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون.

رابعاً- صور الجرائم المعلوماتية الواردة في التشريع الجزائري:

على اعتبار اختلاف تصنيفات الجريمة المعلوماتية في مختلف التشريعات المقارنة وعدم وجود معيار محدد للتصنيف وجد المشرع الجزائري نفسه مضطراً إلى تحديد هذه الجرائم ووضع

(1) عماد مجدي عبد الملك، المرجع السابق، ص من 52 إلى 54.

إطار قانوني تكفل نصوصه عدم إفلات مرتكبي هذه الجرائم من المتابعة و العقاب، ولذلك فإن المشرع الجزائري أورد تحت القسم السابع مكرر من قانون العقوبات جرائم المساس بأنظمة المعالجة الآلية للمعطيات كتعديل تضمنه القانون 15/04 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات وقبله كانت النصوص الخاصة قد تطرقت إلى بعض أنواع الجريمة المعلوماتية من منظور الحماية.

ونرجع أنواع الجرائم المعلوماتية، وتصنيفها حسب ما احتوى عليه قانون العقوبات الجزائري و أهم الجرائم التي تستهدف الأنظمة المعلوماتية هي⁽¹⁾:

أ- الجرائم المنصوص عليها في المادة 394 مكرر:

- الدخول خلسة للأنظمة المعلوماتية.
- البقاء غير المشروع في الأنظمة المعلوماتية.
- تعديل أو حذف معطيات المنظومة نتيجة الدخول غير المشروع.
- الإضرار بنظام تشغيل المنظومة على إثر الدخول أو البقاء غير المشروع.

ب- الجرائم المنصوص عليها في المادة 394 مكرر 1 :

- إدخال معطيات في منظومة معلوماتية خلسة.
- إزالة أو تعديل معطيات في منظومة معلوماتية خلسة .

ج- الجرائم المنصوص عليها في المادة 394 مكرر 2 من قانون العقوبات:

القيام عمدا وخلسة بـ:

- بتصميم أو تجميع أو توفير أو نشر أو البحث عن معطيات تمكن من ارتكاب جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

(1) مختار الأخضر، بحث بعنوان "الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الافتراضي"، نشرة القضاة القانونية العدد 66، الجزائر، سنة 2010.

- بحيازة أو إفشاء أو نشر أو استعمال معطيات متحصل عليها من جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

الثالث

المطلب

أطراف الجريمة المعلوماتية

في إطار المفاهيم التي تسير في فلك الجريمة المعلوماتية ارتأينا أن نضيف مطلباً نتناول فيه طرفي الجريمة، لنزيل اللبس عن الأشخاص الذين تقترب في حقهم الاعتداءات المعلوماتية وبالمقابل نلقي الضوء على فئة نبنت في مستتق الأرقام لتفرض نفسها كرقم جديد في معادلة الإجرام المعلوماتي فمن يكون هؤلاء الأشخاص يا تري؟

الفرع الأول: الضحية المعلوماتية.

تقع الجريمة المعلوماتية على المجني عليه، لكن في نفس الوقت قد تتعدى آثارها لتصيب أشخاص آخرين غير المجني عليهم وهم من يطلق عليهم تسمية المتضرر من الجريمة، لذلك أطلق مصطلح الضحية المعلوماتية على المجني عليه و المتضرر من الجريمة⁽¹⁾. وهو ما أكد عليه الإعلان العالمي بشأن المبادئ الأساسية لتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة الذي اعتمده الجمعية العامة للأمم المتحدة⁽²⁾ الذي أكد أن مصطلح الضحية يشمل كلا

(1) رشاد خالد عمر ، المشاكل القانونية و الفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث ، الإسكندرية مصر، سنة 2013، ص55.

(2) اعتمد بالقرار رقم 401434 الصادر بتاريخ 1985/11/29 إذ تنص الفقرة أ-3،2،1 " يقصد بالضحايا وفق الإعلان العالمي المشار إليه عاليه: الأشخاص الذين أصيبوا بضرر فردي أو جماعي بما في ذلك الضرر البدني أو العقلي أو المعانات النفسية أو الخسارة الاقتصادية أو الحرمان بدرجة كبيرة من التمتع بحقوقهم الأساسية عن طريق أفعال أو حالات إهمال تشكل انتهاكا للقوانين الجنائية النافذة في الدول الأعضاء بما فيها القوانين التي تحرم الإساءة الجنائية لاستعمال السلطة، كما يشمل المصطلح أيضا عند الاقتضاء، العائلة المباشرة للضحية الأصلية أو فاعليها المباشرين و الأشخاص الذين أصيبوا بضرر من جراء التدخل لمساعدة الضحايا في محنتهم أو لمنع الإيذاء.

المبحث التمهيدي.....الإطار المفاهيمي للإثبات الجنائي و الجريمة المعلوماتية.

من المجني عليه و المضرور من الجريمة⁽¹⁾، وإجمالاً يمكن تقسيم ضحايا الجريمة المعلوماتية إلى طائفتين رئيسيتين هما:

أولاً - الأشخاص المعنوية:

والتي تنقسم بدورها حسب درجة استهدافها إلى: المؤسسات المالية، و الجهات الحكومية، ثم المؤسسات العسكرية.

أ-المؤسسات المالية والجهات الحكومية:

تعتبر المؤسسات و الشركات المالية كالبنوك والبورصات من أكثر الأماكن المستهدفة بواسطة الجرائم المعلوماتية بحثاً عن الأموال وكذا التأثير على سوق التعاملات المالية⁽²⁾، ففي تقرير الأخير لمؤسسة الأمن المعلوماتي نورتون منجز سنة 2010 فإن الخسارة العالمية التي تسببت فيها جرائم المعلوماتية قد حددت بـ 388 مليار دولار، والدراسة اعتمدت على المعلومات التي تم جمعها من 12000 ضحية تتوزع على 121 دولة عبر العالم، واشتمل تقييم الوقت الضائع بسبب هذه الجرائم بـ 274 مليار دولار وطبعا كلفت مصاريف معالجة هذه المشاكل 114 مليار دولار⁽³⁾.

والى جانب ذلك فان المؤسسات و الدوائر الحكومية والوزارات و الإدارات المركزية هي محل اعتداءات مستمرة ما يشكل تهديداً أمنياً خصوصاً للدول التي لا تتوفر على جدران الحماية اللازمة لتوفير تامين الكتروني متكامل يجنبها خسائر مادية كبيرة، بالإضافة إلى تعطل المصالح الحيوية. كما تستهدف الشركات الخاصة أيضاً من طرف مرتكبو الجاسوسية المعلوماتية، بحيث يعتمد أصحاب الشركات إلى التجسس على الشركات المنافسة لمعرفة حجم المبيعات و شخصيات

(1) مصطفى محمد موسى ، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى، مطابع الشرطة ، سنة 2009، القاهرة، ص 158.

(2) خالد ممدوح إبراهيم، الجرائم المعلوماتية، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، سنة 2009، ص150.

(3) **Fernanda Prates, Frédérick Gaudreau et autre**, la cybercriminalité état des lieux et perspectives d'avenir , institut canadien d'études juridiques supérieures, Editions Yvon Blais, Cowansville,2013,p419.

العملاء وغيرها من المعلومات التي قد تساهم في تقليل الفرص على الشركات الأخرى للمنافسة في مجال الإنتاج⁽¹⁾.

ب- المؤسسات العسكرية:

تعد الجرائم المعلوماتية الواقعة على هذه المؤسسات من أخطر الجرائم من حيث إضرارها بالدولة وأسرارها ونجد في مقدمة هذه الجرائم التجسس على المواقع و المنشآت و المصانع و المختبرات العسكرية أو جرائم رصد البيانات المتعلقة بحجم القوات العسكرية وعدادتها ونوعها وإمكانياتها⁽²⁾، حيث أصبحت الدولة التي تملك المعلومات هي الدولة الأقوي، لذلك بدأ الاهتمام ينصب على الجوسسة بإطلاق الأقمار الصناعية، وهو المحور الأساسي في تطوير آليات ما يسمى بالحرب الالكترونية، هذا ما دفع بالدول إلى تعزيز منظوماتها و أنظمتها بحيث تكون قادرة على استيعاب المعلومات و البيانات و معالجتها و ترجمتها بسرعة لتعرض بصورة مناسبة أمام القادة لاتخاذ القرارات المناسبة، ولقد أكدت وكالة الاستخبارات الأمريكية على لسان احد ضباطها وهو لورانس جيرشن من أن الحروب الالكترونية المقبلة سوف تعتمد على برامج كومبيوتر ذكية أكثر من اللصوص الذين يخترقون مختلف المواقع الالكترونية على الانترنت⁽³⁾.

ثانيا - الأشخاص الطبيعيين:

تشمل هذه الطائفة كل الأفراد المستخدمين للكمبيوتر وشبكة الانترنت باعتبارها مجالا خصبا لارتكاب الجرائم المعلوماتية بالإضافة إلى الهواتف المحمولة خصوصا مع توفر خدمة الهواتف النقالة على أجيال جديدة كما أن الهواتف الذكية تتوفر على برامج حديثة بإمكانها الولوج إلى أي نافذة عبر العالم، وأمام الإقبال المتزايد لمستعملي شبكات الانترنت فان الجرائم المعلوماتية المرتكبة ضد الأفراد ستعرف لا محالة تزايدا لوجود علاقة طردية بين العاملين.

(1) خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 150.

(2) رشاد خالد عمر، المرجع السابق، ص 55.

(3) خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 151-152.

فحسب الاتحاد الدولي للاتصالات فان عدد مستعملي شبكة الانترنت قد بلغ 2.08مليار نسمة عبر العالم في جانفي 2011 مقارنة بـ: 1.03 مليار نسمة من عدد المستخدمين في سنة 2005⁽¹⁾، وتعتبر جرائم الإلتلاف عن طريق الفيروسات من أكثر الجرائم التي يتعرض لها الأشخاص الطبيعيون عبر البريد الالكتروني بالإضافة إلى سرقة أرقام بطاقات الائتمان و التشهير بالأفراد عبر الانترنت، ومثال على الجرائم المعلوماتية الواقعة على الأفراد وقوع المواطنين الأمريكيين ضحايا بعد قيامهم بتقديم تبرعات عبر شبكات الانترنت لمواقع انشأت خصيصا لمساعدة المتضررين من أحداث 11 سبتمبر ليقوم المحتالون بالاستيلاء عليها مباشرة دون أن تصل إلى مستحقيها في صورة تعكس قمة الاحتيال المعلوماتي⁽²⁾، وهي الطائفة التي نتعرف عليها في الفرع الموالي.

الفرع الثاني : المجرم المعلوماتي.

هناك تفرقة تقليدية في دراسات علم الإجرام ، تقوم على التمييز بين الإجرام الطبيعي و الإجرام الاصطناعي المكتسب ونادي بهذه التفرقة الفقيه الايطالي جارونالو⁽³⁾، ولعل اندثار نظريات عدة في مجال علم الإجرام وفي مجال تصنيف المجرمين ونتيجة لتطور العلوم و الدراسات تم بلورة سمات عامة للمجرم عموما وسمات خاصة يمكن استظهارها لطائفة خاصة من المجرمين تبعا لطبيعة الجريمة، فكان طبيعيا أن تحمل ظاهرة الجريمة المعلوماتية في جنبتها ولادة طائفة من المجرمين يحملون سمات خاصة تبعا لمميزات الجرائم المعلوماتية و الأغراض المراد تحقيقها، رغم عدم اتضاح الصورة في شأن تحديد هذه الصفات⁽⁴⁾. لذلك نتطرق أولا إلى أنواع المجرمين المعلوماتيين حسب التصنيف المتفق عليه في اغلب المؤلفات، ثم ننقل ثانيا إلى معرفة خصائص المجرم المعلوماتي .

أولا- تصنيفات المجرم المعلوماتي:

(1) Fernanda Prates, Frédéric Gaudreau et autre, op cite, p415.

(2) خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص 153.

(3) عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الإنترنت في القانون العربي النموذجي، المرجع السابق، ص 81.

(4) نسرين عبد الحميد نبيه، المرجع السابق، ص 117.

يتجه الباحثون مؤخرًا إلى الإقرار بأن أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الاعتداء و ليس على أساس التقنية الفنية المتبعة في الاعتداء ، و يعد أفضل تصنيف للمجرم المعلوماتي هو الذي أورده David icove, Karl seger & William Vonstorch في مؤلفهم جرائم الكمبيوتر الصادر عام 1995 حيث تم تقسيم مجرمي التقنية إلى عدة طوائف⁽¹⁾:

أ- المخترقون أو المتطفلون Crackers & Hackers :

هذه الطائفة تسمى أيضا بالقراصنة وه ي صنفان ، يسمى الصنف الأول الهواة Hackers⁽²⁾: وهم من الشباب الفضوليين الذين يسعون إلى التسلية و لا يشكلون خطورة على الصناعات و أنظمة المعلومات فهم يتحدون إجراءات امن النظم والشبكات ولا تتوافر لديهم دوافع حاقدة أو تخريبية ، أما الصنف الثاني فهم المحترفون Crackers⁽³⁾: وهم أكثر خطورة من الصنف الأول وقد يحدثون أضرارًا كبيرة وقد يؤلفون أندية لتبادل المعلومات فيما بينهم وتعكس اعتداءاتهم عن ميول إجرامي خطر⁽⁴⁾.

(1) نسرين عبد الحميد نبيه، المرجع السابق ، ص 117.

(2) أطلق مصطلح هاكلر في أول الستينيات من القرن الماضي على المبرمج الماهر القادر على التعامل مع الحاسب الآلي ومشاكله بخبرة و دراية ، حيث انه كان يقدم حلولًا لمشاكل البرمجة بشكل تطوعي في زمن لم يكن الوينداوز النواذ قد ظهر بعد ولكن البرمجة بلغة البيك واللغو و الفورتران كانت جديرة بالاهتمام و العارف بها يطلق عليه اسم هاكلر وتعني الملم بالبرمجة ومقدم الخدمة للآخرين، ويطلق خبراء امن المعلومات هذا المصطلح على من يخترق الحاسب الآلي، وينقسم الهاكلر الى محترفين وهم ممن يحملون درجات جامعية عليا في التخصص ويعملون محلي نظم ومبرمجين ويكونون على دراية ببرامج التشغيل ، والى الهواة إذ ظهر هذا النوع خلال عامي 2005 و 2007 على مستوى العالم ولهم هواية قوية في تعلم البرمجة ونظم التشغيل وينقسم هذا النوع بدوره الى نوعين الخبير الذي لا يلحق ضرر بالاجهزة و المبتدئ الذي يتميز بالعشوائية ويقوم احيانا بدمار واسع دون أي قصد جنائي. أنظر مصطفى محمد موسى، المرجع السابق، ص 143 الى 147.

(3) هو مصطلح مرادف للهاكرز ، يطلق عليهم خبراء امن المعلومات هذا المصطلح الى قدرتهم وقوتهم في الاختراق ، ويعتبرون من الأشخاص الذين يدخلون عنوة الى الأنظمة بقصد التخريب او التطفل، ففي عام 1984 كانت البدايات الأولى لحرب الكراكرز حيث انشا شخص يدعى "ليكس لوثر" مجموعة اطلق عليها اسم LOD وهي مجموعة من الكراكرز الهواة يقومون باختراق اجهزة الآخرين و القرصنة الى ان ظهرت مجموعة اسمها MOD بقيادة "قيبر" وفي 1990 بدأت حرب كبيرة بين الكراكرز دامت اربع سنوات انتهت بالقبض على "قيبر"، انظر مصطفى محمد موسى، نفس المرجع، ص 143-146.

(4) على جبار الحسيناوي، جرائم الحاسوب و الانترنت، الطبعة العربية دار اليازوري العلمية للنشر و التوزيع ، عمان الأردن، 2009 ص 49.

تقوم هذه الطائفة بارتكاب الجرائم المعلوماتية بدافع التحدي الإبداعي ونجدهم متفقيين إلى درجة ينصبون أنفسهم أوصياء على امن نظم الكمبيوتر، والسمة الغالبة على هذه الطائفة صغر السن وقلة الخبرة وعدم التمييز بين الأنظمة محل الاختراق مع تميز الكريكرز عن الهاكرز في مستوي المعرفة التقنية، كما تتميز هذه الطائفة في التشارك بينهم في وسائل الاختراق وآليات نجاحها وكشف مواطن الضعف بتبادل المعلومات عن طريق النشرات الإعلامية الالكترونية كما تعقد مؤتمرات بحضور خبراء للتشاور حول وسائل الاختراق ووسائل تنظيم عملهم (1).

ب-المحترفون (career criminals):

تتميز هذه الطائفة بسعة الخبرة و الإدراك الواسع للمهارات التقنية، كما تتميز بالتنظيم والتخطيط للأنشطة التي ترتكب من قبل أفرادها لذلك تعتبر هذه الطائفة الأخطر من بين مجرمي التقنية، وتهدف اعتداءاتهم إلى تحقيق الكسب المادي لهم وللجهات التي سخرتهم لارتكاب الجرائم المعلوماتية، ويتم تصنيف أفراد هذه الطائفة تبعاً لتخصصهم بنوع الجريمة أو الوسيلة المتبعة في ارتكابها ، مثل طائفة محترفي التجسس الصناعي، وطائفة مجرمي الاحتيال و التزوير (2).

ويتشابه مرتكبو هذه الأفعال الآثمة مع المجرمين ذوي الياقات البيضاء من حيث كونهم من أصحاب الشخصيات العالية، ويتميزون بالذكاء و الهيمنة الكاملة على تقنية الالكترونيات (3).

ت- الحاقدون (personal problem solvers):

إن المجرمون من هذه الطائفة لا يسعون إلى إثبات المقدرة التقنية، و المهارية، وفي نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية إنما يحرك أنشطتهم الرغبة في الانتقام والثأر كرد فعل على تصرف صاحب العمل أو المؤسسة المستخدمة بعد انقطاع أو تدهور علاقة العمل بينهم(4).

(1) نسرين عبد الحميد نبيه، المرجع السابق، ص 120.

(2) جعفر حسن جاسم الطائي، المرجع السابق، ص162.

(3) محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة الإسكندرية، سنة 2011، ص 81-82.

(4) جعفر حسن جاسم الطائي، المرجع السابق، ص163.

وتتقسم هذه الطائفة إلى نوعين مجرمون من داخل المؤسسة وهم الأخطر لمعرفتهم بنظام المؤسسة وتشغيل النظام و العبث به ومعرفة نقاط الضعف و القوة بذلك النظام⁽¹⁾، والحل الوحيد لمواجهة هذا النوع هو أن تحسن الشركات التعامل مع الموظفين و إنهاء خدماتهم عند الضرورة القصوى فقط وبصورة ودية ومجزية.

والنوع الثاني من خارج المؤسسة وهم بدورهم على ثلاثة أصناف الأول هم الأشخاص الذين يخرقون شبكات الحاسوب مستعينين بقدراتهم المتميزة ورغباتهم الجامحة للاختراق ، والصنف الثاني هم الأشخاص ناسخو البرامج "قراصنة البرامج" ويقومون باختراق مقاييس الحماية التي تمنع استنساخ البرامج ، أما الصنف الثالث هم صانعو الفيروسات ويتمتع هؤلاء بمهارات برمجة في استطاعتهم اختراق الأنظمة والتسبب في انهيارها⁽²⁾.

ث- صغار نوابغ المعلوماتية (pranksters):

هذه الطائفة من صغار السن ويصفهم بعضهم بأنهم الشباب البالغ المفتون بالمعلوماتية و الحاسبات الآلية، وشاع في نطاق الدراسات الإعلامية و التقنية وصفهم بمصطلح " المتلعثمين " الدال حسب تعبير احد الفقهاء على الصغار المتحمسين للحاسب بشعور من البهجة دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسب⁽³⁾.

(1) مثال ذلك حالة تتلخص وقائعها في قيام موظف قسم معالجة البيانات في احد مصانع اسطوانات بجنوب ألمانيا بإعداد ووضع برامج تصحيحية في برامج حاسب المصنع تلغي بصفة دائمة مديونية شركة معينة (تابعة لشريكه) في معاملاتها المالية في المصنع وذلك بجعلها الحساب المدين لهذه الشركة "صفراً" دائماً ، كما استخدم برنامجاً ، آخر للحيلولة عند غيابه أو قيامه بإجازة دون إخراج حاسب المصنع مخرجات تتعلق بحسابات هذه الشركة و المشتريات التي لم يسدد ثمنها للمصنع ، إضافة إلى تفرغ قاعدة البيانات المخزنة بحاسب المصنع من أية بيانات تتعلق بمديونيتها. جلال محمد الزعبي، أسامة احمد المناعسة، جرائم تقنية نظم المعلومات الالكترونية (دراسة مقارنة) ، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان الأردن، 2010 ، ص 75.

(2) مصطفى محمد موسي، المرجع السابق، ص 150-151.

(3) أيمن عبد الله فكري، المرجع السابق، ص 112.

وتعتبر هذه الفئة الأقل خطورة، إذ يرتكب المخالفات غالبا من غير قصد أو عن غير إرادة تامة بالأضرار، وقد يقتصر عملها على مجرد البيانات، وتكمن الخطورة فقط في احتمالية نشر ما تطلع عليه هذه الفئة من معلومات وبيانات سرية على شبكات الانترنت⁽¹⁾.

وقد تباينت الآراء بالنسبة لهذه الطائفة، حيث يري البعض انه لا يبدو من المناسب أن نصنف هذه الطائفة ضمن الطوائف الإجرامية بسبب ميلهم للمغامرة والتحدي و الرغبة في الاكتشاف، ونادرا ما تكون أهداف أفعالهم محظورة فهم لا يدركون النتائج المحتملة لأفعالهم، بينما هناك اتجاه آخر يناصر هذه الفئة ويعتبرها ممن يقدم خدمة لأمن المعلومات ويصفهم بالأخيار وأنهم لا يسببون ضررا للنظام، أما الاتجاه الأخير فيصنف هذه الطائفة ضمن مجرمي المعلوماتية بسبب خطورة أفعالهم المتمثلة في انتهاك الأنظمة واختراق الحواجز الأمنية ناهيك عن الحواجز الجغرافية وفي الواقع فانه يجب عدم التقليل من خطورة هذه الطائفة من منظور مستقبلي بسبب إمكانية تعديهم إلى مراحل احتراق الإجرام⁽²⁾.

ثانيا - خصائص المجرم المعلوماتي:

يتسم المجرم المعلوماتي بخصائص عديدة منها⁽³⁾:

- أ- المجرم المعلوماتي مجرم متخصص: فقد ثبت في عديد من القضايا أن عددا من المجرمين لا يرتكبون سوي جرائم الكمبيوتر أي أنهم متخصصون في هذا النوع من الجرائم.
- ب- المجرم المعلوماتي مجرم عائد إلى الإجرام: حيث يعود الكثير منهم انطلاقا من الرغبة في سد الثغرات التي أدت إلى التعرف عليهم، ويؤدي ذلك إلى العود إلى الإجرام.

(1) جلال محمد الزعبي، أسامة احمد المناعسة، المرجع السابق، ص 74.

(2) نهلا عبد القادر مومني، الجرائم المعلوماتية، الطبعة الأولى الإصدار الأول، دار الثقافة للنشر و التوزيع، عمان الأردن، 2008 ص 81-82.

(3) عب الفتح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي، المرجع السابق، ص من 83 الى 86.

المبحث التمهيدي.....الإطار المفاهيمي للإثبات الجنائي و الجريمة المعلوماتية.

ت- المجرم المعلوماتي محترف: إذ لا يسهل لشخص مبتدئ ارتكاب جرائم بطريق الكمبيوتر فالأمر يقتضي كثير من الدقة والتخصص للتغلب على أنظمة الحماية مثلاً.

ث- المجرم المعلوماتي مجرم غير عنيف: ذلك انه ينتمي إلى إجرام الحيلة، فهو لا يلجأ إلى العنف في ارتكاب جرائمه.

ج- المجرم المعلوماتي شخص ذكي ومتكيف اجتماعياً ، ذلك أن ذكائه يسمح له بالتكيف، بل يري الكثيرون أن الذكاء يعني القدرة على التكيف وتزداد خطورته مع توافر الشخصية الإجرامية لديه.

لم يضمّر الدليل التقليدي في عصر المعلومات و التكنولوجيا فمع أن الدليل التقليدي ليس له تلك القوة المعروفة في إثبات جرائم العالم المادي، إلا أنه يلعب دورا لا غني عنه في إطار الجرائم المعلوماتية باختلاف أنواعها فهي لا محالة من اللبّات التي يستعين بها القاضي الجزائي في بناء اقتناعه، ولو أن طفرة التكنولوجيا وما صاحبها من البحث عن سبل حديثة تسعى بها إلى تطوير في طرق إثباتها إلا أن الشهادة والاعتراف و الخبرة و الدليل الكتابي و القرائن هي من الوسائل التي حافظت على وجودها وسط الزخم المعلوماتي ومنظوماته التي نعيشها الآن، ولعل التساؤلات التي تطرح نفسها على الباحث في هذا الفصل هي: ما هي الأحكام العامة لكل وسيلة تقليدية وما مدي تجاوبها مع الجريمة المعلوماتية؟ وهل اتخذت لها شكل حديث في عالم المعلوماتية؟ وما هو دورها وحجبتها في إثبات الجريمة المعلوماتية؟

المبحث الأول

إثبات الجريمة المعلوماتية بالطرق الشخصية.

تتمثل الوسائل الشخصية لإثبات الجريمة المعلوماتية من مجموع الأدلة القولية المنبثقة من عناصر شخصية، وتتمثل فيما يصدر من الغير من أقوال تؤثر في اقتناع القاضي بطريق غير مباشر بعد تأكده من صدق هذه الأقوال، وتسمى بالأدلة الاستنباطية وهي التي يستنتجها الفكر من تحليله للوقائع و الظروف أو الدوافع التي تلابس ارتكاب الجريمة⁽¹⁾ ومنها الشهادة المستمدة من سماع الشهود، واعتراف المتهم المعلوماتي المستمد بدوره من الاستجواب، لذلك فإننا سنتناول كل وسيلة إثبات شخصية من منظور إجرائي وموضوعي وهي جوهر العملية الإثباتية.

المطلب الأول

الشهادة.

(1) سعدون بن محمد بن طويق العتيبي ، استخدام وسائل الإثبات التقنية في الدعوى الجنائية في مجال التعازير، رسالة مقدمة استكمالاً لنيل درجة الماجستير في العلوم الأمنية، المركز العربي للدراسات الأمنية والتدريب الرياض السعودية، سنة 1994 ، ص 109.

تعد الشهادة من وسائل الإثبات الجنائي ذات الأهمية البالغة، إذ كثيرا ما تكون للشهادة وخاصة تلك التي يدلى بها فور وقوع الحادث أكبر الأثر في الحكم بالإدانة أو البراءة، وغالبا ما تقوم بدور الدليل في الدعوى بمفردها ودون أن يؤازرها دليل آخر⁽¹⁾.

ونتيجة لهذا الأثر البالغ الأهمية في إثبات قيام الجريمة من عدمها وصف الفيلسوف الانجليزي بنتام الشهادة بأنها "أعين القاضي و آذان العدالة"⁽²⁾، لكن وقبل التطرق للشهادة في مجال الجريمة المعلوماتية بالدراسة والتفصيل يجب التطرق أولا إلى تعريف الشهادة، وبيان شروطها، و أنواعها في إطارها التقليدي.

الفرع الأول : الأحكام العامة للشهادة.

في إطار الأحكام العامة للشهادة يتوجب علينا تعريف الشهادة (أولا)، ثم تحديد شروط الإدلاء بالشهادة(ثانيا)، دون أن ننسى التطرق إلى أنواع الشهادة(ثالثا)، فكل عنصر له أهمية تتجلى في الفرع الثاني و الثالث.

أولا- تعريف الشهادة:

تعددت التعريفات الواردة بشأن الشهادة ويمكن أن نعرض أهمها ومنها أن الشهادة هي: " ما يقر به شخص ما أمام جهة قضائية عما يكون قد رآه أو سمعه أو أدركه بحاسة من حواسه متعلقا بالجريمة"⁽³⁾، سواء فيما يتعلق بذات الوقائع المكونة لها، أو الوقائع السابقة عليها التي قد تفيد في

(1) سليمان أحمد فضل ،المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)،دار النهضة العربية، القاهرة، 2013، ص326.

(2) عماد محمد ربيع ،حجية الشهادة في الإثبات الجزائي دراسة مقارنة، الطبعة الأولى ، دار الثقافة للنشر و التوزيع ، عمان الأردن 2011 ، ص105

(3) مثل استعمال حاسة السمع فقد تأتي الشهادة نتيجة سماع الشخص لأقوال صدرت عن شخص آخر ،وقد تكون ناتجة عن حاسة البصر كأن يشاهد الشخص الواقعة التي يدلي عنها الشهادة وقد تكون ناتجة عن حاسة الشم .

معرفة بواعث الجريمة أو الوقائع التي تلت وقوعها ⁽¹⁾. أو هي " المعلومات التي تتعلق بالجريمة التي يدلي بها الشاهد أمام سلطة التحقيق" ⁽²⁾.

وعموما هي " إخبار صدق لإثبات حق بلفظ الشهادة في مجلس القضاء". و يجب أن تكون الشهادة دالة دلالة قاطعة على إثبات الشيء المشهود به، بحيث يدلي الشاهد بما شاهده أو سمعه بطريقة تجعل القاضي كالمشاهد للمشهود عليه ⁽³⁾.

أما المشرع الجزائري فإنه لم يورد أي تعريف للشهادة وترك الأمر للقضاء والفقهاء واكتفي بتنظيم أحكام وقواعد الشهادة سواء أمام جهات التحقيق بعنوان "سماع الشهود" تضمنته المواد من 88 إلى 99 من ق.إ.ج، أو أمام جهات الحكم في الفصل الأول من الكتاب الثاني الخاص بقانون الإجراءات الجزائية بعنوان "في طرق الإثبات" تضمنتها المواد من 220 إلى غاية 234 من ق.إ.ج، شأنه في ذلك شأن بعض التشريعات العربية المقارنة ⁽⁴⁾ ، والشهادة في تقديرنا " هي كل المعلومات التي يدلي بها شخص ما إلى جهة قضائية يكون قد أدركها بإحدى حواسه حول إثبات واقعة ما أو نفيها بأدق تفاصيلها دون أن تكون له أي مصلحة سوى قول الحقيقة ".

ثانيا- شروط صحة الشهادة : لصحة الشهادة يجب توفر مجموعة من الشروط أهمها:

أ- الإدراك عند الشاهد:

⁽¹⁾ فوزية عبد الستار ، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات، الطبعة الثانية، دار النهضة العربية، القاهرة مصر سنة 2010، ص556.

⁽²⁾ عبد الفتاح بيومي حجازي ،الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية ، الطبعة الأولى ، دار النهضة العربية، مصر 2009، ص607.

⁽³⁾ سعدون بن محمد بن طويق العتيبي، المرجع السابق، ص 46.

⁽⁴⁾ لم يعرف المشرع الجزائري اللبناني الشهادة وإنما وضع لها قواعد تنظمها في فصل خاص بعنوان "في سماع الشهود" يتضمن المواد من 75 إلى 90 والخاصة بسماع الشهود أمام قاضي التحقيق فضلا عن مواد أخرى تنظم سماعهم تمام جهات الحكم وهو نفس المنهج الذي سلكه المشرع الأردني ونظم قواعدها لدى المدعى العام في قانون أصول المحاكمات الجزائية بعنوان "سماع الشهود" في المواد من 68 إلى 80 فضلا عن سماعهم لدى المحكمة نفس الشيء قام به المشرع الجزائري المصري الذي حدد أحكامها في المواد من 110 إلى 122 كفصل خاص بعنوان "في سماع الشهود" من قانون الإجراءات الجنائية المصري والتي تتم أمام سلطات التحقيق فضلا عن وجود مواد أخرى تنظم سماع الشهود أمام جهة الحكم.انظر عماد محمد ربيع ،المرجع السابق ص89-90 .

تنصب الشهادة حول ما يدركه الشاهد من وقائع بأحد حواسه فيقوم العضو بتسجيل المدركات وتقدير نوعها ومعناها وتمييزها عن غيرها وتنقل هذه المدركات إلى العقل الذي يمثل الجزء الرئيسي في الجهاز العصبي المركزي⁽¹⁾، وتفترض هذه العمليات الذهنية المتعددة أن يكون الشاهد مميزا بمعنى أن له القدرة على فهم ماهية الفعل وطبيعته و توقع الآثار التي من شأنه إحداثها⁽²⁾. والأصل أن لا تقبل الشهادة إلا ممن توافر لديه التمييز وقت تحمل الشهادة ووقت أدائها ، فإذا تخلف التمييز في أي من هاذين الوقتين كأن يكون الشخص صغيرا غير مميز أو مجنونا فإنه يكون غير أهل لأداء الشهادة⁽³⁾، إلا أن المشرع الجزائري سمح لجهة التحقيق أو لجهة الحكم أن تسمع القصر الذين لم يكملوا سن السادسة عشرة بغير حلف اليمين على سبيل الاستدلال وهذا ما نصت عليه المادة 1/228 من ق.إ.ج⁽⁴⁾.

ولعل أن أهم مسألة تطرح نفسها هي مدى قبول القصر للإدلاء بشهاداتهم حول وقائع متصلة بجرائم المعلوماتية باعتبارهم غير مميزين خصوصا فئة صغار نوابغ المعلوماتية الذين يتمتعون بقدرات ذهنية عالية تسمح لجهات التحقيق بجمع الأدلة بكل سهولة وإفادتهم تكون حاسمة في كثير من الأحيان، إلا أن كل ذلك يرجع إلى سلطة قضاة التحقيق في اختيار الشهود الذين يرون أن شهادتهم تكون مفيدة في كشف الحقيقة استنادا إلى الفقرة الأولى من نص المادة 01/88 ق.إ.ج التي تنص على أنه " يستدعي قاضي التحقيق أمامه بواسطة أحد أعوان القوة العمومية كل شخص يري فائدة من سماع شهادته " والى السلطة التقديرية لقضاة الموضوع أثناء إجراءات المحاكمة التي يمكن لها الاستعانة بشهادة القصر وتقديرها.

كما أن شهادة الأصم والأبكم تكون مقبولة بطريق الكتابة بعد أن توضع له الأسئلة ويجب عليها وان كان لا يستطيع الكتابة يتم الاستعانة بمترجم قادر على التحدث معه بناء على طلب

(1) إحمود فالح الخرابشة، الإشكالات الإجرائية للشهادة في المسائل الجزائرية دراسة مقارنة ، الطبعة الأولى الإصدار الأول، دار الثقافة للنشر و التوزيع، عمان الأردن، 2009، ص52.

(2) عماد محمد ربيع، المرجع السابق، ص 333.

(3) فوزية عبد الستار ، المرجع السابق ص 557

(4) تنص المادة 1/228 من ق.إ.ج على أنه " تسمع شهادة القصر الذين لم يكملوا السادسة عشرة بغير حلف اليمين... "

قاضي التحقيق ويتم تحرير محضر بذلك، وهو ما نصت عليه المادة 92 من ق.إ.ج.⁽¹⁾. " في حين قررت المحكمة العليا في إحدى قراراتها بجواز سماع شهادة الكفيف⁽²⁾.

ب- حلف اليمين :

اليمين نداء روعي صادر عن الضمير وتعهد على قول الحق أمام من يقدهه الشاهد، فالشاهد عندما يحلف اليمين يتخذ الله سبحانه وتعالى رقيباً على صدق شهادته ويعرض نفسه لغضبه وانتقامه إن كذب فيها⁽³⁾، ويلزم المشرع الجزائري الشاهد بحلف اليمين في المرحلة القضائية للدعوى الجنائية دون مرحلة التحقيق الابتدائي طبقاً لنص المادة 97 من ق.إ.ج.ج، فيؤديها أمام قاضي التحقيق حسب المادة 2/93 من ق.إ.ج.ج بالصيغة التالية " أقسم بالله العظيم أن أتكلم بغير حقد ولا خوف، وأن أقول كل الحق ولا شيء غير الحق " وأقرت المحكمة العليا الجزائرية أن عدم الإشارة إلى أداء اليمين في محضر المرافعات أو في الحكم يؤدي إلى نقضه، كما أن حلف اليمين من النظام العام فلا يمكن للشاهد أن يمتنع عن أدائه، كما لا يمكنه أن يطلب إعفاءه منه⁽⁴⁾.

بينما اعفي المشرع طائفة من الأشخاص من أداء اليمين ويسمعون على سبيل الاستدلال وتبقي مسألة حلفهم اليمين جوازياً شريطة عدم معارضة أطراف الخصومة⁽⁵⁾.

(1) تنص المادة 92 من ق.إ.ج.ج. على انه "إذا كان الشاهد أصماً أو أكمأ توضع الأسئلة وتكون الإجابات بالكتابة وإذا لم يكن يعرف الكتابة يندب له قاضي التحقيق من تلقاء نفسه مترجماً قادراً على التحدث معه ويذكر في المحضر اسم المترجم المنتدب ولقبه ومهنته وموطنه و ينوه على حلفه اليمين ، ثم يوقع على المحضر".

(2) قرار المحكمة العليا رقم 310572 مؤرخ في 2005/12/28 و المبدأ " لا يمنع قانون الإجراءات الجزائية القاضي من سماع شهادة كفيف".

(3) عماد محمد ربيع، المرجع السابق ، ص 351.

(4) محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية الجزائر ، سنة 1999 الجزء الثاني، ص 366-367.

(5) تنص المادة 228 من ق.إ.ج.ج.ج. على انه " تسمع شهادة القصر الذين لم يكملوا السادسة عشرة بغير حلف يمين وكذلك الشأن بالنسبة للأشخاص المحكوم عليهم بالحرمان من الحقوق الوطنية

ويعفي من حلف اليمين أصول المتهم وفروعه وزوجه، وإخوته وأخواته وأصهاره على درجته من عمود النسب غير أن الأشخاص المشار إليهم في الفقرتين السابقتين يجوز أن يسمعو بعد حلف اليمين إذا لم تعارض في ذلك النيابة العامة أو أحد أطراف الدعوي".

ت- حرية الإرادة:

يقصد بحرية الإرادة قدرة الإنسان على توجيه نفسه إلى اتخاذ عمل معين أو إلى الامتناع عنه دون تهديد أو إكراه، فالشاهد الذي يكون تحت تأثير تهديد أو إكراه تكون شهادته باطلة⁽¹⁾، وتسعي الأنظمة التي تأخذ بنظام الأدلة القانونية إلى وضع أنظمة خاصة بحماية الشهود من التأثير عليهم تجنباً لأي ترهيب أو ترغيب ما يطرح مسألة توفير الحماية لإرادة الشاهد التي تتبع من تصميمه على إظهار الحقيقة.

وقد نص ميثاق منظمة العفو الدولية على حماية الشهود وتأمين الجو الملائم لهم عند الإدلاء بشهاداتهم وربطت هذه الحماية بحقوق المجني عليهم عندما نصت في المادة 04/22 منه على أنه "يجب الموازنة بين حقوق الضحايا وغيرهم من الشهود في الحصول على الحماية من التعرض لأية محاولة للانتقام، أو أي ضرب آخر غير ضروري للمعانة... الخ"⁽²⁾.

أما المشرع الجزائري فقد خص في نص المادة 236 من قانون العقوبات الحماية القانونية للشهود بصفاتهم هذه⁽³⁾ ولم يتناول اثر الشهادة بالنسبة للشاهد المسلوب الإرادة، وبالمقابل من ذلك وضع نصوص تلزم الشهود بالإدلاء بشهاداتهم تحت طائلة العقوبة إن اقتضى الأمر ذلك، طبقاً للمواد 97 و 98 من ق.إ.ج، أما بالنسبة للتشريعات المقارنة فقد سنت بدورها نصوصاً تقرر حماية إرادة الشاهد من أي تأثير ونقرر البطلان لأي شهادة أخذت بغير إرادة حرة منه، منها المادة 302 من قانون الإجراءات الجزائية المصري⁽⁴⁾. والدفع ببطلان أقوال الشاهد لصدورها تحت تأثير

(1) عماد محمد ربيع، المرجع السابق، ص338.

(2) إحمود فالح الخرابشة، المرجع السابق، ص 59.

(3) لقد قرر المشرع الجزائري حماية الشاهد من أي تأثير خارجي قد يؤثر على إرادته في جرائم القانون العام بينما شملت هذه الحماية المقربين منه في القانون 01/06 المتعلق بمكافحة الفساد فقد خص في المادة 45 منه بعنوان "حماية الشهود والخبراء والمبلغين والضحايا" حماية خاصة للشهود وأفراد عائلاتهم وذوي الصلة بهم حينما نص في المادة 45 على أنه "يعاقب بالحبس من 6 أشهر إلى 5 سنوات وبغرامة من 50.000 دج إلى 500.000 دج كل شخص يلجأ إلى الانتقام أو الترهيب أو التهديد بأية طريقة كانت أو بأي شكل من الأشكال ضد الشهود أو الخبراء أو الضحايا المبلغين أو أفراد عائلاتهم وسائر الأشخاص الوثيقي الصلة بهم".

(4) تنص على أن " .. وكل قول يثبت أنه صدر من أحد الشهود تحت وطأة الإكراه أو التهديد به يهدر ولا يعول عليه". انظر فوزية عبد الستار، المرجع السابق ص 558.

الإكراه أو التهديد دفع جوهرى يجب على المحكمة مناقشته والرد عليه وإلا كان حكمها قاصرا وهو ما أكدته محكمة النقض المصرية⁽¹⁾.

ث - صلاحية الإدلاء بالشهادة:

يقصد بصلاحية الشهادة أن لا تتعارض صفة المدلى بشهادته في الدعوى مع صفة الشاهد وان لا تتوافر الصلاحية فيمن يحظر القانون عليهم أداء الشهادة وفي الحدود التي يقرها، فلا يصلح للشهادة من كان خصما أو أحد أعضاء هيئة المحكمة الناظرة للدعوى، والقاعدة انه لا يجوز الجمع بين صفة الشاهد و الخصم ،كما لا تصلح شهادة متهم على متهم بيد أن له مصلحة تحقيق البراءة ما يجعله يحيد نحو تحقيق هدفه⁽²⁾.

وتعتبر سيرة و أخلاق الشاهد مسألة جوهرية في الأخذ بصلاحية شهادته، وقد دأبت بعض التشريعات على استبعاد شهادة المحكوم عليهم بجناية مثل المشرع المصري استنادا إلى نص المادة 03/25 من قانون العقوبات المصري على عكس المشرعين اللبناني و الأردني الذين نصيا على عدم حرمان المحكوم عليهم من الشهادة⁽³⁾، في حين نص المشرع الجزائري في المادة 228 من ق.إ.ج.ج على جواز سماع شهادة الأشخاص المحكوم عليهم بالحرمان من الحقوق الوطنية على سبيل الاستدلال فقط أي دون حلف اليمين القانونية.

بينما يستبعد قاضي التحقيق سماع بعض الأشخاص كشهود بنص القانون مثل الأشخاص الذين سبق و أن وجه لهم الاتهام ،أو من رفع ضدهم شكوى مصحوبة بادعاء مدني، أو من تتوافر ضدهم دلائل قوية متوافقة على قيام دلائل ضدهم عملا بنص المادة 89 من ق.إ.ج، وكذا الأشخاص الأمتاء على الأسرار إذ لا يمكن إرغامهم على الشهادة تطبيقا لأحكام المادة 286 من

(1) عماد محمد ربيع، المرجع السابق، ص339.

(2) فوزية عبد الستار، المرجع السابق، ص558-559.

(3) عماد محمد ربيع، المرجع السابق، ص 340-341.

ق.إ.ج .ج لأن شهادة هذه الفئة تكون تحت طائلة عقوبة إفشاء السر المهني المنصوص عليها في المادة 301 / 01 من ق.ع.ج(1).

ثالثا - أنواع الشهادة:

تنقسم الشهادة إلى الشهادة المباشرة، والشهادة السماعية، بالإضافة إلى الشهادة الالكترونية كصيغة جديدة للشهادة.

أ- الشهادة المباشرة:

يقصد بالشهادة المباشرة أن يدلي الشاهد بالمعلومات التي وصلت إلى حواسه عن طريق مباشر ودون وساطة شخص آخر فهذا الشاهد هو من رأي أو سمع أو شم... الخ ، فالشهادة في هذا النوع يمكن الوثوق بها قانونا، ويمكن الاستناد عليها كدليل في الإثبات الجنائي(2).

ب- الشهادة السماعية:

وتسمى الشهادة غير المباشرة ، وهي التي يدلي بها الشاهد عن وقائع لم يدركها بإحدى حواسه وإنما سمعها من شخص آخر أدرك الوقائع بإحدى حواسه بعد فترة وجيزة من ارتكاب الفعل شريطة أن يكون الشخص المنقول عنه شاهدا في الدعوى(3) ، والمشرع الجزائري لم يتطرق إلى هذا النوع من الشهادة بالنص وترك المجال لحرية الإثبات وتقدير السلطة القضائية.

ت- الشهادة الالكترونية :

يطلق على هذا النوع من الشهادة اسم الشهادة الالكترونية الفورية ، وتفترض هذه النوعية من الشهادة حصولها في مرحلة التحقيق النهائي أمام محكمة الموضوع ، حيث يكون الشاهد غير حاضر ماديا أو جسديا أمام المحكمة ، وإنما يتم سماعه عبر وسائل الكترونية من خلال شبكة

(1) محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري ، الجزء الأول، المرجع السابق، ص 310-311.

(2) خالد ممدوح إبراهيم ، فن التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، دار الفكر الجامعي ، الإسكندرية مصر ، سنة 2009، ص 259.

(3) إحمود فالج الخرابشة ، المرجع السابق، ص 37.

الفصل الأول.....إثبات الجريمة المعلوماتية بالوسائل التقليدية .

الانترنت أو الأقمار الصناعية بشكل سمعي ومرئي، والشاهد يبرز في هيئته الكاملة بحيث تظهر لهيئة المحكمة ردود أفعاله الطبيعية عندما توجه له الأسئلة، ما يسمح للمحكمة بتقدير قيمة هذه الشهادة⁽¹⁾.

وقد أوضحت هذه الطريقة مقبولة لدى اغلب الفقهاء ومنها أجاز المشرع الفرنسي بالنص الصريح في المادتين 102 و17/706 من قانون الإجراءات الجزائية الفرنسية الأخذ بهذه الطريقة وغيرها من الوسائل التقنية في أخذ الإفادات أو استجواب الأشخاص على أن تضمن هذه الوسائل سرية الاتصال⁽²⁾. كما سمح بنص المادة 86/706 بسماع العون المتسرب كشاهد سواء أثناء التحقيق أو المحاكمة، شريطة مراعاة مقتضيات المادة 61/706 أين اشترطت أن يتم السماع عن طريق وسيلة تقنية تستعمل عن بعد وتجعل من الصوت غير متعرف عليه، وموقف المشرع الفرنسي إنما جاء استجابة لاجتهاد المحكمة الأوروبية لحقوق الإنسان وكذا محكمة النقض الفرنسية⁽³⁾، بينما تبني القضاء الأمريكي الأخذ بنظام الشهادة الالكترونية الفورية عندما واجه القضاء مشكلة إداء الشهادة من قبل أشخاص وضعوا في برنامج حماية الشهود⁽⁴⁾، واشترط أن تتم الشهادة عبر دوائر تليفزيونية مغلقة⁽⁵⁾.

أما المشرع الجزائري فلم يتطرق إلى مسألة الشهادة الإلكترونية في قانون الإجراءات الجزائية شأنه في ذلك شأن المشرع المصري، و العراقي، و السوري، بالرغم من أنها أصبحت مسابرة

(1) محمد طارق عبد الرؤوف الحن، جريمة الاحتيال عبر الانترنت (الأحكام الموضوعية والأحكام الإجرائية) (الطبعة الأولى منشورات الحلبي الحقوقية بيروت لبنان، 2011، ص 306-307.

(2) رشاد خالد عمر، المرجع السابق، ص154.

(3) مصطفى عبد القادر، دراسة بعنوان أساليب البحث و التحري الخاصة وإجراءاتها، مجلة المحكمة العليا، العدد 02، الجزائر، سنة 2009، ص 69.

(4) في احدي القضايا قرر القاضي jack B. weinstein قبول طلب الاتهام بسماع شاهد عبر دوائر تليفزيونية مغلقة حيث كان الشاهد موضوعا في برنامج حماية الشهود شريطة أن يكون حضور الشاهد عبر الدوائر المغلقة كما لو كان حاضرا الجلسة بالفعل ويكون كل ما يدور في الجلسة مرئيا له بالمقابل لرؤية من هو في الجلسة له. انظر سليمان أحمد فضل، المرجع السابق، ص 331.

(5) الدارة المغلقة تعني انغلاق الدارة الاتصالية بين جهتين فأكثر، يتم تحديدها مسبقا، بحيث لا يستطيع الغير الدخول إلى هذه الدارة، فقد قررت المحكمة الفيدرالية الأمريكية العليا قبول نظام الشهادة عن بعد عبر الدارات المغلقة، أنظر محمد طارق عبد الرؤوف

الحن، المرجع السابق، ص307

للتطور التكنولوجي فهي مفيدة في كثير من الأحيان، خصوصا عندما تلجأ جهة التحقيق إلى إجراء الإنابة القضائية لسماع بعض الأشخاص يتعذر حضورهم ويتطلب وقتا، كما أنه أثناء المحاكمة وفي حالة تغيب الشهود فإنها تلجأ إلى تلاوة الشهادة في الجلسة ، ما يطرح فكرة الاستعانة بالشهادة الإلكترونية في جلسة المحاكمة، وهي تتناسب مع مبدأ حرية الإثبات الذي نص عليه المشرع الجزائري في المادة 212 من ق.إ.ج " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص .

ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات و التي حصلت المناقشة فيها حضوريا. " لذلك فإننا نؤيد ما ذهب إليه الدكتور محمد طارق عبد الرؤوف الحن من انه يمكن الاستعانة بالشهادة الالكترونية ومناقشتها في الجلسة حضوريا كأى دليل آخر خصوصا في الجريمة المعلوماتية التي تتوزع أحيانا على أكثر من قطر والتي تطرح مسألة تواجد الشهود في أماكن بعيدة يصعب حضورهم وشهادتهم حاسمة، ولكن يجب ربطها بتوفر شروط معينة أهمها :

- أن تتم وفقا لإجراءات سماع الشهود الحاضرين ماديا.
- أن تتم في دارة مغلقة تجنباً لأي تشويش أو اختراق .
- أن تتم بحضور مختصين فنيين في مجال الاتصالات مع ضمان نقل مباشر .
- أن يتم إبلاغ أطراف الخصومة وإبداء ملاحظاتهم بشأنها.

ومع إطلاق وزارة البريد وتكنولوجيات الإعلام و الاتصال خدمة الجيل الثالث في ديسمبر 2013 أصبح من السهل تلقي شهادة أي شخص عبر متعاملي الهاتف النقال وعبر وسائط الكترونية من شأنها تسهيل سماع الأشخاص صوتا وصورة، ما يجعل من المشرع الجزائري ملزم بمسايرة التطور التكنولوجي وذلك بصياغة نصوص إجرائية تحدد كيفية قبول الشهادة الالكترونية.

الفرع الثاني: الشاهد المعلوماتي.

يعتبر الشاهد المعلوماتي على اختلاف طوائفه من أهم العوامل التي يركز عليها المشرعين والمحققين في مجال الجريمة المعلوماتية من أجل الوصول إلى الحقيقة الرقمية فماذا يقصد به؟ وما هي طوائف هذا الشاهد؟ وما هي أهم الالتزامات المنوطة بهذه الطائفة؟

أولاً- تعريف الشاهد المعلوماتي:

الشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة و المتخصص في تقنية وعلوم الحاسب الآلي، والذي تكون لديه معلومات جوهرية لازمة للدخول إلى نظام المعالجة الآلية للبيانات system traitement information متى كانت مصلحة التحقيق تتطلب التنقيب عن المعلومات داخله، ويطلق عليه اسم الشاهد المعلوماتي تمييزاً له عن الشاهد التقليدي⁽¹⁾.

ثانياً- طوائف الشاهد المعلوماتي:

يشمل الشاهد المعلوماتي عدة طوائف أهمها مقدمو الخدمة ، مشغلو الحاسوب، خبراء البرمجة المحللون، مهندسو الصيانة، مديرو النظم.

أ- مقدمو الخدمات: وضح المشرع الجزائري المقصود بمقدمي خدمة الانترنت في المادة 04 من المرسوم التنفيذي رقم 257/98 المتعلق بضبط شروط و كفاءات إقامة خدمات الانترنت واستغلالها بأنهم : الأشخاص المعنويين الخاضعين للقانون الجزائري وبرأسمال يملكه فقط أشخاص معنويون خاضعون للقانون العام و/ أو أشخاص طبيعيين من جنسية جزائرية⁽²⁾، ويصدر القانون

(1) عبد الفتاح بيومي حجازي ، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية،المرجع السابق،ص 612.انظر كذلك سليمان أحمد فضل المرجع السابق ،ص 332،كذلك الشحات ابراهيم محمد منصور، الجرائم الالكترونية في الشريعة الإسلامية و القوانين الوضعية ،بحث فقهي مقارن ،الطبعة الأولى،سنة2011دار الفكر الجامعي الإسكندرية مصر، ص 197.

(2) عرفت المادة 03/01 من اتفاقية بودابست لسنة 2001 مزودي الخدمة بأنهم كل شخص طبيعي أو معنوي يقوم بتزويد المستخدمين بالخدمات التي تمكن وتسهل الاتصالات بين أجهزة الكمبيوتر وكذلك كل من يتولى معالجة المعطيات المخزنة نيابة عن مزود الخدمة، زبيحة زيدان،الجريمة المعلوماتية في التشريع الجزائري و الدولي،دار الهدي للطباعة والنشر و التوزيع، عين اميلية الجزائر، سنة2011، ص 154.

04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها عرف مقدمي الخدمات في الفقرة "د" من المادة 02 بأنهم:

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

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

ب- القائم على تشغيل الحاسب الآلي: وهو المسئول عن تشغيل جهاز الحاسب الآلي و المعدات المتصلة به و يجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز و استخدام لوحة المفاتيح في إدخال البيانات كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج (1).

ت- المبرمجون: وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين:

1- مخطوطو برامج التطبيقات : وهم يقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات.

2- مخطوطو برامج النظم : هذه الفئة تقوم باختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية، أي انه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج و الأجزاء الداخلية التي تتحكم في وحدات الإدخال و الإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج (2).

ث- المحللون : المحلل وهو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية

(1) عائشة بن قارة مصطفي، المرجع السابق، ص127.

(2) سليمان أحمد فضل، المرجع السابق، ص 332. كذلك عائشة بن قارة المرجع السابق، ص 127.

الفصل الأول.....إثبات الجريمة المعلوماتية بالوسائل التقليدية .

من هذه الوحدات ،كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب.

ج- مهندسو الصيانة والاتصالات : وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الإيصال المتعلقة به.

ح- مديرو النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية⁽¹⁾.

ثالثا - التزامات الشاهد المعلوماتي :

باعتبار الشاهد المعلوماتي وليد الجريمة المعلوماتية ونظرا لموقعه في التعامل مع المجرمين المعلوماتيين بشكل أو بآخر، وقع جدل فقهي حول التزاماته (أولا)، رغم تناول هذا المسألة بعناية في التشريعات المقارنة (ثانيا)، وهو ما دفع بالمشرع الجزائري بدوره إلى تحديد التزامات الشاهد المعلوماتي (ثالثا)، باعتبارها من ميكانيزمات المواجهة.

أ- الجدل الفقهي حول التزامات الشاهد المعلوماتي:

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق⁽²⁾ ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، ولكن هل يلتزم الشاهد بطبع الملفات ومنح كلمات المرور والشفرات؟ في هذا الصدد هناك اتجاهين:

1- الاتجاه الأول: ويرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة ويميل إلى هذا الاتجاه المشرع الألماني على أساس أن الالتزام بالشهادة لا يتضمن هذا الواجب⁽¹⁾.

(1) عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 613 .
(2) لقد أوصى المؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات في ريوديجانيرو سنة 1994 بضرورة إيجاد آليات تعاون فعالة مابين الشهود وسلطات الاستدلال والتحقيق على وجه الخصوص فيما يتعلق بإباحة المعلومات في صورة يمكن استخدامها للأغراض القضائية، وقد تأثرت بهذا الإجراء معظم التشريعات الأوروبية. رشاد خالد عمر، المرجع السابق، ص 156.

2- الاتجاه الثاني: ذهب هذا الاتجاه إلى انه من الممكن إلزام الشاهد المعلوماتي بالإفصاح عن تلك المعلومات و القيام بتلك الأعمال، وذلك من خلال النص الصريح في القانون على فرض التزام على عاتقه يسمى بالالتزام الشاهد المعلوماتي بالإعلام⁽²⁾ في الجرائم المعلوماتية، الذي يفرض عليه واجبا بتقديم أية معلومات ضرورية ولازمة من أجل إعانة سلطات التحقيق في الحصول على أدلة إثبات عن الجريمة المعلوماتية الواقعة⁽³⁾.

ب- التزامات الشاهد المعلوماتي في التشريع المقارن:

لقد سارت اغلب التشريعات الغربية إلى تبني الاتجاه الثاني، لذا اتجه الفقه الفرنسي إلى أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية مما يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم، كما تنص عليه المواد 138،109،62 من قانون الإجراءات الجزائية الفرنسي، وان إعطاء المعلومات غير معاقب عليه إلا في مرحلة التحقيق و المحاكمة⁽⁴⁾، فيما ألزم المشرع الأمريكي مزودي خدمات الاتصالات الالكترونية بتقديم ما يلزم من عون فني تقني لسلطات التحقيق في الجرائم المعلوماتية، وعاقب المخالف بغرامة قدرها 10.000 دولار عن كل يوم تأخير⁽⁵⁾.

(1) عبد العال الديري و محمد صادق إسماعيل ، الجرائم الالكترونية دراسة قانونية قضائية مع احدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت ، الطبعة الأولى ،المركز القومي للإصدارات القانونية ، القاهرة مصر ، سنة 2012، ص 315-316.

(2) ويمكن تلخيص أسباب إلزام الشاهد المعلوماتي بالالتزام بالإعلام في الجريمة المعلوماتية في:

1- تحقيق التوازن في المعلومات الجوهرية المتصلة بالنظم المعلوماتية بين شهود ومستخدمي الحاسبات الآلية وسلطات التحقيق.

2- تحقيق التعاون والتضامن بين المتعاملين في بيئة تكنولوجيا المعلومات.

3- تدارك أوجه القصور و العجز الذي تتسم به الوسائل التقليدية. سليمان غازي العتيبي، درجة توافر كفايات البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة ، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية تخصص قيادة أمنية الرياض ، جامعة نايف العربية للعلوم الأمنية، سنة 2010، ص77-78.

(3) رشاد خالد عمر ، المرجع السابق، ص156.

(4) عبد العال الديري و محمد صادق إسماعيل، المرجع السابق، ص316.

(5) رشاد خالد عمر، المرجع السابق، ص157.

أما المشرع الانجليزي فحول بموجب القانون الصادر سنة 1984 بشأن البوليس و الأدلة الجنائية المحققين الحق في أن يطلبوا من الغير تمكينهم من الدخول إلى المعلومات المخزنة في الحاسب الآلي أو بالاطلاع عليها أو قراءتها⁽¹⁾.

ت - التزامات الشاهد المعلوماتي في التشريع الجزائري:

من خلال القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها قام المشرع الجزائري بتكريس نوعين من الالتزامات الموجبة لمقدمي الخدمات، وهي الالتزامات المشتركة على جميع مقدمي الخدمات، وكذا الالتزامات الخاصة بالنسبة لمقدمي خدمات الانترنت.

1- الالتزامات الموجبة على جميع مقدمي الخدمات:

ألزم المشرع الجزائري مقدمي الخدمات بما يلي:

- تقديم المساعدة للسلطات المكلفة بالتحقيق القضائي عملا بنص المادة 10 من القانون 04/09 من خلال جمع وتسجيل كل المعطيات⁽²⁾ المتعلقة بمحتوي الاتصالات في حينها.

- كتمان السر⁽³⁾ بخصوص العمليات التي ينجزونها بطلب من المحققين وما تحصل عن ذلك من معلومات تحت طائلة العقوبات المقررة لإفشاء أسرار التحري و التحقيق المادة02/10.

- حفظ المعطيات⁽¹⁾ المتعلقة بحركة سير الاتصالات لمدة سنة تبدأ من تاريخ التسجيل ووضعها تحت تصرف سلطة التحقيق (اعتراض الاتصالات من خلال مثلا تسهيل وضع الإجراءات التقنية

(1) عائشة بن قارة مصطفى، المرجع السابق، ص130.

(2) تجدر الإشارة إلى أن المعطيات المعلوماتية محل البحث و التتقيب الجزائري ليست نوعا واحدا بل لها نماذج متعددة بما في ذلك ثلاثة أنواع خاصة : 1- المعطيات المتصلة بالمرور التي سماها المشرع الجزائري في المادة 11 بحركة سير 2- معطيات المحتوي 3- ومعطيات المشترك رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت لبنان، 2012، ص 448.

(3) تنص المادة 02/14 من المرسوم التنفيذي 257/98 المحدد لشروط و كفيات استخدام الانترنت على ما يلي " يلتزم مقدم خدمات انترنت خلال ممارسة نشاطه بما يأتي:...المحافظة على سرية كل المعلومات المتعلقة بحياة مشتركه الخاصة وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون..."

لإنجاز وتنفيذ عمليات الاعتراض، كما أنهم ملزمون بان يضعوا تحت تصرف سلطة التحقيق المعطيات الغير مشروعة التي تم حفظها تطبيقا لنص المادة 11 من القانون 04/09 كمعطيات البحث مثل: عنوان الـ IP بروتوكول التبادل المستعمل، مدة الاتصال، المواقع التي تم الدخول إليها وكذا المعطيات التي تسمح بالتعرف على مستعملي هذه الخدمات⁽²⁾.

2- الالتزامات الخاصة بمقدمي خدمة الانترنت :

مقدمي خدمة الإنترنت رتبت لهم التزامات خاصة قررها المشرع الجزائري في نص المادة 12 من القانون 04/09 فإلي جانب التزامهم بحفظ حركة سير الاتصالات المحددة في نص المادة 11 من نفس القانون، فهم ملزمون بالتدخل الفوري لسحب المحتويات المخالفة للقوانين الوطنية وتخزينها أو جعل الدخول إليها غير ممكن بمجرد اطلاعهم عليها بصورة مباشرة أو غير مباشرة بالإضافة إلى إلزامهم بوضع الترتيبات التقنية التي تسمح بحصر إمكانية الدخول إلى الموزعات التي تحوي معلومات مخالفة للنظام العام، أو الآداب العامة، وإخبار المشتركين بوجودها .

الفرع الثالث: قيمة الشهادة في إثبات الجريمة المعلوماتية.

إذا كان المشرع الجزائري ألزم الشاهد المعلوماتي بمساعدة سلطات التحقيق بالتزامه بحفظ وتسجيل المعطيات، وكتمان السر بكل الوسائل المتاحة تحت طائلة العقوبة، فلنا أن نتساءل هل أن جهة الحكم ملزمة بالأخذ بما صرح به الشاهد كدليل إثبات وله من الحجية ما يكفي للاقتناع ؟

(1) لقد تضمنت اتفاقية بودابست مصطلح التحفظ في المادة 16 منها و التي تعني في اللغة المعلوماتية حفظ المعطيات سبق وجودها في شكل مخزن وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة في حين استعمل المشرع الجزائري مصطلح حفظ في المادة 11 الذي يعني أرشفة المعطيات وهي تخزين للمعطيات فقط ولم يعر الاهتمام لأمر أمن المعطيات من خطر التغيير، انظر رشيدة بوكور، المرجع السابق، ص 448.

(2) **Hadjira Boudet**, communication sous titre « fournisseurs de service internet : prévention et lutte contre la cybercriminalité », commis dans l'Actes du séminaire international Alger le 5-6 Mai 2010, centre de recherche juridique et judiciaire, Ibsen édition & diffusion, P 206-207.

إن الدارس في مجال المعلوماتية يري بأن الشهادة في مجال المعلوماتية انتقلت من مبدأ الالتزام بأداء الشهادة إلى مبدأ الالتزام بالإعلام في الجريمة المعلوماتية⁽¹⁾، وأن الشهادة في مجملها تسعى ليس فقط لإثبات الجريمة وإنما إلى البحث من خلالها على تكوين الدليل الالكتروني الفني الذي يتم الإثبات بواسطته.

ومنه من يري أنه ليس بلازم أن تتطابق أقوال الشهود مع مضمون الدليل الفني بل يكفي أن يكون جماع الدليل القولي غير متناقض مع الدليل الفني تناقضا يستعصى على الملائمة و التوفيق، وليس بلازم أن ترد على الحقيقة المراد إثباتها بأكملها وبجميع تفاصيلها بوجه دقيق إذ يكفي أن يكون من شأنها أن تؤدي إلى تلك الحقيقة باستنتاج سائغ تجريه المحكمة⁽²⁾.

و في تقديرنا فان الشهادة في الجريمة المعلوماتية لها مكانتها يمكن للقاضي أن يستأنس بها في مجموع الأدلة فلا يمكن القول بعدم جدواها مطلقا، ولكنه زاد بريقها من الناحية التشريعية، من حيث الاهتمام بطوائف الشاهد المعلوماتي، والزامهم بالإبلاغ، وهو دور ايجابي في التصدي للجريمة، وفي تقديرنا تبقي الشهادة وسيلة يتجلى دورها أكثر عند استخلاص الدليل الالكتروني وليست وسيلة كافية لوحدها في إثبات الجريمة في حد ذاتها، وهو ما يدفعنا إلى البحث في الوسيلة الشخصية المتبقية وهي الاستجواب المؤدي إلى الاعتراف.

المطلب الثاني

الاستجواب و الاعتراف.

من خلال تقديرنا لمقتضيات الموضوع ارتأينا تناول هذا المطلب من الزاوية الإجرائية وهي الاستجواب بضماناته كوسيلة إثبات للوصول إلى الوسيلة الموضوعية وهي الاعتراف فهما وسيلتين متلازمتين تتطلب دراستهما من حيث الجدوى في إثبات الجريمة المعلوماتية، وعليه نتطرق إلى

(1) عائشة بن قارة مصطفى، المرجع السابق، ص 137.

(2) محمد زكي أبو عامر ، الإثبات في المواد الجنائية محاولة فقهية وعملية لإرساء نظرية عامة، دار الجامعة الجديدة، الإسكندرية مصر، 2011، ص230.

الأحكام العامة للاستجواب(كفرع أول)، ثم معرفة ضمانات الاستجواب في الجريمة المعلوماتية في (فرع ثاني)، لننتقل إلى الاعتراف وقيمه في إثبات الجريمة المعلوماتية في (فرع ثالث).

الفرع الأول: الأحكام العامة للاستجواب.

أولاً- تعريف الاستجواب: الاستجواب في الفقه الجنائي مصنف ضمن وسائل الإثبات له مكانة خاصة في بعض أنظمة الإثبات الغرض منه الحصول أساساً على إقرار المتهم على نفسه ونتيجة لذلك فهو يطبق على جميع الجرائم كإجراء وجوبي بما فيها الجريمة المعلوماتية.

و يمكن تعريف الاستجواب بصفة عامة بأنّه" مناقشة المتهم تفصيلاً في الأدلة و الشبهات القائمة ضده، ومطالبته بالرد عليها إما بإنكارها وإثبات فسادها، وإما بالتسليم بها وما يستتبعه ذلك من اعتراف بالجريمة"⁽¹⁾.

والحقيقة أن استجواب المتهم في الجريمة المعلوماتية المتميزة بطابعها التقني تطرح مسألة مدي نجاح الاستجواب، لأن الأصل في الاستجواب كوسيلة تحقيق قضائية لا يختلف عن الجرائم التقليدية منه في الجريمة المعلوماتية ، إلا أن هذه الأخيرة تتطلب توفر محققين قضائيين يتمتعون بخبرة ودراية بالمصطلحات التقنية حتى يمكن لهم استيعاب واقعة التحقيق ، والتعامل مع مفردات الجريمة و مصطلحاتها، سيما و أن المجرم المعلوماتي محل الاستجواب ليس مجرماً عادياً فهو يحسن لغة العالم الافتراضي، ومن هذا المنطلق ولإنجاح الاستجواب في الجريمة المعلوماتية يتعين تأهيل المحققين الجنائيين بمفردات الحاسب الآلي وتطبيقاته كضرورة ملحة⁽²⁾.

وعلى هذا الأساس فإن جمع البيانات في إطار التحقيقات يتطلب توفير هياكل قاعدية ذات تكنولوجيا عالية تحتوي على طاقم بشري مؤهل لإنجاز تحقيقات في الجرائم المعلوماتية في أعلى مستوى، وفي هذا السياق أنشئ في أوروبا سنة 2006 مركز للتحقيقات في الجرائم المعلوماتية

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقاً لأحدث التعديلات التشريعية، دار النهضة العربية، القاهرة مصر، سنة 2013، الجزء الأول، ص 628.

(2) عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق ، ص 681.

بجامعة " College Dublin " وهو مركز للبحث و التعليم في الجرائم المعلوماتية يقوم على التعاون بين قوات الأمن والصناعيين، وهو ما مكن من تكوين مختصين في الأمن للتحقيق بفعالية في هذه الجرائم، وبالمقابل فان المحققين لابد وان يتوفروا على معارف في مجال الإعلام الآلي القضائي و تقنيات خاصة في التحقيق في الجرائم المعلوماتية، وهذا المركز متاح لكل منظمات الشرطة وجهات التحقيق في أوروبا كما سهل تكوين منظمة خبراء في الجرائم المعلوماتية (1). وفي تقديرنا فان الاستجواب في الجريمة المعلوماتية يعني " مجابهة المتهم المعلوماتي تقنيا وتفصيلا في الأدلة المعلوماتية القائمة ضده ومطالبته بالرد عليها تقنيا إما بإقرار على نفسه أو نفيها لها تفصيلا."

ثانيا- الطبيعة القانونية للاستجواب في الجريمة المعلوماتية:

يختلف استجواب المتهم عن مجرد سؤاله بواسطة أحد ضباط الشرطة القضائية أثناء قيامه بإجراءات جمع الاستدلالات ، فسماع أقوال المشتبه فيه من طرف الضبطية القضائية يكون بخصوص الواقعة المنسوبة إليه دون مناقشة تفصيلية ودون تحقيق دفاعه بخصوصها ، وذلك لأن الاستجواب ليس من سلطات الضبطية القضائية وإنما من السلطات القضائية، وقد كان نتيجة ذلك عدم وضع ضمانات في القانون للمشتبه فيه عند سماع أقواله أمام الضبطية مثل تلك المقررة للمتهم عند الاستجواب(2)، لأن الضمانات المقررة للمشتبه فيه على مستوي مراكز الضبطية هي مجرد ضمانات عامة تراعي مسالة حقوق الإنسان أكثر منها مراعاة مسائل قانونية متعلقة بقيمة السماع في حد ذاته وأثره على مسالة الإثبات.

و يختلف الاستجواب الذي تجريه المحكمة عن ذلك الذي تجريه سلطة التحقيق ، فالاستجواب أمام سلطة التحقيق يعتبر وسيلة إثبات ووسيلة دفاع ،بينما هو أمام المحكمة وسيلة دفاع تستهدف

(1) Mohand Tahar Kechadi, communication sous titre « investigation en cybercriminalité» commis dans l'Actes du séminaire international Alger le 5-6 Mai 2010 , centre de recherche juridique et judiciaire, Ibsen édition & diffusion p 194-195.

(2) عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 681، انظر كذلك سعدون بن محمد بن طويق العتيبي، المرجع السابق، ص 115.

إتاحة السبيل أمام المتهم لإثبات براءته⁽¹⁾، وهو ما ينطبق على الاستجواب في الجريمة المعلوماتية من حيث المبدأ لأن سلطة التحقيق بسماعها للشهود المعلوماتيين وأمرها بإجراء الخبرات التقنية بناء على ما تمت معاينته ، و ضبطه ومواجهة المتهم المعلوماتي بها بحضور الخبراء يشكل وسيلة إثبات قد تدفع بالمتهم إلى الانهيار ثم الاعتراف، بينما من جهة أخرى تمنح له فرصة إبداء دفاعه من خلال إنكاره لها وتقديم الإيضاحات التقنية وأدلة النفي التي من شأنها درء التهمة عنه.

ونخلص القول إلى أن الاستجواب في الجريمة المعلوماتية ذو طبيعة فنية غاية في الدقة يتطلب تأهيل القضاة لإجرائه، في حين تم طرح دراسات جديدة لتبني الاستجواب الإلكتروني باستعمال برامج آلية تقوم بالاستجواب وفقا لحسابات دقيقة ومؤكدة لتجنب نقص كفاءة المحققين⁽²⁾.

ثالثا - صور الاستجواب: يتجسد الاستجواب في صورتين فإما أن يكون حقيقيا وإما حكما.

أ - الاستجواب الحقيقي:

يتحقق الاستجواب بتوجيه التهمة ومناقشة المتهم تفصيليا عنها ومواجهته بالأدلة القائمة ضده، فلا يتحقق الاستجواب بمجرد سؤال المتهم عما هو منسوب إليه أو إحاطته علما بنتائج التحقيق إذا لم يتضمن ذلك مناقشة تفصيلية في الأدلة المسندة إليه، أي أن الاستجواب يقتضي توافر عنصرين

(1) فوزية عبد الستار، المرجع السابق، ص 582.

(2) وهو ما تم طرحه في المؤتمر الدولي الثاني للاتجاهات الحديثة في الإثبات و التحقيق الجنائي المنعقد في أمستردام بين 5-15 ديسمبر 1999 إذ وفر المؤتمر دراسات وتجارب مقنعة تشجع على استبدال إجراءات الشرطة في مجال جمع الاستدلالات من الأسلوب العلمي على قدرة الحاسب الآلي على التحليل و الاستنتاج و الملاحظة بكفاءة أكثر من المحقق وقد وفرت تلك الدراسات برامج يمكن تطويرها لمعاينة مسرح الجريمة وجمع الآثار وصناعة الأدلة والاستجواب الفني للمتهمين والشهود وفق ترتيبات حسابية مؤكدة. انظر أمين البشري، الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات، المجلة العربية للدراسات الأمنية و التدريب المجلد 17 العدد 33. متاح على الموقع الإلكتروني: <http://www.nauss.edu.sa/Ar/em-dar-33-3pdf>

لا قيام له بدونهما أولهما توجيه التهمة ومناقشة المتهم تفصيلا عنها والعنصر الآخر هو مواجهة المتهم بالأدلة القائمة ضده، ولا يلتزم المحقق بترتيب معين في استيفاء هذين العنصرين⁽¹⁾.

ب- الاستجواب الحكمي "المواجهة" :

يعد القانون مواجهة المتهم بغيره من الشهود أو المتهمين في حكم الاستجواب، فهذه المواجهة تتطوي على إحراجه ومواجهته بما هو قائم ضده، وتقتضي المواجهة أن تقتزن بمناقشة المحقق للمتهم تفصيلا في الموقف الحرج الذي قد يتعرض له مما يجعلها في حكم الاستجواب⁽²⁾.

وتفترض المواجهة توافر عنصران وتعاصرهما في وقت واحد للقول بتحققها بمفهومها القانوني الدقيق الأول يتمثل في المقابلة الشخصية والثاني يتجسد في المقابلة القولي هـ ولا تتحقق المواجهة بسقوط أحد هاذين العنصرين⁽³⁾.

الفرع الثاني: إجراءات الاستجواب وضمانات المتهم في الجريمة المعلوماتية.

الاستجواب في الجريمة المعلوماتية يتخذ نفس الأشكال المقررة للجرائم التقليدية وهو كإجراء قضائي يتم إما أمام قاضي التحقيق أو أمام قاضي الموضوع الفاصل في الخصومة الجزائية⁽⁴⁾ ويكون محاطا بمجموعة من الضمانات المقررة في قانون الإجراءات الجزائية.

(1) أحمد فتحي سرور، المرجع السابق، ص 814-815.

(2) أحمد فتحي سرور، نفس المرجع، ص 815.

(3) حسن الجوخدار، مقالة بعنوان السلطة المختصة باستجواب المتهم وحقه في الاستعانة بمحام في قانون أصول المحاكمات الجزائية الأردني و المقارن، منشورة في مجلة أبحاث اليرموك "سلسة العلوم الإنسانية و الاجتماعية، مجلد 24 العدد 02، العراق، جوان 2008، ص 401.

(4) لم يتضمن قانون الإجراءات الجزائية الجزائري أي نص صريح يخول للشرطة القضائية حق استجواب المشتبه فيه إذ وبإجراء تحليل بسيط للفقرة الأولى من نص المادة 01/52 من القانون 08/01 المعدل لقانون الإجراءات الجزائية الجزائري التي تنص على انه " يجب على كل ضابط للشرطة القضائية أن يضمن محضر سماع كل شخص موقوف للنظر مدة استجوابه وفترات الراحة التي تخللت ذلك واليوم و الساعة الذين أطلق سراحه فيهما، أو قدم إلى القاضي المختص". فحتي لو أخذنا بالدلالة اللفظية للنص فان ضابط الشرطة يعد محضر سماع فقط وليس محضر استجواب ومهمته تلقي أقوال المشتبه فيه فقط كشخص لم يحدد مركزه القانوني بعد لتقرر له الضمانات اللازمة للاستجواب ولا يمكن مواجهته بالأدلة القائمة ضده، أما في الواقع العملي فان محاضر سماع الضبطية القضائية تتضمن أسئلة المحقق وأجوبة المشتبه فيه دون المواجهات سواء الشخصية أو القولية، وعموما فإن محاضر السماع لا تعتبر حجة قاطعة ولا دليلا منتجا مادام لا يأخذ بها القضاء إلا على سبيل الاستدلال فقط لأن الهدف الحقيقي من الاستجواب هو

أولاً- إجراءات الاستجواب وضماناته أمام قاضي التحقيق:

نتناول في هذا العنصر إجراءات الاستجواب و ضماناته أمام قاضي التحقيق ثم الاستجواب وضماناته أثناء المحاكمة.

أ- إجراءات الاستجواب أمام قاضي التحقيق:

يتم الاستجواب في الجريمة المعلوماتية عبر مرحلتين باعتبارها جنحة أين يتم استجواب المتهم عند الحضور الأول ثم في مرحلة ثانية يتم تحديدها من طرف قاضي التحقيق يسمع المتهم في موضوع التهمة من جديد ليصدر القاضي أمراً مناسباً بعد ذلك.

1- إجراءات الاستجواب عند المثل الأول:

يتأكد القاضي من هوية المتهم المعلوماتية أثناء الاستجواب الأول ثم يقوم بإعلامه صراحة بالواقعة المنسوبة إليه منوها إياه بأن له الحق في تقديم إقراره بشأن التهمة أو الاحتفاظ بحقه في ذلك مع حقه في توكيل محام للحضور معه⁽¹⁾، أما إذا أصر المتهم على الإدلاء بأقواله بدون دفاعه فإن قاضي التحقيق يسجل تصريحاته عن طريق كاتب الجلسة في محضر الاستجواب وبنوه على ذلك في المحضر، ويختتم الاستجواب عند الحضور الأول بتوقيع المتهم للمحضر بعد قراءته، ثم توقيع القاضي وكاتب الضبط المحرر له (المادة 108 من ق.إ.ج.ج)، ويمكن لممثل النيابة العامة حضور الاستجواب وتوجيه أسئلة مباشرة للمتهم، في حين يكون طرح أسئلة محامي المتهم بترخيص من قاضي التحقيق.

الوصول إلى اعتراف المتهم كدليل له الحجية المطلقة في الإدانة أو البراءة، ومن هذا المنطلق فإن الاستجواب يكون أمام القضاء بمراحله المختلفة فقط.

(1) تنص المادة 100 من ق.إ.ج.ج على أن " يتحقق قاضي التحقيق عند حضور المتهم لديه لأول مرة من هويته ويحيطه علماً صراحة بكل واقعة من الوقائع المنسوبة إليه وينبهه بأنه حر بعدم الإدلاء بأي إقرار وبنوه عن ذلك التنبيه في المحضر فإذا أراد المتهم أن يدلي بأقوال تلقاها قاضي التحقيق منه على الفور كما ينبغي للقاضي أن يوجه المتهم بأن له الحق في اختيار محام عنه فإن لم يختار له محامياً عين له القاضي محامياً من تلقاء نفسه إذا طلب منه ذلك وبنوه عن ذلك بالمحضر كما ينبغي للقاضي علاوة عن ذلك أن ينبه المتهم إلى وجوب إخطاره بكل تغيير طرأ على عنوانه ويجوز للمتهم اختيار مواطن له في دائرة اختصاص المحكمة". في نفس السياق نصت المادة 114 من قانون الإجراءات الجزائية الفرنسي على أنه يجب على المحقق أن يخطر المتهم بأنه حر في ألا يدلي بأي تصريح. انظر محمود نجيب حسني، المرجع السابق، ص 631.

وتجب الإشارة إلى أن قاضي التحقيق يمكن له أن يقوم باستجوابات أو مواجهات على وجه الاستعجال بغض النظر عن الضمانات المقررة للمتهم إذا وجدت إمارات على وشك الاختفاء (1) وهو ما ينطبق على الجريمة المعلوماتية التي تتطلب سرعة في حفظ الدليل المعلوماتي من خلال تتبع البيانات قبل محوها وتخريبها أو إطلاق سراح المتهم ليقوم بإتلافها نهائياً.

2- إجراءات الاستجواب في الموضوع:

يمتثل المتهم في جلسة لاحقة أمام قاضي التحقيق لسماعه في موضوع الواقعة المتابع بها كإجراء وجوبي بعد استدعاء دفاعه إن اختار ذلك وبعد اطلاع محاميه على ملف الإجراءات كشرطين جوهريين(2)، يقوم قاضي التحقيق بطرح أسئلته بشكل تفصيلي دقيق و مرتب، ويستند المحقق في طرح الأسئلة إلى المعلومات السابقة المتحصل عليها من مزودي الخدمات وإلى تعاونهم في التحقيق(3)، أو مما تم ضبطه من مسرح الجريمة، أو من الخبرات التقنية المنجزة المأمور بها، ويجب على قاضي التحقيق أن يكون ملماً بالجوانب التقنية لهذا النوع من الجرائم. وفي هذا الصدد يجب على المحقق أن يتحاشى قدر الإمكان ذكر الاصطلاحات القانونية التي لا يدرك المتهم مضمونها(4)، فمثلاً قد يكون من الأفضل ألا يقول المحقق للمتهم أنت متهم بارتكاب جريمة معلوماتية ، بل يقول له مثلاً أنت متهم بدخولك إلى نظام معين دون إذن من صاحبه ، أو أنك متهم باستعمال برنامج معين أدى إلى إتلاف مجموعة من الحواسيب، وتجدر الإشارة إلى أن تحديد نوع الجريمة المعلوماتية يتطلب مهارة ومعرفة خاصة من قاضي التحقيق بالمجال المعلوماتي، إلى جانب المجال القانوني.

(1) تنص المادة 101 من ق.إ.ج.ج على أن "يجوز لقاضي التحقيق على الرغم من مقتضيات الأحكام المنصوص عليها في المادة 100 أن يقوم في الحال بإجراء استجوابات أو مواجهات تقتضيها حالة الاستعجال ناجمة عن وجود شاهد في خطر الموت أو وجود إمارات على وشك الاختفاء."

(2) محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، المرجع السابق، ص385-386.

(3) بن شهرة شول، الحماية الجنائية للتجارة الالكترونية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق ، تخصص قانون جنائي جامعة محمد خيضر بسكرة ، السنة الجامعية 2010/2011، ص231.

(4) أحمد فتحي سرور، المرجع السابق، ص834.

كما يمكن للمحقق أن يستعين بخبير في المجال المعلوماتي أثناء الاستجواب، للتنسيق معا من أجل إنجاز عملية الاستجواب وفق منهجية مدروسة مسبقا من أجل الوصول إلى الحقيقة⁽¹⁾.

واستنادا إلى نص المادة 151 من ق.إ.ج فقد سمح المشرع الجزائري للخبير باستجواب المتهم على سبيل الحصول على المعلومات وفي الحدود اللازمة لأداء مهامهم ولكن بحضور قاضي التحقيق وفقا للضمانات المقررة للمتهم في الاستجواب، ومن الأنسب في حالة الدول التي لا تسمح قوانينها بمثل هذه المشاركة استصدار قرارات بتشكيل لجان تحقيق تضم في عضويتها الخبرات الفنية المطلوبة في كل حالة⁽²⁾.

أ - ضمانات المتهم المعلوماتي عند استجوابه أمام قاضي التحقيق:

يتمتع المتهم المعلوماتي بنفس الضمانات المقررة للمتهمين في الجرائم التقليدية عند مثولهم أمام قاضي التحقيق دون نقصان وتتمثل هذه الضمانات فيما يلي:

1- ضمان الجهة المختصة بالاستجواب:

(1) من أجل ذلك لا بد من إيجاد أسلوب خاص يجمع بين الخبرة الفنية و الكفاءة المهنية للتحقيق في هذه الجرائم ويمكن إتباع الخطوات التالية:

أ- تبادل المعلومات بين المحقق و خبير الحاسب الآلي قبل البدء في التحقيق و استجواب المتهمين، بحيث يشرح المحقق للخبير أهمية ترتيب سماع الشهود و المتهمين وطريقة توجيه الأسئلة إليهم ، ومن جهة أخرى يقوم الخبير بشرح الأبعاد الفنية و النقاط التي ينبغي استجلاؤها من الأشخاص وكافة المصطلحات الحاسوبية التي يمكن استخدامها و بيان معانيها.

ب- حصر النقاط التي سيتم استجلاؤها من طرف المحقق و الخبير قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب هذه النقاط.

ج- يتم استجواب المتهمين من قبل المحقق و بحضور الخبير الذي يمكن له طرح أسئلة فرعية وفقا للخطة المتفق عليها قبل البدء في الاستجواب.

د- التنسيق بين المحقق و الخبير في الحصول على البيانات المخزنة في الحاسب الآلي وملحقاته الخاصة بالمتهم الذي تم التحقيق معه. أنظر محمد الأمين البشري ، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون و الكمبيوتر و الإنترنت في الفترة من 1 إلى 3/5/2000، الطبعة الثالثة، كلية الشريعة و القانون جامعة الإمارات العربية المتحدة ، سنة 2004، ص 1073.

(2) محمد أمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، سنة 2004، ص 124.

وهي ضمانات إجرائية هامة تضمن أكثر حياد و استقلال بين جهة الاتهام و التحقيق ، يخضع التحقيق فيها لقاضي مستقل يسمى قاضي التحقيق⁽¹⁾، و هو المخول وحده قانونا باستجواب المتهم باعتباره صاحب الاختصاص ، فإذا ما تعذر عليه القيام بذلك بنفسه لسبب أو لآخر يقوم بإصدار إنابة قضائية لقاضي آخر للقيام بالاستجواب نيابة عنه⁽²⁾، بالنظر لطبيعة الجريمة المعلوماتية التي تتوزع أركانها أحيانا على أكثر من قطر، ولو أن الجريمة المعلوماتية تتطلب قاضي تحقيق مؤهل للتحقيق في مثل هذا النوع من الجرائم كضمانة أساسية للمتهم المعلوماتي، ونطرح بدورنا إمكانية استخدام " الاستجواب الالكتروني"⁽³⁾ بالنظر لطبيعة الجريمة.

2- كفالة حق المتهم في أن يدلي بأقواله بكل حرية:

يدلي المتهم بأقواله بكل حرية دون أي تأثير على إرادته مهما قل شأن هذا التأثير، إذ لا يجوز تحليف المتهم لما لذلك من ضغط أدبي يؤثر على إرادته وهو ما اجمع عليه الفقهاء ، كما يحرم أي تعذيب للمتهم لإكراهه على إبداء أقوال معينة ، أو أي إجهاد نفسي للمتهم وذلك بتجنب إطالة وقت الاستجواب ، في حين انعقد الإجماع على تحريم استعمال الوسائل العلمية الحديثة كالنتويم المغناطيسي و استعمال عقار كشف الحقيقة، حتى ولو لم يوجد نص تشريعي يقضي بتحريمه⁽⁴⁾.

3- كفالة حق الدفاع:

(1) أحمد براك، دراسة بعنوان " استجواب المتهم وسماع الشهود في الدعوى الجزائية دراسة مقارنة "، منشورة في مجلة العدالة والقانون الصادرة عن المركز الفلسطيني لاستقلال المحاماة و القضاء "مساواة" سبتمبر 2007، ص 58.

(2) محمد مروان ،نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، المرجع السابق، ص377.

(3) فيمكن تبنيه في حالات معينة كحالة الاستعجال مخافة زوال الدليل المعلوماتي، وبشروط صارمة كأن يتولي قاضي التحقيق مصدر الإنابة استجواب متهم مائل أمام قاضي تحقيق آخر مستقبل الإنابة في دائرة اختصاص مختلفة بعيدة باستعمال النقل الالكتروني المباشر عن طريق أسلوب الدارة المغلقة شأنه في ذلك شأن الشهادة الالكترونية، ويطرح الأسئلة الدقيقة التقنية بشأن الجريمة المعلوماتية على أن يقوم قاضي التحقيق المستقبل بإعداد محضر يتضمن الاستجواب التفصيلي وتضمينه توقيع المتهم على أن يوقعه هو نيابة عن القاضي المصدر الإنابة القضائية .

(4) أنظر أحمد براك، المرجع السابق، ص من 58 الى 71.

الفصل الأول.....إثبات الجريمة المعلوماتية بالوسائل التقليدية .

من الضمانات المقررة للمتهم أثناء الاستجواب حقوقه في الدفاع من ذلك التسليم في حقه في الصمت وعدم الإدلاء بأقواله⁽¹⁾، مع إلزام المحقق تضمين محضر الاستجواب هذا التنبيه، و الهدف من ذلك هو الحفاظ على مصلحة المتهم والتحقيق معا وذلك بعدم استغلال الاضطراب، أو الخوف الذي ينتاب المتهم من جراء الصدمة التي تحدث له بعد مفاجئته بالتهمة المنسوبة إليه فيتسرع بالإجابة عنها بشكل متسرع غير مدروس، ومن التشريعات التي كفلت هذا الحق قانون أصول المحاكمات الجزائية الأردني في نص المادة 63 منه⁽²⁾. وهو ما نص عليه المشرع الجزائري في نص المادة 100 من ق.إ.ج.ج، و للمتهم الحق في الاستعانة بمحام يحضر معه الاستجواب للدفاع عن حقوقه، وان لم يكن قادرا على ذلك عين له القاضي محاميا، والقاضي ملزم بالتنويه عن هذا الحق في محضر الاستجواب، وللمتهم أيضا الحق في الاتصال بدفاعه بكل حرية إذا تم حبسه طبقا لنص المادة 102 من ق.إ.ج.ج⁽³⁾.

ومن الضمانات المقررة لحق الدفاع تحت طائلة البطلان ما تضمنته نص المادة 105 من ق.إ.ج.ج من تمكين المحامي من أوراق الملف ووضعها تحت تصرفه بأربع وعشرين ساعة قبل جلسة الاستجواب، كما انه يجب على جهة التحقيق إعلام محامي المتهم بجلسة الاستجواب يومين قبل ذلك بكتاب موصي به، ولا يمكن في أي حال إجراء الاستجواب أو المواجهة إلا بحضور دفاع المتهم إلا إذا تنازل المتهم عن ذلك صراحة وينوه عن ذلك في المحضر.

وقد أقر المشرع الجزائري ضمانات غاية في الأهمية للمتهم وهي عدم جواز حبس متهم قبل أي استجواب وإبداء دفاعه حول الواقعة⁽⁴⁾، كما أنه في حالة اعتقال المتهم فإنه يجب استجوابه خلال

(1) إلى جانب التشريعات المقارنة أوصت بهذا الحق العديد من المؤتمرات الدولية منها المؤتمر السادس لقانون العقوبات المنعقد في روما سنة 1953، وكذلك أوصت به لجنة حقوق الإنسان بهيئة الأمم المتحدة في 5 يناير 1962، كما قضت المحكمة العليا الأمريكية بأنه ليس لممثل الادعاء أن يستغل صمت المتهم كقرينة ضده، بينما رفضت بعض التشريعات هذا الحق مثل مقاطعة جنيف و مقاطعة زيوريخ. أحمد براك، نفس المرجع، ص 72.

(2) حسن الجوخدار، المرجع السابق، ص 413.

(3) تنص المادة 102 من ق.إ.ج.ج على أنه "يجوز للمتهم المحبوس بمجرد حبسه أن يتصل بمحاميه بكل حرية، ولقاضي التحقيق الحق في أن يقرر منعه من الاتصال لمدة عشرة أيام ولا يسري هذا المنع في أي حالة على محامي المتهم".

(4) تنص المادة 01/118 من ق.إ.ج.ج على أن "لايجوز لقاضي التحقيق إصدار مذكرة إيداع بمؤسسة إعادة التربية إلا بعد استجواب المتهم...".

ثمان وأربعين ساعة الموالية وإلا أُخلي سبيله ، وهو ما جاء في نص المادة 121 من ق.إ.ج.ج وهو ما ذهب إليه المشرع المصري حينما جعل الاستجواب وجوبيا في حالتين، حالة القبض على المتهم في المادة 131 من قانون الإجراءات الجنائية المصري وحالة الحبس الاحتياطي في المادة 134 منه⁽¹⁾.

ثانيا - إجراءات و ضمانات الاستجواب في الجريمة المعلوماتية أمام قضاء الحكم:

نتناول في هذا القسم إجراءات الاستجواب في عنصر أول، ثم ضمانات الاستجواب في العنصر الثاني:

أ- إجراءات الاستجواب في الجريمة المعلوماتية أمام قضاء الحكم:

إن الاستجواب يكتسي أهمية بالغة في هذه المرحلة الأخيرة من مراحل الدعوى الجنائية، فمن المعروف أن التحقيق أثناء انعقاد جلسة المحاكمة يكون شفويا ، وسلوك المتهم اتجاه الأسئلة التي سوف تطرح عليه في إطار استجوابه يدخل في الاعتبار لتكوين اليقين الشخصي لدى القاضي الجنائي⁽²⁾. في حين تنص بعض التشريعات المقارنة مثل التشريع المصري والليبي و اليمني و البحريني على أن الاستجواب أثناء المحاكمة ليس وجوبي بل جوازي فقط يخضع لموافقة المتهم بينما حرمه المشرع الأردني⁽³⁾.

ويكون الاستجواب في الجرائم المعلوماتية أمام محكمة الجناح باعتبارها المختصة في نظر مثل هذه القضايا ،في حين يتولى الاستجواب قاضي الجناح أمام المحكمة الابتدائية ، بينما على مستوى الاستئناف المكون من ثلاث قضاة يستجوب الرئيس المتهم بمساعدة مستشارين اثنين يطرحان أسئلتها عن طريق الرئيس.

(1) محمود نجيب حسني، المرجع السابق، ص 634.

(2) محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، المرجع السابق، ص 386-387.

(3) حسن الجوخدار، المرجع السابق، ص 409.

يبدأ الاستجواب بعد المناداة على المتهم و التأكد من هويته وتسجيل اسم المحامي المكلف بالدفاع عن حقوقه ، يوجه له القاضي التهمة المنسوبة له ، ثم يحيل له الكلمة لإبداء تصريحاته بشأن التهمة ، ويتم مناقشته حول النقاط التي يراها القاضي مناسبة ، وبعد الانتهاء من الاستجواب يحيل الكلمة لدفاع الضحية ، وممثل النيابة ثم دفاعه لطرح الأسئلة على أن تكون أسئلة ممثل النيابة مباشرة للمتهم.

يكون الاستجواب أمام قضاء الحكم شفويا ، وعلنيا ، وحضوريا باعتبار أن إجراءات المحاكمة تخضع لقواعد النظام الاتهامي (1).

و الاستجواب النهائي يعطي لقاضي الحكم فرصة مراجعة وتفحص جميع عناصر الإثبات خصوصا إذا تم استخلاص دليل معلوماتي ، فتتكون لديه فكرة مدى تورط المتهم في الأفعال المنسوبة إليه من عدمها ، وبالتالي فإن الاستجواب في هذه المرحلة غاية في الأهمية يتطلب أن يقوم به قاضي له تكوين في المجال المعلوماتي، كما أنه يمكن الاستعانة بخبير معلوماتي أثناء الجلسة لتوضيح المسائل التقنية وتبسيطها سواء للنيابة أو لقاضي الحكم أو لمحامي الطرفين.

ب- ضمانات الاستجواب أمام قضاء الحكم في الجريمة المعلوماتية:

إن الاستجواب النهائي للمتهم المعلوماتي في جلسة المحاكمة يحاط بمجموعة من الضمانات تدخل في إطار ما يسمى بالمحاكمة العادلة فالاستجواب أثناء الجلسة يعتبر وسيلة دفاع للمتهم يقوم باستجوابه قاض الجلسة وهو قاض محايد ولضمان نزاهة الاستجواب تفتح الجلسة لحضور كافة المواطنين أين تكون علنية كما أن الاستجواب يكون في حضور محام المتهم الذي يتولي الدفاع عنه بينما يدلي المتهم أقواله بكل حرية دون أي قيد ويدون القاضي أقوال المتهم كما يقوم أمين الجلسة بكتابة تصريحات المتهم في محضر بيانات الجلسة.

الفرع الثالث: الاعتراف في الجريمة المعلوماتية.

(1) محمد مروان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الأول، المرجع السابق، ص 389.

إن الهدف من الاستجواب هو البحث عن انتزاع الاعتراف من المتهم المذنب، فغالبا ما ينهار المتهم أثناء استجوابه ويبوح بكل الأفعال التي قام بها، و يعترف للقاضي بالوقائع المنسوبة إليه دون أي ضغط أو إكراه، وبالمقابل فهل أن القاضي يكتفي بمجرد اعتراف المتهم المعلوماتي بارتكابه الجريمة المعلوماتية للأخذ بهذا الاعتراف كدليل إثبات ضده أم أن هناك شروط معينة تقيد هذا الاعتراف ؟

أولاً- تعريف الاعتراف وشروطه العامة:

يعتبر الاعتراف وسيلة هامة من وسائل الإثبات، فهو يساهم في تكوين القاضي لقناعته وفي أحيان كثيرة يريح ضميره، لذلك لا بد أن نتناول تعريفه ، ثم نبين شروطه العامة.

أ- تعريف الاعتراف:

الاعتراف هو " عمل إرادي ينسب به المتهم إلى نفسه القيام بارتكاب الوقائع المكونة للجريمة كلها أو بعضها، والاعتراف قد يكون كتابيا أو شفويا وكلاهما كاف في الإثبات والاعتراف نوعين إما اعتراف قضائي أو غير قضائي⁽¹⁾.

ب- الشروط العامة للاعتراف:

حتى يطمئن القاضي لسلامة اعتراف المتهم بالجريمة التي ارتكبها أو شارك في ارتكابها لابد من توافر أربعة شروط⁽²⁾:

- 1- توافر الأهلية الإجرائية للمعترف.
- 2- صدور الاعتراف عن إرادة حرة .
- 3- أن يكون الاعتراف صريحا لا لبس ولا غموض فيه.

(1) محمد على سكيكر، أدلة الإثبات الجنائي في ضوء التشريع و القضاء و الفقه ، دار الجامعة الجديدة، سنة 2011، ص 24-25.

(2) محمد على سكيكر، نفس المرجع، ص 32.

4- استناد الاعتراف إلى إجراءات صحيحة.

ثانيا- الشروط الخاصة للاعتراف المعلوماتي:

لا تختلف أحكام الاعتراف في الجريمة المعلوماتية عن الأحكام العامة المشار إليها للاعتراف في الجرائم التقليدية ، فلا يكفي مجرد اعتراف المتهم بارتكابه مثلا جريمة تحويل الأموال بطريقة غير مشروعة عن طريق اختراق النظام المعلوماتي العائد لأحد المصارف عبر الانترنت ، بل يجب أن يحدد المعترف الكيفية التي تم بها الاختراق ، ومن ثم يجب أن يتطابق هذا الاعتراف مع الأسلوب الحقيقي الذي تم فيه هذا الاختراق فعلا و البرمجية التي استخدمت في ذلك ،ويمكن لجهات التحقيق التأكد من ذلك عن طريق اللجوء إلى أسلوب تمثيل الجريمة وهو ما يعرف " بالاعتراف العملي" ⁽¹⁾ . مما سبق نقول انه إلى جانب الشروط العامة الضرورية لصحة الاعتراف في أي جريمة تقليدية ، لا بد وأن يضاف للاعتراف المعلوماتي شرط خاص و جوهري ، وهو في رأينا أن يكون الاعتراف مستندا على معارف لا لبس فيها في المجال المعلوماتي ولا بد أن يتم التأكد من صحته بواسطة خبير معلوماتي .

ثالثا - حجية الاعتراف المعلوماتي في إثبات الجريمة المعلوماتية:

ينقسم الفقه إلى رأيان في مسألة قبول الاعتراف وحده كدليل للإدانة إذ يتجه الرأي الأول إلى أن مجرد اعتراف المتهم لا يكفي بمفرده لحمل القضاء على إدانته، وأن الاعتراف بداية الإثبات ويجب لإتمام الاقتناع إضافة أدلة أخرى، و هذا الرأي سائد في الفقه والقضاء الفرنسي والفقه الأمريكي، أما الرأي الثاني فيري انه لا توجد قاعدة تقرر أن الاعتراف لا يكفي وحده كدليل للإدانة فهذا القول يناقض مبدأ الاقتناع القضائي، وما يجوز للقاضي هو أن يمحس الاعتراف ويتحري عن بواعثه ومدى مسابرتة لباقي الأدلة⁽²⁾.

(1) محمد طارق عبد الرؤوف الحن، المرجع السابق، ص 319.

(2) مراد أحمد العبادي، اعتراف المتهم وأثره في الإثبات دراسة مقارنة، الطبعة الأولى الإصدار الثاني، دار الثقافة للنشر و التوزيع الأردن، 2008، ص112-113.

واعتبر المشرع الجزائري الاعتراف مثله مثل باقي الأدلة يخضع في تقدير حجيته للقاضي الجزائري، وهو ما جاء به المشرع في نص المادة 213 من ق.إ.ج بقوله: " الاعتراف شأنه كشأن باقي عناصر الإثبات يترك لحرية تقدير القاضي " ، بمعنى أن الاعتراف ليست له الحجية المطلقة في الإثبات، وإنما يخضع للمناقشة و التمحيص، فإما أن يأخذ به القاضي، و إما أن يستبعده وفقا لاقتناعه القضائي بناء على ما دار من مناقشات في الجلسة.

بين هذا وذاك فإن الاعتراف المعلوماتي يعتبر دليلا لا مرأى من تطبيقه إذا ما تم اعتراف المتهم المعلوماتي⁽¹⁾ بصحة ما وجه إليه من اتهامات في المجال المعلوماتي، وتوافرت جميع شروطه ، وتم التأكد عمليا من ذلك، فالدليل سيد أدلة الإثبات سواء في الجرائم العادية أو الالكترونية، طالما أن القاضي يحكم حسب العقيدة التي تكونت لديه بكامل حريته استنادا إلى الأدلة التي تمت مناقشتها في الجلسة، وعلى ذلك فالاعتراف كدليل يصلح لكي يسمى دليلا جنائيا لإثبات الجريمة المعلوماتية⁽²⁾، وله حجية الإثبات إذا ما تحقق بشروطه الخاصة. إلى ذلك يجب كذلك أن تتوفر أدلة أخرى يدعم بها القاضي الجزائري اقتناعه، وفقا لما يسمى بمبدأ تساند الأدلة لذلك نستكمل دراستنا في المبحث الموالي بحثا عن باقي الأدلة كوسائل تعطي الإضافة في إطارها التقليدي لنحقق تلك الغاية.

(1) المشرع الجزائري أخذ بالاتجاه الثاني إذ يعتبر الاعتراف شأنه شأن جميع عناصر الإثبات يترك لحرية تقدير القاضي (المادة 213 ق.إ.ج) ومن التطبيقات القضائية في الجزائر التي استند فيها القضاء إلى اعتراف المتهم المعلوماتي في الإدانة ، القضية التي عالجها مجلس قضاء باتنة بتاريخ 2010/07/04 ضد المتهم المعلوماتي (ي.عبد الباسط) البالغ من العمر 23 سنة والتي راحت ضحيته المؤسسة الأمريكية SAGO NET WORKS التي تعتبر بنك معلوماتية جهوية كبيرة بولاية فلوريدا الأمريكية بمنطقة TAMPA و بعد التحقيقات في القضية بناء على إرسالية من وزارة العدل الأمريكية تم تحديد شبكة الانترنت ADSL FAWRI المستعملة وتحديد عنوان بروتوكول الانترنت (IP) الخاص بها و المتعلق باتصالات الجزائر وتم على اثره التوصل الى خط الهاتف المستعمل والمسجل باسم والد المتهم .ليتوصل التحقيق بعد ذلك إلى المتهم الذي اعترف أثناء التحقيق معه وكذا أمام القضاء بأنه استعمل شبكة الانترنت و قام بالدخول غير المشروع إلى المعطيات الالكترونية لهذه المؤسسة بواسطة برنامج UBERSMITH باستعمال بريدين إلكترونيين لشخص مجهول وباستعمال عناوين الكترونية موزعة بالجزائر وقام بقرصنة المعلومات الخاصة بالصرف للضحية وعرضها للبيع على الموقع UNKNOWN.WN ، واستلام حوالات من بنك وسترن يونيون لتتم ادانته فيما بعد استنادا الى اعترافه بالجريمة.

(2) عمرو حسين عباس، بحث بعنوان " أدلة الإثبات الجنائي و الجرائم المعلوماتية "مقدم إلى المؤتمر الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية الوطن العربي خلال الفترة من 26-27/4/2008 مقر جامعة الدول العربية، ص 24.

المبحث الثاني

إثبات الجريمة المعلوماتية بالوسائل المادية والقرائن.

يتفق خبراء المعلوماتية إلى جانبهم الفقهاء الجنائيين على صعوبة إثبات الجريمة المعلوماتية لورودها على كيانات معنوية ، ونحن بصدد البحث دائماً على الوسائل الناجعة لإثباتها في الإطار التقليدي، ننقل إلى الوسائل المادية ودورها في إثبات الجريمة، وارتأينا تناولها من خلال تقرير الخبرة (مطلب أول) والدليل الكتابي (مطلب ثاني) ثم نرجع إلى القرائن(مطلب ثالث) التي يجمع على أهميتها الحالية في الإثبات تجاوبا للتطور العلمي الحاصل.

المطلب الأول

الخبرة.

تقرير الخبرة من الوسائل التي يلجأ إليها المحقق الجنائي من أجل إثبات الجرائم التي تتطلب تنويراً في مسألة فنية تستعصي على خبراء القانون، فيجد المحقق أو القاضي نفسه ملزماً في الجرائم المعلوماتية إلى اللجوء إلى خبراء في الرقمنة لإعداد خبرات فنية تساعد المحققين في الوصول إلى الحقيقة ولكن السؤال المطروح ماذا يقصد بالخبرة و إلى أي حد يتم اللجوء إلى الخبير المعلوماتي؟ و ما هو دور تقرير الخبرة التقنية في إثبات الجريمة المعلوماتية باعتبارها وسيلة من وسائل الإثبات؟

الفرع الأول: الأحكام العامة للخبرة.

نتناول في الأحكام العامة للخبرة تعريف الخبرة وشروطها (أولاً) ثم ننقل إلى معرفة كيفية اختيار الخبراء(ثانياً) والجهة المختصة بنديهم (ثالثاً).

أولاً- تعريف الخبرة وشروط قبولها: وفيه يجرأ هذا القسم بدوره إلى عنصرين هما:

أ- تعريف الخبرة:

تعرف الخبرة بأنها " إبداء رأي فني من شخص مختص فنيا ، في شأن واقعة ذات أهمية في الدعوى الجزائية"⁽¹⁾. أو " هي معرفة فنية خاصة بأمور معينة، تتجاوز اختصاص المحقق"⁽²⁾.

و يلجأ إلى الخبرة إذا ثارت أثناء سير الدعوى الجزائية مسألة معينة يتوقف عليها الفصل في الدعوى، خاصة إذا كانت تلك المسألة من المسائل الفنية التي ليس بمقدور القاضي البت فيها ،ويكون طلب الخبرة في شتي المجالات عدا المجال القانوني باعتبار القاضي هو المختص في هذا المجال⁽³⁾.

ب- شروط قبول تقرير الخبرة:

باعتبار تقرير الخبرة وسيلة هامة من وسائل الإثبات يستعين بها القاضي كدليل للوصول إلى قناعته التي يشكلها في جلسة المحكمة بعد مناقشة التقرير وباقي الأدلة حضوريا، كان لا بد للمشرع أن يضع شروطا تعطي لتقرير الخبرة قوة في الإثبات وهو ما جاء به المشرع الجزائري في نص المادة 214 من ق.إ.ج.ج بقوله " لا يكون للمحضر أو تقرير قوة الإثبات إلا إذا كان صحيحا في الشكل ويكون قد حرره واضعه أثناء مباشرة أعمال وظيفته وأورد فيه عن موضوع داخل في نطاق اختصاصه ما قد رآه أو سمعه أو عاينه بنفسه". ويستخلص من نص المادة انه لقبول التقرير لا بد أن يكون صحيحا من الناحية الشكلية المتطلبة في مثل هذه التقارير تحت طائلة عدم قبولها، بالإضافة إلى وجوب قيام الخبير بتحريره أثناء أداء مهامه بحيث لا يكون مشطوبا من الجدول بالإضافة إلى ضرورة تضمين تقرير الخبرة ما تمت معاينته بنفسه وليس بناء على ما توصل إليه غيره، ليحيل المشرع عبر نص المادة 219 من ق.إ.ج.ج بعد ذلك عند انجاز الخبرة إلى الإجراءات المتبعة المنصوص عليها في المواد من 143 إلى 156 من نفس القانون.

ثانيا- كيفية اختيار الخبراء:

(1) محمد طارق عبد الرؤوف الحن ، المرجع السابق، ص 325.

(2) فوزية عبد الستار، المرجع السابق، ص 345.

(3) محمد على سكيكر، المرجع السابق، ص 137.

تنص أغلب التشريعات المقارنة على إمكانية الاستعانة بالخبراء المذكورين سلفا في قوائم الخبراء المعتمدين لدى وزارة العدل ، ويتم اختيار الخبراء في التشريع الجزائري حسب المادة 144 من ق.إ.ج.ج(1) من الجدول الذي تعده المجالس القضائية بعد استطلاع رأي النيابة دون التزام بترتيب معين تبعا لثقة المحقق أو القاضي ،ويتولى وزير العدل تحديد الأوضاع التي يجري بها قيد الخبراء وشطب أسمائهم(2) كما خول القانون لسلطة التحقيق إمكانية ندب خبير من خارج الجدول المعتمد شريطة أن يكون بقرار مسبب.

وأوجب المشرع الجزائري على الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي أن يحلف اليمين أمام ذلك المجلس بحسب الصيغة المقررة في المادة 145 من ق.إ.ج.ج ، و لا يجدد هذا اليمين مادام مقيدا في الجدول، بينما يؤدي الخبير الذي تم اختياره من خارج الجدول اليمين قبل أداء مهامه أمام قاضي التحقيق أو القاضي المعين من الجهة القضائية، وخول القانون لقاضي التحقيق حرية ندب خبير واحد أو خبراء متعددين وهو ما جاء به نص المادة 147 من ق.إ.ج.ج.

ثالثا - الجهات المختصة بندب الخبراء:

يكلف الخبير بمهمته إما من جهات التحقيق وإما بناء على أمر من محكمة الموضوع ، وفي الحالتين يعد الأمر الصادر إليه قضائيا ، فإذا لم تتوافر الصفة القضائية لهذا الأمر فإن ما ينتج من دليل عند عمل الخبير يعد دليلا غير مشروع ومن ثمة يحق لمحكمة الموضوع ألا تأخذ به(3).

أما إذا طلب الخصوم ندب خبير فللقاضي تقدير الحاجة إليه ، ويرد على هذه السلطة قيذان الأول أنه إذا رفض القاضي الطلب تعين عليه أن يرد عليه ، لأن هذا الطلب وسيلة دفاع ومتعلقة

(1) تنص المادة 144 من ق.إ.ج.ج على أن " 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.

ويجوز للجهات القضائية بصفة استثنائية أن تختار بقرار مسبب خبراء ليسوا مقيدين في أي من هذه الجداول.

(2) بينما وضع المشرع المصري في المادتين 18 و 35 من القانون رقم 96 لسنة 1952 شروطا خاصة يجب توافرها في الخبراء ،على عكس المشرع الإماراتي الذي لم يضع شروطا خاصة لتعيين الخبراء ويتضح ذلك من المادة 3 من القانون الاتحادي رقم 8 لسنة 1984. عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماوي، المرجع السابق، ص26.

(3) فتحي محمد أنور عزت، المرجع السابق، ص690.

بإظهار وجه الحق، ومن ثم يكون الحكم قاصرا، أما القيد الثاني أنه إذا كانت المسألة فنية بحتة لا يتصور في الثقافة القانونية للقاضي حسمها، فان رفض طلب الندب فيها مجافاة للأسلوب المنطقي و العلمي في التفكير ويكون الحكم معيبا (1)، وتجب الإشارة إلى أن البحوث الفنية التي يقوم بها أهل الخبرة في مرحلة الاستدلال بناء على طلب الضبطية القضائية لا تعد من قبيل الخبرة ، إذ تؤدي دون إتباع الإجراءات الشكلية التي أوجبها القانون ، وهي الندب من سلطة التحقيق ، وأداء اليمين(2).

وقد نص المشرع الجزائري في المادة 143 من ق.إ.ج.ج على أن الجهات القضائية وحدها المخولة قانونا بندب الخبراء في المسائل ذات الطبيعة الفنية، وذلك من تلقاء نفسها أو بناء على طلب النيابة، أو أحد الأطراف -الذين يمكن لهم الاستعانة بالخبير الاستشاري في بعض التشريعات المقارنة-، مع حق استئناف أمر رفض طلب ندب الخبير المستوجب تسببا قانونيا أمام غرفة الاتهام، باعتبارها درجة ثانية للتحقيق وتملك السلطة القانونية لمراجعة التحقيق الذي قام به قاضي التحقيق أو النيابة العامة.

الفرع الثاني: الخبير المعلوماتي.

لا يمكن التعرض لدراسة الخبرة في المجال التقني دون أن نعني الخبير المعلوماتي بالدراسة ذلك انه من مقومات الخبرة، لذلك نطرح تساؤلات مهمة على بساط بحثنا أهمها ما مفهوم الخبير المعلوماتي ؟ وإذا كان له دور في الخبرة ما هي واجباته التي يتعين عليه التقيد بها ؟ و كيف يؤدي الخبير مهامه في الجريمة المعلوماتية؟ وهو ما سنعرفه في العناصر الموالية.

أولاً- مفهوم الخبير المعلوماتي: ونحن بصدد معرفة مفهوم الخبير المعلوماتي نتناول تعريفا له ثم نبين نظرة جديدة للخبير تختلف عن سابقتها كما يلي:

أ- تعريف الخبير المعلوماتي:

(1) سليمان أحمد فضل، المرجع السابق، ص 340. كذلك محمد زكي أبو عامر، المرجع السابق، ص 193-194.

(2) عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، المرجع السابق، ص25.

الخبير المعلوماتي هو " الشخص الذي تعمق في دراسة عمل من الأعمال الالكترونية وتخصص في أدائه فترة زمنية طويلة ،مما أكسبه خبرة عملية بحيث أصبح ملما بتفصيلاته ،مما جعله متفوقا على الشخص العادي ، وجعله قادرا على إبداء الرأي الالكتروني الرقمي في الأمور المتصلة بهذا العمل " ، ويمكن أن يكون الخبير شخصا طبيعيا أو شخصا معنويا مثل الشركات والمنظمات أو مؤسسات متخصصة تملك موارد مادية من برامج وأجهزة حديثة وكوادر بشرية متخصصة ، كخبير الخبرة و البحث عن البصمات المعلوماتية LERTI الموجود بفرنسا⁽¹⁾. أما بخصوص المشرع الجزائري فإنه لم يحدد طبيعة شخص الخبير سواء كان شخصا طبيعيا أو شخصا معنويا.

ب- الشروط الواجب توافرها في الخبير المعلوماتي : يشترط في الخبير أن يجمع بين المؤهل العلمي⁽²⁾ والخبرة العملية، إلا أن الشخص ذو التجربة و المتقن للقواعد الفنية يمكن اعتباره خبيرا حتى ولو تخلف الجانب العلمي ، بعكس المتعمق في الجانب العلمي دون أن يزاول المهنة فلا يكون خبيرا⁽³⁾، وهو ما ذهب إليه بعض من الفقه أنه لا يشترط في الخبير الشهادة العلمية بل

(1) أنظر عائشة بن قارة مصطفى، المرجع السابق، ص 142.

(2) ثمة توجه من قبل الكيانات الأكاديمية لإدماج مقرر الحاسب الجنائي (أو علم الأدلة الجنائية الحاسوبية) في برامجها التعليمية المتخصصة في علوم الحاسب وذلك عن طريق تخصيص درجة علمية كاملة تفرد لتدريس هذا التخصص ،أما خارج الكيانات الأكاديمية يمكن الحصول على مهارات الحاسب الجنائي عن طريق برمجيات تعليمية مثل التي تقدمها شركة VTC أو برامج تدريبية تابعة لمؤسسات وجمعيات متخصصة مثل الجمعية الدولية لامتحانات الحاسب الجنائي (ISFCE)، ويهتم مجال الحاسب الجنائي بالعمل على تحديد وحفظ واسترجاع وتحليل وتوثيق البيانات الحاسوبية التي يزعم أنها استخدمت في الجرائم المرتكبة بواسطة جهاز الحاسب، كما يعتبر تخصص الحاسب الجنائي علم تطبيقي مقترح من علم الأدلة الجنائية و التي لها جذورها في الطب الشرعي ،لذا فهو يختلف في أهدافه عن تخصص أمن الحاسبات الذي يهدف إلى حماية أجهزة الحاسب و الشبكات من الأعمال التخريبية و الاختراقات ،كما يفرع من تخصص الحاسب الجنائي تخصص دقيق مهم بالشبكات و الانترنت يسمى تخصص الشبكات/الانترنت الجنائي يهتم بالتحري و التحقيق بجرائم الشبكات. انظر هند بنت سليمان الخليفة، ورقة عمل بعنوان الحاسب الجنائي في الدول الغربية دراسة استطلاعية جامعة الملك سعود الرياض. متاحة على الموقع الالكتروني:

[http:// hend-alkhalifa.com/wp.computer_forensic-2007.pdf](http://hend-alkhalifa.com/wp.computer_forensic-2007.pdf).

(3) ويجب على الخبراء المعلوماتيين معرفة ما يلي: - لغات البرمجة وأنظمة التشغيل الجديدة.

- تصميم البرامج وتشغيلها ومعرفة الجديد منها.

- تحليل البرامج أو أنظمة التشغيل ..

- يؤمن بوجود أشخاص آخرين مثله لديهم القدرة على اختراق الشبكة. انظر مصطفى محمد موسي، المرجع السابق، ص 221-222.

تكفيه المهارة وموهبة استخدام تقنية المعلوماتية وأعطوا مثالا بأن أمير مبرمجي نظم التشغيل (Bill Gates) لم يتجاوز تحصيله المرحلة الثانوية⁽¹⁾.

ت- مدى جواز الاستعانة بخبرة المجرم المعلوماتي :

لجأت بعض الجهات الرسمية للدول إلى الاستعانة بالمجرمين المعلوماتيين نتيجة تأثرهم بذكائهم المفرط، وسعوا إلى تجنيدهم ضمن نخب الخبراء لمكافحة الجرائم المعلوماتية كما الانضمام إلى سلطات التحقيق فيها ومن القوانين التي تسمح بذلك نجد القانون الفرنسي و الأمريكي، بينما في التشريعات العربية ذهب جانب من الفقه المصري إلى السماح بانتداب المجرم المعلوماتي ويحق لكل ذي مصلحة الطعن في هذا الأمر، بينما ذهب رأي آخر إلى عدم إمكانية ذلك استنادا إلى نص المادة 06/25 من قانون العقوبات المصري، وهو نفس الاتجاه الذي تبناه المشرع العراقي⁽²⁾، أما المشرع الجزائري فانه نص على عدم أهلية المحكوم عليهم بالحرمان من الحقوق المدنية والسياسية لأن يكونوا خبراء إلا على سبيل الاستدلال (المادة 03/09 من ق.ع.ج) وبالنتيجة فإن غير المحكوم عليهم بعقوبة تبعية بالحرمان في تقديرنا يمكن لجهات التحقيق الاستعانة بهم وندبهم كخبراء مساعدين للخبراء الرئيسيين، خصوصا مع السياسة الجنائية الحديثة التي تبناها المشرع الجزائري المتمثلة في ترشيد العقوبة وإعادة تأهيل المجرمين ودمجهم في المجتمع للاستفادة منهم وهو ما يسهل مع هذه الفئة.

ثانيا- واجبات الخبير المعلوماتي: يتقيد الخبير أثناء انجازه للخبرة بعدة واجبات أساسية وهي:

أ- حلف اليمين القانونية:

يعتبر اليمين شرطا جوهريا قبل القيام بأي مهام تحت طائلة البطلان، وغاية حلف اليمين هي بعث الخبير على الصدق والأمانة في عمله وبث الطمأنينة في آرائه التي يقدمها سواء بالنسبة لتقدير القاضي، أو لثقة بقية أطراف الدعوى، كما استقر الفقه و القضاء على أن أداء الخبير

(1) عائشة بن قارة مصطفى، المرجع السابق ص 143، كذلك رشيدة بوكور، المرجع السابق، ص 426-427.

(2) رشاد خالد عمر، المرجع السابق، ص 169-170.

للميمين يوم تسلمه للمهام يغني عن أداءه اليمين عند مباشرة كل مأمورية⁽¹⁾، و يؤدي الخبير المعلوماتي اليمين كما تم بيانه، ووفقا للأشكال المحددة في المادة 145 من ق.إ.ج.ج.

ولكن بالمقابل تثار مسألة انتداب شخص معنوي لإجراء خبرة تقنية بدل شخص طبيعي فكيف يتم أداء اليمين ، باعتباره شرط جوهري يترتب عن تخلفه البطلان المطلق للإجراء ، و أمام سكوت النص وعدم عثورنا في المؤلفات على صيغة قانونية فإنه في اعتقادنا يلزم الشخص المعنوي بتقديم كل شخص مفوض من الشركة أو المؤسسة للقيام بالخبرة لحلف اليمين لأول مرة أمام قاضي التحقيق أو القاضي المعين من الجهة القضائية عملا بنص المادة 02/145 من ق.إ.ج.ج.

ب- خضوع الخبير للرقابة القضائية:

على الخبير أن يتولى مهمته تحت رقابة القاضي الأمر بإجراء الخبرة ولا يستلزم ذلك حضوره فعلا أثناء قيام الخبير بأعماله، بل يكفي أن يبقى على اتصال معه بهدف إحاطته علما بكل المستجدات التي تطرأ عليه في مجال عمله باعتباره مساعد فني للقاضي فحسب⁽²⁾.

ت- القيام بالمهام المحددة في أمر الندب:

يتفق المختصين على أنه لا وجود لخبير معلوماتي⁽³⁾ لديه الخبرة المتعمقة في سائر أنواع الحاسبات وبرمجياتها وشبكاتها أو القدرة على التعامل مع كل أنواع الجريمة المعلوماتية⁽⁴⁾، هذا بالنسبة للخبراء فكيف هو الحال بالنسبة للجهة القضائية الملزمة بتحديد مهام الخبير، لأن الخبير المعلوماتي ملزم بالتقيد بالمهام المنوطة به، ما يطرح مسألة مدى إلمام ومعرفة جهات التحقيق ما يطلبونه من الخبير، لأن الخبير الرقمي مكلف بإعداد خبرة في مجال محدد على سبيل الدقة حتى لا يطعن في تقرير الخبرة بسبب تجاوز المهام، أو حتى لا تثار مسألة المساس بحرية الأفراد

(1) عائشة بن قارة مصطفى، المرجع السابق، ص 143-144.

(2) رشيدة بوكر، المرجع السابق، ص 428.

(3) هناك عدة طوائف من خبراء المعلوماتية ، وهم نفس أصناف شهود المعلوماتية الذين تطرقنا إليهم في المطلب الأول، على أن ذلك لا يعني المساواة بين الشاهد المعلوماتي و الخبير المعلوماتي فكل واحد منهما أحكامه وقواعده الخاصة. انظر مصطفى محمد موسي ، المرجع السابق ، ص 222-223. كذلك رشاد خالد عمر، المرجع السابق، ص 164 .

(4) عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 602.

الشخصية في حالة الوصول إلى معلومات شخصية استنادا إلى عمومية المهام المسندة له في أمر النذب، لذا يشترط في المحققين تعميق المعارف في المجال المعلوماتي و بالمقابل يجب على الخبير انجاز مهمته بإتقان وفقا لمتطلبات أمر النذب.

ث- احترام الآجال المحددة في أمر النذب:

يجب على الخبير إيداع تقرير خبرته في المهلة المحددة له في أمر النذب، فإن لم يودع تقريره في الآجال الممنوحة له جاز للقاضي في الحال استبداله بغيره، وعلي الخبير تقديم نتائج ما قام به من أبحاث، مع رد جميع الأشياء و الأوراق و الوثائق التي تكون في عهده على ذمة انجاز مهمته، وذلك تحت طائلة التدابير التأديبية التي تصل إلى حد الشطب من جدول الخبراء.

ثالثا- عمل الخبير المعلوماتي:

يعتبر عمل الخبير المعلوماتي من أعقد المهمات بالنظر إلى طبيعة الجريمة و الأدلة الغير مرئية المتوجب عليه استخلاصها، فهي تتطلب تركيز عالي بالإضافة إلى الاحترافية في الأداء وفي هذا العنصر ارتأينا التطرق إلى مجال الاستعانة بالخبير المعلوماتي، ثم أساليب عمله.

أ- مجال الاستعانة بالخبير المعلوماتي: يستعان بالخبير المعلوماتي (¹) في مجال التحقيق في الجرائم المعلوماتية وشبكاتهما في المناظرة والفحص و الوصف و البيان:

1 فحص ووصف:

- مكونات التقنية الالكترونية الرقمية من مادية ومعنوية ونظم وبرامج و كلمات مرور .

(¹) نصت المادة 88 من القانون البلجيكي الصادر في 2000/11/23 انه يجوز لقاضي التحقيق و للشرطة القضائية ان يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفية الدخول فيه أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته ، ويخول نفس القانون لسلطة التحقيق ان تطلب من الخبير تشغيل النظام ،أو البحث فيه ،أو عمل نسخة من البيانات المطلوبة للتحقيق، أو سحب البيانات المخزنة أو المحولة أو المنقولة ،على ان يتم ذلك بالطريقة التي تريدها جهة التحقيق. علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية(دراسة مقارنة)، المكتب الجامعي الحديث سنة 2012، ص 30.

- شبكات التقنية الالكترونية الرقمية وبيئتها الالكترونية من تردد وموجات البث وأماكن اختزانها.

- المواضيع المحتملة للأدلة الالكترونية الرقمية الثبوتية والشكل أو الهيئة التي تكون عليها.

- اثر التحقيق الجنائي في الجرائم المعلوماتية اقتصاديا وماليا على المشاركين في استخدام النظام⁽¹⁾.

2- بيان:

- كيفية عزل النظام المعلوماتي عند الحاجة دون إتلاف الأدلة أو الأجهزة أو تدميرها.

- إمكانية نقل أدلة الإثبات إلى أوعية أخرى دون تلف.

- إمكانية نقل أدلة الإثبات لأوعية مادية كالأوراق على ان تكون مطابقة لما هو مسجل في

الحاسب الآلي أو النظام أو الشبكة⁽²⁾.

ب- أساليب عمل الخبير المعلوماتي:

على الخبير المعلوماتي أن يستخدم الأساليب العلمية استنادا إلى تخصصه ، وليس للمحكمة

أن ترفضها دون تسبيب منطقي، ويستخدم الخبير التقني أسلوبين:

1- الأسلوب الأول: يتمثل في قيام الخبير بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة

في ذاتها ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي

أعدت فيه وتحديد عناصر حركتها ،وكيف تم التوصل إلى معرفتها ومن ثم التوصل في النهاية إلى

معرفة بروتوكول الانترنت IP الذي ينسب إلى جهاز الكمبيوتر الذي صدر عنه هذا الموقع.

(1) خالد ممدوح إبراهيم، المرجع السابق، ص 225. كذلك سليمان أحمد فضل، المرجع السابق، ص 343.

(2) عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 602-603.

2- الأسلوب الثاني : يقوم الخبير بتجميع وتحصيل لمجموعة المواقع التي لا تشكل موضوعها جريمة في ذاته، وإنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم كما هو الحال في المواقع التي تساعد الغير على إعداد القنابل الالكترونية وتخزينها، وكيفية التعامل مع القنابل الزمنية وتركيبها و القيام بفكها و حفظها، وكذلك القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بتحديد مسار مرتكب الدخول من مكان ثابت، وهو جائز الحدوث كما لو كان المشترك لدى مزود الخدمة في مدينة ما ويقوم بالولوج من مدينة إقامته⁽¹⁾.

الفرع الثالث: الخبرة التقنية وحجيتها في الإثبات.

إن الخبرة التقنية في مجال المساعدة القضائية تعد أقوى مظاهر التعامل أو التفاعل القانوني القضائي مع ظاهرة تكنولوجيا المعلومات بالنظر إلى نقص المعرفة القضائية الشخصية لظاهرة المعلوماتية، ما يجعل من الخبرة التكنولوجية أداة رئيسية في صناعة الحكم القانوني الجنائي⁽²⁾ لذلك سنتناول الخبرة التقنية كخلاصة لعمل الخبير وأثرها في إثبات الجريمة المعلوماتية.

أولا - الخبرة التقنية: نتناول في هذا العنصر مضمون الخبرة التقنية وأنواعها.

أ- مضمون الخبرة التقنية :

لقد سار التقليد القضائي إلى ضرورة الاعتماد على الخبرة المتوافر فيها ركنين ، الأول ركن شكلي يتعلق بالجانب العلمي والتخصص في مستوي الدراسة والمقنن من قبل مؤسسة علمية معترف بها كجامعة أو معهد ، بينما الركن الثاني موضوعي له قدر من الحرية العلمية يستخدم فيها الخبير أدواته العلمية و العملية بمقتضاها يجيب على المعضلة الفنية محل سؤال القضاء⁽³⁾.

(1) خالد ممدوح إبراهيم، المرجع السابق، ص من 300 إلى 302، كذلك فتحي محمد أنور عزت، المرجع السابق ص من 692 إلى 694.

(2) فتحي محمد أنور عزت، المرجع السابق، ص 680.

(3) فتحي محمد أنور عزت، نفس المرجع، ص 681.

ويتم إعداد تقرير الخبرة بجميع خطوات وإجراءات البحث ويرفق به في الغالب الملاحق الإيضاحية المصورة والمسجلة (1)، ويتضمن التقرير النتائج التي توصل إليها الخبير من خلال عملية البحث، ويجب أن يتضمن تقرير الخبرة النقاط التالية:

1- مواصفات مسرح الجريمة الافتراضية.

2- ملخص عن عملية الفحص التي تم القيام بها.

3- إعادة رواية أحداث القضية.

4- ملخص النتائج .

5- اقتراحات الخبير المعلوماتي.

وينصح أن يكون التقرير متسلسلا حسب الوقائع، ومختصرا من الناحية التقنية، ومكتوب بأسلوب بسيط وواضح حتى تتمكن المحكمة من فهمه وبسط رقابتها عليه، ويمكن لهذه الأخيرة أو بناء على طلب أحد الخصوم دعوة الخبير المعلوماتي حضور الجلسة، لتوجه له الأسئلة حول النقاط المستعصية في تقرير الخبرة، وتوضيح تقنيا كل ما من شأنه أن يوصل إلى الحقيقة(2).

ب- أنواع الخبرة التقنية: تقسم الخبرة التقنية إلى ثلاثة أنواع وهو التقسيم المتفق عليه في عديد المؤلفات كما يلي:

1- الخبرة الخاصة:

وتعد أقوى أنواع الخبرة على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنظمات الخاصة، وتظم في جنباتها الخبرة الفردية والتي تسعى المنظمات الخاصة إلى الاستعانة بها، وتختلف المنظمات الخاصة ما بين منظمات أهلية تتصدي لمحاولات

(1) رشيدة بوكري، المرجع السابق، ص432.

(2) محمد طارق عبد الرؤوف ألحن، المرجع السابق، ص336-337.

المجرمين التعدي على الحقوق الالكترونية، وبين نوعية من المنظمات تسعى إلى فك طلاسم العالم الافتراضي على أسس تجارية⁽¹⁾.

2- المؤسسات التعليمية:

يمكن القول أن أقوى مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة المعلوماتية يمكن أن تكون من خلال المؤسسات التعليمية، فهذه الأخيرة تعد مصدر متكامل لمؤسسات الدولة التي تعتمد المنهج العلمي غير التجاري وتقدم خبراء مدعومون بالمنهج، والاتجاه العالمي يتجه إلى المؤسسات العلمية والتي يتم دعمها ماديا ومعنويا لتكون أفضل سبل المواجهة، لأن المعتقد السائد في مواجهة الجريمة ينطلق من الوسائل التي من ذات طبيعة السلوك الإجرامي⁽²⁾.

3- جهات الضبط القضائي:

شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجراء عبر الانترنت، وعلى رأسها الولايات المتحدة التي تجاوز نشاطها في هذا المجال الإطار الدولي الممثل في منظمة الانترنت، وكان آخر نشاط مؤسسي لها هو إنشاء المعمل الإقليمي الشرعي للحاسوب⁽³⁾، ويتكون المعمل من التقاء العديد من منظمات الضبط القضائي للتعاون فيما بينها لمكافحة الجريمة المعلوماتية، وذلك بتحليل وتصنيف الدليل الرقمي، مع إعداد محللين شرعيين للحاسب الآلي⁽⁴⁾.

(1) تمكن خبراء من الشركة الاسكتلندية Scottish Software Co المتخصصة في برمجيات الحاسوب والانترنت على مدار ثمانية عشر شهرا بدءا من سنة 1998 من إعداد مشروع خريطة للعالم الافتراضي على غرار الخريطة الجينية للإنسان، ومن أهم نتائج هذه الخريطة أن تمكنت الخبرة الخاصة من رصد حركة الجريمة عبر الانترنت ومعرفة تطورها في كافة مظاهرها وأشكالها، حيث برز أكثر من أربعين مظهرا للإجراء عبر الانترنت واكتشف الخبراء عن وجود ما يربو عن المائتين ألف موقع جديد للدعارة عبر الانترنت، كما تم التعرف على التهديدات الحقيقية التي تواجه الدول و الأفراد فمثلا فن إخفاء النصوص بإضافة نصوص أخرى يعد من اخطر المشاكل التي تواجه العالم الافتراضي وتعد ثالث اخطر مشكلة تواجه النظام الأمني في الولايات المتحدة بعد العدوان البيولوجي و الكيميائي. انظر فتحي محمد أنور عزت، المرجع السابق، ص 683-684.

(2) فتحي محمد أنور عزت، نفس المرجع، ص 684-685. كذلك خالد ممدوح إبراهيم، المرجع السابق، ص 298-299 .

(3) تأسس كفرع جديد في المباحث الفيدرالية الأمريكية FBI في نوفمبر سنة 2000، مقره سان دييغو San Diego وهو بيت خبرة عام غرضه مكافحة التصعيد الخطير في الجريمة المعلوماتية.

(4) خالد ممدوح إبراهيم، المرجع السابق، ص 299-300.

المشرع الجزائري بدوره أنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بموجب المادة 13 من القانون 04/09 و أسند لها مجموعة من المهام المحددة في نص المادة 14 من ذات القانون وتنص على أن: "تتولى الهيئة المذكورة في المادة 13 أعلاه خصوصا المهام التالية:

- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحته.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام و الاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية.

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

وفي انتظار صدور المرسوم التنظيمي المحدد لتشكيلة الهيئة وكيفية سيرها تبقى المسألة حبيسة النص فمنذ صدور القانون خلال سنة 2009 إلى غاية سنة 2014 تعتبر مدة كبيرة وفي تقديرنا غير مبررة مقارنة بالوسائل البشرية والمادية التي تتوفر عليها الدولة، وتبقي فقط الإرادة من أجل المضي قدما في مكافحة الجرائم المعلوماتية التي تعرف تزايدا مستمرا وتشكل تهديدا على الحياة الخاصة للأفراد، وكذا مؤسسات الدولة واقتصادها، خصوصا مع ازدياد عدد المشتركين في شبكات الانترنت التي تعتبر المكان الخصب و الوسيلة الأساسية لاقتراف هذه الجرائم.

ثانيا- حجية الخبرة التقنية في إثبات الجريمة المعلوماتية:

قبل التطرق لحجية الخبرة لا بد من عرض مبدأين القاضي خبير الخبراء ثم القاضي الخبي.

أ -مبدأ القاضي خبير الخبراء:

نشأ هذا المبدأ أساسا في ظل التفسير القضائي الكامل للترابط بين دور الخبير واستعانة القاضي به في إرساء حكمه، فهذا المبدأ يفيد بالضرورة أن المحكمة هي الخبير الأعلى وهذا يؤدي

باللزم العقلي إلى التأكيد على أن كل ما يتعلق بالدعوى يجب أن ينتهي عند قاضي الموضوع للفصل فيه، فالكلمة الأخيرة لمحكمة الموضوع حتى ولو كانت المسألة الفنية في المجال المعلوماتي قد عرض لها خبير رقمي وأخذ الخبير برأيه، بل انه حتى في حالة رفض الأخذ برأي الخبير فإن القاضي ليس ملزماً بسلوك محدد كالاستعانة بخبير آخر يقدم تقريراً فنياً، فليس في القانون ما يبرر الإلزام، وإنما منطق الإلزام هنا هو السعي إلى إبراز الحقيقة، ومثل هذا المنطق لا يجعل الخبير في مستوي عمل القاضي ، بل يظل دور القاضي قائماً في المفاضلة بين التقارير الفنية المقدمة إليه⁽¹⁾.

ب- قاعدة القاضي الخبير:

لقد كانت أقوى المحاولات الفقهية للرد حول تحجيم دور القاضي هي تلك التي نادى بأنه عوض عن المطالبة بأن الخبير هو قاضي الدعوى أن يكون القاضي هو خبير الدعوى، وهو اتجاه يتوافق مع تكنولوجيا المعلومات من حيث أن ثقافة المعلوماتية تتناول في موضوعها ثقافة عامة يحتاج إليها القاضي و الداني، إذ أنها يجب أن تخترق مستوى الرجل المتوسط الذي يعرفه القانون ويرتب عليه تفسير العديد من القواعد القانونية، والقاضي الخبير من الموضوعات التي تخضع لنظام توزيع العمل في المحاكم ولم تتطور في النظام الفرانكفوني على عكس النظام الانجلوسكسوني الذي طور النظام القضائي بالاهتمام بتكوين رجال القضاء بتلقيهم نظام دراسي تأهيلي وتطويري بالموازاة مع تأهيل مباني المحاكم وقاعات الجلسات ليتم توزيع العمل على ضوء التخصصات التأهيلية للقضاة⁽²⁾.

ت- مدى تأثير الخبرة التقنية على قناعة القاضي:

(1) فتحي محمد أنور عزت، المرجع السابق، ص 671.

(2) فتحي محمد أنور عزت، نفس المرجع ، ص 672-673.

إن السلطة التقديرية المخولة للقاضي في تقدير التقرير لا يستخدمها تحكما، و إنما يتحري بجدية وثقة واضعا أمام نظره أدلة الإثبات الاخرى، والقاضي لا يأخذ بتقرير الخبير إلا بعد عرضه في الجلسة ومناقشته⁽¹⁾ شأنه في ذلك شأن باقي أدلة الإثبات.

وفي هذا السياق أقر الاجتهاد القضائي المصري إلى أن السلطة التقديرية للقاضي لا تمتد إلى المسائل الفنية، فلا يجوز تفنيدها إلا بأسانيد فنية، وهو ما ذهبت إليه المحكمة الاتحادية الإماراتية العليا⁽²⁾.

فالمشروع الجزائري و استنادا إلى نص المادة 215 من ق.إ.ج.ج أكد على أن التقارير القضائية أي التي أنجزت بأمر قضائي و المثبتة للجنح ومنها الجرائم المعلوماتية حسب الوصف الجزائري للمشروع الجزائري لا تعتبر إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك بمعنى انه ليس لها أي حجية مطلقة بل هي مجرد دليل كباقي الأدلة تخضع للسلطة التقديرية للقاضي قد يأخذ بها وقد يستبعدا إذا لم تتساند مع باقي الأدلة.

ويري بعض الفقه المصري ضرورة إعطاء قوة إلزامية لتقرير الخبير⁽³⁾، بينما يري جانب من الفقه بأن الخبير هو القاضي الحقيقي للدعوى فكل ما يبديه الخبير المعلوماتي يعد من الحقائق التي تجبر القاضي على الأخذ بها، فالدور الجوهرى للخبير في تحديد الأدلة الرقمية لا يترك مجالا واسعا للقاضي لتحديد مسار الدعوى فهو الملهم الأساسي في القضية⁽⁴⁾، وبالمقابل فقد

(1) محمد علي سكيكر، المرجع السابق، ص 141.

(2) بقولها "...لا يسوغ للمحكمة أن تستند في دحض ما قال به الخبير الفني إلى معلوماتها الشخصية، بل يتعين عليها إذا ما ساورها الشك فيما قرره الخبير في هذا الشأن أن تستجلي حقيقة الأمر بالاستعانة بغيره من أهل الخبرة، لأنها من المسائل الفنية البحتة التي لا يصح للمحكمة أن تحل نفسها محل أهل الخبرة..." أنظر عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري المرجع السابق ، ص 29.

(3) عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، نفس المرجع ، ص 30.

(4) ويستشهد أصحاب هذا الرأي بقضية اتحاد طلبة اليهود في فرنسا حينما رفعوا دعوى قضائية ضد شركة ياهو Yahoo بسبب التقليل من واقعة "الهولوكوست" من خلال فتحها مزاد على صفحاتها عبر الانترنت أين اصدر القضاء حكما يعتمد على تقرير الخبرة التقنية يلزم الشركة بمنع المستخدمين من الدخول إلى المزاد، رغم إصرار الشركة على عدم قدرتها على ذلك . انظر محمد طارق عبد الرؤوف ألحن، المرجع السابق، ص 337-338.

أظهر الواقع العملي أن القاضي غالبا ما يسلم بما خلص إليه الخبير في تقريره، ويبني حكمه على أساسه⁽¹⁾.

في تقديرنا فإن من مقتضيات الإثبات في الجريمة المعلوماتية وجوب تبني انتداب الخبير المعلوماتي كإجراء جوهري في ملف الدعوى بسبب التطور المستمر لتكنولوجيا المعلومات وعدم محدوديتها دون اشتراط التكوين الأكاديمي للخبير المنتدب، و على القاضي أن لا يستبعد تقرير الخبرة التقنية المنتجة للدليل المعلوماتي، شريطة أن تكون مقبولة ومشروعة فهي وسيلة أساسية لاستخلاصه، وحجية الخبرة باعتبارها وسيلة مهمة في إثبات الجريمة المعلوماتية تكمن في مدى توصلها للدليل الرقمي من عدمه ناهيك عن المحافظة على سلامته من حيث المحتوي، ما يتعين على القاضي أن يبني تسببه القانوني وهو المبرر للمنطوق استنادا على نتائج الخبرة وجوبا تحت طائلة القصور في تسبيب الحكم.

المطلب الثاني

الدليل الكتابي.

يعد الدليل الكتابي وسيلة من وسائل الإثبات الجنائي و تخضع كقاعدة عامة لمبدأ حرية القاضي في الاقتناع مع ورود استثناءات على هذا المبدأ⁽²⁾، و يشمل الإثبات بالدليل الكتابي في المسائل الجزائية ثلاثة أنواع من الأدلة الكتابية وهي: المحاضر التي حددها المشرع الجزائري كطريقة من طرق الإثبات ونص عليها في المواد 214 و 215 و 216 من ق.إ.ج.ج أما النوع الثاني فهي المحررات أو الأوراق التي تشكل جسم الجريمة، ثم الأوراق الخاصة الصادرة عن المتهم و التي نص عليها المشرع في المادة 217 من ق.إ.ج.ج والتي أكد على أنها لا تعد طريقا للإثبات⁽³⁾. وستقتصر دراستنا في هذا المطلب على النوع الأول للدليل الكتابي فقط وهي

(1) عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، المرجع السابق، ص 30.

(2) أحمد فتحي سرور، المرجع السابق، ص 447.

(3) تنص المادة 217 من ق.إ.ج.ج على أنه " لا يستنبط الدليل الكتابي من المراسلة المتبادلة بين المتهم ومحاميه " ومن ثم أقر المشرع الجزائري بنص صريح على استبعاد المراسلات التي تتم بين المتهم ودفاعه من مجال استعمالها كوسيلة من وسائل الإثبات

المحاضر بينما النوع الثاني فسوف نتناوله في حجية الدليل المعلوماتي في الفصل الثاني من البحث .

الفرع الأول: تعريف المحاضر وشروط قبولها:

نتناول في هذا الفرع المقصود أولاً بالمحاضر أو الضبوط، ثم نوضح أنواع المحاضر وحجبتها في الإثبات ثانياً.

أولاً - تعريف المحاضر :

في تعريف أبسط يصدق على الغالب تعريف الدليل الكتابي في الإثبات الجنائي بأنه: "المحرر ورقة تحمل بيانات بشأن واقعة ذات أهمية في إثبات ارتكاب الجريمة ونسبتها إلى المتهم" (1). بينما يعرف المحاضر بأنه " المحرر الذي يدونه الموظف المختص لإثبات ارتكاب الجرائم أو الإجراءات التي اتخذت بشأنها وذلك وفق الشروط والأشكال التي حددها القانون" (2).

أما تعريف المحاضر في التحقيق الجنائي في الجرائم المعلوماتية فهو " الوثيقة الرسمية التي يدون فيها مأمور الضبط القضائي ما تم وما سوف يتم من إجراءات التحقيق، فالمحاضر يحتوي على الوقائع التي حدثت مرتبطة بالزمن (التاريخ و الوقت) سواء كانت هذه الوقائع مرتبطة بالأشخاص (مبلغ، شاهد، ضحية، متهم، أو مشتبه فيه) أو الأماكن أو الأشياء حسب طبيعتها مثل: الحاسب الآلي ومكوناته، و الهاتف المحمول(3).

فالمحاضر إذن هي أعمال قانونية تتمثل في التحرير الكتابي الذي يقوم به من يتمتع بصفة الضبطية سواء كان عمومي أو قضائي في قالب رسمي حول ما عاينه بحواسه من أفعال أو تصريحات أو معاينات مادية، أو من أشخاص يتلقي منهم تصريحاتهم بموجب سلطته القانونية

وهو ما ذهب إلىه التشريعات المقارنة من مبدأ ضمانات حقوق وحريات المتهم المستندة أساساً إلى المواثيق و العهود الدولية ومن ثمة يتعين علينا استبعادها من مجال دراستنا.

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقاً لأحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 933.

(2) محمد طارق عبد الرؤوف الحن، المرجع السابق، ص 322.

(3) مصطفى محمد موسي، المرجع السابق، ص 330.

وذلك بغرض إثبات ما يحتويه المحضر أمام الجهات المختصة، وتتمتع المحاضر بأن لها أهمية بالغة كوسيلة للإثبات، إذ أن إجراء المعاينة تتم عن طريق محاضر يحررها ضباط وأعاون الشرطة القضائية وبعض الموظفين و الأعاون في مصالح إدارية مختلفة يحددها القانون⁽¹⁾.

ثانيا - شروط قبول المحاضر كوسيلة للإثبات:

لقبول المحاضر وتصنيفها طريقا من طرق الإثبات كان لا بد من وضع شروط معينة، يجب أن تتوفر عليها ليتم قبولها أمام المحكمة، لذلك حدد المشرع في نص المادة 214 من ق.إ.ج.ج الشروط اللازمة لقبول المحاضر وهي:

أ- أن يكون صحيحا في الشكل أي بذكر الجهة المصدرة و القائم بالتحضير وتحديد الزمان و المكان والإمضاءات⁽²⁾، إذ نجد المادة 18 من ق.إ.ج.ج⁽³⁾ تضمنت شروط وشكل محاضر جمع الاستدلالات التي تقوم بها الضبطية القضائية و أكدت على ضرورة تقديم الأصول المحررة للمحاضر مصحوبة بنسخ مطابقة لها مؤشر عليها، مع كتابة صفة القائم بتحضيرها و ترسل إلى وكيل الجمهورية المختص وهي المحاضر التي تتضمن ما تم معاينته حول الجرائم بما فيها الجريمة المعلوماتية، أما الشروط الشكلية لمحاضر التحقيق القضائي والتي أحاطها المشرع بعناية خاصة و المتعلقة بسماع الشهود واستجواب المتهمين، فقد أكد المشرع في المادة 90 وما بعدها من ق.إ.ج.ج على ضرورة توقيع كل من قاضي التحقيق، والكاتب، والشاهد على كل صفحة من صفحات محضر سماع الشاهد، كما يتعين تجنب أي تحشير بين السطور مع مصادقة قاضي التحقيق، و الكاتب، و الشاهد على كل شطب أو تخريج فيها رفقة المترجم إن كان له محل.

(1) جمال نجيمي ، المرجع السابق، ص 186-187.

(2) جمال نجيمي، نفس المرجع ، ص 188.

(3) تنص المادة 18 على أنه " يتعين على ضباط الشرطة القضائية ن يحرروا محاضر أعمالهم وأن يبادروا بغير تمهل إلى إخطار وكيل الجمهورية بالجنايات و الجنح التي تصل إلى علمهم.

وعليهم بمجرد إنجاز أعمالهم أن يوافوه مباشرة بأصول المحاضر التي يحررونها مصحوبة بنسخة منها مؤشر عليها بأنها مطابقة لأصول تلك المحاضر التي حرروها، وكذا بجميع المستندات و الوثائق المتعلقة بها وكذلك الأشياء المضبوطة وترسل المحاضر الخاصة بالمخالفات و الأوراق المرفقة بها إلى وكيل الجمهورية لدى المحكمة المختصة و يجب أن ينوه في تلك المحاضر عن صفة الضبط القضائي الخاصة بمحضرها".

في حين أن شروط الشكلية في محاضر السماع تتمثل في استدعاء محامي أطراف الدعوي بكتاب موصي به يومين قبل استجواب المتهم أو الطرف المدني وفقا لمقتضيات المادة 107 من ق.إ.ج.ج.

ب- أن يحرره واضعه أثناء مباشرة أعمال وظيفته، فلا يصح منه ذلك قبل أو بعد ممارسة مهامه، فلا يقبل منه إذا كان تحت التدريب ولم يتم تثبيته بعد، كما لا يقبل منه إذا كان في حالة عطله أو بعد إحالته على التقاعد.

ج- أن يكون الموضوع من اختصاص محرر المحضر بمعنى أنه يكون مختص من حيث الزمان و المكان والموضوع، فأحيانا يشترط المشرع إثبات واقعة ما أعوان محددين فيجب أن تكون المعاينة قد تمت من طرف شخصهم دون سواهم. أما في تحرير محاضر إثبات الجرائم المعلوماتية فلا يوجد نص يخول جهة ما بتحرير المحضر بالرغم من أنها جرائم تقنية تتطلب كادر بشري مختص لتحرير مثل هذه المحاضر، ولو أن الضبطية القضائية تتوفر في تقسيماتها على فروع متخصصة.

فمثلا يتوفر جهاز الدرك الوطني على قطبين لمكافحة الجرائم المعلوماتية هما: قطب الشرطة القضائية لجهاز الدرك الوطني يتوفر على خلايا للتحقيق المعلوماتي في كل تجمع ولائي للدرك مهمتها التنسيق بين وحداته في مجال تقنيات الانترنت، وكذا على قطب مسند للشرطة القضائية يتوفر بدوره على مختصين في مكافحة هذه الجرائم وآخرين للبحث والتحري فيها⁽¹⁾.

د- أن يسجل محرر المحضر فيه ما قد رآه أو سمعه أو عاينه بنفسه، فلا يصح مثلا تحرير محضر معاينة بناء على رواية شهود⁽²⁾.

الفرع الثاني: تقسيم المحاضر من حيث قوتها في الإثبات.

(1) Tarek bouzidi, communication sous titre « La Gendarmerie Nationale et la lutte contre la cybercriminalité» commis dans l'Actes du séminaire international Alger le 5-6 Mai 2010 , centre de recherche juridique et judiciaire, Ibsen édition & diffusion p 114-115.

(2) جمال نجيمي، المرجع السابق، ص 188-189.

تنقسم المحاضر من حيث قوتها في الإثبات إلى ثلاثة أقسام محاضر لا حجية لها ومحاضر التي يجوز إثبات عكسها بالطرق العادية ومحاضر لا يجوز إثبات عكسها إلا عن طريق الطعن بالتزوير فماذا يقصد بكل محضر من هذه المحاضر؟ وما مدي حجيتها في إثبات الجريمة المعلوماتية؟

أولاً- المحاضر التي ليس لها أية حجية :

وهي المحاضر التي يتعين على المدعى أن يقيم الدليل على ما ورد فيها وتدخل في ذلك محاضر الاستدلال و التحقيق الابتدائي عامة في التشريع المصري وهذه المحاضر تشكل الأصل العام في الإجراءات الجنائية⁽¹⁾، بينما في التشريع الجزائري تتمثل في محاضر الضبطية القضائية وقد أكد المشرع الجزائري على هذا المعني حيث جاء في نص المادة 215 من ق.إ.ج.ج " لا تعتبر المحاضر و التقارير المثبتة للجنايات أو الجرح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك".

ولعل اعتبار المشرع محاضر الضبطية التي تتضمن وقائع ذات وصف جنائي وجنحي مجرد استدلالات لخلوها من الضمانات القانونية لتحسين الدليل القضائي فلا يجوز لها تحليف الشاهد ولا استجواب المتهم أو إجراء مواجهة بين الأطراف⁽²⁾.

فمن منطلق عدم حجية تلك المحاضر يمكن للخصوم مناقشتها ودحض ما ورد فيها بشتى الطرق، كما يمكن للمحكمة أن تأخذ بها أو أن تستبعد ما دام الدليل الذي بين طياتها لا يستوي مع الحقيقة التي اطمأنت إليها من باقي الأدلة، ولذلك فالمحاضر الاستدلالية المنجزة من طرف الضبطية القضائية المتضمن اعترافات المشتبه فيهم ، أو أقوال الشهود هي عناصر إثبات تخضع لتقدير القاضي ، وتحتمل الجدل و المناقشة كسائر الأدلة ولو أن المشرع المصري أضاف إلى جانب محاضر الاستدلال محاضر التحقيق الابتدائي فلا تتمتع بأي حجية وهذا ما يتضح من نص

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 935.

(2) جمال نجيمي ، المرجع السابق، ص 195.

المادة 300 إجراءات مصري بقولها " لا تتقيد المحكمة بما هو مدون في التحقيق الابتدائي أو في محاضر جمع الاستدلالات إلا إذا وجد في القانون نص على خلاف ذلك"⁽¹⁾.

و تطبيقا لذلك قضت النقض المصرية أن محاضر التحقيق الذي يجريها البوليس أو النيابة العامة وما تحويه من اعترافات المتهمين ومكاتبات المحققين وأقوال الشهود هي عناصر إثبات تخضع في كل الأحوال لتقدير القاضي وتحتمل الجدل و المناقشة كسائر الأدلة⁽²⁾

وهو ما ينطبق على إجراءات البحث والتحري التقليدي في الجريمة المعلوماتية فكل المحاضر التي تتضمن الاعترافات أمام الضبطية القضائية أو الشهود المسموعين حول ذات الوقائع وكل ما تتضمنه بشأن الأدلة التقليدية إنما تعتبر محاضر استدلالية ليس لها أية حجية قانونية تخضع لتقدير القاضي الجزائي كباقي الأدلة استنادا إلى نص المادة 212 من ق.إ.ج.ج.

إذا كانت المادة 215 تناولت الأصل وهو عدم حجية محاضر الاستدلال إلا ما استثنى بنص فقد تناولت المادة 216 مباشرة بعدها الاستثناء الأول فما هو هذا الاستثناء؟ و ما هي هذه المحاضر، وهل لها الحجية وهو ما سنعرفه في العنصر الموالي.

ثانيا- المحاضر التي يجوز إثبات عكسها بالطرق العادية

حدد المشرع في المادة 216 من ق.إ.ج.ج النوع الثاني من المحاضر وهي المحاضر التي تتضمن صحة ما ورد فيها ولها الحجية الكاملة إلى غاية إثبات عكس ذلك، إما بالكتابة، أو شهادة الشهود، إذ تنص على ما يلي: " في الأحوال التي يخول القانون فيها بنص خاص لضباط الشرطة القضائية وأعاونهم الموكلة أيهم بعض مهام الضبط القضائي سلطة إثبات جنح في محاضر أو تقارير تكون لهذه المحاضر أو التقارير حجيتها ما لم يدحضها دليل عكسي بالكتابة أو شهادة الشهود".

(1) فوزية عبد الستار، المرجع السابق، ص539.

(2) كامل السعيد، شرح قانون أصول المحاكمات الجزائية دراسة تحليلية تأصيلية مقارنة في القوانين الأردنية و المصرية والسورية وغيرها، الطبعة الأولى الإصدار الثاني، دار الثقافة للنشر و التوزيع، عمان الأردن، سنة 2008، ص 778.

ويتضح من نص المادة أن المشرع وضع ثلاثة شروط ليلبغ المحضر حجيته وهي⁽¹⁾:

1-تحديد الحالات التي يحزر فيها هذا النوع من المحاضر لإثبات الجرح، وذلك بنصوص خاصة عندما منح لضباط الشرطة القضائية، أو أعوانهم، أو للموظفين، أو أعوانهم الموكلة إليهم بعض مهام الضبط القضائي، و ينظر إليها بعض الدارسين بأنها ضمانة لحقوق المشتبه فيه، فكلما ضيق دائرة حجية المحاضر الغير قضائية اتسعت رقعة ضمان الحقوق و العكس صحيح .

2- تحديد طبيعة الأدلة التي تثبت عكس ما جاء في هذا النوع من المحاضر، وهي شهادة الشهود والكتابة، فلا يتصور نفيها بإنكار أو نفي المتهم أو بالقرائن.

3- المخالفات هي وحدها الجرائم التي يشملها هذا النوع من المحاضر، و المنصوص عليها في المادة 400 من ق.إ.ج.ج " تثبت المخالفات إما بمحاضر أو تقارير وإما بشهادة الشهود في حالة عدم وجود محاضر او تقارير مثبتة له".

بينما فسرت محكمة النقض المصرية هذه الحجية على اعتبار أن حجة هذه المحاضر يعتبر حقا للمحكمة و ليس واجبا عليها، بمعنى أن المحكمة لا تلتزم بالأخذ بما ورد في هذه المحاضر طالما أنه لم يثبت تزويرها، وإنما يكون لها الحق في أن تأخذ بما تتضمنه هذه المحاضر دون أن تعيد تحقيقه بالجلسة ، أي أنها تقدر قيمة هذه المحاضر بكامل حريتها فتأخذ به وتطرده ولو لم يطعن فيه بالوجه الذي رسمه القانون، على أن تمكن المحكمة الخصوم إثبات عكس ذلك بطرق الإثبات العادية. كما أن النص المصري المحدد لهذه الحجية جاء أكثر وضوحا بقوله " تعتبر المحاضر المحررة في مواد المخالفات حجة بالنسبة للوقائع التي يثبتها المأمورون المختصون إلى أن يثبت ما ينفبها⁽²⁾ .

و العلة في اعتبار هذه المحاضر حجة بما ورد فيها أنها تحرر لإثبات المخالفات فهي جرائم يسيرة ولا يتصور تضييع الوقت في إثباتها فيستند القاضي إلى المحاضر دون إعادة التحقيق فيها،

(1) مروك نصر الدين، محاضرات في الإثبات الجنائي أدلة الإثبات الجنائي، الجزء الثاني، المرجع السابق، ص449-450.

(2) فوزية عبد الستار، المرجع السابق، ص 551.

أما إذا أقيمت الدعوى بوصفها جنحة و لكن المحكمة أعادت تكييفها إلى مخالفة، كان لمحضر المحرر بشأنها الحجية، إذ العبرة بالوصف الذي خلصت إليه المحكمة⁽¹⁾.

أما دور المحاضر ذات الحجية إلى غاية إثبات العكس في إثبات الجريمة المعلوماتية فإنه طالما صنف المشرع الجزائري الجرائم المعلوماتية كجنح ولا توجد هناك مخالفة في الكتاب الرابع المتعلق بالمخالفات وعقوباتها بعنوان مخالفة معلوماتية بالإضافة إلى عدم عثورنا على نص خاص يحدد الأشخاص المخولين بإعداد هذا النوع من المحاضر التي تثبت الجرائم المعلوماتية، فإن هذه النوع من المحاضر لا تتناول مسألة إثبات الجريمة المعلوماتية، وتبقى المحاضر العادية كقيلة بذلك إلى غاية صدور النص التنظيمي المتعلق بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحته الذي بإمكانه أن يحمل مواد قانونية تحدد وتنظم هذه المسألة .

ثالثا- المحاضر التي لا يجوز إثبات عكسها إلا بطريق الطعن بالتزوير.

تعتبر هذه المحاضر من أقوى أنواع المحاضر من حيث الإثبات، لأن القاضي ملزم بالأخذ بها، إلا إذا استطاع المتهم إثبات تزويرها⁽²⁾، وهو أمر غاية في الصعوبة بحيث تتضح إرادة المشرع في التشدد حين معالجته لبعض الجرائم فيعطي لجهة المتابعة امتياز تقديم دليل يتناول واقعة مادية بحتة ليس من السهل دحضه وكأنه لا يريد لجرائم معينة أن تقلت من العقاب⁽³⁾، و يحزر هذا النوع من المحاضر لإثبات الجرائم التي تلاشت آثارها و التي لا يمكن الاعتماد فيها على الأفراد في ملاحظتهم وجمع الأدلة، وبالتالي يصعب إثباتها، خصوصا وأن هذا النوع من الجرائم مرتبط بمصالح الدولة⁽⁴⁾.

ونص المشرع الجزائري على هذا النوع من المحاضر في المادة 218 من ق.إ.ج.ج بقوله:

(1) محمود نجيب حسني ، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 936-937.

(2) محمد طارق عبد الرؤوف الحن ، المرجع السابق، 322.

(3) جمال نجيمي ، المرجع السابق، ص 211-212.

(4) مروك نصر الدين، محاضرات في الإثبات الجنائي، الجزء الثاني، المرجع السابق، ص 451.

" إن المواد التي تحرر عنها محاضر لها حجيتها إلى أن يطعن فيها بالتزوير تنظمها قوانين خاصة.

وعند عدم وجود نصوص صريحة تتخذ إجراءات الطعن بالتزوير وفق ما هو منصوص عنه في الباب الأول من الكتاب الخامس".

بينما تناولها المشرع المصري في المادة 30 من القانون 57 لسنة 1959 و المستبدلة بالقانون 74 لسنة 2007، حيث تنص على انه" إذا ذكر في محضر الجلسة أو في الحكم أن الإجراءات قد اتبعت أثناء نظر الدعوى فلا يجوز إثبات عدم إتباعها إلا بطريق الطعن بالتزوير". ويلاحظ أن المشرع المصري قصر هذه الحجية على الإجراءات التي ذكر في محضر الجلسة والحكم أنها أتبعت دون الوقائع ولم يتناول ذكر نصوص خاصة⁽¹⁾، على عكس المشرع الجزائري الذي حدد بصريح العبارة أن هذا النوع من المحاضر تنظمها قوانين خاصة ومن أمثلة هذه القوانين قانون الجمارك وقانون المتعلق بمكافحة التهريب رقم 05-06 المؤرخ في 2005/08/23.

وبإجراء إسقاط على الجرائم المعلوماتية فان هذا النوع من المحاضر التي لا يمكن الطعن في ما احتوته إلا بطريق التزوير لا تجد لها طريقا إليها بمعنى انه في غياب نصوص خاصة تتناول تحرير محاضر قاطعة حول الجرائم المعلوماتية لا يمكن الطعن فيها إلا بالتزوير يبقي إثباتها عن طريق النوع الأول من المحاضر، ولعل الحكمة من ذلك يرجع إلى طبيعة الجريمة المعلوماتية و التي تقع في فضاء افتراضي لا يتناسب مع طبيعة هذه المحاضر التي تتضمن في الغالب الأعم معاينات مادية في أماكن يصعب على باقي الأدلة التقليدية الاخرى إثباتها ومن هنا تقررت لها تلك الحجية.

المطلب الثالث

القرائن————ن.

(1) فوزية عبد الستار، المرجع السابق، ص552-553.

تحتل القرائن في العصر الراهن مرتبة متميزة بين سائر وسائل الإثبات الجزائي ، ذلك أن غالب الأحيان يتعذر إعداد الدليل المباشر لإثبات الوقائع المادية، خاصة إذا وقع تعمد في طمس المعالم لتضليل جهات إنفاذ القانون، ليجد القاضي نفسه مستعينا بالقرائن كسبيل يوصله إلى كشف الحقيقة، ومع التطور العلمي و التكنولوجيا زاد الاهتمام بالقرائن نظرا لاستفادة المجرمين من التطور التقني فكان من الضروري الاستعانة بالقرائن من أجل الإثبات بالوسائل الحديثة ومن هنا طرح تساؤل عن المقصود بالقرائن وما هي أنواعها ؟ و ما هو دورها في إثبات الجريمة المعلوماتية؟

الفرع الأول- الأحكام العامة للقرائن

في إطار الأحكام العامة للقرائن نتناول المقصود بالقرائن أولا ثم نتعرف ثانيا على أنواع القرائن

أولا- تعريف القرائن وتمييزها عن الأمارات و الدلائل:

نتطرق في هذا العنصر إلى تعريف القرائن من الناحية القانونية ثم نميز بين معني القرائن وبين الأمارات و الدلائل من جهة أخرى.

أ-تعريف القرائن:

القرينة عبارة عن " خلاصة لعملية ذهنية يقوم بها المشرع، أو القاضي لاستنباط واقعة مجهولة من واقعة معلومة، وتستلزم تلك العملية وجود واقعتين إحداهما معلومة و الأخرى مجهولة، وأن يكون بين الواقعتين صلة وثيقة وضرورية " (1). و الإثبات بالقرينة هو استنتاج الواقعة المطلوب إثباتها من واقعة أخرى قام عليها دليل إثبات، في هذه الحالة يقال إن إثبات الواقعة التي قام عليها الدليل قرينة على ثبوت الواقعة التي لم يرد عليها دليل (2).

(1) محمد طيب عمور، مقالة بعنوان الإثبات الجزائي بالقرائن القضائية بين الشريعة و القانون ، منشورة في مجلة الأكاديمية للدراسات الاجتماعية و الإنسانية، العدد 09، سنة 2013، ص 81-82.

(2) محمود نجيب حسني، شرح قانون الاجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 940.

بينما لم يعرف المشرع الجزائري القرائن لا في القوانين الجزائية، ولا في القانون المدني وفوض المسألة للفقهاء والقضاء، بينما عرف المشرع المدني الفرنسي القرائن بأنها " هي النتائج التي يستخلصها القانون أو القاضي من واقعة معلومة إلى واقعة مجهولة"⁽¹⁾.

ويفترض الإثبات بالقرائن تغيير محل الإثبات، فبدلاً من أن يرد الإثبات على الواقعة ذات الأهمية في الدعوى (أي واقعة ارتكاب الجريمة ونسبتها إلى المتهم)، يرد على واقعة أخرى مختلفة و لكن بين الواقعتين صلة سببية منطقية بحيث يمكن وفقاً للاستنباط المنطقي أن يستخلص من إثبات هذه الواقعة ثبوت ارتكاب الجريمة ونسبتها إلى المتهم⁽²⁾.

ب- التمييز بين القرينة وبين الأمانة و الدلائل:

ميز الفقه بين الأمانة و القرينة، فالقرينة لا تقرر إلا إذا استخلص القاضي الواقعة المجهولة من الواقعة المعلومة وهي الأمانة، الدليل على ثبوت الواقعة المجهولة فلا قرينة بغير أمانة، وإن هذه الأمانات تعتبر مجردة عن أية قوة في الإثبات قبل أن يخضعها القاضي لعملية استنباط، فهي مجرد إرهاب للقرينة يصل من خلالها إلى إثبات الواقعة ، فالقاضي لكي يصل إلى معرفة الواقعة المجهولة فهو يمحس دلالة الأمانات التي يعتقد أنها مفضية إلى إثبات الواقعة المدعى بها، حتى يخلص له الدليل على ثبوتها قويا نقيا مقنعا لا يتسرب إليه الشك أو الارتياب⁽³⁾.

والتمييز بين القرينة والدلائل يتضح من أنهما يتفقان في استنتاج الواقعة المجهولة من الواقعة الثابتة، ولكن الاختلاف بين الاثنين يبدو في قوة الصلة بين الواقعتين، ففي القرينة تستنتج المحكمة الدليل من علاقة منطقية قاطعة بين الواقعة الثابتة والواقعة المراد إثباتها تؤدي إلى الثبوت اليقيني على سبيل الجزم لها بحكم العقل و المنطق، بينما في الدلائل فإن الصلة بين الواقعتين احتمالية و

(1) جمال نجيمي، المرجع السابق، ص 369. كذلك الغوثي بن ملحمة، المرجع السابق، ص 94-95.

(2) محمود نجيب حسني، شرح قانون الاجراءات الجنائية وفقاً لأحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 941.

(3) فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة)، الطبعة الأولى الإصدار الثاني، دار الثقافة للنشر و التوزيع، عمان الأردن، سنة 2006، ص 321.

ليست قاطعة، فيكون الاستنتاج منها علي سبيل الاحتمال، ولا يجوز الاعتماد عليها وحدها في الادانة، ويكون دورها فقط معززا ومكملا لأدلة الدعوى⁽¹⁾.

ثانيا - أهمية القرائن :

تشكل القرائن أهمية كبيرة في الإثبات الجنائي ذلك أن بعض الوقائع يستحيل إثباتها، فإذا ما اقتصر الإثبات على الأدلة المباشرة لتعذر الوصول إلى الحقيقة بدونها، وفي هذا قال ارش بولد بان القرائن والأدلة الظرفية وان كانت مقبولة في الإثبات الجنائي والمدني، إلا أن أهميتها في الجنائي أكثر لأن إمكان الإثبات عن طريق الأدلة المباشرة كالشهادة و الدليل الكتابي أكثر صعوبة وأقل حدوثا في الجنائي منه في المدني لأن الطرفين في المدني يعدان عادة وسائل إثبات مقدما أما في الجنائي فيكون وجود هذه الأدلة عن طريق المصادفة لأن المتهم عند إقدامه على ارتكاب جريمة يتخذ من الاحتياطات ما يكفل لتضليل و امحاء الأدلة⁽²⁾.

فالقرائن كثيرا ما تكون هي المعيار الذي يوازن به القاضي بين الأدلة المختلفة، كما تتجلى أهمية القرائن أنها اصدق دلالة بالنظر إلى طبيعتها الموضوعية التي تقابل الطبيعة الشخصية لسائر الأدلة الاخرى، وان هذه الطبيعة تجعل من المستحيل أن يدخل عليها التشويه، وان التقدم العلمي سيبتيح السبيل لاكتشاف جميع القرائن ثم إخضاعها لأساليب الفحص العلمي الدقيق واستخلاص دلالتها و الاستعانة بها في إثبات الجريمة⁽³⁾.

الفرع الثاني: أنواع القرائن.

تنقسم القرائن إلى نوعين رئيسيين هما القرائن القانونية و القرائن القضائية فماذا يقصد بكل قرينة منهما ؟

أولا - القرائن القانونية :

(1) أحمد فتحي سرور، المرجع السابق، ص 410-411.

(2) فاضل زيدان محمد، المرجع السابق، ص 321.

(3) فاضل زيدان محمد، نفس المرجع، ص 322.

القرائن القانونية هي القرائن المستمدة من نص القانون وهي واردة على سبيل الحصر ولا يقاس عليها ولا حاجة لإثباتها⁽¹⁾، والقول بأن النص يتضمن قرينة قانونية يجب أن يشتمل صراحة على الواقعة المعلومة و الواقعة المستنبطة، وهاتان الواقعتان معا تشكلان قاعدة النص⁽²⁾ . وتنقسم القرائن القانونية بدورها إلى فئتين يتولى القانون نفسه عبء إثبات الدليل المستمد منهما⁽³⁾ وهما:

أ- القرائن القانونية القاطعة أو المطلقة:

وهي القرائن التي لا يجوز إثبات عكسها⁽⁴⁾، ومثال ذلك ما جاء في المادة 60 من الدستور الجزائري بنصه " لا يعذر بجهل القانون" فوضع المؤسس الدستوري قرينة قانونية قاطعة مفادها أن المخاطبين بالقانون هم على علم به بمجرد صدوره ونشره ولا يقبل منهم التذرع بأنهم يجهلون قانونا معينا، حتى ولو كانوا في الواقع يجهلونه حقيقة⁽⁵⁾.

ب- القرائن القانونية البسيطة:

وهي القرائن التي تقرر حالة قانونية بصورة مبدئية ، ولكن يجوز للمضروب منها أن يقيم الدليل على عكس ما تضمنه⁽⁶⁾، ومن أمثلة ذلك اعتبار ارتكاب جنحة إزالة أو تعديل معطيات في منظومة معلوماتية خلصة طبقا للمادة 394مكرر 01 من ق.ع.ج من حاسوب موصول بخط اشتراك باسم صاحب المنزل، فهي قرينة قانونية على ارتكاب الجريمة، ولكنها قرينة غير قاطعة يمكن للمتهم أن يقيم الدليل على عكسها فتنهار قوتها في الإثبات.

(1) عادل عزام سقف الحيط ، ، جرائم الدم و القرح و التحقير المرتكبة عبر الوسائط الإلكترونية "شبكة الانترنت و شبكة الهواتف النقالة و عبر الوسائط التقليدية و الآلية و المطبوعات " دراسة قانونية مقارنة، الطبعة الأولى، دار الثقافة للنشر و التوزيع ، عمان الأردن سنة 2011، ص 276.

(2) رائد صبار الازيرجاوي ، القرينة ودورها في الإثبات في المسائل الجزائية (دراسة مقارنة في القانونين الأردني و العراقي) مذكرة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير، القسم العام جامعة الشرق الأوسط، سنة 2010-2011 ص 21.

(3) أحمد فتحي سرور، المرجع السابق، ص 403.

(4) محمد طارق عبد الرؤوف الحن، المرجع السابق، ص 312.

(5) جمال نجيمي ، المرجع السابق، ص 375.

(6) محمد طارق عبد الرؤوف الحن، المرجع السابق، ص 312.

وتتمثل أهمية القرائن القانونية البسيطة في كون المشرع قد قصد بها رفع عبء إثبات الأمر الذي افترضه المشرع على كاهل النيابة العامة ويكون على المتهم أن يثبت انتفاء هذا الأمر (1). وفي المقابل قضت المحكمة الدستورية العليا المصرية بعدم دستورية القرائن القانونية لإخلالها بمبدأ الأصل في المتهم البراءة(2).

ثانيا - القرائن القضائية:

سميت بالقرائن القضائية نسبة إلى دور القاضي في استنباطها، لذلك فإن القرائن القضائية هي كل استنباط لواقعة مجهولة من واقعة معلومة، بحيث يكون الاستنتاج ضروريا، وبحكم اللزوم العقلي، والمنطقي، ويترك أمر تقدير القرينة القضائية للقاضي بحيث يستنتج منها ما يطابق عقله ويريح ضميره، فهو الذي يقدر الظروف ودرجة تأثيرها في الدعوى(3).

وتتميز القرائن القضائية بأنها عديدة ولا ترد على سبيل الحصر، كما أنها تصنف ضمن الأدلة الغير المباشرة، وقضت محكمة النقض المصرية أن القرينة القضائية تعتبر دليلا يجوز للمحكمة أن تستند إليه وحده في الحكم، أما تقدير قيمة القرائن في الإثبات فهي مسألة موضوعية لا يجوز المجادلة فيها أمام محكمة النقض، مادامت الظروف التي استندت إليها المحكمة سائغة في الدلالة على ما استخلصته منها(4).

أما بالنسبة للمشرع الجزائري الجزائري، فإنه لم يتطرق للقرائن القضائية بنص صريح في قانون الإجراءات الجزائية لما تناول طرق الإثبات، على عكس ما فعل المشرع المدني الذي أفرد لها فصلا كاملا في الباب السادس من القانون المدني و المتعلق بإثبات الالتزام في المواد من 337الى341.

(1) فوزية عبد الستار، المرجع السابق، ص 597.

(2) أحمد فتحي سرور، المرجع السابق، ص 404.

(3) راند صبار الازيرجاوي، المرجع السابق، ص 29.

(4) فوزية عبد الستار، المرجع السابق، ص 597-598.

في حين لما نطلع على نص المادة 212 من ق.إ.ج.ج يتبين لنا أن المشرع اعتبر القرائن القضائية مثل سائر عناصر الإثبات الأخرى وفقا لمبدأ حرية الإثبات، أما مسألة قبولها فهي متروكة لحرية القاضي طبقا لحرية القاضي الشخصية في الاقتناع، ومن ثمة نصل إلى أن القرائن القضائية تعتبر وسيلة من وسائل الإثبات في قانون الإجراءات الجزائية شأنها شأن وسائل الإثبات الأخرى، لا تقل أهمية عنها⁽¹⁾.

وأكدت المحكمة العليا قبول القرائن القضائية كوسيلة من وسائل الإثبات في عديد القرارات، إذ في إحدى قراراتها قضت بأنه " حيث أن ما ذهب إليه الطاعن في هذا الوجه يرمي إلى مناقشة مدى كفاية القرائن التي اعتمد عليها قضاة الموضوع لتكوين اقتناعهم وهو الأمر الذي يخرج عن صلاحيات المحكمة العليا وفقا لأحكام المادة 212 من قانون الإجراءات الجزائية التي نصت على جواز إثبات الجرائم بأي طريق من طرق الإثبات، وأن قاضي الموضوع يصدر حكمه تبعا لاقتناعه الخاص بناء على الأدلة المقدمة إليه في معرض المرافعات"⁽²⁾.

الفرع الثالث: دور القرائن في إثبات الجريمة المعلوماتية.

مع التطور التقني الهائل و التقدم العلمي بات من الضروري الاستعانة بالقرائن خصوصا عندما نكون بصدد إثبات جريمة معلوماتية ففي هذا النوع من الجرائم أدي تعقيد العمليات الإجرامية الالكترونية والتي غالبا ما تتجاوز الحدود الجغرافية للدول إلى صعوبة وتعقد عملية ملاحقة مرتكبي الجرائم و تتبع آثارهم ، لاسيما بسبب صعوبة جمع الأدلة الجنائية، ومن مظاهر هذا التعقيد استخدام الجناة عناوين بريدية مجهولة، وأجهزة تشفير، ودخولهم إلى طرف ثالث من الأنظمة الحاسوبية، من خلال استخدام مخدم وكيل (proxy server) والمخدم الوكيل عبارة عن جهاز حاسوب وسيط بين المستخدم و الانترنت يسهل الاعتداء على هدف ما، مع عدم ترك أي أثر يدل على بصمة جهاز الجناة⁽³⁾.

(1) محمد طيب عمور، المرجع السابق، ص 84.

(2) قرار غير منشور تحت رقم 518850 صادر بتاريخ 2009/09/09. انظر جمال نجيمي ، المرجع السابق، ص 382.

(3) عادل عزام سقف الحيط، المرجع السابق، ص 182.

ما يفتح المجال للاستعانة بالقرينة كوسيلة للإثبات من أجل الوصول إلى الحقيقة، والقرينة في هذه الحالة تساهم في الوصول إلى الحقيقة من منظورها التقليدي، لأن الخوض في المسائل البيانية والمعطيات والقول بإمكانية الاستعانة بالقرائن التقنية لإثبات الجريمة المعلوماتية أمر لا يستساغ لأن المعطيات تعمل بنظام علمي دقيق لا مجال فيه للخطأ ومن ذلك الكشف على عنوان البروتوكول لأي مستخدم ليس فيه مجال لاحتمالية و لا للخطأ بل هناك حسابات علمية تؤدي إلى النتيجة الحتمية مباشرة ، تبقى مسألة مرتكب الجريمة هنا تدخل مجال تطبيق القرائن القانونية كوسيلة إثبات من شأنها أن تساعد القاضي في الوصول إلى الحقيقة.

ومن الأمثلة على استنتاج القاضي قرينة من الدليل الرقمي ذلك أن يكون المحتال الذي قام بالاستيلاء على أموال بعض المؤسسات المالية عبر الانترنت، له أسلوب خاص به في بناء برمجيات الاختراق، فيتم القبض عليه لأن أسلوبه أضحى معروفاً من قبل جهات الضبط القضائي ثم يجري تقديمه إلى القضاء على هذا الأساس⁽¹⁾.

ونحن حسب تقديرنا لا نوافق ما ذهب إليه الدكتور محمد طارق عبد الرؤوف ألحن، بأن الدليل الرقمي ينتمي إلى فئة القرائن القضائية⁽²⁾، و السبب يعود إلى أن المنطلق يتمثل في إثبات وقوع الجريمة في حد ذاتها يقتضي توفر أدلة علمية وهي الحقيقة العلمية الثابتة بينما انساب الجريمة إلى مرتكبها تلك هي الواقعة المجهولة والعلاقة بين الواقعتين تشكل القرينة لذلك القول بان الأدلة الرقمية هي مجرد قرينة قضائية في الإثبات لا يتأتى، لأنه يجب التمييز بين مسألة تقديم الدليل الرقمي كدليل لقيام جريمة تقليدية هنا نستعين بالدليل الرقمي لنستخلص منه القرينة القضائية ، أما في مسألة إثبات وقوع الجريمة المعلوماتية في حد ذاتها فهي تحتاج إلى نوع حديث من الأدلة التقنية، وهو ما يفتح لنا المجال لدراسة الأدلة الرقمية ومدى حجيتها في الإثبات كوسيلة علمية حديثة في إثبات الجريمة المعلوماتية وهو ما سنتطرق له في الفصل الموالي.

(1) محمد طارق عبد الرؤوف ألحن، المرجع السابق، ص 314.

(2) محمد طارق عبد الرؤوف ألحن، نفس المرجع، ص 313.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

درسنا في الفصل الأول مدى تجاوب الوسائل التقليدية مع إثبات الجريمة المعلوماتية واتضح لنا تجاوز تقنيات الجريمة للقواعد التقليدية إذا استثنينا الخبرة التقنية، لذلك فإن قواعد القانون الإجرائي الجزائي مازالت غير كافية إزاء التصدي لهرتكبي الجريمة، ما ولد الحاجة إلى البحث عن وسيلة حديثة مستمدة من نفس البيئة الافتراضية تقوي على إثباتها، ومع ميلاد الأدلة الرقمية كوسائل لاقت ترحيباً من التشريعات المقارنة، وجد المشرع الجزائري نفسه حبيس نصوص تقليدية معتمداً في كل مرة على مبدأ حرية الإثبات باعتباره ضماناً تقبل بها الأدلة الحديثة إلى غاية اتضاح الصورة الكاملة لهذا النوع من الوسائل، وفي انتظار ذلك طرحت عدة تساؤلات نفسها أهمها ما هي الوسيلة الحديثة التي تضمن إثبات الجريمة المعلوماتية؟ وما مدى حجيتها في بناء القاضي الجزائي قناعته الشخصية؟

و للإجابة على هذه التساؤلات قسمت هذا الفصل إلى مبحثين، نخصص المبحث الأول لماهية الدليل الرقمي، في حين نتناول في المبحث الثاني حجية الأدلة الرقمية في إثبات الجريمة المعلوماتية.

المبحث الأول

ماهية الدليل الرقمي .

لا شك انه كثر الحديث عن الأدلة الرقمية بعد إعلان ميلادها كوسيلة حديثة بدأت تأخذ مكانها ضمن مختلف التشريعات، وأمام حداثة وفعالية هذا النوع من الأدلة، كان لا بد أن يأخذ مكانته في بحثنا بالدراسة و التحليل مادام مقترحاً كحل بديل يكبل سطوة المجرمين المعلوماتيين لذلك نتناول مفهوم الدليل الرقمي أو المعلوماتي (مطلب أول) ، لنكتشف عالمه و نستطيع عرضه على القضاء كوسيلة حديثة للإثبات لمعرفة حجيته في الإثبات الجنائي (مطلب ثاني).

المطلب الأول

مفهوم الدليل الرقمي.

تطرقنا في المبحث التمهيدي إلى معنى الجريمة المعلوماتية والذي يقع الاعتداء في مجمله على البيانات و المعطيات فهي وسائط معنوية تتعرض للاعتداء بأساليب مختلفة، لذلك لا بد من الدليل أن يكون من نفس طبيعة الجريمة الافتراضية بحيث ليقبل أمام القضاء، وعليه يطرح تساؤل عن المقصود بالدليل الرقمي والأدلة ذات الصلة به، وكيف نميزه عن باقي البرامج المشابهة له (الفرع الأول) وما هي الخصائص التي جعلته مميزا عن غيره(فرع ثاني) ؟ وهل وضع له تصنيفات أم يكون على شكل واحد(الفرع الثالث) ؟ وهي التساؤلات التي نجيب عليها في الفروع الموالية.

الفرع الأول : تعريف الدليل الرقمي وتمييزه عن البرنامج المعلوماتي.

نتطرق في القسم الأول لتعريف الدليل الرقمي، ثم في قسم ثاني تمييزه عن البرنامج المعلوماتي.

أولا - تعريف الدليل الرقمي:

تعددت تعريفات الدليل الرقمي⁽¹⁾ وتباينت بين النظرة التقنية و النظرة القانونية، وإجمالا نتطرق إلى أهم التعريفات التي تناولت الدليل الرقمي.

فعرف البعض الدليل الرقمي بأنه " معلومات يقبلها المنطق و العقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحاسوبية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال ،ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة أو جان أو مجني عليه".

وعرفها الأستاذ كيسي " بأنها تشمل البيانات الرقمية التي يمكن أن تثبت أن هنالك جريمة قد ارتكبت ،أو توجد علاقة بين الجريمة و الجاني ، أو توجد علاقة بين الجريمة و المتضرر منها

(1) سبب تسميته بالرقمي أن الحواسيب الرقمية تقوم باستقبال البيانات من المستخدم بشكل منقطع وتحويلها إلى أرقام حسب نظام عددي معين ثم معالجة هذه البيانات ،حيث تقوم وحدة الذاكرة الرئيسية في الحاسب الرقمي بتخزين البرامج و البيانات الداخلة ونتائج المعالجة ويختلف طول الكلمة من حاسب إلى آخر ويتراوح من 8 إلى 64 بايت ، والبايت (Bit) تقاس به سعة الذاكرة و التي تعرف بأنها " عدد الرموز التي تستطيع الذاكرة تخزينها في نفس الوقت" والبايت يتكون من خانات العدد الثنائي 0 أو 1 فمثلا الحرف أ يكون على شكل 11000110، أما البايت فيتكون من ثمانية أرقام ثنائية ويمثل حرف هجائي أو رقمي بين (0-9) أو علامة خاصة، والرقمي يعني أن البيانات تخزن في ذاكرة الحاسب الآلي الرقمي في شكل أرقام وإذا طلبت تخرج على شاشة الحاسب أو الطابعة في الشكل المقروء حسب اللغة التي خزنت بها وليس كما هي مسجلة في ذاكرته. سليمان غازي العتيبي، المرجع السابق، ص35.

و البيانات الرقمية هي مجموعة الأرقام التي تمثل مختلف المعلومات بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت أو الصورة⁽¹⁾. كما عرف كذلك بأنه " كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من انجاز مهمة ما ". أو هو " الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة"⁽²⁾.

فيما عرفته مجموعة العمل العلمية للأدلة الرقمية سنة 1999 بأنه " معلومات ذات قيمة إثباتية مخزنة أو منقولة في شكل ثنائي"⁽³⁾ وأكدت المنظمة العالمية لدليل الكومبيوتر (IOCE)⁽⁴⁾ على ذات المعني حينما عرفت الدليل الرقمي بأنه " المعلومات المخزنة أو المتنقلة في شكل ثنائي ويمكن أن يعتمد عليها في المحكمة"⁽⁵⁾.

بينما يعرفها دليل الشرطة للأدلة الجنائية في المملكة المتحدة (UK Police and Criminal Evidence Code) بأنها " جميع المعلومات الموجودة في الحاسوب " ، وفي نظرة أخرى موسعة تعرف الأدلة الرقمية " بأنها جميع أنواع البيانات المخزنة أو المرسله من خلال تكنولوجيا المعلومات والتي تعتمد عليها نظرية إثبات ارتكاب الجريمة"⁽⁶⁾.

ثانيا- تعريف الأدلة ذات الصلة:

(1) محمد أمين البشري، الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات، المرجع السابق ، ص 109.

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

(3) محمد أمين البشري ، الحلقة العلمية "الإرهاب و الانترنت" لتأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنت في الفترة 15-19/11/2008، جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، ص 25. متاح على الموقع

الالكتروني: <http://www.nauss.edu.sa/Ar/.../training college/.../002.pdf>.

(4) (IOCE): هي تنظيم دولي تم اعتماده في افريل سنة 1995، مقره الولايات المتحدة الأمريكية، تسعى هذه المنظمة الى توفير منتدى دولي لوكالات انفاذ القانون لتبادل المعلومات بشأن التحقيق في جرائم الحاسوب وغيرها من قضايا الطب الشرعي، ويتألف من أجهزة إنفاذ القانون و الوكالات الحكومية المعنية بالتحقيق الرقمي وتحقيقات الطب الشرعي ،وذلك بناءا على المجلس التنفيذي للمنظمة.

(5) عائشة بن قارة مصطفى، المرجع السابق، ص 54-55.

(6) Marco Gercke, COMPRENDRE LA CYBERCRIMINALITE PHENOMENE ,DIFFICULTES ET REPOSES JURIDIQUES, UIT (Union internationale des télécommunications) Genève suisse, septembre 2012, p239.

عرفت المادة 401 من القواعد الاتحادية للعدل و الإثبات (للأدلة) للولايات المتحدة الأمريكية FRE⁽¹⁾ الأدلة ذات صلة بأنها " الأدلة التي لها هدف جعل أي وقائع كنتيجة لتحديد الإجراءات الأكثر أو أقل احتمالاً من عدم وجود أدلة"⁽²⁾.

بينما عرفت المنظمة العالمية لدليل الكمبيوتر الأدلة ذات الصلة على النحو التالي⁽³⁾:

أ- الدليل الرقمي الأصلي: هو الدلائل المادية والأشياء المحتوية على بيانات متعلقة بالأشياء عند الضبط.

ب- الدليل الرقمي المزوج: هو نتاج الكتروني دقيق لكل الأشياء الحاملة للمعلومات و الموجودة بشكل مادي أصلي.

ت- النسخة: هي ناتج دقيق من المعلومات الموجودة في الدليل المادي الأصلي بصرف النظر عن الدلائل المادية الأصلية.

ثالثاً - التمييز بين الدليل الرقمي و البرنامج المعلوماتي:

يتفق المصطلحان في أن كليهما يعدّ آثاراً معلوماتية أو رقمية ، لأن البيانات داخل الحاسب الآلي سواء كانت في شكل نصوص أو أحرف، أم أرقام، رموز، أصوات، أو صور تتحول إلى طبيعة رقمية، ترتكز على تقنية الترقيم قوامها الرقمان (صفر، واحد) إلا أن الفرق بين الدليل الإلكتروني وبرنامج الحاسوب⁽⁴⁾ يكمن في الوظيفة التي يؤديها كل واحد منهما، فالبرنامج له دور

(1) أنشأ الباحثون القانونيون لوزارة الخارجية الأمريكية في عام 2004 قواعد اتحادية للعدل و الإثبات ، مما خلق بلبلة في الأحكام القانونية بشأن القضايا الجنائية التي تشمل الأدلة الرقمية ،مما نجم عنه اختلاف في الآراء و الأحكام ، ومع تحديث 2006 حاولت وزارة العدل تصحيح المشكلة من خلال تركيب كيسي وكبير ووجهات نظر معاصرة في الطب الشرعي و الأدلة الرقمية.

(2) **Jesus Borrego**, The Impact of Acceptance of Electronic Evidence before and after the 2006 Federal Rules of Evidence on Criminal Cases. Dissertation Submitted in Partial Fulfillment of the Requirement for the Degree of Doctor of Philosophy, Walden U.S.A University May 2010, p 37.

(3) مصطفى محمد موسى، المرجع السابق، ص 214-215.

(4) وردت تعريفات مضيفة للبرنامج المعلوماتي وأخري موسعة له فالتشريع الفرنسي على غرار المشرع الياباني أخذ بالتعريف الواسع للبرنامج وهو ما يتضح من القرار الوزاري الفرنسي المؤرخ في 1981/11/22 حينما عرفه بأنه "مجموعة الخطوات و الإجراءات التي تهدف إلى تشغيل نظام متكامل لأنظمة المعالجة المعلوماتية وتوظيفها وفقاً لهذا الغرض الذي من أجله

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

في تشغيل الحاسوب وتوجيهه إلى حل المشاكل ووضع الخطط المناسبة، وبدونها يبقى الحاسوب آلة صماء، بل توجد برامج خاصة تساهم في استخراج الدليل المعلوماتي.

أما الدليل المعلوماتي له أهمية ودور أساسي في معرفة كيفية حدوث الجريمة المعلوماتية بهدف إثباتها ونسبتها إلى مرتكبيها، سيما في البيئة الافتراضية، حيث يمكن تفتيش محتوى القرص الصلب لمعرفة كل المراحل التي مر بها المجرم المعلوماتي وهو في سبيل تحقيقه للهدف الإجرامي⁽¹⁾.

لذلك فإن التحفظ على قطع صلبة لحاسوب مسروق مثلا لا يعني أننا بصدد دليل رقمي وإنما نكون في مواجهة دليل مادي وهو ما يسري على الأقراص المرنة الليزرية ، بينما الحال غير ذلك إذا كان التحفظ على اسطوانة تحتوي على ملفات تتضمن أرقام كروت الائتمان مصرفية أو أرقام دخول سرية لمواقع أو صفحات أو بريد إلكتروني أو كود دخول إلى برمجيات في التداول فكلها تعتبر أدلة رقمية يستلزم التحفظ على القرص لأنه يشكل البيئة التي يعيش فيها الدليل الرقمي⁽²⁾.

الفرع الثاني : خصائص الدليل الرقمي.

بعد استقراء أهم التعريفات الواردة بشأن الدليل المعلوماتي يمكن لنا أن نستخلص مجموعة من الخصائص المستندة أساسا إلى طبيعة الدليل وبيئته ، ويمكن تقسيم الخصائص إلى قسمين الأول يتضمن الخصائص الايجابية للدليل المعلوماتي أما الثاني فيتضمن الخصائص السلبية للدليل.

أولا- الخصائص الايجابية للدليل الرقمي: تجمل الخصائص الايجابية في العناصر التالية:

أ- الدليل الرقمي دليل علمي:

وضع هذا البرنامج ". و هو ما ذهب إليه المشرع المصري على عكس التعريف الضيق الذي جاء به المشرع الأمريكي و كذا الاتفاقية الأوروبية بودابست 2001. أنظر أيمن عبد الله فكري المرجع السابق، ص من 56 إلى 59.

(1) أنظر عائشة بن قارة مصطفى، المرجع السابق، ص من 56 إلى 58.

(2) البيئة التي يحيا فيها الدليل الرقمي هي الحيز الافتراضي وهي بيئة المكان الافتراضي و الزمان الافتراضي ممثلة في الأقراص بأنواعها بالإضافة إلى معالجات حركة البرامج و الذاكرة وكل قطعة يمكن لها أن تقوم بدور في هذا الشأن بما في ذلك القطع المرنة التي لا يعمل الحاسوب بدونها . انظر عمر بن محمد يونس، ندوة الدليل الرقمي للمنظمة العربية للتنمية الإدارية المنعقدة في مقر جامعة الدول العربية القاهرة في الفترة الممتدة من 05-08 مارس 2006، ص 06.

إذا كان الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة " إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة"، ولا يتعارض مع القواعد العلمية السليمة، ولا عن منطقته فكذلك الدليل المعلوماتي له نفس الطبيعة لأنه يتكون من المعطيات، و المعلومات في هيئة الكترونية غير ملموسة لا تدرك بالحواس العادية يحتاج إلى مجال علمي يتعامل معه، فلا يخرج عمّا توصل إليه العلم الرقمي وإلا فقد معناه⁽¹⁾.

ب- إمكانية نسخ الدليل الرقمي:

يمكن نسخ الدليل الرقمي نسخة مطابقة للأصل تماما، بحيث يمكن إجراء الفحص المعلوماتي على هذه النسخة لتفادي خطر إتلاف النسخة الأصلية أثناء عملية الفحص، وهذه الميزة لا تتوفر في الأدلة التقليدية⁽²⁾. وفي هذا السياق قام المشرع البلجيكي بمقتضى قانون 28 نوفمبر 2000 بتعديل قانون التحقيق الجنائي بإضافة المادة (39 bis) التي تسمح بضبط الأدلة الرقمية مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية⁽³⁾.

ت- إمكانية كشف التغيير الحاصل على الدليل الرقمي:

يمكن التعرف على الأدلة الرقمية المزورة أو التي جري تحريفها أو حتى تعديلها بمضاهاتها مع الأدلة الأصلية بالقدر الذي لا يدع مجالاً للشك⁽⁴⁾، وذلك باستخدام برمجيات معينة معدة للغرض، لأن الدليل الرقمي قد يتعرض إلى تعديل مقصود من قبل الجاني، أو غير مقصود من طرف المحقق أو الخبير المعلوماتي أثناء جمع الدليل⁽⁵⁾.

ث- صعوبة التخلص من الدليل الرقمي:

(1) رشيدة بوكر، المرجع السابق، ص 387.

(2) محمد طارق عبد الرؤوف الحنّ، المرجع السابق، ص 342.

(3) عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري، المرجع السابق، ص 15.

(4) محمد أمين البشري، الحلقة العلمية الانترنت و الإرهاب، المرجع السابق، ص 26.

(5) محمد طارق عبد الرؤوف الحنّ، المرجع السابق، ص 343.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

تعد هذه الخاصية من أهم الخصائص المميزة للدليل المعلوماتي على الإطلاق مقارنة بالأدلة التقليدية التي يمكن التخلص منها، مع استحالة استرجاعها، أما بالنسبة للأدلة التقنية فيسهل استرجاعها بعد حذفها⁽¹⁾ وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، وتعتبر هذه الميزة شبيهة بالدليل العلمي المتعلق بالحمض النووي DNA إذ لا يمكن التخلص منهما، ومن ناحية أخرى يمكن إحداث تعديل في تكوينهما. ويضاف إلى ذلك أن نشاط الجاني لمحو الدليل يسجل أيضا في الكمبيوتر كنسخة للفعل يمكن استخلاصه لاحقا كدليل إدانة⁽²⁾.

ج- الطبيعة الرقمية الثنائية (0-1) للدليل الرقمي:

يتشكل الدليل المعلوماتي من تعداد غير محدود لأرقام ثنائية موحدة في الواحد والصفير، و التي تتميز بعدم تشابهها فيما بينها بالرغم من وحدة الرقم الثنائي الذي تتكون منه، فالكتابة مثلا في العالم الرقمي ليس لها الوجود المادي الذي نعرفه في شكل ورقي، وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي، فأى شيء في العالم الرقمي يتكون من الصفير و الواحد، وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة، و أما تكوين معطياته فإنها تختلف من حيث الحجم و الموضوع، إذ كمية (0 - 1) تختلف في حجمها من ملف لآخر⁽³⁾.

ثانيا- الخصائص السلبية للدليل الرقمي: بعدما تطرقنا للخصائص الايجابية للدليل ننتقل إلى معرفة أهم الخصائص السلبية من منظور المواجهة.

أ- الدليل الرقمي غير مرئي:

(1) من القضايا التي أبرزت هذه الميزة أنه أثناء التحقيق مع الكولونيل "أوليفر نورد" في قضية إيران عام 1986 ، تم استعادة جميع الرسائل الالكترونية المتعلقة بالجريمة، بعد أن قام بحذفها من حاسوبه، إذ لم يكن يعلم بأن هذه الرسائل يمكن استعادتها عن طريق النسخ المحفوظة في النظام. محمد طارق عبد الرؤوف الحنّ، المرجع السابق، ص 344.

(2) عائشة بن قارة مصطفى، المرجع السابق، ص 62-63.

(3) رشيدة بوكور، المرجع السابق، ص 390.

ليس للدليل المعلوماتي طبيعة مادية ملموسة كما هو الحال في الأدلة التقليدية، فكل ما تنتجه التقنية هو عبارة عن نبضات الكترونية يمكن أن تدل في مجموعها على أنماط السلوك الإنساني والواقع أن هذه الطبيعة غير المرئية للدليل المعلوماتي تلقي بظلالها على أجهزة الضبط القضائي التي تتعامل مع هذه الجرائم المستحدثة، لأن غياب الدليل المرئي يشكل عقبة كبيرة أمام كشفها⁽¹⁾.

ب- تواجد الدليل المعلوماتي ضمن حجم كبير من البيانات:

يحتوي القرص الصلب مثلا على حجم كبير من البيانات و المعلومات غير المرتبة من ضمنها جزء صغير يتعلق بالدليل المعلوماتي ،ويمكن تشبيه حجم المعلومات بموجات الراديو الموجودة في الهواء و التي تحتوي على بيانات متشابكة ما يشكل عائقا في معرفة الإشارة المطلوبة وترجمتها إلى بيانات مطلوبة ، فالوصول إلى الدليل المعلوماتي يشكل تحديا أمام الخبير المعلوماتي⁽²⁾.

ت- الدليل المعلوماتي دليل ظرفي:

الدليل الرقمي هو عادة دليل ظرفي ،فمعرفة عنوان الانترنت مثلا يشير إلى الحاسوب الذي ارتكبت الجريمة بواسطته فقط ،دون أن يحدّد مرتكبها بالذات ، الأمر الذي يجعل من الصعوبة بمكان نسبة النشاط الجرمي إلى شخص ما، ما لم يتم القيام بالعديد من التحقيقات للتأكد من ذلك⁽³⁾.

ث- صعوبة استخلاص الدليل المعلوماتي:

إن استخلاص الدليل المعلوماتي يتطلب تكوين وتخصص مسبق يتيح لأجهزة إنفاذ القانون القدرة على تتبع آثار الجريمة في المجال الافتراضي لاستخلاص الدليل، ما يسمح في كثير من الأحيان إتلاف الدليل المعلوماتي أو صعوبة تحصيله.

(1) محمد طارق عبد الرؤوف الحنّ، المرجع السابق، ص 344.

(2) محمد طارق عبد الرؤوف الحنّ، نفس المرجع ، ص345.

(3) محمد طارق عبد الرؤوف الحنّ، نفس المرجع ، ص345.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

ففي هذا الإطار تم خلال سنة 2007 تدعيم مخابر الشرطة العلمية و التقنية بأقسام متخصصة في الأدلة المعلوماتية على مستوى المخابر الثلاثة المتواجدة بكل من وهران، وقسنطينة، و العاصمة تكمن مهامها في استغلال الأجهزة الالكترونية التي يشتبه استعمالها في ارتكاب الجرائم بهدف استخراج الأدلة المعلوماتية⁽¹⁾.

ج-التطور المستمر لتقنيات الدليل المعلوماتي:

يترتب على هذه الخاصية عدم إمكانية حصر البرامج التي من شأنها كشف الدليل المعلوماتي نظرا للتطور المتواصل للتقنية المعلوماتية، ما يجعل الجاني المعلوماتي يتفوق أحيانا على أجهزة التحقيق لعدم مسايرتها للتطور الحاصل في حينه .

لذلك أصبح من الضروري إجراء دراسة متأنية للتغيرات القاعدية في مضمون المستخدمين فمثلا توفر اتصالات الكترونية ذات تدفقات عالية وموزعات الكترونية لها تأثير على طريقة تخزين البيانات، فسابقا كان المحققون يضبطون الأدلة بمقر إقامة المتهم، أما اليوم فيجب عليهم أن يأخذوا بعين الاعتبار واقعة أن الملفات يمكن تخزينها ماديا في الخارج وتسمح للجاني بدخولها عن بعد، لذلك فالتطور متزايدة في التخزين ما يطرح صعوبات جديدة على المحققين التفكير فيها⁽²⁾.

الفرع الثالث: تقسيمات الدليل الرقمي.

يأخذ الدليل الرقمي عدة صور بالرغم من انه لم يتم بعد تبني تصنيف موحد لأنواع الدليل المعلوماتي، لا على مستوى الفقه، ولا على مستوى القوانين المقارنة، وهذا لا ينفى وجود محاولات فقهية وتجارب تشريعية وقضائية وهو ما سنتناوله في العناصر الموالية.

أولا- تقسيم الدليل المعلوماتي في نظر الفقه و التشريعات المقارنة:

(1) مصطفى عبد القادر، الشرطة الوطنية ومكافحة الجريمة الالكترونية ، مداخلة مقدمة في الملتقى الدولي حول محاربة الجريمة المعلوماتية المنعقد بالجزائر في الفترة الممتدة 05-06 ماي 2010.مركز البحوث القانونية و القضائية،العدد 01 الإصدار 01 إيسان للنشر و التوزيع، الجزائر، 2011-2012.

(2) Marco Gercke, op cite p 243.

نتناول دراسة هذا العنصر من خلال وجهين الأول يمثل نظرة فقهية والآخر يمثل التشريعات المقارنة.

أ- تقسيم الدليل الرقمي في نظر الفقه:

لم يتفق فقهاء القانون الجنائي في وضع تقسيمات موحدة للدليل المعلوماتي نظرا للحدثة النسبية للدليل و تطوره المستمر، إذ ذهبت إحدى المحاولات الفقهية إلى تقسيم الدليل الالكتروني بشكل يتناسب مع التقسيم الفقهي للجرائم عبر الكمبيوتر، إلا أن هذا الأمر لا يتناسب مع التقنية الحديثة، بسبب أن هذا التقسيم استند إلى الاختلاف في المصطلحات مثل شبكات الانترنت والكمبيوتر وبروتوكول تبادل المعلومات والشبكة العالمية للمعلومات، لكن في الحقيقة ليس هناك اختلافا في المعنى الذي يبقى موحدا للدليل المعلوماتي⁽¹⁾، و هو ما يدفعنا إلى البحث عن تقسيمات أخرى.

ب- تقسيم الدليل الرقمي في التشريعات المقارنة:

على مستوى التشريعات المقارنة فإنه لا يوجد في أوروبا نصوص مشتركة موحدة تنظم الأدلة الرقمية وهو ما يشكل فجوة معتبرة لأن الجريمة المعلوماتية دولية والأدلة الرقمية قد تجتمع في دولة ما أحكامها التشريعية تختلف عن الدولة المرسل إليها و التي لا تقبلها إجراءاتها بدورها، ما يحتم اتخاذ رد فعل سريع بخصوص هذه المسألة بعد تأمين المزايا الإجرائية⁽²⁾.

ولعل التجربة الأمريكية هي الأحسن نموذجا من حيث تقسيمات الدليل المعلوماتي إذ قامت وزارة العدل الأمريكية سنة 2002 بتقسيمه إلى ثلاث مجموعات⁽³⁾:

1- السجلات المحفوظة في الحاسوب.

(1) عائشة بن قارة مصطفى، المرجع السابق، ص من70 إلى73.

(2) Myriam Quéméner et Joël Ferry, cybercriminalité Défi mondial 2è édition ,Ed ECONOMICA PARIS 2009 ,p253.

(3) عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماوي، المرجع السابق، ص 14.

2- السجلات التي تم إنشاؤها بواسطة الحاسوب.

3- السجلات التي جزء منها تم حفظه بالإدخال وجزء آخر تم إنشائه بواسطة الحاسوب.

في حين أن التقسيم الذي نتطرق إليه بشيء من الشرح مرده محتوى الدليل الرقمي.

ثانيا- تقسيم الدليل الرقمي حسب المحتوى:

يصنف الدليل الرقمي حسب هذا التقسيم إلى أدلة مكونة من طرف الحاسوب نفسه وأدلة مخزنة رقميا من طرف الأفراد.

أ- الدليل المكون من طرف الحاسوب:

يقوم الحاسوب بتكوين محتوى الدليل الرقمي Computer Generated Evidence في إشارة إلى تكوين محتواه رقميا دون تدخل للفرد في هذا التكوين⁽¹⁾، ذلك أنه تعتبر من الأدلة التي لم تعد لتكون وسيلة إثبات يترك الجاني أثره دون أن يرغب في وجوده وتسمي بالبصمة الالكترونية تضبطها التقنية آليا ولو بعد فترة زمنية من نشوءها⁽²⁾.

إذ يقوم الحاسوب بتكوين مخرجات حركة البرامج⁽³⁾ التي تتخذ الطبيعة الرياضية الجبرية Algorithm والذي يسيطر عليها تحديدا ليس مستخدم الحاسوب أو الجاني وإنما الحاسوب ذاته حين استقباله للبرمجيات التي تعمل على تشغيله وتفاعله، فمثلا في الإنترنت يكون مزود خدمات الانترنت ISP هو المسيطر تحديدا بحيث يسمح لنا بدخول الانترنت واستعمالها، ولمعرفة زمن دخول الجاني إلى الانترنت فإنه لا يتم اللجوء إلى حاسوب المستخدم في العادة وإنما يتم اللجوء إلى مزود الدخول إلى الانترنت، وتساهم مخرجات حركة البرامج في جرائم المعلوماتية في إقامة

(1) عمر بن محمد يونس، المرجع السابق، ص 05.

(2) خالد عياد الحلبي، المرجع السابق، ص 234.

(3) ومن أمثلة مخرجات حركة البرامج كمحتوي الكتروني نجد الجداول الحوارية Dialogue Box التي تظهر متضمنة في موضوعها إشارات أو تعليمات أو تنبيهات لمستخدم الحاسوب أو لعضو الانترنت عند إبحاره في العالم الافتراضي، وكذلك الحال في التعليمات التي تظهر عند فتح البريد الالكتروني، وتعد أيضا من قبيل المحتوى الالكتروني البرامج التي يتم إعدادها لحركة البرمجيات في العالم الرقمي و التي تتخذ في إطار تكوينها نظام برمجي له طابع المجانية إذا قام مالكه بنشر مصدر الكود وتبين انه مبتكره حقا.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

العلاقة بين السلطات و بين الجاني بالسرعة الكافية، ويمكن القول مثلا أن أفضل مكان لتعقب الهاكر، أو القرصان هو المزود المشترك فيه، ويتمثل دور التقنية في تكوين الدليل الرقمي بجعل إمكانية قيامه لا يبدو بالأمر المستحيل بل يبقى الأمر بعد ذلك فقط في مدى إمكانية قبوله أمام القضاء من منظوره القانوني⁽¹⁾.

ب- الدليل المخزن رقميا من طرف الأفراد:

وهي الأدلة التي أعدت لتكون وسيلة إثبات⁽²⁾ و يكون الفرد مسئولا عن تكوين هذا الدليل في بيئة تكنولوجيا المعلومات و الذي يعيش في بيئته الرقمية ويكون مخزنا رقميا Computer Stored-records في إشارة إلى تدخل الفرد في تكوين الملف أو مجموعة الملفات التي يتم تخزينها بالضرورة في الحاسوب لكونه يشكل بيئتها، و يأخذ تخزين البيانات في الحاسوب أحد شكلين:

- إما بيانات يتم استخدامها وفي هذه الحالة تظهر القوة الاستردادية للبيانات في شكل معلومات محددة.

- و إما بيانات يتم تخزينها دون استخدامها وفي هذه الحالة لا نكون بصدد مساحة مادية في القرص الصلب Hard Disk وإنما فقط مجموعة من الأرقام.

والمعيار المميز لهذه الملفات عن مخرجات حركة الحاسوب هو وجوب تدخل عامل الفرد الإنسان في تكوينها وبشكل مباشر⁽³⁾.

ثالثا - أشكال الدليل الرقمي:

تمثل مخرجات الحاسوب أشكال الدليل الرقمي فقد تكون إما في صورة مخرجات ورقية يتم الحصول عليها بواسطة الطابعات أو الرسومات، أو في شكل الكتروني مثل الأشرطة و الأقراص و

(1) عمر بن محمد يونس، المرجع السابق، ص 05.

(2) خالد عياد الحلبي، المرجع السابق، ص 234.

(3) عمر بن محمد يونس، المرجع السابق، ص 05.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

الدعائم الليزرية وغيرها من الأشكال الالكترونية، وإما يتم عرض المعلومات و البيانات المتعلقة بالدليل الرقمي عن طريق شاشة الحاسوب⁽¹⁾.

أما المشرع الجزائري فقد أورد في نص المادة 06 من القانون رقم 04/09 شكل الدليل الرقمي الجنائي بحيث يتم نسخ المعطيات محل البحث، و كذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية قابلة للحجز، أين حافظ المشرع على البيئة التي يتواجد فيها الدليل الرقمي، ثم وسع من أشكال الدليل حينما قرر إمكانية استعمال الوسائل التقنية لتشكيل وإعادة تشكيل المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، وفي هذه الحالة أعطي المشرع لسلطة التحقيق حرية تشكيل الدليل شريطة عدم المساس بمحتوي المعطيات.

المطلب الثاني

وسائل استخلاص الدليل الرقمي.

الإجراءات التي سنتناولها في هذا المطلب ستكون متماشية مع ما جاء به التشريع الجزائري خصوصا في القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، لذلك سنتناول مراقبة الاتصالات الالكترونية (الفرع الأول)، ثم التفتيش في المنظومة المعلوماتية (الفرع الثاني)، وأخيرا ضبط الدليل الرقمي (الفرع الثالث)، أما باقي الوسائل التقليدية التي تساعد في جمع الدليل كسماع الشهود، والاستجواب، والخبرة فقد تطرقنا إليها في الفصل الأول في إطار دراسة الإثبات بالوسائل التقليدية، لذلك فإننا نستكمل أهم الإجراءات القانونية التي تسمح باستخلاص الدليل الرقمي.

الفرع الأول: مراقبة الاتصالات الالكترونية.

هناك ضروبا من أعمال التفتيش فمنها ما يتم في إطار التفتيش التقليدي وفقا للإجراءات التقليدية ومنها ما نتج عن التقدم التقني الذي انتظم عالم المعلوماتية واستلزم تبني إجراءات جديدة

(1) محمد طارق عبد الرؤوف الحنّ، المرجع السابق، ص349.

تسمح بجمع الدليل بسبب عدم كفاية الوسائل التقليدية منها مراقبة الاتصالات الالكترونية⁽¹⁾ ولدراسة هذا الفرع ارتأينا التطرق إلى الأساس العلمي لمراقبة الاتصالات الالكترونية(أولا)، ثم التنظيم الإجرائي لمراقبة الاتصالات الالكترونية (ثانيا)، كل في إطار العملية الاتباتية للجريمة.

أولا - الأساس العلمي لمراقبة الاتصالات الالكترونية:

يطرح الأساس العلمي لمراقبة الاتصالات الالكترونية تساؤلات جمة أهمها كيف يمكن التعدي على خصوصيات الأفراد؟ والى أي حد تسمح التشريعات بانتهاكها وتحت أي مظلة؟ و هو ما سنتطرق إليه في العناصر الموالية.

أ- مراقبة الاتصالات الالكترونية بين الحظر و الإجازة:

تتمتع الاتصالات الالكترونية⁽²⁾ بحماية العديد من المواثيق والعهود الدولية باعتبارها حق أساسي من حقوق الإنسان حسب المواد (1 و5 و12) من الإعلان العالمي لحقوق الإنسان لعام 1948، والمادة (17/ف1 و2) من العهد الدولي للحقوق المدنية و السياسية لعام 1966، و المادة 17 من الميثاق العربي لحقوق الإنسان لعام 2004، و المادة 08 من الاتفاقية الأوروبية لحقوق الإنسان، و المادة 11 من الاتفاقية الأمريكية لحماية حقوق الإنسان لعام1969⁽³⁾.

ولقد حرصت الدساتير العالمية بمختلف أنواعها بتقرير حرية الخصوصية الشخصية، ومنها المؤسس الدستوري الجزائري حينما نص في المادة 39 من الدستور " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، و يحميها القانون.

سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة".

(1) سعدون بن محمد طويق العتيبي، المرجع السابق، ص 162.

(2) عرفها المشرع الجزائري في المادة02 من القانون 04/09 بأنها "أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".

(3) رشاد خالد عامر، المرجع السابق، ص 176.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

ويلاحظ على هذه المادة أن المؤسس الدستوري الجزائري أضي حماية مطلقة لسرية الاتصالات فلا يجوز انتهاكها، على عكس بعض الدساتير المقارنة التي أوردت استثناء على هذا المبدأ في حالة إجازة القانون ذلك، مثل الدستور المصري لعام 1971 و الدستور العراقي لسنة 2005 و التعديل الدستوري الرابع الأمريكي 1787، فكان عليه في تقديرنا إضافة هذا الاستثناء.

لأن مراقبة الاتصالات الالكترونية باختلاف أشكالها رغم كونها وسائل مثيرة للجدل القانوني حول مدى مشروعيتها، إلا أنه يسمح بها وفق ظروف معينة في جميع التشريعات المقارنة تقريبا فالقانون الفرنسي لعام 1991 يجيز اعتراض الاتصالات عبر شبكات تبادل المعلومات، وفي هولندا يجيز القانون لقاضي التحقيق التتصت على شبكات الاتصالات في حالة وجود جرائم جسيمة ارتكبتها المتهم وتشمل نقل البيانات، أما في الولايات المتحدة الأمريكية فيجوز اعتراض الاتصالات الالكترونية بما فيها شبكات الحاسب الآلي شريطة الحصول على إذن قضائي⁽¹⁾.

أما المشرع الجزائري بالرغم من ضمانه لسرية المراسلات و الاتصالات الخاصة بنص دستوري، وكذا بنصوص خاصة كقانون 03/2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، والمادة 137 من ق.ع.ج، إلا انه أجاز اعتراض المراسلات السلكية و اللاسلكية من خلال تنمة قانون الإجراءات الجزائية في الباب الثاني من الكتاب الأول بالقانون 22/06 المؤرخ 20 ديسمبر 2006 بفصل رابع بعنوان " في اعتراض المراسلات وتسجيل الأصوات والنقاط الصور "، ويشمل المواد من 65مكرر 05 إلى 65مكرر 10 في الجرائم الماسة بالمعالجة الآلية للمعطيات، وجسد المشرع هذا التوجه في مواجهة الجرائم المعلوماتية في القانون 04/09 حينما أورد في الفصل الثاني من هذا القانون بعنوان مراقبة الاتصالات الالكترونية و التي أجاز بموجبه في المادة 04 منه القيام بعمليات مراقبة الالكترونية في حالات محددة للوقاية منها.

ب- النطاق الموضوعي لمراقبة الاتصالات الالكترونية:

(1) أسامة بن غانم العبيدي ، بحث بعنوان التفتيش عن الدليل في الجرائم المعلوماتية، ، المجلة العربية للدراسات الأمنية و التدريب المجلد 29 العدد58، سنة 2013، ص 95 ، متاح على الموقع الالكتروني: www.nauss.edu.sa/Ar/pdf.

في إطار البحث عن الدليل الرقمي تطرح مسألة مراقبة الاتصالات الالكترونية حول طبيعة البيانات التي يتم تجميعها أثناء المراقبة الالكترونية هل يتم تجميع البيانات المتحركة أم حتى البيانات الساكنة.

لقد احتدم الخلاف بين الفقهاء في الولايات المتحدة الأمريكية حول هذه المسألة وانقسموا إلى اتجاهين، إذ يري الفريق الأول بأن إجراء المراقبة يرد على الاتصالات الالكترونية أثناء أو حال إجرائها لأنه لا يرد إلا على البيانات المتحركة، لأن البيانات الساكنة تكون قد تم تخزينها في الكمبيوتر الشخصي للمستخدم، أو في الخادم المعلوماتي لدى مزود الخدمات، أما الفريق الثاني فيري أن الإجراء يرد على جميع أنواع الاتصالات سواء كانت متحركة أو ساكنة⁽¹⁾.

أما موقف المشرع الجزائري من ذلك فيستشف من نص المادة 03 من القانون 04/09 لما أخذ بالاتجاه الأول حين نص بان الترتيبات التقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها يكون في حينها، ونحن نوافق هذا الاتجاه بيد أن النطاق الموضوعي للمراقبة الالكترونية ينصب على البيانات المتحركة فقط والتي لا يمكن تفتيشها ولا ضبطها إلا من خلال هذا الإجراء على عكس البيانات الساكنة التي تم تخزينها بحيث يمكن الوصول إليها بإجراءات أخرى كالتفتيش المعلوماتي بناء على إذن وهو اكفل لمشروعية الدليل المعلوماتي.

ثانيا- التنظيم الإجرائي لمراقبة الاتصالات الالكترونية:

بالنظر إلى أن المراقبة الالكترونية للاتصالات إجراء استثنائي لمساسه المباشر بخصوصية الأفراد الشخصية فقد سعت اغلب التشريعات الإجرائية لوضع مجموعة من القواعد القانونية المنظمة له، ومنها ما هو على شاكلة التفتيش التحقيقي ، والمشرع الجزائري بدوره ساير تطور الجريمة المعلوماتية إلى حد ما فعزز صلاحيات سلطة التحقيق في البحث عن الدليل من خلال هذا الإجراء باعتباره وسيلة هامة لمواكبة تطور الإجرام وبالمقابل أحاطه بضمانات قانونية تحد من تعسف السلطات العامة وتصون الحرية الفردية وهي:

(1) رشاد خالد عامر، المرجع السابق، ص 179.

أ- وجوب صدور إذن من السلطات المختصة:

يتفق الفقه الجنائي على أن المراقبة الالكترونية هي إجراء من إجراءات التحقيق وليس من إجراءات الاستدلال لمساسها الأفراد في أدق أسرار حياتهم الشخصية، فلا يحق للضبطية القضائية اللجوء إليه من تلقاء نفسها دون الحصول على إذن من الجهات المختصة⁽¹⁾. و المشرع الجزائري خول السلطة القضائية وحدها سواء وكيل الجمهورية أو قاضي التحقيق إذا كان الملف على مستوى التحقيق حق منح إذن للاعتراض على المراسلات السلكية واللاسلكية في الجرائم المعلوماتية بنص المادة 65مكرر 05 من ق.إ.ج وفي مراقبة الاتصالات الالكترونية بموجب المادة 04 من القانون 04/09.

ب- أن يكون الإذن الصادر بالمراقبة مكتوبا ومسببا ومحددا:

فلا يجوز إصداره شفاهة تحت طائلة عدم المشروعية فيجب أن يستند إلى أسباب مستساغة ومبررة، خصوصا في مسألة عدم توفر وسائل أخري بديلة يمكن اللجوء إليها لإثبات الجريمة يضاف إلى ذلك ضرورة تحديد نوعية الاتصالات المراد مراقبتها، والجهة المنفذة له، وهو ما أكد عليه المشرعين الأمريكي و الفرنسي⁽²⁾، وكذلك المشرع الجزائري في المادة 65مكرر 07⁽³⁾. كما نصت قواعد الحماية في التشريعات المختلفة الشمولية أو القطاعية على ضرورة حماية البيانات التي تم جمعها، وأوجه استخدامها مع توفير وسائل الأمن التقنية، وتحديد الأشخاص

(1) رشاد خالد عامر، المرجع السابق، ص 179.

(2) رشاد خالد عامر، نفس المرجع، ص 187.

(3) تنص المادة 65مكرر 07 على أن " يجب أن يتضمن الإذن المذكور في المادة 65مكرر 5 أعلاه، كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها و الأماكن المقصودة سكنية أو غيرها و الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها. يسلم الإذن مكتوبا لمدة أقصاها (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية."

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

المسموح لهم الاطلاع على البيانات والخضوع لرقابة الهيئات الموكل إليهم ذلك وهي القواعد المقررة لدى المنظمات و الهيئات الدولية والإفشاء خاصة الأوروبية⁽¹⁾.

ت- وجوب تحديد مدة مراقبة الاتصالات الالكترونية:

تحدد مدة مراقبة الاتصالات الالكترونية وجوبا حسب طبيعة الجريمة المعلوماتية، تفاديا لأي تعسف في استعمال السلطة وحماية لحقوق الأفراد الشخصية، و حددها المشرع الجزائري بأربعة أشهر قابلة للتجديد حسب نص المادة 65مكرر05 و65مكرر 07 من ق.إ.ج، واستثناءا لمدة 06 أشهر قابلة للتجديد في الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، إذ يمنح النائب العام لمجلس قضاء الجزائر إذنا حسب المادة 04 من القانون 04/09.

الفرع الثاني : التفتيش عن الدليل الرقمي.

نظمت القوانين الإجرائية أحكام التفتيش في إطاره التقليدي، باعتباره من إجراءات البحث عن الأدلة، وبظهور الأدلة الرقمية استتبع معه إعادة النظر في وسائل استخلاصه، مع تحيين الوسائل التقليدية لتعطي الشرعية الإجرائية لطرق جمعه، لذلك لا يمكن للمحققين تتبع آثار الجريمة في وقتها دون الاستعانة بالتفتيش المعلوماتي في صيغته الحديثة لوقوعه في عالم افتراضي بعيد العالم المادي، وباعتبار التفتيش المعلوماتي من أهم الوسائل في جمع الأدلة الرقمية نتطرق إلى تعريفه وتبيان خصائصه(أولا)، ثم مدى قابلية مكونات الحاسب الآلي للتفتيش (ثانيا)، و شروطه (ثالثا).

أولا- تعريف التفتيش المعلوماتي وخصائصه:

نخصص العنصر الأول في هذا القسم لتعريف التفتيش الرقمي، في حين العنصر الثاني لخصائصه.

أ- تعريف التفتيش المعلوماتي:

(1) بولين انطونيوس أيوب، الحماية القانونية للحياة الشخصية في مجال المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، 2009، ص 451.

التفتيش بصفة عامة هو إجراء من إجراءات التحقيق يهدف إلى التوصل إلى أدلة جريمة ارتكبت فعلا ، وذلك بالبحث عن هذه الأدلة في مستودع السر ، سواء أجري على شخص المتهم أو في منزله دون توقف على إرادته (1) ، أما التفتيش المعلوماتي فهو " الإطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز حاسوب أو نظمه أو الانترنت" (2) . وعرفه المجلس الأوروبي بأنه " إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني" (3) . أما تعريفنا المقترح هو "قيام أفراد مختصين بالبحث عن أدلة معلوماتية في بيئة معلوماتية خاصة بناءا على إذن من السلطات القضائية".

ب- خصائص التفتيش المعلوماتي: من خلال التعاريف السابقة يمكن لنا استخلاص أهم خصائص التفتيش المعلوماتي وهي(4):

- يحوي في مضمونه على قدر من الجبر والإكراه بتغطية قانونية تمس أسرار المتهم الشخصية الموجودة في حاسوبه أو في أنظمه المعلوماتية .

- أن التفتيش يعد قيذا على حصانة الشخص الذاتية ، ويعتبر قيذا على حرمة أسرار الشخص.

- أن التفتيش بصورته هذه يعد وسيلة للبحث عن الأدلة المادية والمعنوية للجريمة وضبطها لكشف الحقيقة.

ثانيا - مدى قابلية مكونات الحاسب الآلي للتفتيش:

نتطرق في هذا العنصر إلى مدى قابلية جميع مكونات الحاسب الآلي المادية منها و المنطقية وشبكاته إلى التفتيش بحثا عن الدليل الرقمي وهل أن هناك اختلاف حول هذه المكونات القابلة للتفتيش بالنظر إلى طبيعتها.

(1) فوزية عبد الستار، المرجع السابق، ص293.

(2) على حسن محمد الطويلة، التفتيش الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة، الطبعة الأولى ، عالم الكتب الحديث للنشر والتوزيع، سنة 2004، ص 12-13.

(3) على عدنان الفيل، المرجع السابق، ص 39.

(4) على حسن محمد الطويلة، التفتيش الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة، المرجع السابق، ص 13.

أ- مدى قابلية المكونات المادية للحاسب الآلي للتفتيش:

يرتبط تفتيش المكونات المادية⁽¹⁾ للحاسوب (Hardware) بحسب مكان تواجده وفقا للأحكام العامة المقررة للتفتيش بمعنى هل هو من الأماكن العامة أو من الأماكن الخاصة، فإذا كان موجودا في مكان خاص كمسكن المتهم أو أحد ملحقاته فلا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش مسكنه وبنفس الضمانات و الإجراءات المقررة قانونا في التشريعات المختلفة، مع مراعاة التمييز بين ما إذا كانت مكونات الحاسبة المراد تفتيشها منعزلة من غيرها من الحاسبات الاخرى، أم أنها متصلة بها، أو بنهاية طرفية في مكان آخر كمسكن غير المتهم، فإذا كانت كذلك وكانت هناك بيانات مخزنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة تعين مراعاة القيود والضمانات التي يستلزمها المشرع لتفتيشها⁽²⁾.

إلا أن المشرع الجزائري استثنى هذه الضمانات المقررة للتفتيش في الجرائم المعلوماتية حينما أجاز في المادة 03/47 من القانون 22/06 المعدل لقانون الإجراءات الجزائية إجراء التفتيش في كل محل سكني، أو غير سكني في كل ساعة من ساعات الليل، أو النهار وذلك بناء على إذن مسبق من وكيل الجمهورية، ولعل الحكمة من ذلك هو تغليب مصلحة المجتمع على الفرد بالنظر إلى طبيعة الأدلة المعلوماتية التي يمكن إتلافها في زمن قياسي خصوصا إذا كنا أمام مجرم معلوماتي محترف ما يتحتم التدخل بصفة مستعجلة⁽³⁾.

أما بالنسبة للأماكن العامة فإذا وجد شخص وهو يحمل مكونات الحاسب المادية، أو كان حائزا لها أو مسيطرا عليها فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات و القيود المنصوص عليها قانونا⁽⁴⁾.

ب- مدى قابلية المكونات المنطقية للحاسب الآلي للتفتيش:

(1) تشمل:- وحدة الإدخال- وحدة الذاكرة الرئيسية - وحدة الحساب و المنطق- وحدة التحكم - وحدة الإخراج- وحدات التخزين الثانوية.

(2) عدنان علي الفيل، المرجع السابق، ص 41.

(3) عائشة بن قارة مصطفى، المرجع السابق، ص 89-90.

(4) أسامة بن غانم العبيدي، المرجع السابق، ص 89.

انقسم الفقهاء ومعهم التشريعات المقارنة في تبني عدة آراء بشأن جواز تفتيش المكونات المعنوية للحاسوب، لكن وكما فعل الفقه بشأن تكييف الجريمة المعلوماتية ومحاولة تحديد مسارها القانوني فعل كذلك مع تفتيش المكونات المنطقية تمهيدا لضبط الأدلة المعلوماتية.

فذهب الاتجاه الأول: إلى عدم انطباق أحكام التفتيش والضبط في القانون الإجرائي مع ما قد يتطلبه جمع الأدلة المعلوماتية، فهناك جانب من التشريعات الإجرائية حددت هدف التفتيش في البحث عن "شيء" وهو يقتصر بمفهومه على المال ذي الحيز المادي المحسوس ولا يمتد إلى الكيانات المنطقية، لأن الأصل في الأشياء مادية ومن الدول من ذهب إلى حماية هذه الكيانات المنطقية عبر قوانين الملكية الفكرية⁽¹⁾.

ومنهم من اقترح مواجهة هذا القصور التشريعي بتعديل النصوص الخاصة بالتفتيش بما يناسب البحث في الوسط الافتراضي وضبط بيانات الحاسوب وبهذا الاتجاه أخذ المشرع الانجليزي في قانون إساءة استعمال الحاسوب لسنة 1990، وهو ما نصت عليه كذلك اتفاقية بودابست لسنة 2001 في المادة 1/19-3⁽²⁾.

وكذلك المشرع الفرنسي عندما عدل نصوص التفتيش بإضافته لعبارة "المعطيات المعلوماتية" في المادة 94 من قانون الإجراءات الجزائية الفرنسية، والمادة 42 من القانون 2004-545 المتعلق بالثقة في الاقتصاد الرقمي⁽³⁾.

- **بينما ذهب الاتجاه الثاني:** إلى أن بعض القوانين الإجرائية تنص على إصدار الإذن بضبط "أي شيء"، وبالرغم من الإشارة الصريحة للنص بأن الذي يمكن ضبطه في الجرائم المعلوماتية هو الوعاء المادي للبيانات، مثل الأقراص الصلبة، أو المرنة فإن الفقه يفسرها بشكل أوسع إلى حد يسمح بتفتيش وضبط الكيانات المنطقية للحاسوب⁽⁴⁾، مستندا في ذلك إلى مقارنتها بالعلوم

(1) على حسن محمد الطرابلسية، التفتيش الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة، المرجع السابق، ص 30.

(2) خالد عياد الحلبي، المرجع السابق، ص 241.

(3) رشيدة بوكور، المرجع السابق، ص 398-399.

(4) على حسن محمد الطرابلسية، التفتيش الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة، المرجع السابق، ص 31.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

الطبيعية التي تعرف المادة بأنها كل ما شغل حيزا ماديا في فراغ معين، وان الحيز يمكن قياسه و التحكم فيه والكيانات المنطقية تشغل حيزا في ذاكرة الحاسوب يمكن قياسه بمقياس معين، كما أن الكيانات أيضا تأخذ شكل نبضات الكترونية على شكل صفر، وواحد تشبه في كيانها المادي التيار الكهربائي الذي اعتبر في كثير من التشريعات كيان مادي ومن ثمة تصلح لأن تكون محلا للضبط⁽¹⁾.

- أما الاتجاه الثالث: فهو اتجاه توافقي يري ضرورة إهمال الجدل الدائر حول مصطلح الشيء و العبرة عنده بالواقع، فالضبط عمليا لا يمكن وقوعه إلا على أشياء مادية، ومن ثمة المشكلة تتعلق بإمكانية اتخاذ الإجراء وترتيبها على ذلك فان التفتيش في الوسط الافتراضي يكون صحيحا إذا أسفر عن وجود بيانات اتخذت فيما بعد شكلا ماديا، وهذا الاتجاه اخذ به قانون الإجراءات الألماني في القسم 94⁽²⁾.

بين هذه الآراء الفقهية وضع المشرع الجزائري حدا للجدل الفقهي، حينما نص صراحة في المادة 01/05 من القانون 04/09⁽³⁾ على جواز تفتيش المنظومة والمعطيات المعلوماتية للوقاية من الجرائم المعلوماتية، تجريه السلطات القضائية، وكذا ضباط الشرطة القضائية، وفقا للقواعد المقررة للتفتيش في قانون الإجراءات الجزائية الجزائري، وفي الحالات المنصوص عليها في المادة 04 من نفس القانون، وبحسب للمشرع الجزائري هذه المواكبة التشريعية في إطار مكافحته للجريمة المعلوماتية مقارنة مع التشريعات العربية، علما أن المشرع السوري سار على نفس الاتجاه بنصه في المادة 02/26 من المرسوم التشريعي رقم 17-2012 المتعلق بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية بجواز تفتيش البرمجيات وضبطها باعتبارها من الأشياء المادية.

(1) على عدنان الفيل، المرجع السابق، ص 43.

(2) خالد عياد الحلبي، المرجع السابق، ص 242.

(3) تنص المادة 01/05 من القانون 04/09 على انه "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى: أ-منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها. ب-منظومة تخزين معلوماتية."

ت- مدى خضوع شبكات الحاسب الآلي للتفتيش " التفتيش عن بعد " :

مما لا شك فيه أن طبيعة التقنية الرقمية زادت من الصعوبات التي تواجه القائمين على التفتيش المعلوماتي فالبيانات التي تحتوي على أدلة قد تتوزع عبر شبكات الحاسب الآلي (1) في أماكن قد تكون على مسافات بعيدة عن الموقع المادي الذي يتم فيه التفتيش، كما قد يكون الموقع الفعلي للبيانات و المعلومات يدخل ضمن الاختصاص القضائي لدولة أخرى، ما قد يعقد صعوبات جمع الأدلة المعلوماتية ويزيد من أهمية التعاون الدولي في هذا المجال (2). لذلك نفرق بين حالتين للتفتيش عبر شبكات الحاسوب:

1- تفتيش شبكة معلوماتية داخل القطر الوطني:

يثار التساؤل حول مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الجهاز أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص آخر. يرى الفقه الألماني إلى إمكانية امتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الألماني، وهو ما ذهب إليه المشرع البلجيكي في المادة 88 من قانون تحقيق الجنايات البلجيكي (3). وكذا المشرع الفرنسي في تعديله لقانون الإجراءات الجزائية المكرس بالقانون رقم 239-2003 الذي أجاز للضبطية التفتيش في أي نظام معلوماتي عبر الجهاز الرئيسي (4).

أمام هذه التطورات التشريعية قام المشرع الجزائري بدوره على النص بجواز تفتيش شبكات الحاسوب ولو عن بعد ضمن قانون 04/09 من خلال الفصل الثالث منه، بعنوان القواعد الإجرائية ومنها تفتيش المنظومات المعلوماتية ، بحيث تنص المادة 02/ 05 منه على أن " في الحالة

(1) تعرف شبكات الحاسب بأنها " مجموعة أجهزة يتصل بعضها ببعض عن طريق وسائل اتصالات بواسطة برامج تحقق إنسيابا وتدفقا وتبادلا للبيانات" على حسن محمد الطرابلسية، التفتيش الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة، المرجع السابق ص 42.

(2) أسامة بن غانم العبيدي، المرجع السابق، ص 91.

(3) خالد ممدوح إبراهيم، المرجع السابق، ص 203.

(4) رشيدة بوكري، المرجع السابق، ص 402.

المنصوص عليها في الفقرة "أ" من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها ،انطلاقاً من المنظومة الأولى ،يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطات القضائية المختصة مسبقاً". ويلاحظ أن المشرع وحرصاً منه على عدم ضياع الدليل المعلوماتي فإنه أجاز على وجه السرعة تفتيش المنظومة بشرط إعلام الجهات المختصة بغرض وضع تغطية شرعية للإجراء من خلال تمديد الإذن بالتفتيش لتلك المنظومة وهو ما سنتطرق إليه في حينه.

2- تفتيش شبكة معلوماتية تمتد إلى خارج القطر الوطني:

يطرح هنا حالة قيام المتهم بتخزين بياناته في أنظمة تقنية المعلومات خارج إقليم الدولة عن طريق إدراجها في شبكة الاتصالات البعيدة، ما يطرح مشكلة كيفية إجراء التفتيش لتحصيل الدليل⁽¹⁾، لأن تفتيش المنظومة عبر الحدود الجغرافية يطرح مسألة انتهاك سيادة دولة ويشكل جريمة معلوماتية في حد ذاتها وهي الدخول غير المشروع لمنظومة معلوماتية أو الاختراق المباشر.

ولأجل مواجهة هذه المشكلة ينبغي التماس طلب من السلطات الدولية الاخرى بنسخ البيانات المخزنة في الحواسيب الموجودة على أراضيها وفقاً لأسلوب التفويض و الالتماس، ويعاب على هذا الأسلوب انه يفتقر للفعالية نتيجة للإجراءات الروتينية التي تفضي إلى تأخر وصول الدليل وربما ضياعه إذا لجأ المشتبه فيهم إلى استعمال تقنية المفاتيح الساخنة أو أسلوب تسخين الأسلاك من أجل إتلاف الدليل وتدميره⁽²⁾.

(1) بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي سنة 2011، ص 81.

(2) موسي مسعود ارحومة ، بحث بعنوان الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية و القانون، منظم من طرف أكاديمية الدراسات العليا طرابلس خلال الفترة 2009/10/29-28 ص10-12.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

وبالمقابل تتفق اغلب التشريعات بضرورة التعاون الدولي و تتجسد أساسا في الاتفاقيات ذات الصلة، التي تترجم معاهدات التعاون القضائية، ولجان التحقيق، ومعاهدات تسليم المجرمين وبدخول هذه الاتفاقيات حيز التنفيذ تجري التحقيقات بالتنسيق مباشرة بين الدول، فمنذ توقيع اتفاقية بودابست حول الجرائم المعلوماتية كثير من الشركاء وضعوا شبكات للمكافحة ذات تكنولوجيا عالية تعمل على مدار الساعة بدون انقطاع، وتركز عملها على حفظ و إجراء خبرات سريعة على الأدلة الرقمية⁽¹⁾، بينما تجيز هذه الاتفاقية التفتيش و الضبط في شبكات تابعة لدولة أخرى بدون إذنها في حالتين، إذا تعلق التفتيش بمعلومات أو بيانات متاحة للجمهور، أو في حالة رضي صاحب البيانات بهذا التفتيش⁽²⁾، إلى ذلك لنتهت اللجنة الأوروبية للمشكلات الجنائية التابعة للمجلس الأوروبي إلى القول بان التفتيش و الضبط والإجراءات القسرية التي تقع على إقليم دولة أخرى تعتبر غير مشروعة إلا إذا كان القانون الدولي يجيزها⁽³⁾.

و المشرع الجزائري نص في المادة 03/05 من القانون 04/09 على انه يمكن التفتيش عن الأدلة المعلوماتية في دولة أخرى شريطة طلب مساعدة تلك الدولة وفقا لمبدأ المعاملة بالمثل ويلاحظ أن المشرع الجزائري ملتزم في قوانينه الداخلية بالحفاظ على الاتفاقيات الدولية واحترام سيادة كل دولة، في حين سمح المشرع السوري بتفتيش البرمجيات في أي مكان تتواجد بها في حدود الواقعة المسندة للمتهم فقط طبقا للمادة 03/26 من القانون 17-2012.

ثالثا - شروط تفتيش الأنظمة المعلوماتية:

تتلخص شروط تفتيش الأنظمة المعلوماتية باعتبارها الدعامة التي تضيء الشرعية على الإجراء التحقيقي لاستخلاص الدليل الرقمي في شروط شكلية وأخرى موضوعية والتي لا يصح التفتيش المعلوماتي بدونها.

(1) Alber Rees, communication sous titre «partage de la preuve électronique : coopération entre l'Algérie et les États-Unis d'Amérique» commis dans l'Actes du séminaire international Alger le 5-6 Mai 2010, op cite p199.

(2) علي عدنان الفيل، المرجع السابق، ص 47.

(3) شيماء عبد القتي محمد عطا الله، المرجع السابق. ص 304.

أ- الشروط الشكلية للتفتيش المعلوماتي: نجمع أهم الشروط الشكلية للتفتيش الرقمي فيما يلي:

1- وجوب حضور بعض الأشخاص أثناء إجراء التفتيش المعلوماتي: يعد هذا الشرط ضماناً لسلامة الإجراء في الجرائم التقليدية ومنه نص المشرعين الجزائري و الفرنسي على ضرورة حضور شاهدين أثناء حصول التفتيش سواء في الأماكن العامة أو الخاصة على عكس المشرع المصري الذي يفرق بين الحالتين، وبعد صدور القانون 22/06 عدل المشرع الجزائري في نص المادة 45 من ق.إ.ج.ج فأصبح التفتيش في الجرائم المعلوماتية استثناء يتم في غياب الشهود صونا لسرية جمع الدليل المعلوماتي⁽¹⁾.

2- وجوب تحديد وقت إجراء التفتيش المعلوماتي: الأصل أنه يحدد ميقات محدد لإجراء التفتيش، حرصاً على تضيق نطاق الاعتداء على الحرية الشخصية للأفراد، ولكن بالمقابل فإن المشرع الجزائري استثنى هذه الضمانة في المادة 10 من القانون 22/06، عندما نكون بصد التفتيش في البيئة الرقمية عن جرائم ماسة بأنظمة المعالجة الآلية للمعطيات، فإنه سمح بإجراء التفتيش في كل الأوقات إدراكاً منه بطبيعة الجرائم والأدلة المبحوث عليها⁽²⁾.

3- وجوب تحرير محضر بعد الانتهاء من التفتيش المعلوماتي: باعتبار التفتيش المعلوماتي من أعمال التحقيق فلا بد من تحرير محضر يثبت فيه ما تم من إجراءات، وما أسفر عنه التفتيش من أدلة، ويحرر بنفس الأشكال المقررة التي تستوجبها القواعد العامة في المحاضر عموماً، وليس له شكلاً معيناً، على أن يكون مكتوباً باللغة الرسمية ومؤرخ وموقع من القائم بالتفتيش، ومدون عليه كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها، ولا مانع في الاستعانة بخبير في مجال التقنية لصياغة مسودة محضر التفتيش بناء على ما تم تفتيشه⁽³⁾.

إن الملاحظ على الشروط الشكلية للتفتيش المعلوماتي أنها تتجاوز الشروط الشكلية للتفتيش و لا يمكن ضبطها في إطارها التقليدي لأن طبيعة الجريمة والدليل المعلوماتيين يشكلان إطاراً جديداً

(1) عائشة بن قارة مصطفى، المرجع السابق، ص 108-109.

(2) عائشة بن قارة مصطفى، نفس المرجع، ص من 110 إلى 112.

(3) عائشة بن قارة مصطفى، نفس المرجع، ص 112-113.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

للشروط الشكلية وأصبح من اللازم التفكير في تحديده بما يتناسب مع البحث عن الأدلة الرقمية وتحفظ الخصوصية الشخصية للأفراد.

ب- الشروط الموضوعية للتفتيش المعلوماتي:

تتضمن الشروط الموضوعية سبب إجراء التفتيش ثم محل التفتيش وأخيرا السلطات المختصة بالتفتيش المعلوماتي.

1- سبب إجراء التفتيش المعلوماتي:

يعني بسبب التفتيش "الواقعة المنشئة للسلطة في التفتيش" أي الواقعة التي تخول المحقق الحق في أن يصدر الأمر بالتفتيش⁽¹⁾.

ويستند التفتيش على وجود أسباب تجعل الجهات المختصة ملزمة بالتحرك لجمع وضبط الأدلة المعلوماتية لإثبات الجريمة، ومن بين هذه الأسباب يجب أن تكون هناك جريمة معلوماتية معاقب عليها قانونا، سواء كانت جنائية أو جنحة متلبس بها كما ينص على ذلك المشرع الجزائري في المادة 44 من ق.إ.ج، أو في المادة 05 من القانون 04/09 للوقاية من الجرائم المنصوص عليها في المادة 04 من نفس القانون. ويستوي هنا التفتيش لإثبات الجريمة المعلوماتية أو غيرها من الجرائم الاخرى.

ثم لا بد من توفر دلائل كافية تؤيد نسبة الجريمة المعلوماتية إلى شخص معين بوصفه فاعلا أو شريكا⁽²⁾، ويجب أيضا توفر أمارات وقرائن قوية مستمدة من تحريات جديفة تفيد وجود معلومات وأجهزة، أو معدات معلوماتية أو أشياء من شأنها أن تكون لها فائدة في ضبط الأدلة المعلوماتية⁽³⁾.

2- محل التفتيش المعلوماتي:

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الأول، المرجع السابق، 594.

(2) بكرى يوسف بكرى، المرجع السابق، ص 92.

(3) عائشة بن قارة مصطفى، المرجع السابق، ص 103.

ويقصد به تفتيش كل مكونات الحاسوب سواء كانت مادية أو معنوية أو شبكات الاتصال والتي توجد في حوزة شخص، أو تكون موضوعة في مكان له حرمة خاصة، بالإضافة إلى ضرورة وجود الأشخاص المتخصصين في تقنية المعلومات⁽¹⁾.

3- السلطة المختصة بالتفتيش المعلوماتي:

تختلف السلطات المكلفة بالتفتيش حسب اختلاف النظم الإجرائية، فوجد المشرع المصري مثلاً يخول النيابة العامة سلطة التفتيش بصفة أصلية، شأنه في ذلك شأن المشرع الأمريكي ولقاضي التحقيق بصفة استثنائية، أما المشرع الفرنسي فقد أناط الاختصاص الأصلي لقاضي التحقيق ولا يجوز للنيابة العامة إجراء التفتيش إلا في حالة التلبس، أو في حالات بعد موافقة قاضي التحقيق وفي إنجلترا تختص الشرطة بالتفتيش واستثناء في جرائم معينة النائب العام⁽²⁾.

أما المشرع الجزائري فاخذ بمبدأ الفصل بين وظائف التحقيق و الاتهام بمعنى أن التفتيش إجراء تحقيقي مخول لقاضي التحقيق للقيام به وأجاز للنيابة العامة حضوره استناداً إلى نص المادة 79 من ق.إ.ج، ويمتد اختصاصه إلى كامل التراب الوطني، كما يستطيع تكليف ضابط شرطة لإجراء التفتيش في أي مكان على امتداد التراب الوطني بموجب إذن مكتوب في جرائم المعالجة الآلية للمعطيات حسب المادة 47 من ق.إ.ج، و لوكيل الجمهورية استثناء أن يأذن للضبطية القضائية في حالات الجريمة المعلوماتية المتلبس بها لتقوم بإجراء التفتيش بحثاً عن أدلة الجريمة.

الفرع الثالث : الضبط المعلوماتي .

إن عمليات الضبط بمراحلها وتحليل الأدلة الرقمية المخزنة في شبكات المعلوماتية هي التحدي الذي يواجه أجهزة العدالة الجنائية في هذه المرحلة التي تعاني فيها تلك الأجهزة من الأمية المعلوماتية، ففي الوقت الذي تم فيه إعداد الخبراء و المختبرات الجنائية اللازمة للتعامل مع الأدلة

(1) على حسن محمد الطرابلسية، التفتيش الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة، المرجع السابق، ص 72-73.

(2) على حسن محمد الطرابلسية، نفس المرجع ، ص 90-91.

المادية برزت مشكلة الأدلة الرقمية الشيء الذي يتطلب معه استحداث مختبرات خاصة⁽¹⁾ وإعداد خبراء يجمعون بين المعرفة القانونية ومهارة التحقيق وعلوم تقنية المعلومات⁽²⁾، حفاظا على الأدلة الرقمية التي من شأنها إثبات وقوع الجرائم المعلوماتية وانسابها لمرتكبيها وتقرير حق المجتمع في العقاب، لذلك لا بد من التطرق إلى ما هي الأشياء المضبوطة في البيئة الرقمية؟ وما هي قواعد تحريزها وتأمينها فنيا؟

أولا- الأشياء المضبوطة في البيئة الالكترونية:

يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها، ويمكن أن يكون إجراء استدلال أو إجراء تحقيقي حسب طبيعته القانونية، وتحدد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضي الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق، بينما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة إجراء استدلال، والضبط بحسب طبيعته وتنظيمه القانوني عموما وغايته لا يرد إلا على الأشياء المادية⁽³⁾.

غير انه يختلف الضبط في الجرائم المعلوماتية عن الضبط في غير ذلك من الجرائم من حيث المحل، بسبب أن الأول يرد على أشياء ذات طبيعة معنوية وهي البيانات، ويأخذ هنا شكل اخذ نسخة من المعلومات الكائنة في الحاسوب، أو على دعامة مادية أخرى دون حاجة للحفاظ على النظام كله، والقوانين المقارنة تسمح بضبط المعلومات، منها قانون الإثبات في المملكة المتحدة البريطانية⁽⁴⁾، وكذا الفقرة الثالثة من المادة 1/57 من قانون الأمن الداخلي رقم 239 لسنة 2003 المعدل لقانون الإجراءات الجزائية الفرنسي التي تنص على نسخ المعلومات في دعامات

(1) أنشأ مكتب التحقيقات الفدرالي الأمريكي مختبرات لعلوم الحاسوب للطب الشرعي في جميع أنحاء الولايات المتحدة تسمى "المختبرات الإقليمية لكومبيوتر الطب الشرعي (RCFL) لدعم الحكومات الولائية و المحلية ،ويوفر مكتب التحقيقات الفدرالي التمويل الأولي ،التدريب، والمعدات ووكالات دعم القانون للموظفين العاملين في المختبر ،يدعم برنامج التحقيقات الجنائية في مجال مكافحة جرائم الانترنت وجرائم أخرى ،Jesus Borrego ,ibid ,p40.

(2) محمد الأمين البشري، الحلقة العلمية الانترنت والإرهاب، المرجع السابق، ص 28.

(3) عبد العال الديربي و محمد صادق إسماعيل، المرجع السابق، ص320.

(4) شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 357-358.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

تخزينية وتحريزها وختمها طبقا للقانون، وكانت اتفاقية بودابست لسنة 2001 قد نصت في المادة 03/19 من القسم الرابع منها على الضبط بقولها " من سلطة كل دولة طرف أن تتخذ الإجراءات التالية : أن تضبط نظام الكمبيوتر أو جزءا منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر وان تحافظ على سلامة تلك المعلومات"⁽¹⁾.

أما المشرع الجزائري فقد نص بدوره على حجز المعطيات كقاعدة إجرائية من خلال المادة 06 من القانون 04/09.⁽²⁾ واضعا الحد لكل جدل فقهي ومستكملا نظريته التشريعية المتطورة التي تتناسب مع طبيعة الجريمة المعلوماتية، ومن ثمة فإن الحجز المعلوماتي يعتبر نتيجة منطقية لتفتيش الأنظمة المعلوماتية إذا كانت مفيدة في كشف الحقيقة مستطرادا ذلك بضرورة نسخها في دعائم تخزين وحرزها حفاظا على سلامتها.

و المشكلات العملية التي تثور في ضبط المعطيات هو إمكانية حدوث تغييرات في البيانات عند نسخها بسبب صعوبة ضبط النسخة الأصلية، كما لو كانت هذه الأخيرة مسجلة في النظام أو متصلة بالشبكة، ومع ذلك يتعين ضبطها لأنها تتضمن عناصر إثبات الجريمة، ففي هذه الحالة يتعين إعمال مبدأ التناسب وهو اقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة بحيث لا يؤدي الضبط إلى تعطيل كل العمل في النظام و الشبكات المتصل بها، وقد قضت المحكمة الفدرالية الألمانية بإلغاء قرار الضبط ورد على 220ديسك بالإضافة إلى الوحدة المركزية بسبب مخالفتها مبدأ التناسب⁽³⁾.

(1) رشيدة بوكر، المرجع السابق، ص 420.

(2) تنص المادة 01/06 على انه " عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم او مرتكبيها وانه ليس من الضروري حجز كل المنظومة :يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في احرارز وفقا للقواعد المقررة في قانون الاجراءات الجزائية.

(3) شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 358-359.

و المشرع الجزائري تناول ضمناً مبدأ التناسب في المادة السابقة بقوله "وإنه ليس من الضروري حجز كل المنظومة" ويبقى العمل القضائي وحده كقيل بتناول كل هذه الجزئيات عند مناقشتها للدليل الرقمي.

أما بخصوص المكونات المادية للنظام فلا يثير ضبطها أي صعوبات ولها دور لا يستهان به في كشف الحقيقة، فيمكن ضبط المدخلات بما تشمله من مفردات كلوحة المفاتيح، نظام الفأرة نظام القلم الضوئي، أو ضبط عناصر تقنية منفصلة مثل الديسكات و الاسطوانات الممغنطة.

ثانياً - قواعد تحريز المضبوطات المعلوماتية وتأمينها فنياً:

يجب على سلطات التفتيش و الضبط المحافظة على البيانات المنسوخة أو المرفوعة بشكل متكامل وذلك بالتحفظ عليها في الحالة التي تم العثور عليها لحظة الضبط مع مراعاة القواعد التالية⁽¹⁾:

أ - ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخها:

يجب أن يرد الضبط على الدعائم الأصلية للبيانات، لأن الاكتفاء بضبط نسخ دون الأصل من شأنه وضع معوقات أمام إثبات صحة وسلامة النسخة المتحصل عليها، ويضر بسير التحقيق الجنائي من حيث عدم الاستمرار في النشاط التحقيقي.

ب - مراعاة ظروف تخزين الاحراز المعلوماتية:

يجب مراعاة درجة الحرارة والرطوبة أثناء تخزين الأقراص و الأشرطة الممغنطة والدعامات المحرزة بحث توفر درجة حرارة تتراوح بين 04 و32 درجة مئوية في حين تتراوح نسبة الرطوبة بين 20% إلى 80% وبهذه الشروط تصل مدة التخزين إلى ثلاث سنوات.

ت - تأمين نقل الاحراز المعلوماتية وحملها:

(1) عبد الله بن عبد العزيز بن عبد الله الخثعمي ، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية ، جامعة نايف العربية للعلوم الأمنية ، سنة 2011، ص من 115 إلى 117.

كي لا تتعرض الأحرار المعلوماتية أثناء نقلها أو حملها لصدمة متفاوتة قد تؤدي إلى إتلاف كلي، أو جزئي لمحتوياتها، فإنه يجب التحرز من المرور بها، أو تخزينها على مقربة من محطة إرسال لاسلكي، وكذلك يجب حفظها بعيد عن الغبار.

ث- تأمين البرامج المضبوطة قبل تشغيلها:

وذلك بعمل نسخ سليمة وكاملة منها كتأمين فني لتلفها.

ج-إحكام التسلسل الإجرائي للضبط:

وذلك ببيان تسلسل الإجراءات التي مرت بها البيانات المعلوماتية المضبوطة، منذ ضبطها حتى عرضها على القضاء، بذكر اسم من تولى إعداد وتجهيز دعائم البيانات و من تولى عملية التسجيل.

ح-تمييز المادة المضبوطة:

ويكون ذلك بوضع علامة مادية مميزة من قبل من كانت في حيازته، فعند نقل البيانات المخزنة داخل الحاسوب إلى أقراص أو أشرطة ممغنطة يجب على المحقق ومشغل النظام أن يسجل كل منهما اسمه وبياناته التعريفية على كل من اسطوانة الحاسب و الأقراص والأشرطة ذاتها ووضعها في علب مغلقة وتحريزها.

ثالثا- أسباب توثيق الأدلة الرقمية:

يكفل التوثيق مصداقية الأدلة الرقمية مثل غيرها من الأدلة المادية ويبعد عنها العيوب وتكمن أهمية التوثيق من ناحية إثبات الجريمة المعلوماتية في النقاط التالية⁽¹⁾:

(1) محمد أمين البشري، التحقيق في الجرائم المستحدثة، المرجع السابق، ص 244.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

أ- التوثيق يحفظ الأدلة الأصلية مصداقيتها ويضمن عدم تعرضها للتحريف أو التعديل (1) فمثلا يمكن الاستعانة بصورة مسجلة بالفيديو للتأكد من مدى صحة المناقشة الحية بين طرفين بمطابقة النص الرقمي مع النص المصور على الشاشة.

ب- الأشخاص الذين يقومون بجمع الأدلة عليهم الإدلاء بشهاداتهم حول مطابقة الأدلة التي قاموا بجمعها مع تلك المقدمة أمام المحكمة، و التوثيق هو الأسلوب الوحيد الذي يمكن المحققين من القيام بهذا الدور أمام القضاء ويعتبر فشل المحقق في التمييز بين أصل الدليل وصورته أمام القضاء سببا في بطلان هذا الدليل.

ت- من المهم توثيق مكان ضبط الدليل الرقمي في حالة إعادة تكوين الجريمة، إذ أن تشابه أجهزة الحاسب الآلي وملحقاتها يجعل من الصعب إعادة ترتيبها دون وجود توثيق سليم ومفصل يحدد الأجزاء و الملحقات وأوضاعها الأصلية بدقة .

ث- يشكل التوثيق جزءا من عمليات حفظ الأدلة الرقمية حتى انتهاء إجراءات التحقيق و المحاكمة إذ أن التوثيق يشمل تحديدا دقيقا للجهات التي تحتفظ بالأدلة وقنوات تداولها و التي ينبغي حصرها في نطاق محدود قدر المكان.

و عند توثيق الدليل يجب التأكد من، أين، كيف، متى، وبواسطة من تم ضبط الدليل و تأمينه.

لهذه الاعتبارات تظهر أهمية المختبرات الخاصة ودورها الهام في عملية إيجاد الدليل الرقمي، ففي الولايات المتحدة الأمريكية مثلا تبدأ عملية جمع الدليل المعلوماتي عندما تطلب وكالة تنفيذ القانون دعما من مختبر الطب الشرعي للكمبيوتر في شكل مذكرة يتم التأكد من شكل الطلب من الناحية القانونية لتفادي أي إشكال قانوني فيما بعد، وبعد التأكد من شرعية المذكرات يتم قبول الطلب وتأخذ المعدات إلى المختبر حيث تؤسم بشكل صحيح وتجرد للحفاظ على سلسلة الاحتجازات، تحمي المعدات بكتابتها لحمايتها من التغير ويتم إنشاء صورة ويتم نسخ الصورة إلى

(1) تستخدم رسالة التصنيف الحسابي لمضاهاة الأدلة الرقمية الأصلية مع النسخ للتأكد من صحتها وعدم تعرضها لأي تلاعب أو تحريف، وعند إدخال ملف الدليل الرقمي على رسالة التصنيف تظهر قراءة الملف بالحروف و الأرقام مطابقة لقراءة النسخ الصحيحة لنفس الملف.

شبكة محلية سرية قبل بدأ التحليل الشرعي، ويحتوي المختبر على مجالات تحليل منفصلة لأنظمة التشغيل المختلفة وعلى أنواع المعدات بما في ذلك المساعدات الرقمية الشخصية إضافة إلى توفر التقنيين المعينين لإجراء التحليل الطبي الشرعي، ويتم فحص المعدات خارج منطقة تخزين الأدلة ويتم إنشاء مداخل في السجل للحفاظ على سلسلة الاحتجازات، التقنيون فقط هم من لهم الحق في الدخول إلى المعدات، كل خطوة من التحليل يتم تسجيلها في السجلات الالكترونية وهذه السجلات تصبح جزءا من التقرير المقدم إلى الوكالة الطالبة عند الانتهاء من التحليل في قرص مضغوط أو قرص DVD.⁽¹⁾

المبحث الثاني

حجية الدليل الرقمي في إثبات الجريمة المعلوماتية.

إن الحدود الفاصلة بين حرية القاضي الجنائي في قبول الدليل وحرية في تقدير الدليل لا تزال مختلطة في نظر الفقه، سيما في فرنسا حيث يجمع معظم الفقهاء هاتين الحريتين معا لتشكيل في النهاية أمرا واحدا وهو ليس بصحيح فمسألة قبول الدليل ينبغي أن تحضي بدراسة خاصة و سابقة بالتحتم على دراسة حرية القاضي في تقدير الدليل لأن محل الحرية هو الأدلة المقبولة⁽²⁾، لذلك نتناول في هذا المبحث حرية القاضي الجزائي في قبول الأدلة الرقمية في المطلب الأول ثم سلطة القاضي الجزائي في تقدير الأدلة الرقمية في المطلب الثاني.

المطلب الأول

حرية القاضي الجزائي في قبول الأدلة الرقمية.

يعتبر مبدأ حرية القاضي الجزائي في قبول الأدلة بصفة عامة إحدى نتيجتي مبدأ حرية القاضي الجزائي في تكوين اقتناعه وهو السائد في الفقه⁽³⁾، فكان لا بد من معرفة مدى تطابق هذه

(1) Jesus Borrego, ibid, p42-43.

(2) محمد زكي ابو عامر، المرجع السابق، ص 142-143.

(3) فاضل زيدان محمد، المرجع السابق، ص93.

النتيجة مع قبول الدليل الرقمي، وهو ما سنتناوله في هذا المطلب من خلال معرفة مفهوم مبدأ حرية الاقتناع القضائي (الفرع الأول)، ثم الأساس العلمي لقبول الأدلة الرقمية (الفرع الثاني)، و اثر مشروعية الدليل المعلوماتي على قبوله القضائي (الفرع الثالث).

الفرع الأول : مفهوم مبدأ حرية الاقتناع القضائي.

يعتبر مبدأ حرية الاقتناع القضائي الركيزة الثانية في الإثبات بعد مبدأ حرية الإثبات القضائي لذلك تناول في هذا الفرع المقصود بمبدأ حرية الاقتناع القضائي(أولاً)، ثم أساس مبدأ حرية الاقتناع القضائي(ثانياً)، ونخلص إلى النتائج المترتبة عن المبدأ(ثالثاً).

أولاً- المقصود بمبدأ حرية الاقتناع القضائي.

يعني بمبدأ الاقتناع القضائي أن للقاضي أن يقبل جميع الأدلة التي يقدمها إليه أطراف الدعوى فلا وجود لأدلة يحظر عليه القانون مقدا قبولها، وله أن يستبعد أي دليل لا يطمئن إليه فلا وجود لأدلة مفروضة عليه، وله بعد ذلك السلطة التقديرية الكاملة في وزن قيمة كل دليل على حده، وله في النهاية سلطة التنسيق بين الأدلة التي قدمت إليه، واستخلاص نتيجة منطقية من هذه الأدلة مجتمعة متساندة تتمثل في تقرير البراءة أو الإدانة.

وعلة هذا المبدأ أنه يتفق مع أسلوب التفكير العادي و المنطق في الحياة العامة وفي البحث العلمي ويكفل تتطابق الحقيقة القضائية مع الحقيقة الواقعية من خلال تخويل القاضي تحري الواقع من أي مصدر كان⁽¹⁾، وليس معني ذلك أن الأنظمة التي تأخذ بهذه الفكرة تركز لتحكم القاضي و استبداده، لأنها تضع لكل دليل شروطا وتحدد طرق استخلاصه وتقديمه إلى الجهات المسؤولة ويعتبر هذا النظام الأكثر شيوعا في القانون المقارن في العصر الحديث⁽²⁾.

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا للحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص من 846 إلى 850.

(2) ممدوح خليل البحر، المرجع السابق، ص332.

ف نجد المشرع الفرنسي قد أخذ بهذا المبدأ من خلال نص المواد 304 و 353 و 427⁽¹⁾ من قانون الإجراءات الجنائية الفرنسي، وكذلك المشرع المصري من خلال نص المادة 01/302 من قانون إجراءاته الجنائية⁽²⁾، يقابلهم في ذلك المشرع الجزائري الذي تبني صراحة مبدأ حرية الاقتناع القضائي وهو ما يتضح من خلال نص المادة 01/212 من ق.إ.ج.ج الواردة ضمن الأحكام المشتركة لجهات الحكم والتي تنص على انه " يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص". ويتأكد هذا المبدأ حينما نقرأ نص المادة 307 من ق.إ.ج.ج⁽³⁾ التي تخول لتشكيلة محكمة الجنايات حق بناء حكمهم على الاقتناع الشخصي، وكتحصيل لما سبق فان جميع الجرائم سواء الجنايات أو تلك المصنفة كجرح ومنها الجرائم الخاصة بالمعالجة الآلية للمعطيات والخاضعة بدورها "لمبدأ حرية الإثبات"⁽⁴⁾ فان القاضي الجزائري مخول له بأن يصدر حكمه وفقا لاقتناعه الخاص.

ثانيا - أساس مبدأ حرية الاقتناع القضائي:

يستند مبدأ حرية الاقتناع القضائي إلى طبيعة الإثبات في المواد الجنائية، ثم إلى الدور الايجابي للقاضي الجزائري.

(1) Article 427 du C.P.P.f dispose que : Hors les cas ou la loi en dispose autrement, les infractions peuvent être établies par tout monde de preuve et le juge décide d'après son intime conviction ».

(2) ممدوح خليل البحر، المرجع السابق، ص من 332 إلى 338.

(3) تنص المادة 307 من ق.إ.ج.ج.ج المقابلة لنص المادة 304 من قانون الإجراءات الجنائية الفرنسي على أنه " يتلو الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات الآتية التي تعلق فضلا عن ذلك بحروف كبيرة في أظهر مكان من غرفة المداولة. "إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم ، ولا يرسم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام وكفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر، وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم . هل لديهم اقتناع شخصي؟".

(4) هنا يجب التمييز بين مبدأ حرية الإثبات ومبدأ حرية الاقتناع القضائي، وعدم الخلط بينهما حيث يقصد بالأول الطريق الاتباتي المرسوم لكل أطراف الدعوى بما فيهم القاضي في اختيار وسائل الإثبات الملائمة للواقعة محل الإثبات، بينما يتعلق الثاني بنطاق سلطة القاضي في تقدير وتقييم الدليل ، بحيث يمثل المبدأ الثاني الأساس الذي يسيطر على آخر مرحلة من مراحل تقدير الدليل الجنائي منذ نشأته حتى تحقيق غايته. عائشة بن قارة مصطفى، المرجع السابق، ص 184.

أ- طبيعة الإثبات في المواد الجنائية:

يتسم الإثبات بأنه لا يتعلق بإثبات وقائع مادية وإنما يضاف إليها وقائع معنوية نفسية لها طابع استثنائي، كما انه ليس متعلقا بإثبات تصرفات قانونية يحتاط أطرافها بالأدلة المهيأة كما هو الحال في الإثبات المدني، فالإثبات الجنائي ينصرف بالإضافة إلى حقيقة الوقائع المادية إلى إثبات القصد الجنائي و التحقق من قيامه من عدمه، فالجريمة ليست كيانا ماديا خالصا قوامه الفعل وآثاره، إنما هي كذلك الأصول النفسية لماديات الجريمة، ومرد ذلك هو البحث عن إيجاد توازن بين مصلحة المجتمع في توقيع الجزاء على المتهم وحماية مصلحة المتهم بقرينة البراءة⁽¹⁾. فمن ناحية القانون الجزائي الإجرائي يثور التساؤل حول إمكانية الركون دائما إلى مبدأ حرية الإثبات لقبول أي دليل يستند إلى اكتشاف علمي، أو تقني مستحدث فالي أي مدى تجيز حرية الإثبات اللجوء إلى الوسائل العلمية⁽²⁾.

إن ظهور وسائل إثبات علمية يتطلب جعل سلطة القاضي كضمان إزاء هذه الوسائل والحقيقة أن طبيعة الإثبات الجنائي من خلال هذه النظرة يتناسب مع الطبيعة الخاصة للأدلة الرقمية التي تتكون من نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة فهي غير ملموسة ماديا مما يشكل مجالا خصبا لمبدأ حرية الاقتناع القضائي بها.

ب- الدور الايجابي للقاضي الجزائي.

خول الشارع للقاضي الجزائي سلطة واسعة في الإثبات ما فسر بدوره الايجابي في المسألة فلا يجوز له التقيد بفحص الأدلة المقدمة له، و إنما يتعين عليه التحري بنفسه في أدلة الدعوى ويستثير الأطراف إلى تقديم أدلتهم بحثا عن "الحقيقة الموضوعية" في كل نطاقها وفي ادني

(1) فاضل زيدان محمد ، المرجع السابق، ص99.

(2) AMBROISE-CASTEROT, recherc et administration des preuves en procedure penale, la quete de la verite, A.J.pen.2005.no.7-8, p261.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

صورها في الواقع، خلاف القاضي المدني الذي يتحري "الحقيقة الشكلية" و يلزم الحياد بين أطراف الدعوى ويحكم بناء على ما يقدم له من أدلة ولا يتجاوزها⁽¹⁾.

ويقول بعض الفقه أن ما يبرر مقتضيات حسن سير العدالة الجنائية المجسدة بعدم ابتعاد الحقيقة القضائية عن الحقيقة الواقعية في الحكم اقتضاء منح القاضي دورا فعالا لإدراك هذه الحقيقة بحيث يجد القاضي نفسه طليقا في الوصول إليها من أي مصدر كان، وغير ملزم بقيمة معينة لدليل ما، يفرض عليه التسليم بها بما يخالف قناعته القضائية، وطبقا لهذه السلطة يتوصل إلى تطابق الحقيقتين بما يسمح به التفكير البشري⁽²⁾.

ويتجلى الدور الايجابي للقاضي الجنائي في الجرائم المعلوماتية في نقطتين جوهريتين هما توفير الدليل الرقمي من خلال البحث عن الدليل باستعمال سلطاته المخولة له قانونا فيستطيع أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إليه من خلال الإفصاح عن كلمات المرور و الشفرات الخاصة بتشغيل البرامج، كما أن له سلطة الأمر بتفتيش نظم الحاسوب بجميع مكوناته بحثا عن الدليل الرقمي كما سبق وان تطرقنا إليها، مع إمكانية الاستعانة بخبير معلوماتي مختص لفحص الأنظمة وإعداد خبرة فنية دقيقة طالما أن الأصل في التحقيق هو الذي يجريه القاضي في الجلسة، أما النقطة الثانية تتمثل في قبول الدليل الرقمي بعد التأكد من مشروعيته⁽³⁾.

ثالثا - النتائج المترتبة عن مبدأ حرية الاقتناع القضائي:

يترتب على هذا المبدأ نتيجتين أساسيتين هما:

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا للحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 852-853.

(2) فاضل زيدان محمد ، المرجع السابق، ص103.

(3) عائشة بن قارة مصطفى المرجع السابق، ص من 189 إلى 195.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

أ- سلطة القاضي الجزائي في قبول جميع الأدلة لإثبات أية واقعة ذات أهمية في الدعوى الجنائية، فلا يحتج عليه بأن دليلا ما لا يجوز له أن يستمد اقتناعه منها، ويتصل ذلك بسلطته في استبعاد أي دليل لا يقتنع به.

ب- و النتيجة الثانية تجمل في مبدأ تساند الأدلة الجنائية فجميع الأدلة التي تقدم في الدعوى يسند بعضها بعضا ويستمد القاضي اقتناعه منها مجتمعة⁽¹⁾.

ولا يشترط أن تكون الأدلة التي اعتمد عليها الحكم ينبئ كل دليل منها ويقطع في كل جزئية من جزئيات الدعوى، فلا ينظر إلى دليل بعينه لمناقشته على حدة دون باقي الأدلة، بل يكفي أن تكون الأدلة في مجموعها كوحدة مؤدية إلى ما قصده الحكم منها، ومنتجة في تكوين قناعة المحكمة واطمئنانها إلى ما انتهت إليه⁽²⁾.

تعتبر هاتين النتيجتين أساسا لقبول الأدلة المعلوماتية، فالنتيجة الأولى تجد لها أساسا في اختلاف أنواع وأشكال الأدلة الرقمية، خصوصا انه لم يتم إلى حد الآن الاتفاق على شكل موحد لها ما يتعين قبول جميع الأدلة الرقمية لإثبات الجريمة المعلوماتية مع استبعاد تلك التي ليس من شأنها تقديم الإضافة، أما النتيجة الثانية فتجد لها أساس في مراحل تشكيل وتكوين الأدلة فلا يمكن استبعاد دليل والأخذ بالآخر لأن الأدلة الرقمية تتسلسل زمنيا ومنطقيا وتفسح المجال لقبول القرائن العلمية.

الفرع الثاني: الأساس العلمي لقبول الأدلة الرقمية.

نتطرق في هذا الفرع إلى أساس قبول الأدلة المعلوماتية في كل من الأنظمة اللاتينية (أولا) الانجلوسكسونية (ثانيا) ثم في الأنظمة المختلطة (ثالثا)، دون أن ننسى التشريعات العربية(رابعا).

أولا- قبول الدليل الرقمي في النظام اللاتيني:

(1) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا للحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 850.
(2) فاضل زيدان محمد، المرجع السابق، ص136.

إن حجية الأدلة المعلوماتية في الدول المعنتقة النظام اللاتيني مثل فرنسا وألمانيا وتركيا ولكسمبورغ و اليونان و البرازيل لا تثير صعوبات لا في مدى حرية تقديمها ولا في مدى حرية القاضي الجنائي في قبول هذه الأدلة، فكل هذه الدول تخضع الأدلة الالكترونية لحرية القاضي في الاقتناع ، بحيث يمكن طرحها بالرغم من قطعيتها من الناحية العلمية إذا ثبت عدم اتساقها مع ظروف وملابسات الواقعة، ففي فرنسا فإن مشكلة حجية المخرجات المتحصلة من الحاسوب على مستوى القانون الجنائي ليست ملحة، أو عاجلة في نظر الفقهاء، فالأساس هو حرية القاضي في تقدير هذه الأدلة، ويدرس الفقه الفرنسي هذه الحجية تحت نطاق الأدلة الناشئة عن الآلة أو الأدلة العلمية، مثل أجهزة التصوير، وأشرطة التسجيل، وأجهزة التنصت وقد قضت محكمة النقض الفرنسية "إن أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي"⁽¹⁾.

و أيدت محكمة النقض الفرنسية تطبيق مبدأ حرية الاقتناع أمام جميع المحاكم الجنائية إلا إذا نص القانون خلاف ذلك، وتلزم محاكم الموضوع التقيد به، والدائرة الجنائية لمحكمة النقض ترى انه طالما لا يوجد نص قانوني يستبعد صراحة دليل ما فلا يجوز للمحكمة عدم قبول الدليل ولو كان ذلك الدليل غير مشروع بل لو كان عدم المشروعية ناتجة عن ارتكاب جريمة، غير أنها تشترط فقط أن يكون هذا الدليل قد تمت مناقشته حضوريا في الجلسة احتراماً لحقوق الدفاع⁽²⁾. وفي رأينا فإنها أخذت بالمبدأ الموسع في قبول الأدلة الرقمية بمعنى أن جميع الأدلة الرقمية مقبولة إلا ما استبعد بنص.

ثانيا - قبول الدليل الرقمي في النظام الانجلوسكسوني:

على خلاف التشريعات ذات الأصل اللاتيني التي تأخذ بمبدأ الاقتناع الذاتي للقاضي الجنائي فإن التشريعات التي تأثرت بالنظام الانجلوسكسوني مثل الولايات المتحدة الأمريكية، وانجلترا، وكندا واستراليا، وجنوب إفريقيا، تستلزم شروطا خاصة في الأدلة بوجه عام، فلا تقبل مثلا "الشهادة

(1) على حسن محمد الطوالبه، التقني الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة، المرجع السابق، ص 196.

(2) عائشة بن قارة مصطفى، المرجع السابق، ص 185-186.

السماعية"⁽¹⁾ بل يجب أن تكون الشهادة مباشرة على الواقعة وبإسقاط هذا المبدأ على الأدلة الرقمية فإنه يلزم تقديم نسخ أصلية منها مع استدعاء القائم بتحريرها أو إذاعتها وهو ما لا يتوافر في اغلب الأحيان، ما يجعل من النظام المقيد يتعارض مع نظام الإثبات في الجرائم المعلوماتية مما دعا إلى ضرورة قبول الدليل المستمد من الحاسوب باعتباره استثناء على نظام الأدلة القانونية مع استبعادها ممن صنفوها ضمن طائفة الشهادة السماعية⁽²⁾.

وفيما يلي نتطرق إلى أساس قبول الأدلة الالكترونية كأدلة إثبات في كل من الولايات المتحدة الأمريكية وانجلترا:

أ- **في الولايات المتحدة الأمريكية:** بالرغم من تبني قاعدة الدليل الأفضل في المادة 1002 من قانون الإثبات الفيدرالي و التي بمقتضاها يتعين تقديم أصل الدليل إلا أن المشرع الأمريكي حسم هذه المسألة وأقر قبول الدليل الرقمي المنسوخ طبقا لنص المادة 1001 بند 3 من قانون الإثبات الأمريكي بنصها على انه " إذا كانت البيانات مخزنة في حاسوب أو آلة مشابهة، فإن أي مخرجات مطبوعة منها أو مخرجات يمكن قراءتها بالنظر إليها وتعكس دقة البيانات، تعد بيانات أصلية". وبحسبها فان البيانات و المعلومات المتحصل عليها بواسطة طبعها تعد دليلا أصليا دونما حاجة لجلب الحاسوب إلى المحكمة⁽³⁾.

و تنص القاعدة 803 فقرة 6 من القواعد الفيدرالية الإجرائية الأمريكية على قبول الدليل في حالة استثنائية أخرى استنادا إلى مذكرة أو تقرير أو تسجيل أو تجميع تم إعداده عند وقوع حدث

(¹) قدم Morgan تعريفا أساسيا لشهادة السماع وهو السائد حاليا في معظم التشريعات التي تأخذ بالنظام الأنجلو أمريكي وقال بأن " شهادة السماع هو دليل يقدم من خلال شخص نقلا لعبارات أو سلوك صدر خارج المحكمة من شخص آخر، ويؤكد أو لا يؤكد مسألة معينة لإثبات الحقيقة في تلك المسألة، ويعتقد من يقدمه في صحته" والملاحظ على هذا التعريف انه اعتبر شهادة السماع مجرد دلالة وليس دليلا حازما بل لا يرتقي لمستوى الدليل. انظر عائشة بن قارة مصطفى، نفس المرجع، ص 200-201.

(²) شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 387.

(³) محمد طارق عبد الرؤوف ألحن، المرجع السابق، ص 355.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

معين أو في لحظة قريبة من وقوع ذلك الحدث من جانب شخص يعلم به، أو عن طريق معلومات وصلت إليه مادامت تلك التسجيلات قد تم الاحتفاظ بها في أثناء القيام بنشاط تجاري منتظم⁽¹⁾.

أما بالنسبة للقوة الإثباتية للسجلات الالكترونية المخزنة في الحاسوب فهي تعد "كالشهادة على السماع"⁽²⁾ في مجال الإثبات، بخلاف السجلات المأخوذة من الحاسوب فيمكن للمحاكم أن تأخذ بها إذا كان برنامج الحاسوب يؤدي عمله على وجه سليم وجيد، فيما عدد الفقه في أمريكا مجموعة من الشروط يجب توفرها في الدليل الرقمي حتى يتم قبوله أمام المحكمة ، أما القضاء الأمريكي فقد تعرض في العديد من القضايا إلى مسألتي الأصالة والصحة لقبول الدليل الرقمي⁽³⁾.

2- في إنجلترا: صدر في بريطانيا تشريع الإثبات بالحاسوب سنة 1983 أين ركز بصفة أساسية على قبول مخرجات الحاسوب كدليل لإثبات أي حقيقة مسجلة فيه والتي تزود بشهادة شفوية تكون مقبولة، ثم صدر قانون إساءة استخدام الحاسوب في عام 1990م، الذي لم يتناول الأدلة الرقمية، وربما كان السبب هو وجود قانون البوليس و الإثبات الجنائي لسنة 1984 الذي حوي تنظيمًا محددًا لمسألة قبول مخرجات الحاسوب و الإنترنت كأدلة إثبات في المواد الجنائية⁽⁴⁾.

وقد تم تعديل هذا القانون في تشرين الأول عام 2002 وحدد المشرع الانجليزي في المادة 69 من هذا القانون الشروط الواجب توافرها في المستند الناتج عن الحاسوب. و تنص على انه" في أية إجراءات لا يقبل البيان المتضمن في مستند صادر عن طريق الحاسوب كدليل على أية واقعة واردة فيه إلا إذا تبين:

(1) شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 389.

(2) الشهادة على السماع وفق قواعد الإثبات الفيدرالية تقبل على سبيل الاستثناء في المجالات التالية : الأعمال، المذكرات اليومية، التقارير، السجلات، الأحداث، الشروط، الآراء، التشخيص. فإذا تم حفظ هذه الأشكال في الحاسوب بالأسلوب المعتاد ووفق نظام العمل السائد، فإنها تعد كالشهادة على السماع،، بينما المادة 2870 من القانون المدني لمقاطعة كيبك تنص على انه لا تقبل الشهادة السماعية إلا إذا تحققت المحكمة استحالة حضور الشاهد كالوفاة أو الجنون أو انه متواجد في الخارج وان الظروف التي كانت تحيط بتلك الأقوال تدعو إلى الثقة.

(3) محمد طارق عبد الرؤوف ألحن، المرجع السابق، ص 356-357.

(4) علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة، المرجع السابق، ص 196-197.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

- عدم وجود أسس معقولة للاعتقاد بأن البيان يفتقر إلى الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسوب.

- أن الحاسوب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فإن أي جزء لم يكن يعمل فيه بصورة سليمة، أو كان معطلا عن العمل، لم يكن ليؤثر في إخراج المستند أو دقة معلوماته.

- الوفاء بأية شروط متعلقة بالمستند محددة طبقا لقواعد المحاكمة (المتعلقة بالطريقة أو بالكيفية التي يجب أن تقدم بها المعلومات الخاصة بالبيان المستخرج عن طريق الحاسب)⁽¹⁾.

ثالثا - قبول الدليل الرقمي في النظام المختلط:

يقوم على تحديد القانون أدلة معينة لإثبات بعض الوقائع دون بعضها الآخر، أو يشترط في الدليل شروطا في حالات محددة، أو يعطي القاضي الحرية في تقدير الأدلة القانونية، فالمشرع الياباني حصر طرق الإثبات المقبولة في أقوال المتهم، وأقوال الشهود، والقرائن و الخبرة،

أما بالنسبة للأدلة المعلوماتية فيقرر الفقه الياباني أن السجلات الكهرومغناطيسية تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة، إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات ثم يتم قبولها سواء كانت هي الأصل أم كانت نسخة منه، كما يري الفقه الشيلي أن الدليل المعلوماتي يمكن أن يكون مقبولا في المحكمة كدليل كتابي أو مستندي، مثله مثل النظم الحديثة الأخرى لجمع وتسجيل المعلومات، وحجة الفقه الشيلي تستهدف توسيع مظلة الوسائل العلمية الحديثة في الإثبات، لتغطي العناصر الإثباتية الناتجة عن جرائم المعلوماتية⁽²⁾.

(1) علق مجلس اللوردات الانجليزي على المادة 69المشار إليها بأنه" يمكن للشهادة الشخصية الصادرة عن شخص على علم بطريقة تشغيل الحاسوب، أن تعطي الثقة بالدليل، وليس بالضروري أن يكون هذا الشخص خبيرا بالحاسوب "وبناء على ذلك قبلت المحاكم الانجليزية فيما يتعلق بسلامة نظام الحاسوب بشهادة أشخاص لديهم علم بطريقة عمل نظام الحاسوب.انظر محمد طارق عبد الرؤوف ألحن، المرجع السابق، ص 361.

(2) على حسن محمد الطوالبية، التفتيش الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة، المرجع السابق، ص 198.

رابعاً - قبول الدليل الرقمي في التشريعات العربية:

تختلف الأنظمة العربية بين تبنيها للنظام اللاتيني⁽¹⁾ و بين تلك التي تأخذ بالنظام الأنجلوسكسوني وعموما فإن الدول التي تأخذ بالنظام اللاتيني هي الأردن مصر لبنان سوريا تونس المغرب و الجزائر، فالمشرع السوري نص صراحة على الأدلة الرقمية وارجع حجيتها إلى تقدير المحكمة وهو ما نص عليه في المادة 25 من المرسوم التشريعي رقم 17 لعام 2012 المتعلق بتنظيم التواصل على الشبكة ومكافحة الجريمة المعلوماتية بعنوان حجية الدليل الرقمي.

أما المشرع الأردني فلم يورد نصوص خاصة تتناول قبول الدليل الرقمي، وإنما اكتفى بترك مسألة تقديره لحرية القاضي الجنائي استنادا إلى نص المادة 2/147 من قانون أصول المحاكمات الجزائية الأردني شأنه في ذلك شأن باقي الأدلة⁽²⁾، وهو ما ذهب إليه المشرع المصري لما أحال مسألة قبول أي دليل إلى قناعة القاضي عملا بنص المادة 1/302 من قانون الإجراءات الجنائية المصري وتواتر عليه اجتهاد محكمة النقض المصرية⁽³⁾، فيما خلت مواد قانون مكافحة الجرائم المعلوماتية الإماراتي رقم 2 لسنة 2006 من تناول الدليل الرقمي ولا كيفية إثبات الجرائم المعلوماتية واعتنق بدوره مبدأ حرية القاضي في تكوين قناعته وهو ما يتضح في نص المادة 209 من قانون الإجراءات الجزائية الاتحادي، وسار المشرع السعودي على نفس الدرب حينما خلا نظام

(1) تسير اغلب الأنظمة اللاتينية بالنظام التحقيقي المختلط والتي صيغت نظريتها في الإثبات على أساس سيطرة مبدأ حرية الدليل السائد في النظام الاتهامي ليحكم مسألة قبول الدليل أمام القضاء، ومبدأ الدور الايجابي للقاضي الجنائي ليحكم مسألة البحث عن الدليل، ومبدأ حرية القاضي الجنائي في الاقتناع عن النظام الاتهامي ليحكم مسألة تقدير الدليل. أنظر سعيد قاسم علي العاقل و شائف على محمد الشيباني، بحث بعنوان " مدى صلاحية الاجتهاد القضائي لسد الثغرات التشريعية في مجال الإثبات بالوسائل المعلوماتية و التكنولوجيا الحديثة دراسة مقارنة" مقدم للندوة المنعقدة في المركز العربي للبحوث القانونية و القضائية بيروت لبنان في الفترة 6-8/01/2003، ص 14. متاح على الموقع الالكتروني:

<http://agoye.com/userimages/.../research/salaheea.pdf>

(2) خالد عياد الحلبي، المرجع السابق، ص 246-247.

(3) ممدوح خليل البحر، المرجع السابق، ص 338-339.

مكافحة الجرائم المعلوماتية السعودي لسنة 2007 من بيان تعيين وسائل إثبات الجرائم المعلوماتية⁽¹⁾، بما فيها الدليل الرقمي.

المشعر الجزائري بدوره لم يخصص نصوص صريحة تتناول كيفية قبول الدليل الرقمي مما يحيلنا إلى طرق الإثبات العامة المطبقة في قبول الأدلة والتي تخضع إلى السلطة التقديرية للقاضي عملاً بنص المادة 212 من ق.إ.ج كما سبق بيانه، ولو أننا نرى انه تناول ضمناً الأدلة المعلوماتية في القانون 04/09 فبعد الاطلاع على نص المادة 6 منه فان المشعر الجزائري تحدث عن حجز المعطيات المفيدة في كشف الجرائم أو مرتكبيها فانه يتم نسخ المعطيات على دعامة تخزين وحرزها، فالمشعر هنا يقصد الأدلة المعلوماتية، ولو انه لم يسميها إلا انه يحرص على جزؤها في أحسن الظروف لتقديمها أمام الجهات المختصة كأدلة إثبات، وفي تقديرنا لو أكمل المشعر هذا التوجه التشريعي المسير للتقنية بنصه صراحة على الأدلة الرقمية كما فعل المشعر السوري في صورة تزيح كل لبس وتسد الفراغ في هذه المسألة.

الفرع الثالث: أثر مشروعية الدليل الرقمي على قبوله القضائي.

نتناول في هذا الفرع مسألة مدى تأثير احترام الإجراءات القانونية في استخلاص الدليل الرقمي على قبوله أثناء المحاكمة الجزائية فلا بد بداية من التطرق إلى أصالة الدليل المعلوماتي ثم مشروعية طريقة استخلاص الدليل الرقمي و مدى قبول الدليل الرقمي غير المشروع في الإثبات.

أولاً- أصالة الدليل المعلوماتي:

تظل أصالة الدليل المعلوماتي من المشكلات الكبرى حين عرضه على القضاء، خصوصاً إذا علمنا أن الدليل الذي يتم استنباطه في هذا الإطار إنما هو دليل مستوحى من قاعدة مجهولة، أو خوادم غامضة ليس من السهولة التوصل إليها ، مثل خوادم الهكره التي يتم استخدام برمجيات

(1) أحمد بن عبد الرحمن ألبعادي ، ورقة عمل بعنوان " دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع و المأمول" مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية بالخرطوم السودان في الفترة من 23-25 سبتمبر 2012 ص 23-24.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

عالية التقنية تعمل على إخفائها في العالم الافتراضي، كما يمكن للجاني إزالة الدليل من الحاسوب حتى عن بعد ويكون ما تبقي منها نسخة فقط تم التوصل إليها بطريق المراقبة الالكترونية مثلا⁽¹⁾.

والواقع من الأمر أن بحث موضوع الأصالة على المستوى القانوني جعل المشرع المقارن يعتمد منطق الافتراض أكثر من السعي إلى الحقيقة في معني إقرار العدالة في إطار الدليل الرقمي فالاعتراف بأصالة الدليل الرقمي هنا اعترافا قانونيا فقط ما جعل النظام الاتهامي يبني قاعدة مدى إمكانية قبول الدليل المعلوماتي خاضعا لضوابط خاصة تحمل على مفهوم الدليل المادي الملموس⁽²⁾. و سبق لنا وان تطرقنا لقبول الأدلة المنسوخة في التشريع الأمريكي من زاوية الأساس العلمي.

فالمشرع الجزائري مدعو ليأخذ حظه في تقنين هذه المسألة، إذ تبرز أهمية التسليم بمنطق افتراض الأصالة في الدليل التقني على المستوى القانوني في حالة رفضها، إذ لا نكون أمام دليل إدانة وهو ما يؤدي في النهاية إلى رفض منطق التعامل مع هذه النوعية من الأدلة في حالة كونها لازمة⁽³⁾.

ثانيا- مشروعية طريقة الحصول على الدليل الرقمي:

لا شك أن مبدأ شرعية الجرائم و العقوبات الذي يستقيم عليه بنين القانون الجنائي الموضوعي و الإجرائي، ينعكس على قواعد الإثبات الجنائي باعتبارها الضمان الحقيقي لانطباقه، فيفرض خضوعها هي الأخرى "المبدأ الشرعية" بحيث لا يكون الدليل مشروعاً ومن ثمة مقبولاً إلا إذا جرت عملية البحث عنه أو الحصول عليه وعملية حمله إلى القضاء أو إقامته أمامه في ظل احترام سائر القواعد و الشكليات التي قررها القانون. فشرعية الإثبات الجنائي تستلزم عدم قبول أي دليل يكون البحث عنه أو الحصول عليه قد تم بطريق غير مشروع احتراماً لحقوق الدفاع، وقيم العدالة

(1) فتحي محمد أنور عزت، المرجع السابق، ص 637.

(2) فتحي محمد أنور عزت، نفس المرجع، ص 638.

(3) رشيدة بوكور، المرجع السابق، ص 488.

وأخلاقياتها، و حرية الإنسان⁽¹⁾، لذلك كان البحث عن الدليل قد تم باستخدام إجراءات غير مشروعة للتحقيق يترتب عنها حتما عدم مشروعية الدليل المستمد منها وعدم قبوله في الإثبات⁽²⁾.

أ- موقف بعض التشريعات المقارنة من مشروعية طريقة الحصول على الدليل:

قرر المشرع الفرنسي نوعين من البطلان الذي يلحق أعمال قاضي التحقيق وهما البطلان القانوني وهو ذلك النوع من البطلان الذي يتولى القانون وحده تحديد حالاته مسبقا، وكذا البطلان الجوهري والذي نص عليه في المادة 171 من القانون رقم 93-2 المؤرخ في 04/01/1993 المعدل لقانون الإجراءات الجزائية⁽³⁾، فيما أجازت المادة 170 من ذات القانون لأطراف الدعوى أثناء البحث التمهيدي أو التحقيق القضائي تقديم طلب لغرفة الاتهام يتضمن إلغاء إجراء من الإجراءات أو وثيقة معينة استبعادا للدليل الغير مشروع. أما المشرع المصري فقد رتب البطلان في المادة 331 من قانون الإجراءات الجنائية على عدم مراعاة أحكام القانون بأي إجراء جوهري دون تحديد ماهية الإجراء الجوهري ومن ثم فإن أي إجراء جوهري لم تتم احترامه في الخصومة الجزائية يؤدي إلى استبعاد الدليل لعدم مشروعيته. وتجسد هذا المبدأ حينما نص في المادة 309 مكرر من قانون العقوبات على حبس كل من يعتدي على حرمة الحياة الخاصة عن طريق أجهزة استراق السمع أو التسجيل مع مصادرة تلك الأجهزة⁽⁴⁾.

ب- موقف المشرع الجزائري من مشروعية طريقة الحصول على الدليل:

(1) ويعتبر جمعا و تسجيلا غير مشروع وتعدى على حرية الإنسان الجمع الذي يتم دون علم الشخص وفي غير الحالات التي يجيزها القانون كالبيانات التي يتوصل إليها النظام عن طريق التنصت أو التسجيل أو بناءا على تجميع المعلومات من نظم المعلومات المختلفة عن طريق ربط نظم المعلومات المنشئة لتحقيق أغراض مختلفة بعضها ببعض أو عن طريق استعمال الكعك المحلى بعد ضعه في القرص الصلب للحاسوب أو جمع البيانات وراقبتها على شبكة الانترنت خصوصا وان كل اتصال يترك أثرا ما. انظر بولين انطونيوس أيوب، المرجع السابق، ص464-465.

(2) محمد زكي أبو عامر، المرجع السابق، ص 119-120.

(3) تنص المادة 171 على انه " يتحقق البطلان عندما يترتب على إغفال إجراء جوهري منصوص عليه في قانون الإجراءات الجزائية أو نص إجرائي آخر فيه مساس بحقوق الطرف المعني".

(4) ناشف فريد، بحث بعنوان " مدى قبول الدليل غير المشروع في المحاكمة الجزائية دراسة مقارنة"، منشور في دورية دراسات قانونية الصادرة عن مركز البصيرة للبحوث و الاستشارات و الخدمات التعليمية، العدد 15، دار الخلدونية للنشر و التوزيع، الجزائر، سنة 2012، ص من 150الى153.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

لقد اتجه المشرع الجزائري نفس وجهة المشرع الفرنسي و المصري، وذلك بتقرير البطلان بنوعيه القانوني و الجوهري للإجراءات المخالفة للقانون المتخذة من طرف القاضي أو أطراف الدعوى وهو ما يتجلى في العبارات الواردة في العديد من النصوص القانونية مثل " تحت طائلة البطلان، يكون باطلا، ويعتبر ملغي، يترتب عنه البطلان"

فالأدلة المعلوماتية التي لم تراعى في استخلاصها وجمعها القواعد الإجرائية المنصوص عليها سواء في الدستور أو في قانون الإجراءات الجزائية باعتبارها طرقا تقليدية أو الواردة في القانون 04/09 والمحددة للإطار العام لمراقبة وتفتيش الأنظمة المعلوماتية وحجز البيانات و المعلومات. فكل خرق لتلك الضمانات مجتمعة مثل: عدم احترام ضمانات الاستجواب المقررة قانونا والواردة في نص المادة 100 و 105 من ق.إ.ج أو ممارسة الإكراه المعنوي للحصول على الاعتراف أو إلزام الشاهد المعلوماتي بإفشاء سر يتضمن خصوصيات الأفراد دون إذن أو إجراء تفتيش للأنظمة أو دخول للمساكن الخاصة بالأفراد في غياب إذن قضائي أو إجراء ترتيبات لمراقبة اتصالات الكترونية في غير الحالات المحددة قانونا يترتب عنها البطلان القانوني.

فيما يترتب البطلان الجوهري إذا كان الإجراء المتخذ فيه مساس خطير بحقوق الدفاع أو حقوق الأطراف، وهذا ما حدده المشرع الجزائري في المادة 159 من ق.إ.ج.ج⁽¹⁾ في حين قصر حق تقديم طلب إبطال الإجراء المعيب إلى غرفة الاتهام على قاضي التحقيق، أو وكيل الجمهورية دون باقي أطراف الخصومة استنادا إلى نص المادة 158 من ق.إ.ج.ج، وكرسه العمل القضائي المجسد في قرار المحكمة العليا تحت رقم 362769 المؤرخ في 02/02/2005⁽²⁾، وفي تقديرنا فإن المشرع ملزم بإعطاء الحق في تقديم طلب بطلان الإجراء إلى كافة أطراف الدعوى ليتسنى لهم ممارسة حقهم في الدفاع المكفول دستوريا كما فعل المشرع الفرنسي.

(1) تنص المادة 01/159 من ق.إ.ج.ج على انه " يترتب البطلان أيضا على مخالفة الأحكام الجهرية المقررة في هذا الباب خلافا للأحكام المقررة في المادتين 100 و 105 إذا ترتب على مخالفتها إخلال بحقوق الدفاع أو حقوق أي خصم في الدعوى".

(2) ينص القرار على " إن القانون لا يجيز للمتهم أو للطرف المدني طلب بطلان الإجراءات إلا أمام غرفة الاتهام بمناسبة عرض القضية برمتها على تلك الغرفة بعد أمر التسوية لقاضي التحقيق فان طلب البطلان لا يكون إلا من طرف القاضي المحقق نفسه أو وكيل الجمهورية". المجلة القضائية للمحكمة العليا العدد الأول لسنة 2005 ص 387.

ومن ثمة فالمحاكمة المنصفة التي يجريها القاضي لا يمكن إجراؤها إلا على أساس الشرعية الإجرائية ويجب الالتزام بهذه الشرعية روحاً ومضموناً (1).

ثالثاً - مدى قبول الدليل المعلوماتي غير المشروع:

القاعدة المستقرة في الفقه و التشريع و القضاء المقارن تفيد قبول الدليل المشروع، إلا أن هذه القاعدة لا تؤخذ على إطلاقها وإنما ورد بشأنها موقفين متباينين بشأن قبول الدليل غير المشروع وهو ما ينطبق على الدليل المعلوماتي لذلك نتطرق إلى هاذين الاتجاهين كما يلي:

أ- الاتجاه الأول: تبني أنصار هذا الاتجاه قبول الأدلة غير المشروعة وقد كان لهذا الاتجاه الفقهي عدة مبررات أهمها عدم إطلاق احترام حقوق الإنسان والمبالغة فيها أمام ضرورة حماية النظام الاجتماعي، ويرون أنه من غير المنطقي إطلاق سراح متهم خطير نتيجة خطأ في جمع الدليل ما يعيق مكافحة الجريمة، كما أن سيطرة الاقتناع الحر للقاضي من شأنه الأخذ بالأدلة التي اطمأن لها، ومن التشريعات التي اعتنقت هذا الاتجاه نجد التشريع الانجليزي والكندي، فالمشرع الانجليزي يأخذ بمبدأ الدليل المؤثر ذو الحجية بغض النظر عن الطريقة التي تم الحصول بها عليه، والدليل على تكريس هذا المبدأ تأييد مجلس اللوردات لتحليل المحكمة في قضية R.V KHAN SULTAN "بان الظروف التي تم تحصيل الدليل فيها تشكل خرقاً لحرمة الحياة الخاصة، إلا أنها لا تنطوي على خطر الإخلال بنزاهة الإجراءات على نحو يتعين معها استبعاد الدليل، وفقاً للمادة 78 من قانون الشرطة و الإثبات الجنائي الصادر سنة 1984"، كما أن القضاء الكندي تبني هذا الاتجاه من خلال تقرير قاعدة قبول كافة الأدلة طالما أنها منتجة في الإثبات ولو تم تحصيلها بطرق غير شرعية(2).

و المتمعن في هذا الاتجاه يتأكد بان مبررات قبول الدليل غير المشروع تتركز في الأدلة المتعلقة بالإدانة.

(1) أحمد فتحي سرور، المرجع السابق، ص 466.

(2) ناشف فريد، المرجع السابق، ص من 145 إلى 149.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

ب- الاتجاه الثاني: يسوق هذا الاتجاه الفقهي مبررات لاستبعاد الأدلة غير المشروعة والتي كان لها الأثر البالغ في تبنيتها من قبل التشريعات اللاتينية والعربية وكذا الأمريكية ويستندون في ذلك على حماية حقوق الإنسان⁽¹⁾ عامة وحقوق الأفراد في الحياة الخاصة والحق في الدفاع اللصيقة بهم خاصة فلا يجوز التنازل عنها، مما يتعين استبعاد الأدلة غير المشروعة، سيما وان السلطة القضائية لها من الوسائل والإمكانات البشرية والمادية ما يمكنها من البحث عن الأدلة وتحقيق ذلك بطرق مشروعة مقارنة بالمتهم الذي يعتبر خصم ضعيف أمام المحكمة في مواجهة السلطة القضائية أثناء إثبات الجريمة، فلا بد للدولة ممثلة في محاكمها أن تعطي المثل الأعلى في احترام حقوق الإنسان وبامتناعها عن الأدلة غير المشروعة تحقق الوظيفة التربوية و الأخلاقية للقانون⁽²⁾.

ومن التشريعات التي تبنت هذا الاتجاه نجد المشرع الأمريكي فبالرغم من انه كان وفيما في بدايته لقواعد" الكومن لو" الانجليزي التي تأخذ بالدليل المنتج، إلا انه توالت القضايا التي حولت اتجاه التشريع وظل ازدواج الأخذ بهذا المبدأ إلى غاية أن جاء حكم شهير سنة 1961 في قضية Tapp.V.Ohio، والذي ذهب فيه المحكمة الاتحادية العليا إلى أن التعديل الدستوري الرابع ينطبق كذلك على مستوي المحاكم الاتحادية وبالنتيجة يتحتم استبعاد الأدلة المتحصلة بطريقة غير مشروعة. أما المشرع الفرنسي فقد استبعد كل الأدلة الغير مشروعة من دائرة التعامل الإجرائي ويعتبر الاعتماد على دليل غير مشروع فيه مساس بمبدأ النزاهة وهو ما ذهب إليه المشرع

(1) في ذلك أوصي المؤتمر الدولي الخامس عشر للجمعية الدولية لقانون العقوبات و الذي عقد في ريو دي جانيرو بالبرازيل في الفترة 4-9 سبتمبر سنة 1994 في مجال حماية حركة إصلاح الإجراءات الجنائية وحماية حقوق الإنسان بمجموعة من التوصيات منها التوصية رقم 18 التي تنص على أن كل الأدلة التي تم الحصول عليها عن طريق انتهاك حق أساسي للمتهم و الأدلة التي تنتج عنها تكون باطلة، و لا يمكن التمسك بها أو مراعاتها، في أي مرحلة من مراحل الإجراءات، وقد أشار هذا المؤتمر إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب الآلي و الجرائم التقليدية في بيئة تكنولوجيا المعلومات وإلا ترتب عليه بطلان الإجراء فضلا عن تقرير المسؤولية الجنائية لرجل السلطة العامة الذي انتهك القانون. رشيدة بوكور، المرجع السابق ص 493.

(2) ناشف فريد، المرجع السابق، ص 149.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

الجزائري إذ عبر صراحة في نص المادة 160 من ق.إ.ج.ج⁽¹⁾ على استبعاد الأدلة غير المشروعة وبالتالي فإن الأدلة المعلوماتية غير مشروعة واستنادا إلى القواعد العامة تستبعد ولا يؤخذ بها.

ومن زاوية أخرى فإنه يمكن استخراج الأدلة الغير المشروعة بالنظر إلى طبيعة الجريمة المعلوماتية والتي يمكن لأي شخص تعقب آثار الجريمة في الفضاء السيبراني المفتوح مثلا قبل حتى فتح التحقيق من الجهات المختصة، كما أن البحث عن جمع الأدلة بسرعة تقاديا لإتلافها من شأنه أن يخلف عدم احترام الإجراءات المطلوبة قانونا ما يجعل من الدليل غير مشروع، ومن هذا المنطلق فقد يتحصل أحد أطراف الدعوى على دليل معلوماتي غير مشروع تم جمعه في حينه ليقوم الجاني بإتلاف تلك الأدلة، ما يطرح نقاشا جديا حول مدى قبول ذلك الدليل المعلوماتي، ففي تقديرنا المشرع ملزم بوضع ضوابط لهذا النوع من الأدلة وعدم رفضها على إطلاقها من منطلق خصوصيات الجريمة وطبيعة تلك الأدلة.

المطلب الثاني

ضوابط القاضي الجزائري في تقدير الدليل المعلوماتي.

إذا كان المبدأ هو حرية القاضي الجزائري في تكوين اقتناعه من خلال سلطته الواسعة في تقدير الدليل الالكتروني دون إلزامه بقيمة مسبقة له، فإن هذه الحرية ليست مطلقة وتحكمية كما ذهب إليه الفقه السائد وما استقر عليه القضاء، بل لها ضوابط تمثل صمام أمان إزاء انحراف القاضي وهو بصدده ممارسته سلطة قناعته، بيد أن القاضي ملزم بتسيب الأحكام. وتتعلق هذه الضوابط إما بالدليل نفسه (الفرع الأول) و إما تتعلق بالاقتناع القضائي (الفرع الثاني).

الفرع الأول: الضوابط المتعلقة بالدليل الرقمي نفسه.

(1) تنص على انه" تسحب من ملف التحقيق أوراق الإجراءات التي أبطلت ، وتودع لدى قلم كاتب المجلس القضائي ويحظر الرجوع إليها لاستنباط عناصر أو اتهامات ضد الخصوم في المرافعات، وإلا تعرضوا لجزاء تأديبي بالنسبة للقضاة ومحاكمة تأديبية بالنسبة للمحامين المدافعين أمام مجلسهم التأديبي".

تفيد الضوابط المشتقة من الدليل نفسه سلطة القاضي في تقديره للدليل الرقمي، واهم هذه الضوابط تتعلق بضرورة تأسيس الاقتناع القضائي على أدلة رقمية صحيحة (أولاً)، وإلى ضرورة مناقشة الدليل الرقمي في الجلسة (ثانياً)، مع ضرورة وجود أصل الدليل الرقمي في أوراق الدعوى (ثالثاً).

أولاً- تأسيس اقتناع القاضي الجزائي على أدلة معلوماتية صحيحة:

إن القاضي الجزائي ليس حراً في تقدير الدليل المعلوماتي أياً كان بل هو حر في تقدير الدليل الإلكتروني المقبول في الدعوى ولكي يكون الدليل صحيحاً لا بد من توفر شروط محددة ولو أنه متفق علي أهمها ضمناً مع اختلاف في بعض هذه الشروط من تشريع إلى آخر.

فالمشرع الأمريكي يشترط في صحة الدليل الرقمي ما يلي:

- أن لا يطرأ على محتويات السجل الإلكتروني أي تغيير (1) أي أن يكون الدليل المقدم إلى المحكمة هو نفس الدليل الذي تم جمعه ويمكن للشخص الذي قام بجمع الدليل أن يشهد بذلك أمام المحكمة وهذا ما يطلق عليه "سلسلة الرعاية"(2).

- أن تكون المعلومات الموجودة في السجل قد صدرت فعلاً عن المصدر المزعوم، سواء أكان هذا المصدر الإنسان أم الآلة.

(1) تتخذ جملة من الإجراءات الفنية للحصول على الدليل المعلوماتي إلا أنه من الممكن أن تعثرها خطأ قد يشكك في سلامة نتائجها، لذا يمكن في هذا الشأن اعتماد ما يعرف باختبارات (داو بورت) كوسيلة للتأكد من سلامة الإجراءات التقنية المتبعة في الحصول على الدليل المعلوماتي من حيث إنتاجها لدليل رقمي صحيح ومن الخطوات المتبعة للتأكد من سلامة الإجراءات من الناحية الفنية إخضاع الأداة المستخدمة لعدة تجارب للتأكد من دقتها في إعطاء النتائج المرجوة وذلك بإتباع اختبارين رئيسيين هما:

1- اختبار السليبات الزائفة: يتمثل في إخضاع الأداة المستخدمة في الحصول على الدليل لاختبار يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل الإلكتروني، وأنه لا يتم إغفال بيانات مهمة عنه.

2- اختبار الإيجابيات الزائفة: مفادها أن تخضع الأداة المستخدمة للتأكد من أنها لا تعرض بيانات إضافية جديدة. خالد عياد الحلبي المرجع السابق، ص 250-251.

(2) يقصد بسلسلة الرعاية أو الحضانة " مجموعة من الوثائق التي تثبت من الذي عالج الأدلة من وقت القبض عليه حتى تقديمها إلى المحكمة وهي الوثائق والشهادة المتعلقة بالحيازة، الحركة، المعالجة، ومكان الأدلة من وقت الحصول عليها حتى وقت تقديمها إلى المحكمة وتستخدم لإثبات أنه لم يحصل تغيير في الأدلة أو العبث بها بأي شكل من الأشكال وتعتبر هذه الوثائق مهمة سواء لضمان مقبولية الأدلة أو لإعطاء القيمة لها. Jesus Borrego, ibid, p15.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

- أن تكون المعلومات الموجودة في السجل، و المتعلقة بالوقت و التاريخ معلومة" (1).
- بينما تنص القواعد الفيدرالية على أن الشرط الأساسي للتوثيق أو التحقق من صحة وصدق الدليل، كشرط مسبق لقبوله هو أن يفي بأمانة أو بيئة كافية لان تدعم الوصول إلى الأمور التي تتصل بالموضوع بما يؤيد الادعاءات أو المطالبة المدعى بها(2).
- وفي نفس السياق وضعت المنظمة الدولية لدليل الحاسوب المعايير المطلوبة في الدليل المعلوماتي، وتمت المصادقة عليها خلال المؤتمر الدولي للبحث المعلوماتي و الجريمة التقنية المنعقد في تشرين الأول عام 1999 وهذه المعايير هي(3):
- عدم تغيير الدليل أثناء ضبطه.
- أن تتم عملية الضبط من قبل شخص مؤهل في المعلوماتية الشرعية.
- جميع النشاطات المتعلقة بالضبط و الوصول و التخزين ونقل الدليل الرقمي، يجب أن تكون موثقة ومحفوظة بغرض التدقيق.
- أن يكون الشخص الذي بحوزته الدليل الرقمي مسئولاً عن جميع الإجراءات المتعلقة بهذا الدليل.
- أن تكون الجهات المسؤولة عن ضبط وتخزين ونقل الدليل الرقمي و الوصول إليه مسؤولة عن تطبيق هذه المبادئ.
- بينما يري الفقه العربي بأن مخرجات الحاسوب ليس إلا نوعاً من أنواع الأدلة العلمية وفي إطار قناعة القاضي يميز هذا الفقه بين أمرين هما: القيمة العلمية القاطعة للدليل، و الظروف و الملابسات التي وجد فيها الدليل، فتقدير القاضي لا يتناول القيمة العلمية القاطعة للدليل لأن قيمة الدليل تقوم على أسس علمية دقيقة و لا حرية للقاضي في مناقشة الحقائق العلمية الثابتة

(1) محمد طارق عبد الرؤوف ألحن، المرجع السابق، ص 357.

(2) على حسن الطويلة، بحث بعنوان مشروعية الدليل المستمد من التفتيش الجنائي "دراسة مقارنة"، مركز الإعلام الأمني ، سنة 2009 . متاح على الموقع الإلكتروني: <http://www.Policemc.gov.bn/pdf>.

(3) محمد طارق عبد الرؤوف ألحن، المرجع السابق، ص 361.

أما ما يتعلق بالظروف والملابسات التي وجد فيها هذا الدليل فإنها تدخل في نطاق تقديره الشخصي لأنها من طبيعة عمله⁽¹⁾.

أما على المستوى التشريعي فقد حدد المشرع السوري الشروط الواجب توافرها في الأدلة الرقمية بنص صريح تضمنتها المادة 25 من المرسوم التشريعي رقم 17 لسنة 2012⁽²⁾، متقدماً بذلك على التشريعات العربية الأخرى.

بينما المشرع الجنائي الجزائري فإنه لم يحدد صراحة شروط قبول الدليل المعلوماتي، إلا أنه وبعد الاطلاع على نص المادة 06 من القانون 04/09 يتبين بأن المشرع أكد على ضرورة السهر على "سلامة المعطيات"⁽³⁾ في المنظومة المعلوماتية أثناء التفتيش عنها وحجزها، وكذا عدم المساس بها في حالة إعادة تشكيل هذه المعطيات لاستعمالها في التحقيق.

ثانياً- أن يكون الدليل المعلوماتي قد طرح في الجلسة للمناقشة:

كُرس مبدأ ضرورة مناقشة الأدلة في الجلسة في أغلب التشريعات الإجرائية فهو يعد ضماناً للمتهم، فلا يجوز للقاضي الجزائري الاستناد في حكمه إلى أي دليل لم يطرح في الجلسة للمناقشة والتمحيص، ولذلك تنص المادة 02/212 من ق.إ.ج.ج على أنه " ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات و التي حصلت المناقشة فيها حضورياً أمامه".

(1) محمد طارق عبد الرؤوف ألحن، المرجع السابق، ص362.

(2) تنص على أنه " يعود للمحكمة تقدير قيمة الدليل الرقمي شريطة تحقق ما يلي:

1- أن تكون الأجهزة الحاسوبية أو المنظومات المعلوماتية المستمد منها هذا الدليل تعمل على نحو سليم.

2- ألا يطرأ على الدليل المقدم إلى المحكمة أي تغيير خلال مدة حفظه

يعد الدليل الرقمي المقدم إلى المحكمة مستجعماً للشروطين الواردين في الفقرة أ من هذه المادة ما لم يثبت العكس".

(3) نجد لضرورة المحافظة على سلامة المعطيات أصل في المادة 323 مكرر 1 من القانون المدني الجزائري التي اشترط فيها المشرع الجزائري ضرورة حفظ المحرر الإلكتروني بشكل يضمن سلامته كشرط جوهري للأخذ به مثله مثل المحرر الورقي . ويبدو أن المشرع الجزائري انتهج نفس النهج المستقر عليه في قانون الإنيسترال في المادة 01/10 منه بخصوص الشروط الواجب توافرها في الكتابة الإلكترونية حتى يتسنى الاعتداد بها في الإثبات. انظر براهيم حنان، مقالة بعنوان المحررات الإلكترونية كدليل إثبات ، منشورة في مجلة المفكر، العدد التاسع، جامعة محمد خيضر بسكرة، الجزائر، سنة 2013 ، ص 145. كذلك زبيحة زيدان ، المرجع السابق، ص

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

ويستوي الأمر بالنسبة للأدلة المعلوماتية سواء كانت في شكل مخرجات ورقية أو إلكترونية أو معروضة بواسطة الكمبيوتر على الشاشة الخاصة به، فيجب أن تعرض للمناقشة أثناء المحاكمة بوصفها أدلة إثبات، وللقاضي الجزائي الحرية في أن يستمد قناعته منها طالما اطمأن لها ووقعت عليها المرافعات وناقشها أطراف الدعوى⁽¹⁾. ويترب على هذه القاعدة شرطان أساسيان نتناولهما كما يلي:

أ- وجوب مناقشة الدليل الإلكتروني بين أطراف الدعوى:

فلا يجوز للمحكمة أن تقتصر على مجرد الاعتماد على الأدلة التي أنتجها التحقيق الابتدائي إذ يناقض ذلك مبدأ أساسيا هو مبدأ شفوية المحاكمة وإنما على القاضي أن يعيد تحقيق الدعوى تحقيقا نهائيا فتطرح من جديد الأدلة التي أنتجها التحقيق الابتدائي ويتاح لجميع أطراف الدعوى مناقشتها على مسمع من القاضي، ويتاح لكل منهم أن يواجه الآخر برأيه وتقديره لكل دليل وتطبيقا لذلك فإن الحكم يخطئ إذا اعتمد على دليل نتج عن التحقيق الابتدائي دون أن يطرحه على المناقشة في الجلسة ثم يقره فيحيله إلى دليل قضائي يسوغ أن يعتمد عليه الحكم⁽²⁾.
و إجمالا فالقاضي وهو يمارس سلطته في تقدير الأدلة أن يطرح أي دليل لا يطمأن إليه خلال تقديره لا قبل ذلك، فلا يجوز له مثلا استبعاد شهادة احد الشهود قبل سماعه⁽³⁾.

كما يجب أن تكون الأدلة المقدمة للمناقشة أثناء المحاكمة ذات صلة وهو ما أكد عليه المشرع الأمريكي في المادة 401 من FRE⁽⁴⁾.

ولعل مسألة مناقشة الدليل المعلوماتي في الجلسة يطرح مسألتين، أما الأولى فهي ضرورة تكوين قضاة متخصصين في هذا النوع من الجرائم، ويظهر ذلك جليا عند توجيه النقاش للوصول

(1) رشيدة بوكر، المرجع السابق، ص 513.

(2) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الأول، المرجع السابق، ص 555.

(3) فاضل زيدان محمد، المرجع السابق، ص 127.

(4) وتعد فترة الاكتشاف في القانون الإجرائي الأمريكي مرحلة مهمة تتوسط توجيه الاتهام وجلسة المحاكمة، فتتم الاكتشافات في لقاء المؤتمر وفيها يقدم الأطراف الأدلة الإلكترونية الموجودة والمتعلقة بالقضية ، كما يحدد كل من FRE و القواعد الاتحادية للإجراءات المدنية FRCR ماهي طبيعة وأشكال الأدلة التي ستقدم إلى المحكمة34p, ibid, Jesus Borrego

إلى الحقيقة، وكذا أن يكون هناك محامين على قدر عال من الاحترافية التقنية، والمعارف المعلوماتية، حتى نضمن محاكمة عادلة للمتهمين المعلوماتيين، أما المسألة الثانية فتتطلب توفر تقنيات وتجهيزات حديثة لمناقشة الأدلة المعلوماتية المتعلقة بالمعطيات و البيانات، تسمح بمشاهدة الدليل عبر وسائط إلكترونية في قاعة المحاكمة، لأن المعمول به حاليا في المناقشة أنها تكون شفافة استنادا إلى وثائق الدعوى المادية، ففي اعتقادنا فيه نوع من عدم الموازنة بين الطبيعة الفنية للدليل وقرينة البراءة .

ففي الملتقى الدولي المنعقد بالجزائر بتاريخ 5-6 ماي 2010 حول مكافحة الجريمة المعلوماتية، الذي ضم خبراء دوليين متخصصين في الجرائم المعلوماتية، طرح تساؤل مضمونه هل ممكن الحصول على محاكمة رقمية، في هذا الصدد أجاب مايكل موران ضابط في الاستعلامات، وهو خبير متخصص لدى الانترنت بنعم وبكل وضوح، ولهذا أكد على وجوب توفير قاعة جلسات إلكترونية مهيئة (Power Point) و لا بد من تحضير: عرض متعدد الوسائط، قاعة جلسات خاصة، استعمال برنامج عرض، ومحاكمة رقمية، وأضاف انه حاليا في أيرلندا خصصت قاعات سمعية بصرية لنفس الغرض، يقوم المحقق بتوصيل جهازه المحمول بقاعة الجلسات المخصصة ، ليقوم القاضي المتخصص بمراقبة جميع الشاشات في القاعة، وكل ما يحوزه المحقق يظهر تلقائيا للقاضي، وهو وحده من يقرر لمن يسمح له بالاطلاع على هذه البيانات المشككة للدليل، هيئة الدفاع، أو المحلفين⁽¹⁾.

ب- عدم جواز بناء اقتناع القاضي الجزائي على المعلومات الشخصية:

من أهم النتائج المترتبة على قاعدة وجوب طرح الدليل بالجلسة، أنه لا يجوز للقاضي الجزائي أن يحكم بمقتضى معلوماته الشخصية أو بناء على ما رآه أو سمعه⁽²⁾، أو حقه في غير مجلس

(1) Michael Moran, communication sous titre « Les pratiques du recueil de la preuve électronique » commis dans l'Actes du séminaire international Alger le 5-6 Mai 201, op cit, p 191-192.

(2) يجدر على القاضي الذي توافرت لديه معلومات شخصية خاصة عن الدعوى أن يتتحي عن نظرها إعمالا لإجراءات الرد تطبيقا للمواد من 554 إلى 566 من ق.إ.ج.ج وفي ذلك قررت المحكمة العليا انه " يتعين على كل قاض يعلم بقيام سبب من أسباب الرد

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

القضاء، وبدون حضور الخصوم، و السبب في ذلك أن هذه المعلومات لم تعرض بالجلسة ولم تتح فرصة مناقشتها وتقييمها و الاعتماد عليها يكون مناهضا لقاعدة الشفوية و المواجهة التي تسود مرحلة المحاكمة، ولا يعد قضاءا بالمعلومات الشخصية استناد القاضي في حكمه إلى رأي يقول به العلم أو يجري به العرف شريطة ألا يستند إلى أي رأي محل خلاف علمي⁽¹⁾.

ولعل الأدلة المعلوماتية من النوع الذي يقتضي بان يكون القاضي الجزائي محيطا بمعارف تقنية تساعده في تقدير الدليل وفي تقديرنا انه مهما كان مستوى القاضي عاليا ومتخصصا في الجرائم المعلوماتية فانه يتطلب الاستعانة بأهل الخبرة لأن الدليل علمي و يتطلب تقرير فني ليطمئن به أطراف الدعوى وكذا لإتاحة الفرصة لمناقشة الدليل بدلا من أن يستأثر به القاضي في وجدانه، ويحرم بذلك الأطراف من أبداء الرأي بشأنها.

ثالثا- أن يكون للدليل الرقمي أصل في أوراق الدعوى:

يجب أن يكون للدليل المعلوماتي أصل ثابت في أوراق الدعوى، بحيث تتاح للخصوم فرصة الإطلاع عليه ومناقشته احتراما لحقوق الدفاع، لذلك فانه لا يجوز للقاضي أن يبني حكمه على دليل لا صلة له في الأوراق، فالدليل الذي لا يتحقق فيه هذا الشرط يكون منعذما في نظر القانون وذلك استنادا إلى قاعدة وجوب تدوين كافة إجراءات الاستدلال و التحقيق، ليتبين للخصوم ما يقدم ضدهم و تتاح الفرصة لهم لمناقشتها⁽²⁾.

كما أن توافر أصل الدليل لا يؤثر في صحة الحكم إذا ورد خطأ في الإشارة إلى مصدره⁽³⁾ بينما يكون الدليل باطلا لبنائه على أسس فاسدة إذا لم يجد له أصلا في أوراق الدعوى سواء تعلق بالإدانة أو البراءة⁽¹⁾.

أن يصرح بذلك لرئيس المجلس القضائي فإن القضاء بما يخالف أحكام هذا المبدأ يعد خرقا للقانون.المجلة القضائية، العدد 03 سنة 1991 ، ص 241.

(1) مروك نصر الدين، محاضرات في الإثبات الجنائي النظرية العامة للإثبات الجنائي، الجزء الأول، المرجع السابق، ص 642-643.

(2) رشيدة بوكر، المرجع السابق، ص 511.

(3) فوزية عبد الستار، المرجع السابق، ص 531.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

لذلك أوجب المشرع تحرير محضر بيانات الجلسة لإثبات وقائع الدعوى الجزائية وأدلتها لكي يتمكن قاضي الموضوع أو أي من الخصوم من الرجوع إلى هذا المحضر عند الحاجة، وتشترط محكمة النقض المصرية أن يكون الدليل الثابت في أوراق الدعوى عمد الحكم أي استندت إليه المحكمة في تكوين عقيدتها⁽²⁾.

فيما أكدت المحكمة العليا الجزائرية في قرار لها على صحة بناء الاقتناع على أدلة لها أصل في الدعوى بقولها "لقضاة الموضوع السلطة المطلقة في تقدير أدلة الإثبات بدون معقب مادام ما استندوا إليه له أصل ثابت في أوراق الدعوى"⁽³⁾.

بعدما تطرقنا إلى الضوابط المقيدة لحرية اقتناع القاضي المستمدة من الدليل المعلوماتي نفسه ننقل إلى دراسة الضوابط المتعلقة بالاقتناع القضائي نفسه في الفرع الموالي.

الفرع الثاني: الضوابط المتعلقة بالاقتناع القضائي.

إن سلطة القاضي الجزائري في تقدير الأدلة الرقمية وموازنتها وفقا لما يمليه عليه وجدانه لا يخضع في ذلك لمراقبة المحكمة العليا⁽⁴⁾، إلا أنه مع ذلك مقيد بضرورة تأسيس اقتناعه على الجزم و اليقين نتناوله بالدراسة أولا من غير أن يكون هذا الاقتناع مخالفا لمقتضيات العقل و المنطق السليم وهو ما سنتطرق إليه ثانيا.

أولا- بلوغ الاقتناع القضائي درجة اليقين:

(1) انظر سليمان أحمد فضل، المرجع السابق، ص 375.

(2) عائشة بن قارة مصطفي، المرجع السابق، ص 273.

(3) قرار رقم 25814 بتاريخ 1982/01/05 . عادل مستاري ، مقالة بعنوان دور القاضي الجزائري في ظل مبدأ الاقتناع القضائي مجلة المنتدى القانوني، العدد الخامس، ص 189 و191.

(4) وهو ما تصرح به محكمة النقض الفرنسية وكذا المصرية ولكن لا يعدو في حقيقة الأمر أن يكون سوى مظهرا أكثر منه إلى الحقيقة فقد لاحظت محكمة النقض أن رقابتها هي الوسيلة الوحيدة لمنع انزلاق حرية القاضي الجنائي في الاقتناع إلى درجة التحكم فوجدت نفسها مضطرة إلى أن تقوم بدور هام في وضع تلك الحرية في إطاره الطبيعي حتى يبقى اقتناع القاضي يقينيا قائما على أدلة يقينية ففرضت ذلك عن طريق رقابتها لتسبب الحكم حتى يكون غير منطوي على مخالفة لمقتضى العقل و المنطق .انظر محمد زكي أبو عامر، المرجع السابق، ص 151-152.

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

الأصل أن الجزم واليقين المطلوبين في الاقتناع القضائي لا يعني بهما الجزم واليقين المطلقين
فذلك لا سبيل إلى تحقيقه بالنسبة لأدلة الإثبات القولية بصفة خاصة لأن اليقين المطلق إنما هو
شيء يتحقق فقط في الأمور التي لها تكييف مادي بالترقيم أو التحليل أو الإحصاء (1). و أن
اليقين الذي يصل إليه القاضي ليس يقينا مطلقا، بل يقينا نسبيا ومن ثم فالنتائج التي يمكن
التوصل إليها تكون عرضة للتنوع و الاختلاف في التقدير من قاضي إلى آخر لأن الجزم و اليقين
المراد توافره في مجال الإثبات الجنائي هو اليقين النسبي القائم على التدليل و التسبيب، لا اليقين
المطلق لأن ذلك ليس بمقدور البشر(2).

وفيما يلي نتطرق إلى المقصود باليقين القضائي ثم طريقة الوصول إلى اليقين القضائي وأخيرا
البراءة كاستثناء من شرط اليقين.

أ- المقصود باليقين القضائي:

عرف بعض الفقهاء اليقين بأنه عبارة عن "اقتناع مستند إلى حجج ثابتة وقطعية" (3)، أو انه
عبارة عن "حالة ذهنية وعقلية تؤكد وجود الحقيقة" (4)، وعرف كذلك بأنه " حالة ذهنية تلتصق
بالحقيقة دون أن تختلط بأي شك، فهي من الناحية الشخصية تتعارض مع الشك، ومن الناحية
الموضوعية فوق الجهل و الغلط ودرجة اليقين تختلف بحسب المكناات المعطاة، واليقين المادي
هو الدرجة القصوى فيه" (5). واليقين يقوم على أدلة و تسبيب لذلك فهو يقين تقريبي يوصف في
العلم بأنه اقتناع وهو ثمرة اليقين .

ب- طريقة الوصول إلى اليقين القضائي:

(1) مروك نصر الدين، محاضرات في الإثبات الجنائي النظرية العامة للإثبات الجنائي، الجزء الأول، المرجع السابق، ص 644.
(2) بلولهي مراد، الحدود القانونية لسلطة القاضي الجزائي في تقدير الأدلة، مذكرة مقدمة لنيل درجة الماجستير في العلوم القانونية
تخصص علوم جنائية، جامعة الحاج لخضر باتنة، السنة الجامعية 2010-2011، ص 119.
(3) رشيدة بوكري، المرجع السابق، ص 517.
(4) عائشة بن قارة مصطفى، المرجع السابق، ص 277.
(5) محمد زكي أبو عامر، المرجع السابق، ص 136.

إن الوصول إلى اليقين يتم عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال وقائع الدعوى وما يرتبه ذلك في ذهنه من تصورات ذات درجة عالية من التوكيد وعندما يصل القاضي إلى هذه المرحلة من اليقين يصبح مقتنعا بالحقيقة⁽¹⁾.

و المطلوب عند الاقتناع ليس اليقين الشخصي المتمثل في وجدان القاضي وما يطمئن إليه فحسب⁽²⁾، وإنما هو يقين قضائي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل بذاتها معالم قوتها في الإقناع بحيث لو طرحت على قاض آخر لتوصل إلى نفس الحكم و اليقين الذي توصل إليه القاضي الأول⁽³⁾، وعموما تتلخص عملية الوصول إلى اليقين في ثلاث نقاط أساسية:

- ما يستخلص من الواقعة من إمكانات، فالصور التي تنقلها حواس الإنسان وتتفق مع الأفكار الممكنة ويزداد تأكدها عن طريق الخبرة الإنسانية المكتسبة ينظر إليها بأنها حقيقة.

- الاستدلال المستمد من تقييم الوقائع وهذا يتطلب أن يكون هناك قدرا من التشابه بشيئين وعلى قدر هذا التشابه أو الاختلاف يمكن التوصل إلى الأسباب الصحيحة المقنعة.

- الاستنتاجات المستمدة من الظروف إذا كانت مرتبطة بالواقعة⁽⁴⁾.

وعلى هذا الأساس فالقاضي يصل إلى يقينية الأدلة المعلوماتية المجسدة بمخرجات الكمبيوترية تتطلب نوعين من المعرفة: أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه المخرجات وتفحصها وثانيهما المعرفة العقلية عن طريق التحليل و الاستنتاج من خلال الربط بين هذه المخرجات و الملابسات التي أحاطت بها⁽⁵⁾.

(1) عائشة بن قارة مصطفى، المرجع السابق، ص 277-278.

(2) أشرف عبد القادر قنديل، النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي، دار الجامعة الجديدة، الإسكندرية مصر، سنة 2011، ص 238.

(3) محمد محدة، مقالة بعنوان السلطة التقديرية للقاضي الجزائي منشورة في مجلة البحوث و الدراسات، العدد الأول المركز الجامعي الوادي، الجزائر، أبريل 2004، ص 35.

(4) سليمان أحمد فضل، المرجع السابق، ص 372.

(5) سليمان أحمد فضل، المرجع السابق، ص 373.

والقاضي الجزائي بدوره الايجابي في الإثبات يتطلب عليه أن يكون متمكنا من نوع جديد من المعرفة تتمثل في التقنيات المعلوماتية⁽¹⁾، وبالمقابل لابد من اتخاذ كل الاحتياطات التقنية اللازمة بدءا من العثور على الدليل الرقمي، إلى حفظه وتحليل المعطيات تمهيدا أو تحسبا لعرضها أمام القاضي الجزائي⁽²⁾.

فإذا لم ينته بعد ذلك القاضي إلى الجزم بإنساب الجريمة المعلوماتية إلى المجرم المعلوماتي كان من المتعين عليه تبرئة ساحتها، لأن الدليل المعلوماتي ذو طبيعة رقمية علمية لا يترك مجالا للشك، ما يتعين معها شرط اليقينية، بمعنى يجب أن يكون يقين القاضي قاطعا، لأنه لا مجال للنسبية في المسائل العلمية فكما يقال أن القانون يوصلنا إلى العدالة بينما العلم يوصلنا إلى الحقيقة.

ثانيا - أن يكون الاقتناع القضائي متوائما مع مقتضيات العقل و المنطق .

يلتزم القاضي بأن يبني اقتناعه على عملية عقلية منطقية تقوم على الاستقراء و الاستنباط ينتهي في ختامها إلى نتيجة معينة كاستخلاص للواقعة⁽³⁾.

وهذا الاستخلاص السائغ عقلا ومنطقا هو الشرط الذي يجعل الحكم القضائي تعبيراً عن اقتناع موضوعي وليس نتيجة رأي شخصي، كما أن انتفاء التناقض و التضارب من الحكم هو إحدى تطبيقات هذا الاستخلاص، بينما الإيجاز المخل ينتج عنه غموض وإبهام وهذا يعيب الاستخلاص السائغ عقلا ومنطقا⁽⁴⁾.

لذلك تواترت محكمة النقض المصرية على أن يكون استخلاص محكمة الموضوع لواقعة الدعوى استخلاصا معقولا سائغا، ومعيار معقولية الاقتناع هو أن يكون الدليل بما في ذلك الدليل

(1) عائشة بن قارة مصطفى، المرجع السابق، ص 279.

(2) Marie Barel, article sous titre Fraude informatique et preuve ; la quadrature du cercle, acte du symposium SSTIC05, p06.disponible sur le site : <http://www.actes.sstic.org/.date>.

(3) أحمد فتحي سرور، المرجع السابق، ص 470.

(4) أشرف عبد القادر قنديل، المرجع السابق، ص 239.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

المعلوماتي مؤديا إلى ما رتبته الحكم عليه، من غير تعسف في الاستنتاج، ولا تتأفر مع مقتضيات العقل و المنطق، وفي ذلك قضت " انه وإن كان من حق محكمة الموضوع أن تستخلص الواقعة من أدلتها و عناصرها المختلفة، إلا أن شرط ذلك أن يكون هذا الاستخلاص سائغا تؤدي إليه ظروف الواقعة و أدلتها وقرائن الأحوال فيها.."⁽¹⁾.

و ضمانا للوصول إلى الاقتناع القضائي بالعقل و المنطق استقر قضاء محكمة النقض المصرية على المعايير الآتية⁽²⁾:

- لا يجوز الاعتماد في الإثبات على الدلائل وحدها، بل يجب أن تكون مكملة للدليل.
- لا يجوز للمحكمة أن تحل نفسها محل الخبير في مسألة فنية بحتة ، بل عليها ألا تشق طريقها لإبداء الرأي فيها دون الاستعانة بخبير يخضع رأيه لتقديرها، كل ذلك دون إخلال بسلطة المحكمة في تقدير رأي هذا الخبير وفقا لاقتناعها، وهو ما ينطبق على الخبراء المعلوماتيين والأدلة المعلوماتية التي توصلوا إلى استخلاصها.
- الالتزام بمبدأ تساند الأدلة عند الإدانة فيجب أن تكون متكاملة بعضها ببعض ومنها مجتمعة تتكون عقيدة المحكمة . فلا بد في الجريمة المعلوماتية أن تتساند الأدلة التقليدية و الأدلة التقنية الحديثة بعد مناقشتها حضوريا من اجل بناء عقيدة القاضي الجزائي.

ثالثا - الاستثناء الوارد بشأن الاقتناع اليقيني:

إن اليقين الذي تستند إليه المحكمة في حكمها يستمد جذوره من "قرينة البراءة"⁽³⁾ فإذا قضى القاضي الجزائي بالإدانة فلا بد أن يكون هذا القضاء مبنيا على اليقين الذي ينفي الأصل وهو

(1) عائشة بن قارة مصطفى، المرجع السابق، ص 281.

(2) أحمد فتحي سرور، المرجع السابق، ص 470-471.

(3) تعني قرينة البراءة أن الأصل في المتهم بريء حتي يقوم الدليل على ادانته وتترتب على هذه القرينة نتيجتان الأولى وقوع عبء الإثبات على عاتق النيابة العامة، و الثانية تفسير الشك لفائدة المتهم. انظر فوزية عبد الستار، المرجع السابق، ص 523. وقد اقرها الدستور الجزائري في المادة 45 بقوله "كل شخص يعتبر بريئا حتي تثبت جهة قضائية نظامية إدانته، مع كل الضمانات التي يتطلبها القانون"

الفصل الثاني.....إثبات الجريمة المعلوماتية بالدليل الرقمي.

البراءة، فالشك في الإثبات يعني إسقاط أدلة الاتهام والعودة إلى الأصل العام في المتهم وهو البراءة⁽¹⁾ ويسود رأي في الفقه مفاده وجوب تطبيق قاعدة تفسير الشك لصالح المتهم في كل الحالات التي يكون فيها شك في إدانة المتهم سواء كان هذا الشك موضوعيا يتعلق بماديات الجريمة أو شخصيا يتعلق بتقدير القاضي لأدلة الدعوى⁽²⁾.

واستنادا إلى قرينة البراءة فإن الإدانة لا تبني إلا على الجزم واليقين، أما البراءة فيجوز أن تبني على الشك، فالقاضي لا يتطلب للحكم بالبراءة دليلا قاطعا على ذلك، ولكنه يكفيها ألا يكون ثمة دليل قطعي على الإدانة، وتستوي البراءة التي تستند على اليقين بها، وبراءة تستند على الشك في الإدانة، ويعبر عنها كذلك بالبراءة لعدم كفاية الأدلة⁽³⁾.

وعلى هذا الأساس فإن القاضي الجزائي وهو بصدد النظر في قيام أركان الجريمة المعلوماتية، والبحث عن الأدلة المعلوماتية وكفايتها للإدانة فإنه في حالة عدم كفايتها تكون التهمة غير ثابتة في حق المجرم المعلوماتي، يتعين عليه التصريح ببراءة المتهم بسبب عدم وصوله درجة الاقتناع اليقيني تطبيقا لقاعدة تفسير الشك لفائدة المتهم، والتي تعتبر إحدى نتيجتي قرينة البراءة،

وهو ما نص عليه المشرع الجزائري في المادة 364 من ق.إ.ج.ج⁽⁴⁾. وكذلك المشرع المصري في المادة 304 من قانون إجراءاته الجنائية، غير أن محكمة النقض المصرية وضعت شرطا لذلك يتمثل في أنه يجب أن يتضمن الحكم ما يفيد أن المحكمة قد فحصت الدعوى وأحاطت بأدلتها عن بصر وبصيرة، ووازنت بين أدلة الثبوت وأدلة النفي، ولم تقتنع على وجه اليقين بإدانة المتهم⁽⁵⁾.

(1) ممدوح خليل البحر، المرجع السابق، ص 369.

(2) بلولهي مراد، المرجع السابق، ص 121.

(3) محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، الجزء الثاني، المرجع السابق، ص 859.

(4) تنص المادة 364 ق.إ.ج.ج. على أنه "إذا رأت المحكمة أن الواقعة موضوع المتابعة لا تكون أية جريمة في قانون العقوبات أو أنها غير ثابتة أو غير مسندة للمتهم قضت ببراءته من المتابعة بغير عقوبة ولا مصاريف.

(5) عائشة بن قارة مصطفى، المرجع السابق، ص 279-280.

الفصل الثانيإثبات الجريمة المعلوماتية بالدليل الرقمي.

والحقيقة انه حتى محكمة النقض الجزائرية اشترطت أن يكون الحكم القاضي بالبراءة معللا ومسببا تسببيا كافيا شأنه في ذلك شأن الحكم بالإدانة⁽¹⁾.

وخلاصة فان الإثبات بالدليل الرقمي أضحى حقيقة علمية و ضرورة حتمية فهو دليل علمي أفرزته البيئة المعلوماتية كمسار يمكن من خلاله تقصي الحقائق المعلوماتية، فهو وسيلة تعطي الثقة في الإثبات وتسد الثغرة التي أنتجتها الجرائم المعلوماتية في موازين الإثبات بشكل عام.

فالدليل الرقمي وان لم يتناوله المشرع الجزائري بنصوص صريحة إلا أنه تناوله ضمنا فهياً له إجراءات استخلاصه من خلال التعديلات التي مست قانون الإجراءات الجزائية بالقانون 06-22 ليعزز منظومته القانونية بالقانون 04/09 والتي تعتبر نقلة نوعية ومسايرة للتطور التشريعي المقارن المصاحب للجريمة المعلوماتية.

أما بالنسبة لحجية الدليل الرقمي فيجد مكانته ضمن طرق الإثبات، وفقا لمبدأ الإثبات الحر المنصوص عليه في المادة 212 من ق.إ.ج.ج، و يبقى أن له نفس الحجية في الإثبات، مثله مثل سائر الأدلة التقليدية شريطة أن يكون مشروعا مع التأكيد على تفوقه من الناحية الفنية، كل ذلك في إطار مبدأ السلطة التقديرية للقاضي .

(1) في شأن تسبب أحكام البراءة قضت المحكمة العليا الجزائرية في قرارها الصادر بتاريخ 1981/11/12 تحت رقم 22416 " إن القرارات القضائية بالبراءة مثلها مثل القرارات الصادرة بالإدانة يجب أن تعلل تعليلا كافيا حتي تتمكن المحكمة العليا من مراقبة صحة تطبيق القانون، فالقرار الذي يكتفي بالحكم بالبراءة بمقولة أنه يوجد في الدعوى شك لصالح المتهم يعتبر ناقص التسبب ويستوجب النقض. انظر بلولهي مراد، المرجع السابق، ص120.

الخاتمة:

قدمنا في هذه المذكرة دراسة متواضعة لموضوع وسائل الإثبات في الجريمة المعلوماتية، ما يتوجب على الباحث في نهاية الدراسة أن يضع في إطار واحد النتائج وبعض الاقتراحات التي توصل إليها في مختلف جوانب المذكرة، وتلخص أهم هذه النتائج والاقتراحات في ما يلي:

أولاً- النتائج:

- خلص البحث إلى اعتبار وسائل الإثبات مجموع الأدلة والطرق القانونية التي تؤدي إلى إظهار الحقيقة، وان وسائل الإثبات محل الدراسة لا تتناول المسائل التقنية في البرمجة ودراسة المعطيات كنوعية البرامج المستخدمة في استرجاع البيانات مثلاً فهي مسائل تخرج من نطاق البحث باستثناء ذكرها على سبيل توضيح الفكرة.

- في الإطار المفاهيمي للبحث اتضح وجود خلاف بين الفقهاء في وضع إطار شامل ونموذجي للجريمة سواء من حيث التعريف أو من حيث التقسيمات أو من حيث طريقة المعالجة، وهو ما ينعكس سلبياً على موضوع الإثبات.

- إن صعوبة الإثبات في الجريمة المعلوماتية تعد من أبرز خصائصها باتفاق الباحثين بسبب خفاء الأثر المادي لها، بسبب استخدام الجاني وسائل فنية وتقنية معقدة، علاوة على سهولة محو الدليل والتلاعب به في وقت تفتقر فيه هذه الجرائم إلى الدليل المادي التقليدي.

- مبدأ حرية الإثبات ومبدأ الاقتناع القضائي هما الضابطان في تقديم وتقدير الأدلة أمام القضاء لإثبات الجريمة المعلوماتية، مع إدخال تعديلات نالت جانب التحقيق تضمنه القانون 04/09.

- مسايرة لطبيعة الجريمة تم اللجوء إلى فئة جديدة من الشهود هم الشهود المعلوماتيين فهم ليسوا من فئة الأشخاص العاديين، وإنما من فئة تحسن التعامل مع المعطيات و البيانات وانتقل دورهم من مرحلة الالتزام بأداء الشهادة إلى مبدأ الالتزام بالإعلام في الجريمة المعلوماتية ومساعدة جهات التحقيق تحت طائلة المساءلات، وهو ما جاء به المشرع الجزائري في القانون 04/09.

- الاعتراف في الجريمة المعلوماتية يتطلب شروط خاصة إلى جانب الشروط العامة المتعارف عليها وهي أن يكون له مستوى معرفي في المجال المعلوماتي يسمح بتحديد طرق ارتكاب الجريمة.
- تعد الخبرة في الجريمة المعلوماتية من الوسائل المتطلبة في الإثبات من خلالها يقدم الدليل المعلوماتي، ويمكن القول أنها عامل جوهري أمام نقص التكوين المعلوماتي لأجهزة العدالة.
- مع ظهور الأدلة العلمية صاحبها بروز دور القرائن في مساعدة القاضي الجزائي من ناحية تكوين القناعة من أجل الوصول إلى الجاني.
- سمح المشرع بإجراء مراقبة الاتصالات الالكترونية في القانون 04/09 وقبله في تعديل قانون الإجراءات الجزائية بالقانون 22-06، ويرى الباحث أن هذا السماح فيه مخالفة لقاعدة دستورية تضمنتها المادة 39 منه بنصها على سرية المراسلات والاتصالات بكل أشكالها مضمونة، دون أن تتضمن المادة عبارة الاستثناء كما فعلت باقي التشريعات المقارنة مما يتطلب التدارك القانوني لها.
- يمكن إجراء التفتيش في المنظومة المعلوماتية ولو عن بعد، هو إجراء يحسب للمشرع الجزائي في خضم الغموض القانوني الذي تعيشه التشريعات المقارنة في هذه المسألة، ويمكن إجراء التفتيش في جميع الأوقات وان اقتضت الضرورة دون حضور صاحب محل التفتيش وذلك تغليباً لمصلحة المجتمع على مصلحة الفرد بالنظر إلى طبيعة الجريمة والأدلة المثبتة لها.
- أثبت البحث أن معظم أدلة الإثبات التقليدية التي شملتها الدراسة ليست لها الحجية الكافية في إثبات الجريمة المعلوماتية وجل الوسائل إنما أثبتت أنها تتلاءم مع استخلاص الدليل الرقمي، وانتقل دورها من وسائل قائمة بنفسها إلى دور تكميلي يتمثل في المساعدة على الوصول إلى الدليل الأهم وهو الدليل الرقمي.
- الأدلة الرقمية هي نوع متميز من وسائل الإثبات ولها من الخصائص العلمية و المواصفات القانونية ما يؤهلها لتكون إضافة جديدة لأنواع الأدلة، وهي تعرف قبولا قانونيا في مختلف التشريعات المقارنة اللاتينية والانجلوسكسونية وحتى المختلطة مع ضبطها لشروط خاصة لقبولها

يقينا منها بأنه الوسيلة الوحيدة التي باستطاعتها إخراج الحقائق الرقمية إلى العالم المادي للحكم عليها.

- لم يتناول المشرع الجزائري الدليل الرقمي لا بالتعريف و لا بنصوص تحدد شروط قبوله أمام القضاء بالرغم من انه تناولها ضمنيا في القانون 04/09 وترك المسألة خاضعة لإطارها التقليدي في الإجراءات و التي تخضع لمبدأ حرية الإثبات استنادا إلى نص المادة 212 من ق.إ.ج وبالمقابل قيد هذه الحرية بالافتناع القضائي الحر المحدد بضوابط متعلقة بالدليل نفسه، وأخري بالافتناع نفسه.

- يمكن للقاضي الجزائري الأخذ بالدليل الرقمي إذا توفرت مجموعة من الشروط، أهمها المشروعية ومطابقة الدليل الرقمي للأصل مع سلامة أنظمة الحاسوب بشكل لا يرقى إليه الشك في مصداقيته، أما مسألة التقدير فلا بد من التمييز بين الحجية العلمية القاطعة للدليل و الملابسات المحيطة به ، فالأولي لا مجال فيها لمنازعة ما توصلت إليه التكنولوجيا أما الثانية فهي تخضع لتقدير القاضي، ويساعده في ذلك الأدلة التقليدية الأخرى كالاقرار و الشهادة والقرائن. مع التأكيد على ضرورة إسناد هذا النوع من القضايا إلى قضاة متخصصين تلقوا تكويننا خاصا في المجال المعلوماتي إلى جانب كونهم خبراء في القانون.

ثانيا - الاقتراحات:

يقدم الباحث مقترحات متواضعة خلص إليها من دراسته للموضوع وهي:

- ضرورة الإسراع في إصدار النصوص المفعلة للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال المنشأة بالقانون 04/09.

- دعوة المشرع إلى وضع نصوص قانونية تعطي الغطاء التشريعي للأدلة الرقمية مع تحديد شروط قبولها، و إضفاء لها نوع من الحجية بشكل يسمح للمنظومة القضائية بتبنيها في معالجة قضايا الجرائم المعلوماتية.

- صياغة قانون جديد للإثبات الجنائي مستقل عن المنظومة الإجرائية التقليدية، يتماشى مع تطور الجريمة، كما هو معمول به في أغلب التشريعات المقارنة.
- ضرورة الاهتمام بالتكوين وبصورة جدية على جميع المستويات فالي جانب الضبطية القضائية التي عرفت نقلات نوعية واهتمام بالموضوع، يجب التفكير في توظيف قضاة يجمعون بين المعرفة التقنية والمعرفة القانونية كقضاة متخصصين، وإخضاعهم لتكوين متخصص، مع استفادتهم من تريضات لضمان تكوين عال المستوي للرفع من مستوى المنظومة القضائية، مع التأكيد كذلك على نقابات المحامين بتوفير شروط التكوين وإجراء ندوات و ملتقيات علمية في هذا المجال.
- تعميم إنشاء مختبرات لمعالجة واستخراج الأدلة الرقمية، مع تشجيع الفئات المختصة في المجال التقني على تبني الفكرة، وذلك بتقديم تسهيلات مادية وإزالة العراقيل الإدارية.
- السماح للمتقاضين باللجوء إلى الخبرات التقنية الاستشارية، كما هو معمول به في التشريعات المقارنة، كضمانة لحقوق المتقاضين وتجنباً للأخطاء القضائية المترتبة على محدودية الكفاءات في الخبرات المعتمدة.
- في إطار السياسة الجنائية الحديثة لترشيد العقوبة، التأكيد على ضرورة الاستفادة من خبرات المجرمين المعلوماتيين، باستبدال العقوبات الأصلية بعقوبة العمل للنفع العام، حتى ولو كان المتهم مسبقاً، بعد إعادة النظر في الشروط المحددة في قانون الاستفادة من قانون النفع العام ، مع السعي على دمجهم في مصالح تستفيد منهم وتحتويهم في نفس الوقت.
- بعث التعاون الدولي في المجال القضائي، للاستفادة من تجارب الدول المتقدمة في مجال المتابعات و المحاكمات الجزائية المتعلقة بالجرائم المعلوماتية.
- إدراج تخصص "علم الأدلة الجنائية الرقمية" كفرع جديد، يدرس في الجامعات الوطنية في إطار النظرة المستقبلية لمواجهة التطور المستمر لعلوم التكنولوجيا التي أصبحت لغة العصر.

تم بحمد الله.

قائمة المراجع.

أولاً- الرسائل و المذكرات الجامعية:

أ- الرسائل الجامعية:

1- العبد سعادنة ، الإثبات في المواد الجمركية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق، تخصص قانون جنائي، جامعة الحاج لخضر باتنة، السنة الجامعية 2006/2005.

2- بن شهرة شول، الحماية الجنائية للتجارة الالكترونية، أطروحة مقدمة لنيل شهادة دكتوراه علوم في الحقوق، تخصص قانون جنائي، جامعة محمد خيضر بسكرة، السنة الجامعية 2011/2010.

ب-المذكرات الجامعية:

1- بلولهي مراد ، الحدود القانونية لسلطة القاضي الجزائري في تقدير الأدلة، مذكرة مقدمة لنيل درجة الماجستير في العلوم القانونية تخصص علوم جنائية، جامعة الحاج لخضر باتنة السنة الجامعية 2011-2010.

2- تافرونت الهاشمي ، وسائل إثبات الدفاع الشرعي، مذكرة مقدمة استكمالاً لنيل درجة الماجستير تخصص الشريعة و القانون ، جامعة العقيد الحاج لخضر باتنة ، السنة الجامعية 2002-2001.

3- رائد صبار الازيرجاوي ، القرينة ودورها في الإثبات في المسائل الجزائية (دراسة مقارنة في القانونين الأردني و العراقي) ، مذكرة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير، القسم العام جامعة الشرق الأوسط، السنة الجامعية 2011-2010.

4- سعدون بن محمد بن طويق العنبي ، استخدام وسائل الإثبات التقنية في الدعوى الجنائية في مجال التعازير، رسالة مقدمة استكمالاً لنيل درجة الماجستير في العلوم الأمنية ،المركز العربي للدراسات الأمنية والتدريب الرياض السعودية، سنة 1994.

5- سليمان غازي العتيبي ، درجة توافر كفايات البحث عن الدليل الرقمي في الجرائم المعلوماتية لدى ضباط شرطة العاصمة المقدسة ، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية تخصص قيادة أمنية الرياض ، جامعة نايف العربية للعلوم الأمنية ، سنة 2010.

6- صالح عبد الحي ، الإثبات الجنائي في الجريمة الدولية، مذكرة مكملة لنيل شهادة الماجستير في القانون الجنائي تخصص القانون الجنائي الدولي ، المركز الجامعي عباس لغرور خنشلة ، السنة الجامعية 2011-2012.

7- عبد الله بن عبد العزيز بن عبد الله الخثعمي ، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، رسالة مقدمة استكمالاً لمتطلبات الحصول على درجة الماجستير في العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية السعودية، سنة 2011 .

ثانياً- المراجع العامة:

أ- القرآن الكريم.

ب- القواميس و المعاجم:

1- عصام نور الدين ، معجم نور الدين الوسيط عربي عربي، الطبعة الثانية ، دار الكتب العلمية بيروت لبنان، سنة 2009.

2- ابن منظور أبو الفضل جمال الدين محمد بن مكرم بن منظور الإفريقي المصري ، لسان العرب، الطبعة الأولى، دار إحياء التراث، بيروت.

3- محمد بن أبي بكر الرازي، مختار الصحاح، دار الجيل، بيروت 1987.

ج- الكتب العامة:

- 1- أحمد ضياء الدين محمد ، مشروعية الدليل في المواد الجنائية دراسة تحليلية مقارنة لنظريتي الإثبات و المشروعية في مجال الإجراءات الجنائية، دار النهضة العربية، مصر، سنة 2010.
- 2- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية في ضوء التعديلات الحديثة الطبعة الثامنة(مطورة)، دار النهضة العربية، القاهرة مصر، سنة2012.
- 3- إحمود فالح الخرايشة ، الإشكالات الإجرائية للشهادة في المسائل الجزائية دراسة مقارنة الطبعة الأولى الإصدار الأول ، دار الثقافة للنشر و التوزيع، عمان الأردن، 2009 .
- 4- أشرف عبد القادر قنديل ، النظرية العامة للبحث الجنائي وأثرها في عقيدة القاضي،دار الجامعة الجديدة الإسكندرية مصر، سنة2011.
- 5- الغوثي بن ملحّة ، قواعد وطرق الإثبات ومباشرتها في النظام القانوني الجزائري، الديوان الوطني للأشغال التربوية، الطبعة الأولى، سنة 2001.
- 6- عماد محمد ربيع ، حجية الشهادة في الإثبات الجزائي دراسة مقارنة، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان الأردن، سنة2011.
- 7- فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة (دراسة مقارنة) ، الطبعة الأولى الإصدار الثاني، دار الثقافة للنشر و التوزيع، عمان الأردن، سنة 2006.
- 8- فوزية عبد الستار، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات، الطبعة الثانية دار النهضة العربية، القاهرة مصر، سنة 2010.
- 9- كامل السعيد ، شرح قانون أصول المحاكمات الجزائية دراسة تحليلية تأصيلية مقارنة في القوانين الأردنية و المصرية والسورية وغيرها، الطبعة الأولى الإصدار الثاني دار الثقافة للنشر و التوزيع، عمان الأردن، سنة 2008.
- 10- محمد زكي أبو عامر ، الإثبات في المواد الجنائية محاولة فقهية وعملية لإرساء نظرية عامة دار الجامعة الجديدة، الإسكندرية مصر، 2011.

- 11- محمد على سكيكر ، أدلة الإثبات الجنائي في ضوء التشريع و القضاء و الفقه ، دار الجامعة الجديدة، سنة 2011.
- 12- محمد مروان ، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، ديوان المطبوعات الجامعية، الجزائر، سنة 1999 ، الجزء الأول .
- 13- محمد مروان ، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري ، ديوان المطبوعات الجامعية، الجزائر، سنة 1999، الجزء الثاني .
- 14- محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، دار النهضة العربية، القاهرة مصر، سنة 2013، الجزء الأول.
- 15- محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية، دار النهضة العربية، القاهرة مصر، سنة 2013، الجزء الثاني.
- 16- مصطفى يوسف ، مشروعية الدليل في المسائل الجنائية في ضوء الفقه و القضاء، دار الجامعة الجديدة للنشر ، سنة 2011، الإسكندرية.
- 17- مراد أحمد العبادي ، اعتراف المتهم وأثره في الإثبات دراسة مقارنة ، الطبعة الأولى الإصدار الثاني، دار الثقافة للنشر و التوزيع، الأردن، 2008 .
- 18- جمال نجيمي ، إثبات الجريمة على ضوء الاجتهاد القضائي دراسة مقارنة، دار هومة للطباعة والنشر و التوزيع، الجزائر، سنة 2012.
- 19- نصر الدين مروك، محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي، الطبعة الثالثة، دار هومة ، الجزائر، 2009، الجزء الأول.
- 20- نصر الدين مروك ، محاضرات في الإثبات الجنائي، أدلة الإثبات الجنائي، الطبعة الثالثة دار هومة، الجزائر، 2009، الجزء الثاني.

ثالثا- المراجع المتخصصة:

- 21- الشحات إبراهيم محمد منصور ، الجرائم الالكترونية في الشريعة الإسلامية و القوانين الوضعية ، بحث فقهي مقارن ، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية مصر، سنة 2011.
- 22- أيمن عبد الله فكري ، جرائم نظم المعلومات دراسة مقارنة، دار الجامعة الجديدة للنشر الإسكندرية مصر، سنة 2007.
- 23- بكري يوسف بكري ، التفتيش عن المعلومات في وسائل التقنية الحديثة ، الطبعة الأولى ، دار الفكر الجامعي، سنة 2011 .
- 24- بولين انطونيوس أيوب ، الحماية القانونية للحياة الشخصية في مجال المعلوماتية دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، 2009.
- 25- جبار الحسيناوي، جرائم الحاسوب و الانترنت ، الطبعة العربية، دار اليازوري العلمية للنشر و التوزيع، عمان الأردن، 2009.
- 26- جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات رؤية جديدة للجريمة الحديثة الطبعة الأولى، دار البداية للنشر و التوزيع، سنة 2007.
- 27- جلال محمد الزعبي و أسامة احمد المناعسة ، جرائم تقنية نظم المعلومات الالكترونية (دراسة مقارنة) ، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان الأردن، 2010.
- 28- خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان الأردن، سنة 2011.
- 29- رشاد خالد عمر ، المشاكل القانونية و الفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية مصر، سنة 2013.

- 30- رشيدة بوكر ، جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت لبنان، 2012.
- 31- سليمان أحمد فضل ، المواجهة التشريعية و الأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة مصر، 2013.
- 32- زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدي للطباعة والنشر و التوزيع، عين أمليلة الجزائر، سنة 2011.
- 33- شيماء عبد الغني محمد عطا الله ، الحماية الجنائية للتعاملات الإلكترونية، دار الجامعة الجديدة، سنة 2007.
- 34- عادل عزام سقف الحيط ، جرائم الدم و القرح و التحقير المرتكبة عبر الوسائط الإلكترونية "شبكة الانترنت و شبكة الهواتف النقالة و عبر الوسائط التقليدية و الآلية و المطبوعات" دراسة قانونية مقارنة، الطبعة الأولى، دار الثقافة للنشر و التوزيع، عمان الأردن، سنة 2011.
- 35- عبد العال الديربي و محمد صادق إسماعيل ، الجرائم الالكترونية دراسة قانونية قضائية مع احدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والانترنت ، الطبعة الأولى ،المركز القومي للإصدارات القانونية، القاهرة مصر، سنة 2012.
- 36- عبد الفتاح بيومي حجازي ، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، سنة 2007.
- 37- عبد الفتاح بيومي حجازي ، مكافحة جرائم الكمبيوتر و الإنترنت في القانون العربي النموذجي، الطبعة الأولى، 2009.
- 38- عبد الفتاح بيومي حجازي ، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية ، الطبعة الأولى، دار النهضة العربية، مصر، 2009.

- 39- عماد مجدي عبد الملك، جرائم الكمبيوتر و الإنترنت، دار المطبوعات الجامعية، الإسكندرية مصر، سنة 2011.
- 40- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف و المصنفات الفنية ودور الشرطة و القانون دراسة مقارنة، منشورات الحلبي الحقوقية، بيروت لبنان، سنة 2003.
- 41- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا دراسة مقارنة، دار النهضة العربية للنشر والتوزيع، القاهرة مصر، سنة 2010.
- 42- على حسن محمد الطوالبه، التفتيش الجنائي على نظم الحاسوب و الانترنت دراسة مقارنة الطبعة الأولى، عالم الكتب الحديث للنشر والتوزيع، سنة 2004.
- 43- علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الإبتدائي في الجريمة المعلوماتية(دراسة مقارنة)، المكتب الجامعي الحديث، سنة 2012.
- 44- فيصل سعيد غريب، التوقيع الالكتروني و حجبيته في الإثبات، منشورات المنظمة العربية للتنمية الإدارية، سنة 2005.
- 45- محمد أمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، سنة 2004.
- 46- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري و المقارن، دار الجامعة الجديدة، الإسكندرية مصر، سنة 2007.
- 47- محمد طارق عبد الرؤوف ألحن، جريمة الاحتيال عبر الانترنت (الأحكام الموضوعية والأحكام الإجرائية) الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت لبنان، 2011.
- 48- محمد على العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية مصر سنة 2011.

49- محمد محمد محمد عنب ، استخدام التكنولوجيا الحديثة في الإثبات الجنائي ، مطبعة السلام الحديثة ، مصر ، سنة 2007.

50- نسرين عبد الحميد نبيه ، الجريمة المعلوماتية و المجرم المعلوماتي، منشأة المعارف الإسكندرية، سنة 2008.

51- نهلا عبد القادر مومني ، الجرائم المعلوماتية، الطبعة الأولى الإصدار الأول دار الثقافة للنشر و التوزيع، عمان الأردن، 2008.

رابعاً- المقالات و المداخلات.

أ- المقالات و البحوث:

1- أحمد براك ، دراسة قانونية بعنوان استجواب المتهم وسماع الشهود في الدعوى الجزائية دراسة مقارنة، مجلة العدالة والقانون الصادرة عن المركز الفلسطيني لاستقلال المحاماة و القضاء "مساواة" سبتمبر 2007 .

2- أسامة بن غانم العبيدي ، بحث بعنوان التفتيش عن الدليل في الجرائم المعلوماتية العدد58المجلد 29 المجلة العربية للدراسات الأمنية و التدريب ، سنة 2013، منشور على الموقع الإلكتروني: www.nauss.edu.sa/Ar/pdf

3- براهيم حنان ، مقالة بعنوان المحررات الالكترونية كدليل إثبات، العدد التاسع، مجلة المفكر جامعة محمد خيضر بسكرة الجزائر، سنة 2013.

4- حسن الجوخدار ، السلطة المختصة باستجواب المتهم وحقه في الاستعانة بمحام في قانون أصول المحاكمات الجزائية الأردني و المقارن، العدد 02 مجلد 24 مقالة علمية منشورة في مجلة أبحاث اليرموك "سلسة العلوم الإنسانية و الاجتماعية، العراق، جوان 2008.

5- سميرة معاشي، ماهية الجريمة المعلوماتية، مقالة منشورة في مجلة المنتدى القانوني ، دورية تصدر عن قسم الكفاءة المهنية للمحاماة العدد السابع، جامعة محمد خيضر بسكرة، الجزائر، أبريل 2010.

6- عادل مستاري، مقالة بعنوان دور القاضي الجزائري في ظل مبدأ الاقتناع القضائي ، مجلة المنتدى القانوني، دورية تصدر عن قسم الكفاءة المهنية للمحاماة العدد الخامس ، جامعة محمد خيضر بسكرة، مارس 2008 .

7- محروس نصار غايب، الجريمة المعلوماتية، مقالة منشورة في مجلة التقني ،مجلد 24 ،العراق سنة 2011. متاح على الموقع الالكتروني: <http://www.iasj.net/iasj>.

8- على حسن الطوالبه ، مشروعية الدليل المستمد من التفتيش الجنائي "دراسة مقارنة"، مركز الإعلام الأمني سنة 2009 متاح على الموقع الالكتروني: <http://www.Policemc.gov.bn/>.

9- محمد أمين البشري ، بحث حول الأدلة الجنائية الرقمية مفهومها ودورها في الإثبات، العدد 33 المجلد 17 المجلة العربية للدراسات الأمنية و التدريب ، جامعة نايف العربية للعلوم الأمنية متاح على الموقع الالكتروني: <http://www.nauss.edu.sa/Ar/em-dar-33-3pdf>.

10- محمد طيب عمور ، الإثبات الجزائي بالقرائن القضائية بين الشريعة و القانون، العدد 09 مقالة منشورة في مجلة الأكاديمية للدراسات الاجتماعية و الإنسانية، جامعة حسيبة بن بوعلي الشلف، سنة 2013.

11- محمد على سالم و حسون عبيد هجيج ، الجريمة المعلوماتية، مقالة منشورة في مجلة جامعة بابل للعلوم الإنسانية العراق، العدد 06 المجلد 14 العراق، سنة 2007. متاح على الموقع الالكتروني: <http://www.iasj.net/iasj.pdf>.

12- محمد محدة، مقالة بعنوان السلطة التقديرية للقاضي الجزائري، العدد الأول، مجلة البحوث و الدراسات، المركز الجامعي الوادي، أبريل 2004 .

- 13- مختار الأخصري، بحث بعنوان الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الافتراضي، العدد 66 ، نشرة القضاة القانونية، الجزائر، سنة2010.
- 14- مصطفى عبد القادر، دراسة بعنوان أساليب البحث و التحري الخاصة وإجراءاتها، العدد 02 مجلة المحكمة العليا، الجزائر سنة 2009.
- 15- ممدوح خليل البحر ، بحث بعنوان نطاق حرية القاضي الجنائي في تكوين قناعته الوجدانية العدد الحادي و العشرون في مجلة الشريعة و القانون ، الإمارات العربية المتحدة ، جوان 2004 متاح على الموقع الالكتروني: <http://www.sljournal.uaeu.ac.ae/issues/21/docs/6.pdf>.
- 16- ناشف فريد ، بحث بعنوان مدى قبول الدليل غير المشروع في المحاكمة الجزائية دراسة مقارنة، العدد 15 ، دورية دراسات قانونية الصادرة عن مركز البصيرة للبحوث و الاستشارات و الخدمات التعليمية ،دار الخلدونية للنشر و التوزيع، الجزائر، سنة 2012.
- ب- المداخلات:

- 1- أحمد بن عبد الرحمن ألبعادي ، ورقة عمل بعنوان " دعاوى الجرائم الإلكترونية وأدلة إثباتها في التشريعات العربية بين الواقع و المأمول" مقدمة إلى المؤتمر الثالث لرؤساء المحاكم العليا بالدول العربية في الفترة من 23-25 سبتمبر 2012م بالخرطوم السودان.
- 2- سعيد قاسم علي العاقل و شائف علي محمد الشيباني ، بحث بعنوان " مدى صلاحية الاجتهاد القضائي لسد الثغرات التشريعية في مجال الإثبات بالوسائل المعلوماتية و التكنولوجية الحديثة دراسة مقارنة" مقدم للندوة المنعقدة مابين 6-8/01/2003 في المركز العربي للبحوث القانونية و القضائية ببيروت لبنان.منشور على الموقع الالكتروني: <http://www.agoye.com/userimages/.../research/salaheea.pdf>.

- 3- عبد الناصر محمد محمود فرغلي و محمد عبيد سيف سعيد المسماري ، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية (دراسة تطبيقية مقارنة)، بحث مقدم إلى المؤتمر

العربي الأول لعلوم الأدلة الجنائية والطب الشرعي ، المنعقد بالرياض في 12-14 نوفمبر 2007
جامعة نايف العربية للعلوم الأمنية.

4- عمر بن محمد يونس ، ندوة الدليل الرقمي للمنظمة العربية للتنمية الإدارية المنعقدة في مقر
جامعة الدول العربية القاهرة في الفترة الممتدة من 05-08 مارس 2006.

5- عمرو حسين عباس ، أدلة الإثبات الجنائي و الجرائم المعلوماتية بحث مقدم إلى المؤتمر
الإقليمي الثاني حول تحديات تطبيق الملكية الفكرية الوطن العربي خلال الفترة من 26-
27/4/2008 مقر جامعة الدول العربية.

6- مصطفى عبد القادر ، الشرطة الوطنية ومكافحة الجريمة الالكترونية مداخلة مقدمة في
الملتقى الدولي الجزائر حول محاربة الجريمة المعلوماتية المنعقد بالجزائر في الفترة الممتدة 05-
06 ماي 2010. منشور في مجلة صادرة عن مركز البحوث القانونية والقضائية ، الطبعة الأولى
إبسان للنشر و التوزيع ، الجزائر، سنة 2012.

7- محمد أمين البشري ، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون و
الكمبيوتر و الإنترنت ، كلية الشريعة و القانون بجامعة الإمارات العربية المتحدة في الفترة من 1
إلى 3/5/2000 الطبعة الثالثة، 2004.

8- محمد أمين البشري ، الحلقة العلمية "الإرهاب و الانترنت" لتأهيل المحققين في جرائم الحاسب
الآلي وشبكات الانترنت في الفترة 15-19/11/2008 ،جامعة نايف العربية للعلوم الأمنية
بالتعاون مع جامعة عين شمس، متاح على الموقع الالكتروني:

http://www.nuss.edu.sa/ar/.../training_college/.../002pdf.

9- موسى مسعود ارحومة ، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية
بحث مقدم إلى المؤتمر ألمغربي الأول حول المعلوماتية و القانون، منظم من طرف أكاديمية
الدراسات العليا طرابلس خلال الفترة 28-29/10/2009 .

10- هند بنت سليمان الخليفة ، ورقة عمل بعنوان الحاسب الجنائي في الدول الغربية دراسة استطلاعية جامعة الملك سعود الرياض منشور على الموقع الالكتروني:

[http// hend-alkhalifa.com/wp.computer_forensic/pdf](http://hend-alkhalifa.com/wp.computer_forensic/pdf).

خامسا- المراجع باللغات الأجنبية.

أ- المراجع باللغة الفرنسية:

I. CONVENTIONS INTERNATIONALES :

- Déclaration universelle des droits de l’homme 1948, disponible sur le site : [http//www.ohchr.org/documents/publications/ABCannexes.fr.pdf](http://www.ohchr.org/documents/publications/ABCannexes.fr.pdf)
- Convention sur la cybercriminalité Budapest 23.11.2001, disponible sure le site : [http//www.conventions.coe.int/treaty/fr](http://www.conventions.coe.int/treaty/fr).

II. LOIS ET OUVRAGES:

- 1- code de la procédure pénale française.
- 2- **AMBROISE-CASTEROT**, recherche et administration des preuves en procédure pénale, la quete de la vérité, A.J.pen.2005.
- 3- **MARCO GERCKE**, comprendre la cybercriminalité phénomène, difficulté et réponses juridiques, UIT (Union internationale des télécommunications) Genève suisse, septembre 2012.
- 4- Myriam Quéméner et Joël Ferry, cybercriminalité Défi mondial 2è édition, Ed ECONOMICA PARIS 2009.

5- Fernanda Prates, Frédérick Gaudreau et autre, la cybercriminalité état des lieux et perspectives d'avenir, institut canadien d'études juridiques supérieures, Editions Yvon Blais, Cowansville, 2013.

III. ARTICLES ET COMMUNICATIONS:

1- **Alber Rees**, communication sous titre partage de la preuve électronique : coopération entre l'Algérie et les États-Unis d'Amérique» commis dans l'Actes du séminaire international Alger le 5-6 Mai 2010, centre de recherche juridique et judiciaire, Ibsen édition & diffusion

2- **Hadjira Boudier**, communication sous titre « fournisseurs de service internet : prévention et lutte contre la cybercriminalité », commis dans l'Actes du séminaire international Alger le 5-6 Mai 2010, centre de recherche juridique et judiciaire, Ibsen édition & diffusion.

3-**Marie Barel**, article sous titre ; Fraude informatique et preuve ; la quadrature du cercle, acte du symposium SSTIC05, disponible sur le site : <http://www.actes.sstic.org/>.

4- **Michael Moran**, communication sous titre « Les pratiques du recueil de la preuve électronique» commis dans l'Actes du séminaire international Alger le 5-6 Mai 2010 , centre de recherche juridique et judiciaire, Ibsen édition & diffusion

5- **Mohand Tahar Kechadi**, communication sous titre « investigation en cybercriminalité» commis dans l'Actes du séminaire international Alger le 5-6 Mai 2010, centre de recherche juridique et judiciaire, Ibsen édition & diffusion.

6- **Tarek bouzidi**, communication sous titre « La Gendarmerie Nationale et la lutte contre la cybercriminalité» commis dans l'Actes du séminaire international Alger le 5-6 Mai 2010, centre de recherche juridique et judiciaire, Ibsen édition & diffusion.

ب- المراجع باللغة الانجليزية:

7-**Jesus Borrego**, The Impact of Acceptance of Electronic Evidence before and after the 2006 Federal Rules of Evidence on Criminal Cases. Dissertation Submitted in Partia Fulfillment of the Requirement for the Degree of Doctor of Philosophy, Walden May 2010.U.S.A.University.

سادسا- القوانين و المراسيم:

1- الدستور الجزائري لسنة 1996 المعدل بالقانون 19/08، المؤرخ في 15 نوفمبر 2008
الجريدة الرسمية عدد63، المؤرخة في 2008/11/16.

2- القانون رقم: 06-22 المؤرخ في 2006/12/20 المعدل و المتمم للأمر 155-66
المتضمن قانون الإجراءات الجزائية الجزائري ، المنشور في الجريدة الرسمية ، عدد 84 بتاريخ
2006/12/24.

3- القانون 04-14 المؤرخ في المؤرخ في 2004/11/10 المعدل و المتمم للأمر 155-66
المتضمن قانون الاجراءات الجزائية الجزائري، المنشور في الجريدة الرسمية ، عدد 71 بتاريخ
2004/11/10.

4- القانون رقم: 04-15 المؤرخ في 2004/11/10 المعدل و المتمم للأمر 156-66
المتضمن قانون العقوبات الجزائري ، المنشور في الجريدة الرسمية ، عدد 71 بتاريخ
2004/11/10.

- 5- القانون رقم: 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المنشور في الجريدة الرسمية، عدد 47 بتاريخ 16 أوت 2009.
- 6- القانون رقم: 03-2000، المؤرخ في 5 أوت 2000، المحدد للقواعد العامة المتعلقة بالبريد و المواصلات السلكية واللاسلكية.
- 7- الأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية المعدل و المتمم.
- 8- المرسوم التنفيذي رقم: 98-256، المؤرخ في 25 أوت 1998، المعدل و المتمم للجزء التنظيمي من الأمر 89-75، المؤرخ في 30/12/1975، المتضمن قانون البريد و المواصلات المنشور في الجريدة الرسمية، عدد63، بتاريخ 26/08/1998.
- 9- المرسوم التنفيذي رقم: 98-257، المؤرخ في 25 أوت 1998، المتضمن ضبط شروط وكيفيات إقامة خدمات الانترنت واستغلالها، المنشور في الجريدة الرسمية، عدد 63، بتاريخ 26/08/1998.

سابعا- المجالات و الأحكام القضائية:

- 1- المجلة القضائية، العدد03، قسم المستندات و النشر ، المحكمة العليا، الجزائر، سنة 1991.
- 2- المجلة القضائية، العدد01، قسم الوثائق، المحكمة العليا، الجزائر، سنة 2005.
- 3- قرار رقم 10/5808 مؤرخ في 04/07/2010، الغرفة الجزائرية، مجلس قضاء باتنة.

قائمة المختصرات:

أثناء الدراسة استعان الباحث بمجموعة من الرموز، و المختصرات، نورد معناها كما يلي:

- د.س..ط: بدون سنة الطبع.

- ص: الصفحة.

- ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري.

- ق.ع.ج: قانون العقوبات الجزائري.

- حجم خط المذكرة: المتن 15، الهوامش 11.

- فواصل المذكرة تحسب و لا ترقم.

- نوع خط المذكرة: العربية Simplified Arabic و الأجنبية Traditional Arabic.

-C.P.P.F:Code des Procédures Pénale Français.

- F.R.C.P: The Federal Rules of Civil Procedure.

- F.R.E: The Federal Rules of Evidence.

-IP : Internet Protocol .

- ISP : Internet Server Provider.

الملخص:

تتميز الجريمة المعلوماتية بصعوبة إثباتها، وهو الموضوع الذي مازال يشغل بال المشرعين ويشكل مصدر اهتمام لهم، بالنظر إلى حجم المخاطر التي تهدد المجتمعات المختلفة، من هذا المنطلق ومن زاوية مدى تجاوب وسائل الإثبات بصورتها التقليدية والحديثة مع إثبات الجريمة المعلوماتية كان موضوع الدراسة.

وقد تبين من خلال دراستنا للموضوع أن الإثبات الجنائي في منظومتنا القانونية لا يزال في إطاره الإجرائي العام، محتفظا بنصوصه التقليدية المبنية على مبدأي حرية الإثبات، وحرية الاقتناع القضائي، مع عدم كفاية الوسائل التقليدية من الناحية التقنية والحجية العلمية للاستناد عليها وحدها لإثبات الجريمة، وإن دورها يكمن في المساهمة بشكل أو بآخر في استخلاص الأدلة الرقمية، ومن ثم، فإن لها دورا في العملية الإثباتية بقدر يسمح معه ببناء اقتناع وفقا لمبدأ تساند الأدلة.

في حين تعتبر الأدلة الرقمية من الوسائل الحديثة الأكثر دقة و نجاعة على الإطلاق من الناحية الفنية في إثبات الجريمة المعلوماتية، ما دفع بالتشريعات المقارنة إلى تبنيه وتحديد شروط قبوله، بالرغم من اصطدامها بالطبيعة الخاصة به، ما تطلب معه توفير عناية خاصة في طرق استخلاصه ضمانا لمصداقيته، وفي خضم كل هذا اكتفى المشرع الجزائري بضبطه بالنصوص التقليدية لضمان الشرعية، مع أكثر مرونة في طرق الاستخلاص لحماية البيانات ذاتها، بينما تبقى حجيتها في الإثبات خاضعة للسلطة التقديرية للقاضي.

وخلصت الدراسة إلى مجموعة من النتائج و الاقتراحات، أهمها ضرورة الاهتمام بالتكوين في المجال المعلوماتي وإعداد منظومة قضائية متخصصة، مع سد النقص التشريعي من خلال صياغة نصوص متكاملة خاصة بالدليل الرقمي تضمن إضفاء أكثر حجية له بعيدا عن الإطار التقليدي.

Abstract.

Résumé :

La cybercriminalité qui se caractérise par le fait d'être difficile à prouver est le sujet qui préoccupe les législateurs et constitue une source de souci pour eux, par rapport à l'ampleur des risques qui menacent les entités de différentes sociétés. La preuve des moyens de constatation quels que soient traditionnels ou modernes afin de constater la cybercriminalité était le thème de cette étude.

Il s'est avéré à travers notre étude de ce thème que la constatation de criminalité dans notre système juridique est encore dans son cadre procédural général, gardant ses textes traditionnels basés sur les deux principes de liberté de constatation et liberté de conviction judiciaire, avec l'insuffisance des moyens traditionnels du point de vue technique et la preuve scientifique sur lesquels on peut s'appuyer afin de résoudre le problème de crime et son rôle consiste à contribuer d'une manière ou d'une autre à la déduction des preuves numériques, ainsi ils ont un rôle dans l'opération de constatation de manière qui nous permet de construire une conviction conformément au principe de preuve à l'appui.

Cependant, les preuves numériques sont considérés parmi les moyens modernes les plus précis et efficaces du point de vue technique concernant la constatation de la cybercriminalité, ce qui a poussé les législations comparatives à les adopter en déterminant les conditions de leur acceptation, malgré leur heurt à leur nature, ce qui a nécessité une attention particulière concernant les méthodes de leur déduction pour garantir leur crédibilité. Dans tout cela, le législateur algérien se limitait à les réglementer avec les textes traditionnels pour garantir la légitimité avec plus de souplesse dans les méthodes de déduction afin de protéger les données elles-mêmes, néanmoins leur preuve dans la constatation reste soumise à l'autorité d'appréciation du juge.

L'étude a abouti à un ensemble de résultats et recommandations, les plus importants relèvent de la nécessité d'accorder suffisamment d'importance à la formation dans le domaine de l'informatique et la préparation d'un système judiciaire spécialisé, en comblant les lacunes législatives par le biais de la formulation des textes complémentaires relatifs au guide numérique qui leur garantissent plus de preuve loin du cadre traditionnel.

Abstract.

Abstract:

Cybercrime, which is characterized by the fact of being difficult to prove is the subject matter which preoccupies legislators and is a source of worries for them, regarding the magnitude of the risks to the entities of different societies. The evidence of the means of proving whatever they may be traditional or modern was the topic of this study.

It was revealed through our study of this topic that proving of the crime in our legal system is still in its general procedural framework, keeping its traditional texts based on the two principles of freedom of proving and freedom of judicial conviction, with the inadequacy of traditional methods from technical point of view and scientific evidence on which we can rely to solve the problem of crime and its role consists in contributing in a way or another to the deduction of digital evidence, so they have a role in the operation of proving in a way that allows us to build a conviction in accordance with the principle of supporting evidence.

However, numerical evidence is considered among the most accurate and efficient modern means from technical point of view in proving cybercrime, which has prompted comparative legislations to adopt them and determine the conditions of their acceptance, despite their clash with their nature, which required special attention regarding the methods of their deduction to ensure their credibility. In all this, the Algerian legislator limited himself to their regulation with traditional texts to ensure legitimacy with more flexibility in the methods of deduction to protect data themselves; however their evidence in proving remains subject to the appreciation authority of the judge.

The study resulted in a set of findings and recommendations, the most important ones are related the need of giving importance to training in the field of informatics and the preparation of a specialized judicial system, filling legislation gaps through the formulation of complementary texts related to the digital guide that guarantee to them more evidence away from the traditional framework.