الإثبات الجنائي للجريمة الاليكترونية

الدكتـــــور
عادل حامد بشير
أستاذ القانون الجنائي المساعد
كلية الحقوق – جامعة أسوان
والأستاذ المشارك بكلية الحقوق
جامعة البحرين

الإثبات الجنائي للجريمة الاليكترونية

المقدمة:

أصبحت تكنولوجيا المعلومات والاتصالات من أهم المتغيرات التى تجتاح العالم حالياً ، فالإنترنت هو الثورة الكبرى فى عالم الاتصالات عن بعد، وجاء التقدم الفنى والتقنى للمعلومات والاتصالات مصحوباً بصور مستحدثة لارتكاب الجرائم التى تستعير هذه التقنية أساليبها المتطورة فأصبحنا أمام ظاهرة جديدة هى ظاهرة الجريمة المعلوماتية أو الإلكترونية .

فإذا كانت التكنولوجيا تحقق الرفاهية للإنسان فى عالمنا الحديث ، إلا أنها تجلب له أيضاً المتاعب حيث تطورت معها وسائل ارتكاب الجريمة بحيث أصبحت عملية ملاحقتها وضبط مرتكبها فى غاية الصعوبة ، ولذلك فإنه يجب التعامل مع التطورات الحديثة لتقنية المعلومات والاتصالات بشكل مختلف عن النظرة التقليدية القديمة ، إذ كانت صور السلوك الإجرامى تتسم بالبساطة والوضوح ، وكان يكفى لاكتشافها وإسنادها لمرتكبها استخدام وسائل الإثبات التى تعتمد على الإدراك الحسى المباشر كالاعتراف وشهادة الشهود والقرائن وغيرها من وسائل الإثبات التقليدية . ثم أخذت أساليب الجريمة تتطور بتطور المجتمع الذى وقعت فيه حتى أصبحت بأسلوب أكثر تنظيماً فالمتهمين يستخدمون اليوم الوسائل العلمية المتطورة فى ارتكاب جرائمهم . وإزاء تطور أساليب ارتكاب الجريمة أصبح اكتشاف أمر الجانى أمراً عسيراً ولذلك كان لزاماً على المجتمع أن يستخدم نفس السلاح (سلاح العلم) باستخدام وسائل علمية حديثة للكشف عن الجريمة وإثباتها . ومع ذلك فإن الوسائل العلمية الحديثة فى ذاتها أصبحت مصدراً للمشاكل الفنية، فإساءة استخدام شبكات الحاسبات الآلية أو الجرائم المتعلقة بالإنترنت تثير مشاكل عديدة فى مقدمتها مسألة الإثبات الجنائى حيث يصعب فى كثير من الأحيان العثور على أثر مادى للجريمة الإلكترونية أو المعلوماتية والتى لا تكتشف إلا بمحض الصدفة .

والجريمة المعلوماتية مشكلة معقدة تؤرق الدول والأفراد ، وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشرى ، وهذه الجرائم لا تفرق بين الدول المتقدمة والنامية فالإجرام واحد وإن اختلفت صوره أو تعددت وسائله ، بل إن الأمر تعدى أنماط الجرائم إلى ظهور أنماط جديدة ، على وجه الخصوص فى مجالات الإرهاب وتجارة المخدرات ، والاتجار

بالسلاح ، والدعارة المنظمة باستخدام الإنترنت والحرب الإلكترونية [١] التى تهدد الأمن القومى والسيادة الوطنية ، ولعل السبب فى زيادة الجرائم الإلكترونية هو انخفاض تكلفة الهجمات الإلكترونية مقارنة بتكلفة استخدام الجيوش والسلحة التقليدية ، وافتقار العديد من مواقع الإنترنت لوسائل التأمين الفعالة ضد الهجمات الإلكترونية ، وأن تنفيذها لا يستغرق بضع ثوانى ، ولسهولة محو آثار الجريمة وإتلاف أدلتها ، وتخزين البيانات المتعلقة بالأنشطة الإجرامية فى أنظمة إلكترونية مع استخدام شفرات أو رموز سرية لإخفائها عن أعين أجهزة العدالة مما يثير مشاكل كبيرة فى جمع الأدلة الجنائية وإثبات هذه الجرائم قبلهم . وإن الاحصاءات الجنائية حول الجريمة المعلوماتية أو الإلكترونية لا تكون معبرة عن الحجم الحقيقى للجرائم المرتكبة فعلاً ويصعب عمل سياسة جنائية فعالة للقضاء عليها نظراً لعدم معرفة الحجم الحقيقى لهذه الظواهر الإجرامية .

والجرائم المعلوماتية أو الإلكترونية التى تعتمد فى موضوعها على التشفير والأكواد السرية والنبضات والأرقام والتخزين الإلكترونى يصعب أن تخلف وراءها آثاراً مرئية قد تكشف عنها أو يستدل من خلالها على الجناة، ويتضح جلياً أن خطر هذه الجرائم يكمن فى أنها فى طبيعتها تجمع بين الذكاء الاصطناعى والذكاء البشرى ، مما يجعل إثباتها جنائياً يمثل صعوبة لأجهزة إنفاذ القانون ورجال القضاء والنيابة والمحامين ورجال البحث الجنائى فى عملية البحث والتحرى والضبط والتفتيش ، لاستخلاص الدليل الرقمى وإبراز قيمته كدليل إدانة ، ذلك أن التطبيقات أو البرامج والبيانات المرقمة عناصر أساسية يتحتم على أجهزة إنفاذ القانون وخبراء الأدلة الجنائية التعالم معها بمهارة تقنية .

١ -أهمية البحث :

تبدو أهمية البحث فى أنه يقدم أسلوباً علمياً وقانونياً ، يمكن الاستعانة به فى إثبات الجريمة التى تتم عبر أجهزة الكمبيوتر والأجهزة

---

(١)- وعلى سبيل المثال لا الحصر نشر الأفكار المتطرفة ، إساءة العلاقات السياسية بين الدول ، تهديد الأمن العسكرى والقومى للدول ، إتلاف أجهزة الحاسب الإلكترونى ، التجسس الصناعى وسرقة الأسرار الخاصة ، عرض الشذوذ الجنسى وتشويه سمعة الشرفاء ، سرقة المعلومات السرية من مستخدمى الشبكة الدولية ، نشر الرئسائل الإلكترونية المزعجة ، هجمات البريد الإلكترونى ، الاحتيال والتجسس – الإرهاب الإلكترونى .

الإلكترونية المختلفة ، كما أنه يساعد على الفهم الأكاديمى للدليل الرقمى المقدم لأجهزة إنفاذ القانون وتطبيق القانون ويدعم حجية مخرجات الحاسب الآلى فى المواد الجنائية .

وتتضح أهمية البحث أيضاً فى التأكيد على ضرورة اكتساب رجال الضبط القضائى والقضاة للمهارات الفنية والتقنية المختلفة مع ضرورة الاستعانة بخبراء استشاريين فى مجال الجرائم الإلكترونية ، حيث أنه لا بد من توافر الخبرة والمهارة التقنية لكشف الأدلة الناتجة عن الجرائم المعلوماتية ، وأيضاً لفت انتباه المعنيين والمسئولين عن الأجهزة والتنظيمات والمؤسسات العلمية للمساهمة فى مكافحتها والحد منها والتحذير من مخاطرها .

كما أن عملية سهولة محو الدليل الإلكترونى أو الرقمى تعد من أهم العمليات التى تعترض العملية الإثباتية للجريمة المعلوماتية ، حيث يستطيع الجانى محو أدلة الإدانة أو تدميرها فى وقت قصير وخاصة فى حالة تفتيش الشبكات أو عمليات الاتصال . كما أن الجرائم الإلكترونية أو المعلوماتية تثير بعض المشاكل فيما يتعلق بجمع الأدلة حيث يوجد بعض الصعوبات التى تتعلق بالتفتيش فقد تكون البيانات التى يجرى البحث عنها مشفرة ولا يعرف شفرة الدخول إلا أحد العاملين على الشبكة فيثور التساؤل عن مدى مشروعية إجباره على فك الشفرة ، فسلطات جمع الاستدلالات والتحقيق اعتادت أن يكون الإثبات مادياً ملموساً ، ولكن فى مجال الجرائم المعلوماتية لا يستطيع المتحرى أو المحقق تطبيق إجراءات الإثبات التقليدية على المعلومات وهى من طبيعة معنوية ومن هنا تبدو أهمية البحث فى إيضاح قصور قانون العقوبات والإجراءات الجنائية فى مواجهة الجرائم المعلوماتية الأمر الذى يتطلب إيجاد استراتيجية مكملة للقوانين الجنائية الموضوعية والإجرائية التقليدية لمواجهة الجرائم المعلوماتية ، والعمل على تطوير الآليات التقليدية لوسائل الإثبات على نحو يتفق مع الوسائل العلمية الحديثة التى تتواكب مع تقنية المعلومات والاتصال وذلك من خلال سن القوانين اللازمة لمواجهة المشاكل الإجرائية الناتجة عن جرائم الحاسوب والإنترنت .

٢ -أهداف البحث :

نهدف من خلال البحث إلى بيان العلاقة بين الجرائم الإلكترونية أو المعلوماتية والدليل الرقمى المتحصل من أجهزة الحاسب الآلى ، وتمكين أجهزة إنفاذ القانون والشرطة ، والنيابة ، والقضاء من التعامل مع الدليل

الرقمى ، لبناء دليل جنائى مقبول أمام العدالة حتى يتمكن القاضى من إصدار حكم بالإدانة أو البراءة .

بالإضافة إلى تمكين هذه الأجهزة من معرفة متى وأين يمكن استدعاء خبراء الحاسب الآلى وكيفية المحافظة على مسرح الجريمة المعلوماتى وكيفية استخلاص الدليل الرقمى .

- بيان مدى صلاحية الدليل الرقمى للإثبات ومدى مشروعية الأدلة المتحصلة بواسطة الإنترنت وقبولها لدى القاضى الجنائى لحين صدور الحكم الجنائى الجازم فى أسرع وقت ممكن تماشياً مع نفس سرعة ارتكاب هذه الجرائم .
- كما يهدف البحث إلى بيان الصعوبات التى تواجه الجريمة المعلوماتية كصعوبة التوصل إلى الأدلة الرقمية والتحفظ عليها ، والقصور التشريعى فى تعريف مفهوم الجريمة الإلكترونية ، وعدم وجود مفهوم قانونى ودولى مشترك لتعريف الجريمة الإلكترونية .
- حث المشرع الإجرائى على إصدار القوانين اللازمة لمواجهة المشاكل القانونية والإجرائية الناتجة عن الجرائم الإلكترونية .
- تحديد أنواع أدلة الإثبات التقنية الدالة على ارتكاب الجرائم الإلكترونية أو المعلوماتية .
- بيان الدليل الرقمى المقدم لأجهزة إنفاذ القانون بما يدعم حجية المخرجات الإلكترونية فى المواد الجنائية والمدنية .
- تمكين المحاميين ليتعرفوا عن قرب على على إمكانية الإدانة أو البراءة باستخدام الدليل الرقمى مما يمكنهم من إعداد دفاعهم بالشكل المتفق مع الدليل المستخرج.

٣ -منهج البحث :

انتهج الباحث من خلال هذا البحث منهجاً مختلطاً يجمع بين المنهج التأصيلى والذى استطلعنا من خلاله رد الفروع والجزئيات إلى أصولها العامة الواردة فى قانون العقوبات وقانون الإجراءات الجنائية وذلك فيما يتعلق بوسائل الإثبات الجنائى ومبدأ حرية القاضى الجنائى فى الاقتناع ومدى سلطة القاضى الجنائى فى قبول وتقدير الأدلة الإلكترونية ، فضلاً عن ذلك ينتهج البحث المنهج الوصفى التحليلى الذى يعتمد على وصف الظاهرة قيد البحث ، ثم تحليل مفرداتها ومكوناتها ، ثم بناؤها فى إطار

جديد ، وهو ما تنتهجه الدراسة من خلال محاولة وصف الحقائق والمعلومات المرتبطة بموضوع البحث ، والعمل على تحليلها لاستخلاص أهم القواعد والأحكام التى ترتبط بالموضوع ، ومن ثم بلورة رؤية شاملة ومرنة حول الإثبات الجنائى للجريمة الإلكترونية .

ولاشك أن هذا البحث له مسارات متشابكة ، وتقاطعات أساسية فى مختلف اهتماماته القانونية والتقنية ، الأمر الذى يتطلب التزام منهجية البحث العلمى قدر المستطاع ، والتطرق للمتطلبات البحثية الضرورية فى خصوص إمكانيات البحث وانشغالاته .

كما يتطلب البحث أيضاً استخدام العديد من المصطلحات التقنية المناسبة فى مختلف سياقات الموضوع تتعلق بالمفاهيم الفنية المتعددة لتقنيات الحاسوب وشبكة الإنترنت إلى جانب المصطلحات والمفاهيم القانونية المختلفة – وما قد يبرز من مفاهيم جديدة تستلزم وضع مصطلحاتها الخاصة بها .

٤ -خطة البحث :

من أجل القاء الضوء على موضوع الإثبات الجنائى للجريمة الإلكترونية نقسم البحث إلى ما يلى :

مبحث تمهيدى : نتناول فيه ماهية الجريمة الإلكترونية .

المطلب الأول : التعريف بالجريمة الإلكترونية .

المطلب الثانى : أنواع الجريمة الإلكترونية .

الفصل الأول : أهمية ومضمون الإثبات الجنائى للجريمة الإلكترونية .

المبحث الأول : أهمية دراسة الإثبات الجنائى للجريمة الإلكترونية .

المبحث الثانى : مضمون الإثبات الجنائى للجريمة الإلكترونية .

الفصل الثانى:مدى تأثير الأدلة الإلكترونيةعلى مبدأ حرية القاضى الجنائى فى تكوين عقيدته .

المبحث الأول : مشروعية الأدلةالإلكترونية فى الإثبات الجنائى

المبحث الثانى : سلطة القاضى الجنائى فى قبول وتقدير الأدلة الإلكترونية.

الإثبات الجنائي للجريمة الاليكترونية

مبحث تمهيدى

ماهية الجريمة الإلكترونية

6- تمهيد :

تشكل الجريمة الإلكترونية تهديداً خطيراً سواء بالنسبة للمواطن العادى أو رجال الأعمال، أو رجال الأمن والبحث الجنائى ، أو رجال القضاء ، لما لهذه الجرائم من مخاطر تصل أحياناً لحد الكارثة ، نظراً للخسائر أو الأضرار أو التهديدات التى تترتب عليها ، سواء على الجانب الاقتصادى أو الجانب الأمنى . ولما كانت هذه الجرائم تتميز بكون مرتكبها على قدر عالى جداً من العلم والثقافة والحرفية ، للدرجة التى لا يمكن معها مواجهتهم وكشفهم وضبطهم والتحقيق معهم ، ومن ثم محاكمتهم وفقاً للفكر الأمنى والقضائى التقليدى وقواعد الإثبات الجنائى التقليدية ، لذا كان ضرورياً بل وحتماً استحداث طرق وأساليب خاصة قوامها العلم والمعرفة والحرفية ، وهذا لا يتأتى إلا بالتعليم والتدريب المستمرين لجميع المعنيين بكشف ومكافحة هذه الجرائم بكافة صورها وأشكالها ، واستخدام الوسائل العلمية والتكنولوجية ، فضلاً عن التعاون الفعال بين الجهات المعنية فى الداخل والخارج ، وقد أثبت الواقع العلمى أن هذا النوع من الجرائم يتميز بتعدد أشكاله وأنواعه(١).

وسوف نتناول من خلال هذا المبحث التعريف بالجريمة الإلكترونية من حيث مفهومها وخصائصها ، ودوافع ارتكابها وأنواعها ، لذا نقسم هذا المبحث إلى مطلبين :

المبحث الأول : التعريف بالجريمة الإلكترونية.

المبحث الثانى : أنواع الجريمة الإلكترونية.

المطلب الأول

التعريف بالجريمة الإلكترونية

تعتبر الجريمة الالكترونية من الظواهر الحديثة وذلك لارتباطها بتكنولوجيا حديثة وهى تكنولوجيا المعلومات والاتصالات والكمبيوتر ، فهى الجريمة التى يستخدم فى ارتكابها الحاسب الإلكترونى من خلال

---

(١)- د / يونس العزب المحامى – بحث بعنوان جرائم الكمبيوتر والإنترنت – المعنى والخصائص والصور واستراتيجية المواجهة القانونية – الطبعة الأولى – 2003 – ص 2.

الاتصال بشبكة الانترنت . فهى من أهم وأخطر التحديات التى تواجه التعاملات الإلكترونية والتجارة الإلكترونية وغيرها من الاستخدامات : فارتكاب الجرائم باستخدام أشخاص لتبادل الحقائب والملفات والصور السرية ونقل المعلومات المهمة انتهى دوره ، حيث يمكن حالياً نقل كل المعلومات الخطرة والمحظورة من معلومات استخباراتية أو تخريبية أو صور سرية بشكل سهل جداً عبر ضغطة خفيفة على زر لوحة المفاتيح لجهاز الكمبيوتر ، فالمجال متاح لارتكاب كل أنواع الجرائم المعلوماتية التى يصعب حصرها أو تعددها نظراً لازديادها وتنوع أساليبها . فالجرائم الإلكترونية تتحدى الأجهزة الأمنية والقضائية ، حيث يصعب تحديد مكان او زمان ارتكاب الجريمة مما يثير مشاكل قانونية من أهمها الاختصاص القضائى والإثبات الجنائى للجريمة الإلكترونية .

وبناء على ما تقدم سوف نوضح مفهوم الجريمة الإلكترونية – وخصائصها ودوافع ارتكابها .

أولا: مفهوم الجريمة الالكترونية :

يصعب الاتفاق على تعريف موحد للجريمة الإلكترونية ، حيث بذل الفقه جهوداً مضنية لوضع تعريف موحد للجريمة المعلوماتية ، ويرجع ذلك إلى سرعة وتيرة تطور التقنية المعلوماتية من جهة ، وتباين الدور الذى تلعبه هذ التقنية فى الجريمة من جهة أخرى .

فعرف البعض[١]الجريمة الإلكترونية بأنها كل سلوك غير مشروع أو غير اخلاقى أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها ، أو أنها نشاط غير مشروع موجه لفسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلى والتى تحول عن طريقه[٢] .

---

(١)- أنظر د / نائلة عادل محمد فريد – جرائم الحاسب الآلى – دراسة نظرية تطبيقية– منشورات الحلبى 2005 – ص 2.

- د / هدى حامد قشقوش – جرائم الحاسب الإلكترونى فى التشريع المقارن – دار النهضة العربية 1992ص 20 .

(٢)– أنظر د / هشام فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات مكتبة الآلات الحديثة – أسيوط - 1992 ص 31.

ومن التعريفات المضيفة للجريمة الإلكترونية أنها الفعل الإجرامى الذى يستخدم فى اقترافه الحاسب الآلى كأداة رئيسية [١] أو أنها " مختلف صور السلوك الإجرامى التى ترتكب باستخدام المعالجة الآلية للبيانات ونقلها"[٢].

ومن التعريفات الموسعة لمفهوم الجريمة المعلوماتية بأنها سوء استخدام الحاسب الآلى فتمتد لتشمل الاعتداءات المادية على جهاز الحاسب الآلى ذاته أو المعدات المتصلة به ، كذلك الحالات المتعلقة بالولوج غير المصرح به لحاسب المجنى عليه أو بياناته وكذلك الاستخدام غير المشروع لبطاقات الائتمان ، وانتهاك ماكينات الحاسب الآلية ، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق الكترونية ، وتزييف المكونات المادية والمعنوية للحاسب، بل وسرقة جهاز الحاسب الآلى فى حد ذاته أو أى مكون من مكوناته[٣].

و يرى البعض أن تعريف الجريمة الإلكترونية له ثلاث اتجاهات :-

---

(١)- د / هلالى عبداللاه أحمد – تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى – دراسة مقارنة – دار النهضة العربية 1997.

(٢)- د / راشد حمد البلوشى – ورقة عمل حول الدليل فى الجريمة المعلوماتية – مقدمة إلى المؤتمر الدولى الأول حول حماية أمن المعلومات والخصوصية فى قانون الإنترنت برعاية الجمعية الدولية لمكافحة الإجرام بفرنسا – فى الفترة من 2 : 2 يونيو 2008 – القاهرة – ص 6 .

- أيضاً – انظر د / على عبدالقادر القهوجى – الحماية الجنائية لبرامج الحاسب – بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية – كلية الحقوق – جامعة الاسكندرية – العدد 24 سنة 1992 – ص 172 .

- ومن التعريفات أيضاً – تعريف وزارة العدل الأمريكية فى دارسة وضعها معهد ستانفورد للأبحاث وتبنتها الوزارة فى دليلها لعام 1979 ، حيث عرفت الجريمة الإلكترونية بأنها " جريمة يكون لفالعها معرفة تقنية بالحاسبات تمكنه من ارتكابها "

(٣)- د / هلالى عبداللاه أحمد – التزام الشاهد والإعلام فى الجرائم المعلوماتية – دراسة مقارنة – القاهرة – دار النهضة العربية 1997.

- وعرفت الجريمة الإلكترونية بأنها " الجرائم التى تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً " . أنظر

TOM forester , Essential proplms to hig-tech socieuty first .mitpres edition , cambridge Massachusetts , 1989.p.104

يرى أصحاب الاتجاه الأول لزوم أن يكون نظام الحاسب الآلى هو محل الجريمة ، فقد عرفها **Rosenblatt** بأنها نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلى ، أو الاعتداء على نظامه [١].

أما الاتجاه الثانى : يستند أنصاره إلى معيار شخصى يستوجب أن يكون فاعل هذه الجرائم ملماً بتقنية المعلومات واستخدام الحاسوب ، لإمكانية اعتبارها من جرائم الحاسب الآلى[٢].

وعليه يعرف ديفيد ثومبسون (**David Thompson**) الجريمة المعلوماتية بأنها فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائياً [٣]. ولذلك لابد أن يكون مرتكبى الجريمة الالكترونية على درجة كبيرة من المعرفة التكنولوجية بالحاسبات .

أما الاتجاه الثالث : يستند إلي وسيلة ارتكاب الجريمة فيشترط وجوب ارتكابها بواسطة الحاسب الآلى كما عرفها تايدمان (**Tideman**) بأنها كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذى يرتكب باستخدام الحاسبأو هى كل جريمة تتم فى محيط الحاسبات الآلية [٤]ويعد هذا التعريف توسعاً كبيراً فى مفهوم الجريمة الالكترونية .

---

(١)- د / هشام فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات – المرجع السابق ص 35.

(٢) - د / مأمون سلامة – قانون الإجراءات الجنائية معلقاً عليه بالفقه والقضاء – دار الفكر العربى سنة 1981 – ص 183.

(٣) - د / نائلة عادل محمد فريد – جرائم الحاسب الآلى – المرجع السابق – ص 26 .
- د / أحمد عوض بلال – التطبيقات المعاصرة للنظام الاتهامى فى القانون الانجلوأمريكى – دار النهضة العربية 1992- ص 85.

(٤) - د/ أحمد ضياء الدين محمد خليل – مشروعية الدليل فى المواد الجنائية كلية الحقوق – جامعة عين شمس 1984ص 76 .
- خبراء منظمة التعاون الاقتصادى والتنمية OECD عرف الجريمة الإلكترونية بأنها سلوك غير مشروع أو غير أخلاقى أو غير مصرح به يتعلق بالمعالجة الإلكترونية للبيانات أو نقلها- وهذا التعريف كان فى اجتماع باريس الذى عقد سنة 1983 – ويعتمد هذا التعريف على معيارين الأول : وصف السلوك ، والثانى اتصال السلوك بالمعالجة الإلكترونية للبيانات أو نقلها .

وعرف القانون المصرى فى مادته الأولى : جرائم المعلوماتية بأنها كل فعل يتم ارتكابه عبر أى وسيط الكترونى .

وعلى ضوء ما تقدم من تعريفات للجريمة الالكترونية وللوقوف على ماهية الجريمة الإلكترونية نخلص إلى العديد من النتائج:-

1- أن الاعتداء على الكيانات المادية للكمبيوتر وأجهزته يخرج عن نطاق جرائم الكمبيوتر ، لأن هذه الكيانات محل صالح لتطبيق نصوص التجريم التقليدية المنظمة لجرائم السرقة والاحتيال ، وإساءة الأمانة والتدمير والإتلاف وغير ذلك .

2- أن محل جريمة الكمبيوتر هو دائماً المعطيات ، إما بذاتها أو بما تمثله هذه المعطيات التى تكون مخزنة داخل النظام ، أو على أحد وسائط التخزين أو تكون فى طور النقل والتبادل ضمن الوسائل المندمجة مع نظام الحوسبة .

3- أن كل جرم يمس مصلحة يقدر المشرع أهمية التدخل لحمايتها والمصلحة محل الحماية فى ميدان الجريمةالإلكترونية هى الحق فى المعلومات كعنصر معنوى ذى قيمة اقتصادية عالية ، ويشمل هذا الحق فى الوصول إلى المعلومات وانسيابها وتدفقها وتبادلها وتنظيم استخدامها ، كل ذلك على نحو مشروع ودون مساس بحقوق الآخرين فى المعلومات

4- إن تعريف الجريمة عموماً يتأسس على بيان عناصرها المناط بالقانون تحديدها ، إذ من دون نص القانون على النموذج القانونى للجريمة لا يتحقق إمكان المساءلة عنها (استناداً إلى قاعدة الشرعية الجنائية ، التى توجب عدم جواز العقاب عند انتفاء النص ، واستناداً إلى أن القياس محظور فى ميدان النصوص التجريمية الموضوعية)

ولذلك يمكننا تعريف الجريمة الإلكترونية بأنها سلوك غير مشروع ينصب على معطيات الحاسب الإلكترونى (بيانات ومعلومات وبرامج) وتطال الحق فى المعلومات ، ويستخدم لارتكابها وسائل تقنية معلوماتية ومحل الجريمة الإلكترونية هو دائماً معطيات الكمبيوتر بدلالتها الواسعة (البيانات المدخلة) ، وبيانات ومعلومات معالجة ومخزنة ، البرامج بأنواعها ، المعلومات المستخرجة المتبادلة بين النظم ، أما جهاز الحاسب الآلى فهو النظام التقنى بمفهومه الشامل المزدوج بين تقنيات الحوسبة بما فى ذلك شبكة المعلومات .

ثانيا: خصائص الجريمة الإلكترونية :

تتميز الجريمة الإلكترونية بعدة خصائص تميزها عن الجريمة التقليدية نذكر أهمها :-

1- الجريمة الإلكترونية جريمة عابرة للحدود :

تتميز الجريمة الإلكترونية أو المعلوماتية غالباً بالطابع الدولى ، بالطابع العالمى لشبكة الانترنت – يجعل معظم دول العالم فى حالة اتصال دائم على الخط **on lhne**، ويسهل ارتكاب الجريمة من دولة إلى دولة أخرى فالجريمة الإلكترونية هى جريمة جريمة عابرة للقارات [١] ، كما أنها من نوع الجرائم التى يتم ارتكابها عبر المسافات حيث لا يتواجد الفاعل على مسرح الجريمة بل يرتكب الجريمة عن بعد وهو ما يعنى عدم التواجد المادى للمجرم المعلوماتى فى مكان الجريمة ، ومن ثم تتباعد المسافات بين الفعل الذى يتم من خلال جهاز كمبيوتر الفاعل وبين النتيجة أى المعطيات محل الاعتداء ، وبالتالى لا تقف الجريمة الإلكترونية عند الحدود الإقليمية لدولة معينة بل تمتد إلى الحدود الإقليمية لدولة أخرى مما يزيد من صعوبة اكتشافها[٢].

2-: صعوبة الاحتفاظ الفنى بدليل الجريمة المعلوماتية[٣]

حيث يستطيع المجرم المعلوماتى فى أقل من ثانية أن يمحو أو يحذف أو يغير البيانات والمعلومات الموجودة فى الكمبيوتر ، لذا فإن للمصادفة وسوء الحظ دوراً فى اكتشافها يفوق أساليب التدقيق والرقابة ، ومعظم مرتكبيها الذين تم ضبطهم وفقاً لما لاحظه أحد الخبراء فى مجال الجريمة المعلوماتية إما أنهم قد تصرفوا بغباء أو لم يستخدموا الأنظمة المعلوماتية بمهارة .

3-: وقوع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات .

---

(١)- د / عبدالله حسين على محمود – سرقة المعلومات المخزنة فى الحاسب الآلى – دار النهضة العربية – سنة 2002 – ص 15.

(٢)- د / خالد ممدوح ابراهيم – التقاضى الإلكترونى – دار الفكر الجامعى – الاسكندرية 2008 – ص 323.

(٣) John Eaton jermysmithirs.Amanagers guide to information technology, London , Philip Appan 1982 p. 263.

- د / هشام محمد فريد رستم – بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت والذى عقد بدولة الإمارات العربية المتحدة خلال الفترة من 1-3 مايو 2000.

من خصائص الجريمة الإلكترونية وكذلك المعلوماتية أنها تقع أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصةبالكمبيوتر ، ويمثل هذا الشرط الأساس الذى يتعين توافره حتى يمكن البحث فى قيام أو عدم قيام أركان الجريمة المعلوماتية الخاصة بالتعدى على نظام المعالجة للبيانات ، ذلك انه فى حالة تخلف هذا الشرط تنتفى الجريمة المعلوماتية(١).

وترتكب الجرائم المعلوماتية أثناء أى مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الإلكترونية للبيانات (الإدخال – المعالجة – الإخراج)(٢).

4-: الجريمة الإلكترونية تعتمد على الذكاء فى ارتكابها .

حيث أنها توصف بجرائم الذكاء بالإضافة إلى أنها ليست جريمة منظمة فى الغالب ، بل تتم على المستوى الفردى وأهم دوافعها الطمع والجشع والانتقام ، وأحياناً ترتكب بدافع إثبات الذات ، فالمجرم المعلوماتى ذو مهارات وتقنية عالية وإلمام بتكنولوجيا النظم المعلوماتية (٣)

كما انها لا تترك أى آثار مادية لها بعد ارتكابها فهى جريمة تقع فى بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الإلكترونية غير المرئية (٤)

5- أن محل الجريمة المعلوماتية أو الإلكترونية هو معطيات الكمبيوتر :

أى ان البيانات والمعلومات والبرامج بكل انواعها ، سواء المدخلة أو المخزنة على الجهاز ، وتستهدف هذه الجرائم الحق فى المعلومات ويمتد تغيير المعلومات ليشمل الحق فى انسيابها وتدفقها والحق فى

---

(١)- د / على سليمان احمد فضل – المواجهة التشريعية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية والإنترنت ، - دار النهضة العربية – 2007 – ص 23 .
- د على عبدالقادر القهوجى – المرجع السابق – ص 43.

(٢) – د / نائلة عادل محمد فريد – المرجع السابق – ص154.

(٣) – د / أحمد خليفة الملط – الجرائم المعلوماتية – دار الفكر العربى – 2005 – ص 114.

(٤) – د / فهد عبدالله العبيد – الإجراءات الجنائية المعلوماتية – جامعة عين شمس – 2012 – ص 61.

المعلومات ذاتها أو بما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية[١].

وفى قضية تتخلص وقائعها أن احد الأشخاص ويدعى " كافين متنك " وهو من أشهر مرتكبى جرائم السطو على نظم الحاسوب بدأ نشاطه فى السبعينيات فى الثانية عشرة من عمره ، حيث كان يمضى وقت فراغه فى ممارسة هواية الاعتداء على نظم الهاتف فى لوس أنجلوس ، وفى عام 1981 تم إلقاء القبض عليه لأول مرة بسبب إتلافه بيانات شبكة حاسوب وسرقة دليل العمليات من إحدى شركات الهاتف ، منذ ذلك الوقت اعتاد " متنك " ارتكاب العديد من جرائم السطو فى نظم الحاسوب وسرقة البرامج والمعلومات وأرقام بطاقات الائتمان حتى تم القبض عليه عام 1989 بعد أن سرق برامج تقدر قيمتها بملايين الدولارات من شركة المعدات الرقمية "**D E C** " وأصبح ممن تم إدانته تحت قانون التزوير وسوء استخدام الحاسوب ، حكم عليه بالسجن لمدة عام ثم أفرج عنه لصغر سنه . اختفى بعد ذلك وواصل نشاطه الإجرامى حتى تم القبض عليه عام 1995 وهو يحالو السطو على شبكة معلومات مكتب التحقيقات الاتحادى "**P B I**"[٢].

ثالثا: دوافع ارتكاب الجريمة الإلكترونية :

يرتكب المجرم الإلكترونى أو المعلوماتى مختلف أنواع الاعتداءات على نظم الكمبيوتر وتحديداً الاختراقات بدافع التحدى وإثبات المقدرة العملية والتقنية ، فالمجرم الإلكترونى ذو مهارات تقنية ودراية بالتكنيك المستخدم فى نظام الحاسب الإلكترونى[٣] ومن أهم دوافع ارتكاب

---

(١) – د/ محمد سامى الشوا – الغش المعلوماتى كظاهرة إجرامية مستحدثة ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائى – القاهرة – 25 – 28 – أكتوبر 1993 – ص 2 .

(٢)- د / محمد الأمين البشرى – الأدلة الجنائية الرقمية – مفهومها ودورها فى الإثبات – المجلة العربية للدراسات الأمنية – المجلد 17 – العدد 33 السنة 17 – أبريل 2002 - الرياض – ص 136.

(٣)–د / هدى حامد قشقوش – جرائم الحاسب الإلكترونى فى التشريع المقارن – المرجع السابق – ص 27.

الجريمة الالكترونية الشغف بالإلكترونيات ، والسعى إلى الربح ، والدوافع الشخصية أو المؤثرات الخارجية ، والأسباب الخاصة بالمنشأة[١].

ومن أهم دوافع ارتكاب الجريمة الالكترونية ما يلى :-

١ -السعى إلى تحقيق كسب مالى :

إن السعى وراء مكاسب مالية يعد أحد أهداف ارتكاب الجرائم الإلكترونية أوالمعلوماتية وهو ما يترتب عليه إدخال تعديل على عناصر الذمة المالية ، فطمع الاستيلاء على المال دافعها وبريق المكسب السريع محركها[٢].

٢ -الانتقام من رب العمل أو أحد الزملاء ، وإلحاق الضرر به :

يتعرض العاملون فى قطاع التقنية أو المستخدمين لها فى نطاق قطاعات العمل الأخرى لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح مما يدفع بعض العاملين لارتكاب جرائم الحاسب الإلكترونى وتحديداً جرائم إتلاف البيانات والبرامج وزرع الفيروسات باعثها الانتقام من المنشأة أو رب العمل أو أحد الزملاء .

٣ -الرغبة فى قهر النظام والتفوق على تعقيد وسائل التقنية :

قد يكون الدافع إلى ارتكاب جرائم الحاسب الإلكترونىالرغبة فى قهر النظام وتخطى الحواجز حوله ، أكثر من رغبة الحصول على الربح[٣] ، ويتجسد ذلك فى نسبة متغيرة من جرائم الحاسب الإلكترونى خاصة ما يعرف بأنشطة الـ (**hackers**) المتطفلين الدخيلين على النظام والمتجسدة فى جرائم التواصل مع أنظمة الحاسب – تحديداً عن بعد – الاستخدام غير المصرح به لنظام الحاسب واختراق مواقع الانترنت ومرتكبى هذه الجرائم لديهم (شغف الآلة) دائماً يحاولون إيجاد الوسيلة إلى التفوق عليها .

المطلب الثانى

---

(١)–د / محمد سامى الشوا – المرجع السابق – ص 44 .
(٢)- د / فهد عبدالله العبيد – المرجع السابق – ص 50 وما بعدها.
(٣)- د / جميل عبدالباقى الصغير – القانون الجنائى والتكنولوجيا الحديثة – الكتاب الأول – دار النهضة العربية – 1992 – ص 16.

أنواع الجريمة الإلكترونية

مما لا شك فيه أن تقدم وسائل الاتصالات والمعلومات وذيوع استعمال الكمبيوتر وسهولة استخدام الإنترنت ، أدى إلى ظهور أنواع جديدة من الجرائم أصبحت معه نصوص قانون العقوبات والإجراءات الجنائية التقليدية عاجزة عن مواجهتها أو التصدى لها ،ولعل هذا ما دفع العديد من مشرعى دول العالم إلى إصدار قوانين جديدة لمواجهة الجرائم المعلوماتية الإلكترونية ، بينما فضلت بعض الدول إجراء تعديل فى بعض قوانينها القائمة .

والجريمة الإلكترونية والمعلوماتية تعتبر شكلاً جديداً من أشكال الجرائم العابرة للحدود الدولية بين كافة دول العالم ، إذ يمكن عن طريق جهاز الكمبيوتر وشبكة الانترنت ارتكاب العديد من الجرائم مثل جريمة سرقة الأموال من البنوك عبر شبكة الإنترنت ، وجريمة الدخول إلى النظام المعلوماتى والبقاء فيه بدون تصريح ، وجريمة قرصنة البرامج ونسخها وجريمة تزوير التوقيع الإلكترونى ، وجريمة انتهاك حرمة الحياة الخاصة وجريمة الإتلاف المعلوماتى ، والجرائم المخلة بالآداب ، وجريمة التلاعب فى أنظمة المعالجة للبيانات ، وغير ذلك من أنواع الجرائم الإلكترونية[١].

فالجرائم الإلكترونية والمعلوماتية لها صور متعددة بتعدد دور التبعية المعلوماتية " إلا أننا فى صدد هذا البحث لن نعرض لكافة أنواع هذه الجرائم فهذا يخرج عن نطاق بحثنا ، بل سنتناول الجرائم الإلكترونية التى تثير مشكلة فى تطبيق النصوص القانونية إما لتعذر المطابقة بينها وبين النصوص التقليدية أو بسبب الفراغ التشريعى لمواجهة هذه الجرائم ، نتعرض لأهم الجرائم الإلكترونية وأكثرها إثارة للمشكلات القانونية خاصة فيما يتعلق بالإثبات الجنائى لهذه الجرائم :

اولا: جرائم التعدى على الحياة الخاصة :

الحياة الخاصة لها خصوصيتها بما تحتويه من أسرار ، والمحافظة على هذه الأسرار يحظى بحماية دستورية وقانونية فى كافة دساتير الدول وقوانينها وقد عنى المشرع المصرى بإضفاء الحماية على الحياة الخاصة سواء بالدستور وفقاً للمادة 45 منه ، أو بالقانون وفقاً لنص المادة 309

---

(١)- أنظر د / أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب الآلى – دار النهضة العربية – سنة 2000 – ص 201 وما بعدها .

من قانون العقوبات ويصعب بداية حصر عناصر الحق فى الحياة الخاصة فهى تشمل حرمة جسم الإنسان والمسكن والصورة والمحادثات والمراسلات والحياة المهنية(١).

أما علاقة الحياة الخاصة بالتقنية الحديثة وتكنولوجيا المعلومات ظهرت أهميتها بانتشار بنوك المعلومات فى الآونة الأخيرة لخدمة أغراض متعددة وتحقيق أهداف المستخدمين فى المجالات العلمية والثقافية والعسكرية(٢).

هكذا أصبحت الشبكات المعلوماتية مستودعاً خطيراً للكثير من أسرار الإنسان التى يمكن الوصول إليها بسهولة وسرعة لم تكن متاحة فى ظل سائر وسائل الحفظ التقليدية فأصبحت بنوك المعلومات أهم وأخطر عناصر الحياة الخاصة للإنسان فى العصر الحديث .

فقد يستخدم النظام المعلوماتى فى الاعتداء على حرمة الحياة الخاصة ، كما لو قام شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوى على معلومات تخص آخر بدون علمه وبغير إذنه ، أو أن يكون تجميع هذه المعلومات بموجب موافقة سابقة من صاحبها ولكن قام الشخص المكلف بحفظها باطلاع الغير عليها بدون إذن صاحبها (٣) كما فى حالة الأسرار المودعة لدى المحاسبين أو لدى المحاميين أو لدى الأطباء ، فكل هذه الأسرار يحميها القانون ويجرم إفشائها بالطرق غير المشروعة ودون موافقة صاحبها .

وجريمة التعدى على الحياة الخاصة والاطلاع على الأسرار أو إفشائها ، قد تتم باستدعاء المعلومات وفتح السجلات الإلكترونية والاطلاع عليها من خلال شاشة الكمبيوتر .

ويدخل فى نطاق جرائم التعدى على الحياة الخاصة جريمة تسجيل المحادثات الشخصية أو مراقبتها بأية وسيلة حيث نجد بعض المتسللين يستطيعون اختراق شبكة الإنترنت بطرق غير مشروعة والتصنت على هذه المكالمات .

---

(١)- د / ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائى – دار النهضة العربية 1982 – ص 207 .

(٢)- د / اسامه عبدالله فايد – الحماية الجنائية للحياة الخاصة – وبنوك المعلومات – دار النهضة العربية – 1994 – ص 48 .

(٣)- د / أحمد خليفة الملط – المرجع السابق - ص 221.

وقد اهتمت القوانين المقارنة بمسألة الحفاظ على المعلومات الخاصة بالأفراد وحماية أسرارهم فاتجهت إلى تبنى العديد من الضمانات[١] يمكن تلخيصها فى الآتى :

١ - مبدأ الإخطار العام : وهو أن يعلم الجمهور الهيئات التى تقوم بجمع هذه البيانات وتنوع المعلومات التى تقوم بتسجيلها [٢] ، فيجب أن تكون هناك قيود على إنشاء الأنظمة المعلوماتية المختلفة لمعالجة البيانات .

٢ - شرعية الحصول على المعلومة : فيجب أن يتم الحصول على المعلومة بطريقة تخلو من الغش والاحتيال ، حيث تمنع المادة 25 من القانون الفرنسى للمعلوماتية تسجيل أى معلومة إلا إذا كانت برضاء صاحب الشأن .

٣ - التناسب بين المعلومات الشخصية والهدف من ذلك التسجيل ، فعلى الجهة الراغبة فى إقامة أى نظام معلوماتى أن تحدد الهدف من إقامته[٣].

٤ - ولقد تضمنت بعض التشريعات العربية العديد من النصوص والقواعد التى تحمى البيانات الشخصية وتقرر عقوبات على إفشاء هذه البيانات ومن هذه التشريعات قانون التجارة الإلكترونية المصرى الصادر 2004 الذى نص فى الفصل العاشر منه على حماية سرية البيانات المشفرة واحترام الحق فى الخصوصية[٤].

---

(١)- د / عبدالفتاح بيومى حجازى – صراع الكمبيوتر والإنترنت – فى القانون العربى النموذجى – دار الكتب القانونية – القاهرة 2007 – ص 609.

(٢)- د/ بدر سليمان يونس – أثر التطور التكنولوجى مع الحريات الشخصية فى النظم السياسية – رسالة دكتوراه – جامعة القاهرة 1982 – ص13.

(٣)- أنظر د / عبدالفتاح بيومى حجازى – المرجع السابق – ص620.

(٤)- أيضاً قانون التجارة الإلكترونية وقانون التجارة والمعاملات الإلكترونية فى إمارة دبى الصادر 2002 ، وقانون التجارة الإلكترونية التونسى الصادر 2000.

ثانيا: جرائم واقعة على الأموال :

صاحب ظهور شبكة الإنترنت تطورات كبيرة فى شتى المجالات ، حيث أصبحت معظم المعاملات المالية والتجارية تتم من خلال هذه الشبكة ، مثل البيع والشراء ، مما ترتب على ذلك تطور وسائل الدفع والوفاء وأصبحت جزءاً لا يتجزأ من هذه المعاملات ، وفى خضم هذا التداول المالى عبر الإنترنت انتهز بعض المجرمين من أجل السطو عليها ، حيث ابتكرت عدة طرق من أجل ذلك ، على غرار السطو والسرقة ، والتحويل الإلكترونى غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة .

١ - جرائم السطو على بطاقات الائتمان والتحويل الإلكترونى غير المشروع للأموال .

واكب استخدام البطاقات الائتمانية من خلال شبكة الإنترنت ظهور الكثير من المتسللين للسطو عليها باعتبارها نقوداً إلكترونية ، خاصة من جهة الاستيلاء على بطاقات الائتمان أمراً ليس بالصعوبة بما كان ، فلصوص بطاقات الائتمان يستطيعون الآن سرقة الألوف من أرقام البطاقات فى يوم واحد من خلال شبكة الإنترنت ومن ثم بيع هذه المعلومات للآخرين(١).

وفى قضية حدثت فى عام 1990 تتلخص وقائعها بأن وكالات سرية تتبع للحكومةالاتحادية فى الولايات المتحدة بالاعتداء على شركة " استيف جاكسون " للألعاب بحثاً عن أدلة تتعلق بعصابة من المتطفلين **HACKERS** تطلق على نفسها " لفيون دووم " كانت شركة استيف جاكسون للألعاب تقوم بتصميم ونشر ألعاب على طرق خيالية للسطو على نظم الحاسوب ، كما كانت تقوم بإصدار نشرة دورية لتقديم خدمات البريد الإلكترونى لعملائها . قامت الوكالة الإتحادية بمصادرة جميع اجهزة الحاسوب وملحقاته ونسخ من كتب تحت الطبع . ولم توجه تهم جنائية لشركة جاكسون إلا أنها تعرضت لخسائر مالية كبيرة وبعد فشل العديد من المحاولات لاسترداد الأشياء المصادرة ، قررت الشركة مقاضاة الوكالة

---

(١)- د / حسن طاهر داوود – جرائم نظم المعلومات – أكاديمية نايف العربية للعلوم الأمنية – الرياض – الطبعة الأولى – 2000 ص 73.

السرية الحكومية بتهمة الاعتداء على مقر الشركة وسرقة ممتلكاتها . ووضح أثناء المحاكمة أن موظفي الوكالة الحكومية قاموا بمحو رسائل بريدية خاصة لم تكن قد سلمت لأصحابها وقد أنكرت الوكالة التهم . ولصعوبة التعامل الفنى مع الأدلة الجنائية الرقمية سحبت الشركة التهمة الجنائية ، ومع ذلك حكمت المحكمة بإدانة الوكالة الحكومية تحت قانون سرية الاتصالات الإلكترونية وقانون حماية الحريات الشخصية وقررت تعويض الشركة بمبلغ (300000 دولار) مقابل الأضرار التى لحقت بالشركة .[١]

وتتم عملية التحويل الإلكترونى غير المشروع للأموال من خلال الحصول على كلمة السر المدرجة فى ملفات أنظمة الكمبيوتر الخاصة بالمجنى عليه ، مما يسمح للجانى بالتوغل فى النظام المعلوماتى وعادة ما يكون هؤلاء من العاملين على إدخال البيانات فى ذاكرة الجهاز أو من قبل المتواجدين على الشبكة أثناء عملية تبادل البيانات [٢] وتتم عملية التحويل الإلكترونى غير المشروع للأموال من خلال أحد الطرق الآتية :

٢ - الاحتيال :

ويتم ذلك بطرق مختلفة باستعمال الطرق الاحتيالية التى من خلالها يوهم من أجلها المجنى عليه بوجود مشروع كاذب أو يحدث الأمل لديه بحصول ربح ، فيسلم المال للجانى بطريق معلوماتى أو من خلال تصرف الجانى فى المال وهو يعلم أن ليس له صفة التصرف فيه [٣] وقد يتخذ اسم أو صفة كاذبة تمكنه من الاستيلاء على مال المجنى عليه فيتم التحويل الإلكترونى للأموال وذلك من خلال اتصال الجانى بالمجنى عليه

---

(١)- د / محمد الأمين البشرى – الأدلة الجنائية الرقمية – مفهومها ودورها فى الإثبات – المجلة العربية للدراسات الأمنية – المجلد 17 – العدد 33 السنة 17 – أبريل 2002 - الرياض – ص 136.

(٢)- د / خالد ممدوح ابراهيم – أمن الجريمة الإلكترونية – الدار الجامعية – الاسكندرية – 2010 – ص 76.

(٣) - يونس عزب " قراءة فى الاتجاهات التشريعية للجرائم الإلكترونية مع بيان موقف الدول العربية وتجربة سلطنة عمان " ورشة عمل التشريعات فى مجال مكافحة الجرائم الإلكترونية ، المنعقدة بمسقط ، سلطنة عمان من الفترة 2 -4 ابريل 2006 ص 16.

عن طريق الشبكة أو يتعامل الجانى مباشرة مع بيانات الحاسب فيستعمل البيانات الكاذبة التى تساعده فى إيهام الحاسب والاحتيال عليه فيسلمه النظام المال .

- الاحتيال باستخدام بطاقات الدفع الالكترونى :

يعتمد نظام بطاقة الدفع الإلكترونى على عمليات التحويل الإلكترونى من حساب بطاقة العميل بالبنك المصدر للبطاقة إلى رصيد التاجر أو الدائن الذى يوجد حسابه وذلك من خلال شبكة التسوية الإلكترونية للهيئات الدولية "هيئة الفيزا كارد "[١] وتعطى بطاقة الدفع الإلكترونى الحق للعميل بالحصول على السلع والخدمات على الشبكة عن طريق تصريح كتابى أو تليفونى ، بخصم القيمة على حساب بطاقة الدفع الإلكترونى الخاصة وتتم العملية بدخول العميل أو الزبون إلى موقع التاجر ويختار السلعالمراد شرائها ويتم التعاقد بملأالنموذج الإلكترونى ببيانات بطاقة الائتمان الخاصة بالمشترى [٢] وأمام التطور الإلكترونى أصبحت إمكانية خلق مفاتيح البطاقات والحسابات البنكية بالطريق غير المشروع ممكنة عبر قنوات شبكة الإنترنت [٣].

٣ - جرائم الاستيلاء على النقود الإلكترونية :

فالنقود الإلكترونية هى " قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً ، وغير مرتبطة بحساب مصرفى ، تحظى بقبول غير من

---

(١) - عمر الشيخ الأصم – البطاقات الائتمانية المستخدمة الأكثر انتشاراً فى البلاد العربية " أعمال ندوة تزوير البطاقات الائتمانية – أكاديمية نايف العربية للعلوم الأمنية – الرياض – الطبعة الأولى – 2002 – ص12 .

(٢) - أنظر د أحمد شوقى أوخطوة – جريمة الاحتيال ماهيتها وخصائصها " دورة عمل حول جرائم الاحتيال والإجرام المنتظم – جامعة نايف العربية للعلوم الأمنية ، من 18 – 20 جوان 2007 – الرياض الطبعة الأولى 2008 ص 39.

- أنظر د / محمد عبدالرسول خياط " عمليات تزوير البطاقات الائتمانية – أعمال ندوة تزوير البطاقات الائتمانية أكاديمية نايف العربية للعلوم الأمنية الرياض 2002 ص 41.

(٣)- SEDALLAN Valerie Drait de l'internet Reglementation – Responsabilites – contrat ,Edilion Net press, paris, 1997,p149.

قام بإصدارها ، وتستعمل كأداة دفع " وتتمثل أهم عناصرها فى أن قيمتها النقدية تشحن على بطاقة بلاستيكية ، أو على القرص الصلب للحاسب الشخصى للمستهلك ، فهى تختلف عن البطاقات الائتمانية ، لأن النقود الإلكترونية يتم دفعها مسبقاً ، بالإضافة إلى أنها ليست مرتبطة بحساب العميل ، أى أنها استحقاق عائم على مؤسسة مالية ، يتم بين طرفين هما العميل والتاجر ، دون الحاجة إلى تدخل طرف ثالث ، كمصدر هذه النقود مثلاً[١]، فهى مجموعة من البروتوكولات والتوقيعات الرقمية التى تتيح للرسالة الإلكترونية أن تحل فعلياً محل تبادل العملات النقدية [٢] ومن هذه البطاقات ما يعمل عن طريق إدخالها إلى المركز الخاص بالمعاملة المصرفية لدى البائع أو الدائن حيث تم انتقال البيانات الإسمية من البطاقة إلى الجهاز الطرفى للبائع تحول عليه نتائج عمليات البيع والشراء إلى البنك الخاص بالبائع[٣].

ثالثا: جرائم واقعة على الأشخاص :

يعد الهدف الأول والأسمى لوضع القوانين وسن التشريعات ، حماية سلامة الأشخاص من مختلف الانتهاكات التى قد يتعرضون لها ، سواء فى أبدانهم أو فى حياتهم الخاصة أو فى سمعتهم وشرفهم .

تطور الأمر بعد ذلك مع ظهور شبكة الانترنت ، فرغم الفوائد التى أدت بها ، والتسهيلات التى قدمتها فى الحياة اليومية للفرد والمجتمع على حد سواء ، إلا أنها أصبحت سلاح فتاك فى يد المجرمين ، بالإضافة إلى ذلك فإن المعلومات المتعلقة بالأفراد متداولة بكثرة عبرها ، مما يجعلها عرضة للانتهاك والاستعمال من طرف هؤلاء المجرمين ، وجعلت سمعة وشرف الأفراد مستباحة .

وسوف نعرض لأهم هذه الجرائم :

١ -جرائم السب والقذف على الإنترنت :

---

(١)- د / محمد ابراهميم محمد الشافعى – النقود الإلكترونية – مجلة الأمن والحياة – أكاديمية شرطة دبى س 12 ، ع 1 – يناير 2004 – ص 142 – 148.

(٢)- منير الجنبهى – البنوك الإلكترونية – الطبعة الثانية – دار الفكر الجامعى الاسكندرية – 2006 – س47.

(٣)- د / عبدالفتاح بيومى حجازى – صراع الكمبيوتر والإنترنت فى القانون العربى النموذجى – دار الكتب القانونية – 2007 – ص 609.

تعتبر جرائم القذف والسب من أكثر الجرائم انتشاراً عبر شبكة الإنترنت . وقد عرفت المادة 1/302 من قانون العقوبات القذف بأنه " يعد قاذفاً كل من أسند بواسطة إحدى الطرق المبينة بالمادة 171 من هذا القانون أموراً لو كانت صادقة لأوجبت عقاب من أسندت إليه بالعقوبات المقررة قانوناً ولأوجبت احتقاره عند أهل وطنه ... "

كما نصت المادة 306 عقوبات على أنه " كل سب لا يشتمل على إسناد واقعة معينة بل يتضمن بأى وجه من الوجوه خدشاً للشرف أو الاعتبار يعاقب عليه فى الأحوال المبينة بالمادة 171 بالحبس مدة سنة وغرامة لا تقل عن ألف جنيه ولا تزيد على خمسة آلاف جنيه أو إحدى هاتين العقوبتين "[1].

ويتضح من النصوص السابقة أن المشرع يتطلب أن تتوافر العلانية المنصوص عليها بالمادة 171عقوبات لتطبيق عقوبة القذف والسب المقررة بهذه النصوص ، وقد تضمنت المادة 171عقوبات بياناً بطرق التعبير وصورة العلانية دون أن تحصرها حصراً ، فهذه الطرق وردت على سبيل المثال لا الحصر ، ويستفاد من نص المادة السابقة

---

(١)- وقد نصت المادة 209 من قانون الجزاء الكويتى " كل من أسند لشخص فى مكان عام أو على مسمع أو مرأى من شخص آخر غير المجنى عليه ، واقعة تستوجب عقاب من تنسب إليه أو تؤذى سمعته ، يعاقب بالحبس مدة لا تجاوز سنتين وبغرامة لا تجاوز ألفى روبية أو بإحدى هاتين العقوبتين " ، كما نصت المادة 210 كويتى على أنه " كل من صدر منه ، فى مكان عام أو على مسمع أو مرأى من شخص آخر غير المجنى عليه ، سب لشخص آخر على نحو يخدش شرف هذا الشخص أو اعتباره دون أن يشتمل هذا السب على إسناد واقعة معينة له ، يعاقب بالحبس مدة لا تجاوز سنة واحدة وبغرامة لا تجاوز ألف روبية أو بإحدى هاتين العقوبتين "

- وقد اعتبرت محكمة التميزالكويتية أن مواقع التواصل الاجتماعى مكان عام وبالتالى أرست هذه المحكمة مبدأ جديداً أن موقع (تويتر) وهو أحد مواقع التواصل الاجتماعى الكويتية ، يعتبر مكاناً عاماً ومن ثم يخضع لقانون الجزاء الكويتى ، وتطبيقاً لذلك الحكم فإن كل من يغرد فى (تويتر) ممن داخل دولة الكويت يخضع لقانون الجزاء الكويتى وذلك لتحقيق ركن العلانية فى موقع التواصل الاجتماعى فتنطبق أحكام مادتى (209) و (210) من قانون الجزاء الكويتى على المغردين . أنظر مجلة الحقوق الكويتية – العدد رقم 1 – السنة 40 – مارس 2016 – ص 188.

والتى قررت " .... أو بأى وسيلة أخرى من وسائل العلانية .. لما قد يظهر فى المستقبل من وسائل علانية حديثة ، وهو ما يعنى جريمة القذف والسب عبر شبكة الانترنت يتحقق به العلانية وبالتطور أصبح الإنترنت إحدى الوسائل الحديثة بل أكثرها رواجا لارتكاب جرائم السب والقذف من خلال عبارات بذيئة تمس وتخدش شرف المجنى عليه ، فعادة ترسل عبارات السب والقذف عبر البريد الوصتى أو ترسم أو تكتب على صفحات الويب ما يؤدى بكل من يدخل هذا الموقع لمشاهدتها أوالاستماع إليها ، ويتحقق بذلك ركن العلانية الذى تطلبه الكثير من التشريعات فى السب العلنى وإذا لم يطلع عليه أحد فإنه يمكن تطبيق مواد السب أو القذف غير العلنى(١).

٢ -الجرائم المخلة بالآداب العامة عبر الإنترنت :

وعرفت شبكة الإنترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية ، فالانترنت جعل الممارسات غير الأخلاقية بشتى وسائل عرضها من صور وفيديو ورسائل نصية وبرامج اجتماعية وتسجيلات صوتية فى متناول الجميع ، وسهلت صناعة الإباحية بشكل كبير ، وقد وجد العاملون فى مجال الرزيلة والإباحية فى شبكة الإنترنت وسيلة حديثة ذات كفاءة عالية فى الدعوة إلى ممارسة البغاء والإعلان عن الفجور عن طريق الإعلانات الإلكترونية عبر مواقع الويب المنتشرة على الشبكة ، وذلك كله فى إطار التقنية الفنية التى يستخدمها الجانى فى ارتكابه للجريمة وصعوبة اكتشاف هذه الجرائم وتحديد مصدرها وإقامة الدليل عليها ، بالإضافة إلى عدم وجود تشريعات حديثة تواجه الجرائم الإضافية التى ترتكب عبر شبكة الإنترنت(٢).

وفى قضية تتلخص وقائعها حدثت عام 1996 حيث أقام المتهم علاقة صداقة بينه وبين المجنى عليها عبر شبكة الإنترنت ثم قام المتهم بالتحضير لمقابلة المجنى عليها عبر رسائل إلكترونية ، ثم وجه لها الدعوة لمشاهدة أفلام مسجلة على الفيديو وعند وصول الفتاة قام المتهم باحتجازها

---

(١)- د / سامى على حامد عياد – الجريمة المعلوماتية وإجرام الإنترنت ، دار الفكر الجامعى – الاسكندرية – 2007 – ص 77.

(٢) - د / خالد ممدوح ابراهيم – التقاضى الإلكترونى – الدعوى الإلكترونية وإجراءاتها أمام المحاكم – دار الفكر الجامعى – الاسكندرية – 2008 – ص 352

لمدة عشرين ساعة ، وقام بالاعتداء عليها جنسياً بوحشية مع الضرب والحرق والتعذيب ، وقد لعب الإنترنت دوراً فى ارتكاب الجريمة كأداة للتواصل والتعارف ونقل الدعوى بعد تهيئة الضحية نفسياً وفى مرحلة المحاكمة لم يتمكن الاتهام من استخدام معظم الأدلة الرقمية المتوافرة فى البريد الإلكترونى للمتهم ، لعدم ضبطها بالطرق المشروعة . كما حرم الدفاع من استخدام الأدلة الرقيمة المخزنة فى البريد الإلكترونى للمجنى عليها لأن قوانين نيويورك تمنع كشف المعلومات الخاصة للأفراد بما فى ذلك التحقق من الشخصية أو كشف تاريخها الجنسى . أخذت المحاكمة اهتمام أجهزة الإعلام وأصبحت منفذاً لإثارة مفهوم الجريمة الجنسية عبر شبكة الإنترنت مما أثر على نتائج المحكمة . ورغم تناقض الأدلة التى قدمتها المجنى عليها حكمت المحكمة على المتهم بالسجن ، وتشير وقائع القضية إلى الكم الهائل من الأدلة الجنائية الرقمية التى وفرها الإنترنت فى أكثر من مسرح افتراضى ، إلا أن القوانين المحلية القديمة السابقة لعصر الإنترنت وقفت دون استخدان الأدلة لكشف الحقائق ، كما أن جهل رجال التحقيق بالإجراءات القانونية الخاصة لضبط الأدلة الرقمية كان سبباً فى الإضرار بالعدالة(١).

ويرتبط نشر المواد الإباحية والمخلة بالآداب العامة على شبكة الإنترنت بمجالين رئيسيين : الأول يتعلق بنشر الصور المخلة والممارسات الغير أخلاقية المرتبكة بالأطفال **child prnography** والذى يتعلق بالمواد المخلة بالكبار **Adult prnography** (٢).

ولعل هذا الوضع يستدعى ضرورة تدخل المشرع المصرى لمواجهة القصور فى التشريعات والقوانين القائمة أو تحديثها بالنص

---

(١)- د / - د / محمد الأمين البشرى – الأدلة الجنائية الرقمية – مفهومها ودورها فى الإثبات – المرجع السابق – ص 138.

(٢) - د / نائلة عادل محمد فريد – جرائم الحاسب الآلى الاقتصادية – منشورات الحلبى الحقوقية – 2005 – ص 39.

- وفى عام 2014 قامت دولة الكويت من خلال وزارة الداخلية عن طريق إدارة مكافحة الجرائم الإلكترونية بإغلاق أكثر من 300 حساب على موقع (الانستجرام) من ضمنها ما هو إباحى أو يحرض على الفسق والفجور أو حتى يقوم ببيع منتجات ممنوعة من مختلف برامج التواصل الاجتماعى أنظر مجلة الحقوق الكويتية – العدد 1 – السنة 40 – مارس 2016- ص 185.

صراحة على تجريم استخدام شبكة الانترنت والتقنيات الحديثة فى الإعلان عن الممارسات المخلة بالآداب .

٣ -انتحال الشخصية والتغرير والاستدراج :

يقصد بانتحال الشخصية ما يعمد إليه المجرم من استخدام شخص آخر للاستفادة من سمعته مثلاً أو ماله أو صلاحياته ، ولذلك فهذا سبب وجيه يدعو للاهتمام بخصوصية وسرية المعلومات الشخصية للمستفيدين على شبكة الإنترنت ، وتتخذ جريمة انتحال الشخصية عبر شبكة الإنترنت أحد أمرين :انتحال شخصية الفرد ، و انتحال شخصة المواقع[١].

ولقد سماها بعض المختصين فى أمن المعلومات جريمة الألفية الجديدة ، وذلك نظراً لسرعة انتشار ارتكابها خاصة فى الأوساط التجارية[٢]

---

(١)- انتحال شخصية الفرد : تتيح شبكة الإنترنت للمجرمين القدرة على جمع أكبر قدر من المعلومات عن الشخصية المطلوبة وهي الضحية والاستفادة منها في ارتكاب جرائمهم فتنتشر على شبكة الإنترنت الكثير من الإعلانات المشبوهة والتى تداعب عادة غريزة الطمع الإنسانى فى محاولة الاستيلاء على معلومات اختيارية من الضحية ، فهناك مثلاً إعلان عن جائزة فخمة يسكبها من يساهم بمبلغ رمزى لجهة خيرية ، وهذا يتطلب بطبيعة الحال الإفصاح عن بعض المعلومات الشخصية كالاسم والعنوان والأهم رقم بطاقة الائتمان لخصم المبلغ الرمزى لصالح الجهة الخيرية ، الأمر الذى يؤدى إلى الاستيلاء على رصيده البنكي أو السحب من بطاقته الإئتمانية أو حتى الإساءة إلى سمعة الضحية.
- انتحال شخصية المواقع : مع أن هذا الأسلوب حديثاً نسبياً ، إلا أنه أشد خطورة وأكثر صعوبة فى اكتشافه ، من انتحال شخصية الأفراد ، حيث يمكن تنفيذ هذا الأسلوب حتى مع المواقع التى يتم الاتصال بها من خلال نظم الاتصال الآمن حيث يمكن وبسهولة اختراق مثل هذا الحاجز الأمنى ، وتتم عملية الانتحال بهجوم يشنه المجرم على الموقع للسيطرة عليه ومن ثم يقوم بتحويله كموقع بينى ، أو يحاول المجرم اختراق موقع لأحد مقدمى الخدمة المشهورين ، ثم يقوم بتركيب البرنامج الخاص به هناك ، مما يؤدى إلى توجيه أى شخص إلى موقعه بمجرد كتابة اسم الموقع المشهور ويتوقع أن يكثر استخدام انتحال شخصية المواقع فى المستقبل ، نظراً لصعوبة اكتشافها ، أنظر محمد بن عبدالله بن على المنشاوى – جرائم الإنترنت فى المجتمع السعودى – أكاديمية نايف للعلوم الأمنية – الرياض – 2003 – ص 54 – 55 .

(٢)– د / عمرو عيسى الفقي - 0 الجرائم المعلوماتية – جرائم الحاسب الآلى والانترنت فى مصر والدول العربية ، المكتب الجامعى الحديث – الاسكندرية – 2006 – ص 102.

أما فيما يخص التغرير والاستدراج فغالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمى شبكة الإنترنت ، حيث يوهم المجرمون ضحاياهم برغبتهم فى تكوين صداقة على الإنترنت والتى قد تتطور إلى التقاء مادى بين الطرفين ، إن مجرمى التغرير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم فى بلد والضحية فى بلد آخر ، وكون معظم الضحايا من صغار السن ، فإن كثير من الحوادث لا يتم الإبلاغ عنها ، حيث لا يدرك كثير من الضحايا أنهم قد غرر بهم(١).

(١)– د / صغير يوسف – الجريمة المرتكبة عبر الإنترنت – جامعة مولود محمدى – 2013 – ص 51 .

الفصل الأول
أهمية ومضمون الإثبات الجنائى للجريمة الإلكترونية

يعد الإثبات الجنائى بالأدلة الرقمية من أبرز تطورات العصر الحديث فى كافة النظم القانونية ، تلك التطورات جاءت لتلائم الثورة العلمية والتكنولوجية والتقنية فى عصرنا الحالى ، والتى تطور معها الفكر الإجرامى ، فظهر نوع جديد من الجرائم الرقمية ، مما ألقى على عاتق القائمين على مكافحة الجريمة فى الدولة عبئاً شديداً ومهاماً جساماً تفوق القدرات المتاحة لهم وفق أسس وقواعد البحث الجنائى والإثبات الجنائى التقليدية[١] .

ونظراً لعدم كفاية وملائمة هذه النظم التقليدية سواء من الناحية القانونية أو التقنية وكان حتماً على المشرع أن يستحدث فى التشريعات ما يلائم هذا النوع من الجرائم فضلاً عن إنشاء أجهزة فنية متخصصة يناط بها عملية الإثبات العلمى لهذه الجرائم ، وتشكل الجرائم المعلوماتية تهديداً خطيراً ، سواء بالنسبة للمواطن العادى ورجال الأعمال أو لرجال البحث الجنائى ورجال القضاء ، لما لهذه الجرائم من مخاطر تصل أحياناً إلى حد الكارثة ، نظراً للخسائر والأضرار والتهديدات التى تترتب عليها سواء على الجانب الاقتصادى أو الجانب الأمنى ولما كانت هذه الجرائم تتميز بكون مرتكبها على قدر عال جداً من العلم والثقافة والحرفية ، للدرجة التى لا يمكن معها مواجهتهم وضبطهم وكشفهم والتحقيق معهم [٢] . ومن ثم محاكمتهم وفقاً للفكر الأمنى والقضائى التقليدى وقواعد الإثبات الجنائى التقليدية لذا كان ضرورياً بل وحتمياً استحداث طرق وأساليب خاصة قوامها العلم والمعرفة والحرفية ، وهذا لا يتأتى إلا بالتعليم والتدريب المستمرين لجميع المعنيين بكشف ومكافحة هذه الجرائم بكافة صورها وأشكالها ، واستخدام أحدث الوسائل العلمية والتكنولوجية ، فضلاً عن التعاون الفعال بين الجهات المعنية فى الداخل والخارج .

وسوف نقسم هذا الفصل إلى مبحثين :

---

(١) - أنظر د / أحمد يوسف الطحطاوى – الأدلة الإلكترونية ودورها فى الإثبات الجنائى – دراسة مقارنة – دار النهضة العربية – 2015 – ص 119

(٢) - د / أحمد خليفة الملط – الجرائم المعلوماتية – المرجع السابق – ص 114.

المبحث الأول : مفهوم وأهمية دراسة الإثبات الجنائى فى الجريمة الإلكترونية .

المبحث الثانى : مضمون الإثبات الجنائى فى الجريمة الإلكترونية .

المبحث الأول

مفهوم وأهمية الإثبات الجنائى وصعوبته في الجريمة الإلكترونية

سوف نتناول من خلال هذا المطلب تعريف الإثبات الجنائى بوجه عام ثم نوضح الطبيعة الخاصة للجريمة الإلكترونية وأثر ذلك على إثباتها جنائياً – ومدى ملاءمة وسائل الإثبات التقليدية فى مجال الجريمة الإلكترونية :

المطلب الأول

مفهوم وأهميةالإثبات الجنائى

أولا:مفهوم الاثبات الجنائي بوجه عام.

الإثبات فى المواد الجنائية هو إقامة الدليل على وقوع الجريمة أو عدم وقوعها وعلى إسنادها إلى المتهم أو براءته منها [١] أو بعبارة أخرى فإن الإثبات هو كل ما يؤدى إلى إظهار الحقيقة فى الدعوى الجنائية ، فإنه لكى يتم الحكم على المتهم فى المسائل الجنائية يجب ثبوت وقوع الجريمة فى حقه عن طريق اتباع إجراءات الخصومة الجنائية المقررة فى هذا الشأن ، أى إثبات وقوع الجريمة فى ذاتها بوجه عام وأن المتهم هو المرتكب لها بوجه خاص .

كما عرف البعض الإثبات بأنه إقامة الدليل على وقوع الجريمة لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية وذلك بالطرق التى حددها القانون[٢]

وأن القواعد التى تحكم عملية الإثبات الجنائى تدور حول تحقيق هدف أساسى ، هو الوصول إلى العدالة الجنائية التى يتطلع إليها المجتمع

---

(١) - د / محمود محمود مصطفى – الإثبات فى المواد الجنائية – المرجع السابق – ص 2.

(٢) - د / محمود نجيب حسنى – الاختصاص والإثبات فى قانون الإجراءات الجنائية – دار النهضة العربية – 1992 – ص 53.

الإنسانى ، إذ الجريمة فى النهاية تعد اعتداء على هذا المجتمع لأنها تشكل خروجاً على نظامه الاجتماعى[١].

والإثبات فى المواد الجنائية يكون أكثر أهمية ، حيث أن الجريمة تمثل اعتداء على المجتمع بأسره ، ووسائل الإثبات هى التى تساعد على توقيع العقوبة على الجانى من أجل تحقيق الأمن والعدالة الاجتماعية ، إذ أن العقوبة تكون بمثابة ردع خاص للجانى وردع عام لكل من تسول له نفسه أن يحذو حذو الجانى فى مخالفة القانون[٢].

وأيضاً فإن الإثبات الجنائى يكون اكثر أهمية نظراً لأن العقل الإجرامى محل الدعوى الجنائية لا يحدث أمام قاضى الموضوع ، وليس فى إمكانه أن يصل إلى الحقيقة إلا إذا استعان بوسائل الإثبات المختلفة التى تعيد أمامه رواية وتفاصيل الأحداث [٣] ، فالقاضى يستمد اقتناعه بإدانة المتهم أو ببراءته من خلال عناصر الإثبات المختلفة التى تتضمنها الدعوى الجنائية ، ويهدف الإثبات الجنائى إلى إمكانية الوصول إلى الحقيقة الواقعية التى هى غاية الدعوى الجنائية ، ومن أجل ذلك يجب أن توضع عملية الإثبات الجنائى هذه فى إطار قانونى دقيق وفعال يحتوى على مجموعة من الإجراءات التى تساعد فى كشف هذه الحقيقة واتجاهاتها ، ومما لا شك فيه أن الحقيقة الواقعية لا تنكشف من تلقاء نفسها دائماً هى دائماً ثمرة جهد شاق وبحث دقيق ، وبالتالى فإن الركيزة الأولى لعملية الإثبات الجنائى هو مدى توافر الدليل القاطع الذى بمقتضاه يستطيع القاضى أن يبرر الإدانة أو البراءة التى يحكم بها .

ونخلص من ذلك أن الإثبات الجنائى ما هو إلا إقامة الدليل أمام القضاء بالطرق التى حددها القانون على وجود واقعة قانونية متنازع عليها ويؤكدها أحد أطراف الخصومة وينكرها الطرف الآخر . وبالتالى فالإثبات هو التنقيب عن الدليل وتقديمه وتقديره .

ثانيا: الطبيعة الخاصة للجريمة الإلكترونية وأثر ذلك على إثباتها جنائياً .

---

(١) - د / مامون محمد سلامة – الإجراءات الجنائية فى التشريع المصرى - طبعة 1986 – ص 160.

(٢) - أنظر د / محمود محمود مصطفى – الإثبات فى المواد الجنائية – المرجع السابق – ص 4.

(٣) - د / محمود نجيب حسنى – شرح قانون الإجراءات الجنائية – الطبعة الثالثة - دار النهضة العربية – 1998 – ص 770 ، 771.

من الحقائق المسلم بها أن التقدم العلمى له تأثيره البالغ على القانون، وعلى الواقع الذى يطبق عليه هذا القانون ، ولكن لكى تتحقق الفائدة المرجوة من هذا التقدم فإن القانون يجب ألا ينفصل عن الواقع الذى يفرزه ويطبق عليه ، بل يجب أن يكون متجاوباً معه ومنظوراً بتطوره.

والجدير بالذكر أن التطور الحالى الذى لحق ثورات الاتصال والمعلومات وما أفرزته هذه الثورة من وسائل الكترونية متقدمة ومتعددة ، كان له اثره على الجرائم التى تمخضت عن ذلك ، بحيث يميز فى هذه الجرائم بطبيعة خاصة (١)، من حيث الوسائل التى ترتكب بها وهى الحاسوب أو إحدى وسائل التقنية الحديثة فهذه الجرائم تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً(٢) ، وكذلك من حيث المحل الذى تقع عليه ، وأيضاً من حيث الجناة الذين يرتكبونها فهم يتمتعون بقدرات فنية وتقنية عالية تمكنهم من تنفيذها بدقة بالغة ، كما أن المجرم المعلوماتى شخص محترف فى التعامل مع شبكات الحاسبات والمعلومات كما أنها جرائم لا يلجأ مرتكبها إلى العنف ، ويتمتع بذكاء حيث يمكنه التغلب على كثير من العقبات التى تواجهه أثناء ارتكابه للجريمة ، علاوة على أنه شخص اجتماعى له القدرة على التكيف مع الآخرين (٣) فالأساس فى خطر هذه الجرائم يكمن فى أنها طبيعتها تجمع بين الذكاء الاصطناعى والذكاء البشرى ، مما يجعل إثباتها جنائياً فى منتهى الصعوبة

فالتطور الحالى الذى انعكس أثره على قانون العقوبات قد انعكس أثره أيضاً على قانون الإجراءات الجنائية ، بحيث أن هذا الأخير قد لا يطبق بسبب عجز قانون العقوبات عن استيعاب الجرائم المستحدثة التى ترتكب بالوسائل الإلكترونية (٤) كما وأن الإثبات الجنائى وهو أحد الموضوعات الهامة لهذا القانون قد تأثر بدوره بالتطور الهائل الذى لحق بالأدلة الجنائية بسبب تطور طرق ارتكاب الجريمة الإلكترونية ، الأمر

---

(١)- GELBSTEIN Eduardo , Gouvernance de l,internet enjeux – acteurs et fractures, publie por diplofoundation et global knawledge partnership suisse 2005 , p 98.

(٢)- د / مصطفى حمد موسى – أساليب إجرامية بالتقنية الرقمية (ماهيتها ، مكافحتها) – دار الكتب القانونية – مصر 2005 – ص 56.

(٣)- أنظر د / طارق ابراهيم الدسوقى – الأمن المعلوماتى (النظام القانونى لحماية المعلومات) دار الجامعة الجديدة للنشر – 2009 – ص 176 – 177.

(٤)- MASCALA corinne " eriminalite et contrat electronique " le contrat electronique , travaux de l'association CAPLTANT Henri, Journos mational, paris 2000 p. 118.

الذى يتعين معه تغير النظرة إلى طرق الإثبات الجنائى ، لكى تقترب الحقيقة العلمية فى واقعها الحالى من الحقيقة القضائية[١].

فإثبات الجرائم التى تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية سيتأثر بطبيعة هذه الجرائم ، وبالوسائل العلمية التى قد ترتكب بها ، مما يؤدى إلى عدم اكتشاف العديد من الجرائم فى زمن ارتكابها ، أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم ، أو تعذر إقامة الدليل اللازم لإثباتها مما يترتب عليه إلحاق الضرر بالأفراد والمجتمع .

المطلب الثانى

الصعوبات التى تواجه اكتشاف وإثبات الجريمة الإلكترونية

تتميز الجرائم الإلكترونية بصعوبات بالغة فى اكتشافها وبالعجز فى حالات كثيرة عن إمكان إثباتها فى حالة اكتشافها – فالجرائم الإلكترونية تتسم بكون محلها معلومات أو برامج معالجة آلياً عبر الحواسيب ، أو جرائم تتعلق بالأشخاص عبر عالم افتراضى غير متناهى وغير محدود ، مما يعطى طابع خاص ليس فقط فى طريقة ارتكابها ، بل كذلك فى الوسيلة التى ترتكب بها . الأمر الذى ينجم عنه صعوبات فى اكتشاف الجريمة الإلكترونية ، وتلك الصعوبات تقودنا حتماً إلى صعوبة اثباتها جنائياً .

وسوف نقسم هذا المطلب إلى فرعين نتناول فى الفرع الأول صعوبات اكتشاف الجريمة الإلكترونية ، والفرع الثانى نتناول فيه صعوبات إثبات الجريمة الإلكترونية .

(١ - د / على محمود على حموده – الأدلة المتحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائي – مقدم ضمن أعمال المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية – أكاديمية شرطة دبى – فى الفترة من 26 – 2003/4/28

الفرع الأول

صعوبات اكتشاف الجريمة الإلكترونية

يعترض اكتشاف الجرائم الإلكترونية والمعلوماتية العديد من الصعوبات وذلك راجع لعدة اعتبارات نذكرها على النحو التالى :-

أولاً : فقدان الآثار التقليدية للجريمة :

تظل الجرائم الإلكترونية أو المعلوماتية مجهولة ما لم يبلغ عنها للجهات المعنية بالاستدلالات أو التحقيق الجنائى ، وهنا تجدر الإشارة أن أهم الجرائم لا تصل إلى علم السلطات المعنية بطريقة اعتيادية كباقى جرائم قانون العقوبات ، فالجرائم الإلكترونية جرائم غير تقليدية لا تخلف آثار مادية كتلك التى تخلفها الجريمة العادية مثل الكسر فى جريمة السرقة وهى جريمة تقليدية[١] بالإضافة إلى أن العديد من الجرائم الإلكترونية تتم دون أن يشعر بها القائمون على تشغيل الأجهزة المعلوماتية ، كجرائم التجسس التى تتم عن طريق اعتراض النبضات الإلكترونية ، وجرائم الاختلاس التى تتم غير تعديل البرامج والتلاعب بالأنظمة المعلوماتية ، ويرجع السبب في افتقاد الآثار التقليدية للجريمة الإلكترونية إلى أن هناك بعض العمليات التى يجرى إدخال بياناتها مباشرة فى جهاز الحاسب الآلى دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها كما لو كان البرنامج معداً ومخزناً على جهاز الحاسب[٢].

بالإضافة إلى أن الوسيلة التى ترتكب بها الجرائم الإلكترونية أو المعلوماتية تجعلها ضمن قالب غير تقليدى ، نظراً لأن ارتكابها يتم عادة عن طريق نقل المعلومات على شكل نبضات الكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلى ، وشبكة الاتصال العالمية (الإنترنت) بصورة آلية ، كما تنساب الكهرباء عبر الأسلاك[٣].

---

(١)- أنظر د / عبدالفتاح بيومى حجازى – الدليل الجنائى والتزوير فى جرائم الكمبيوتر – دراسة متعمقة فى جرائم الحاسب الآلى والإنترنت – بهجات للطباعة والتجليد – مصر 1995 – ص41.

(٢)- أنظر د / / عبدالفتاح بيومى حجازى – مبادئ الإجراءات الجنائية – جرائم الكمبيوتر والإنترنت – الطبعة الأولى – دار الوارقين للنشر والتوزيع – بيروت – 2004 – ص 83.

(٣)- د / محمد حماد مرهج البهينى – جرائم الحاسوب – موضوعها – ماهيتها – اهم صورها والصعوبات الى تواجهها – دراسة تحليلية – الطبعة الأولى – دار المناهج للنشر والتوزيع – عمان – 2006 – ص 539.

ثانياً : تعمد الجناة لإخفاء جرائمهم :

يلجأ المجرم الإلكترونى أو المعلوماتى إلى إخفاء جريمته وإزالة آثارها عن طريق التلاعب بقواعد البيانات والقوائم فى جهاز الكمبيوتر والبرامج ، ودون ترك أى أثر ، وخاصة أن التخزين الإلكترونى غير مرئى والبيانات مكتوبة بلغة رقمية لا يفهمها إلا الآلة ما لم تستفاد على شاشة الكمبيوتر ليتمكن من قراءتها وفهمها ، وهذا يشكل عقبة أمام إقامة الدليل على الجريمة الإلكترونية وإثباتها من قبل سلطات الضبط والتحقيق القضائى(١)

فالمجرمون الذين يرتكبون جرائمهم بالوسائل الإلكترونية الحديثة من فئة المجرمين الأذكياء الذين يضعون سياجاً أمنياً على أفعالهم غير المشروعة قبل ارتكابها لكى لا يقعوا تحت طائلة العقاب فهم يزيدون من صعوبة إجراءات التفتيش التى يتوقع حدوثها للبحث عن الأدلة التى قد تدينهم باستخدام كلمات السر التى لا تمكن غيرهم من الوصول إلى البيانات المخزنة إلكترونياً أو المنقولة عير شبكات الاتصال ، وقد يلجأ هؤلاء المجرمون أيضاً إلى دس تعليمات خفية بين هذه البيانات أو استخدام الرمز أو التشفير بالنسبة بها بحيث يستحيل على غيرهم الاطلاع عليها ويتعذر على جهات التحرى والضبط الوصول إلى كشف أفعالهم غير المشروعة(٢) . بالإضافة إلى ذلك فقد يلجأ المجرم الإلكترونى أو المعلوماتى إلى إخفاء هويته أو انتحال شخصية أخرى حتى لا يمكن

---

(١)- أنظر د / هدى حامد قشقوش – تزوير المستندات المعالجة الآلية – بحث مقدم حول الكمبيوتر والقانون – كلية الحقوق – جامعة عين شمس – 1994 – ص 151.

- د / سليمان أحمد فضل – المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت) – دار النهضة العربية – 2007 – ص 382.

- هلال بن محمد بن حارب البورسعيدى – الحماية القانونية والفنية لقواعد المعلومات المحوسبة – دراسة قانونية وفنية مقارنة – دار النهضة العربية – 2009 – ص 239 – 264.

(٢)- انظر د / على محمود على حموده – الأدلة المتحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائى – المرجع السابق – ص 20.

التعرف عليه فى حالة اكتشاف الجريمة وذلك من خلال استخدام الكثير من البرامج والآليات التى تمكنه من إخفاء شخصيته[١]

ثالثاً : عدم الإبلاغ عن الجريمة الإلكترونية للجهات المختصة .

يبدو من أكبر الصعوبات التى تواجه اكتشاف الجريمة الإلكترونية هو امتناع الجهات المجنى عليها عن التبليغ عن الجرائم المرتكبة للجهات المسئولة[٢] . حيث تحرص الجهات المجنى عليها عدم الإبلاغ أو الإعلان عن الجرائم المعلوماتية حفاظاً على سمعة الجهة التى بها الحاسب الآلى ، وتخشى تلك الجهات من أن يؤدى الإعلان عن تلك الجرائم إحاطة المجرمين علماً بنقاط الضعف فى أنظمتها ، وحفاظاً على ثقة العملا ولمنع إشاعة الذعر بينهم [٣] . بالإضافة إلى أنه تحرص أكثر الجهات وخاصة البنوك أو المؤسسات الادخارية على عدم الكشف عما تعرضت له ، وعدم بيان عجزها عن تحقيق الأمان الكافى للمعلومات ، وبالتالى لأصول الأموال التى تتعامل معها فتكتفى الجهة عادة باتخاذ إجراءات إدارية داخلية[٤] دون الإبلاغ عما تعرضت له للسلطات المختصة ، تجنباً للإضرار بسمعتها ومكانتها وهز الثقة فى كفاءتها ، وهى لا تقف عند حد الامتناع عن الإبلاغ عن الجرائم إنما يمتد الأمر إلى أنها تمتنع عن تقديم الأدلة أو تقديم أى مساعدة لجهات التحقيق (إذا علمت السلطات بالجريمة) الأمر الذى يشكل صعوبة أمام الجهات ليس فى اكتشافها فحسب بل وفى إثباتها أيضاً ، وتفضل تلك الجهات تقديم الترضية المالية لعملائهم حتى لا يفقدوهم ، ولا تتأثر سمعتهم المالية بدلاً من البحث عن الجناة[٥].

---

(١)- أنظر د / حسن طاهر داوود – جرائم نظم المعلومات – الطبعة الأولى – أكاديمية نايف للعلوم الأمنية – الرياض – 2000 – ص 87 .

(٢)- أنظر د / محمد حماد مرهج البهينى – جرائم الحاسوب – المرجع السابق – ص 217.

(٣)- د /هشام محمد فريد رستم – الجوانب الإجرائية المعلوماتية مكتب الآلات الحديثة – 1994 – ص 25 ..

(٤)- د / حسن ابراهيم – الحماية الجنائية لحق المؤلف عبر الإنترنت – رسالة دكتوراه – دار النهضة العربية – 2006 – ص 148.

(٥)- د / فهد عبدالله العبيد – الإجراءات الجنائية المعلوماتية – المرجع السابق - ص 147.

رابعاً : نقص خبرة سلطات الاستدلال والضبط بالجرائم المعلوماتية والإلكترونية .

ما يزيد من صعوبة اكتشاف الجرائم المعلوماتية هو نقص الخبرة لدى أجهزة الضبط القضائى وجهات الادعاء والقضاء فى مجال الجرائم الإلكترونية لتمحيص عناصر الجريمة وجمع المعلومات والأدلة عنها ، وتجد تلك الجهات المكلفة بالتحقيق والقبض نفسها غير قادرة على التعامل بالوسائل الاستدلالية ، والإجراءات التقليدية مع هذه النوعية من الجرائم ، فمحترفى انتهاك الحاسبات الإلكترونية ومرتكبى هذه الجرائم يقومون بتخزين البيانات المتعلقة بأنشطتهم الإجرامية فى أنظمة تقنية المعلومات وعلى نحو متطور باستخدام إشارات أو رموز سرية لإخفائها عن أعين أجهزة العدالة ، مما يثير مشكلات كبيرة فى جمع الأدلة الجنائية ، وتصطدم الأجهزة المكلفة بالتحقيق بهذا التكنيك لتخزين المعلومات وهى تسعى للحصول على أدلة الإثبات[١] بالإضافة إلى أن أغلب رجال الشرطة المختصين فى التحقيق فى الجرائم الإلكترونية ، من غير ذوى الخبرة والمعرفة التقنية حيث تنحصر خبراتهم ومعلوماتهم فى جرائم قانون العقوبات[٢].

كما أن التكوين العلمى والتدريبى والخبرات المكتسبة لرجال الضبط القضائى وسلطات التحقيق الابتدائى والحكم من حيث حداثة الجرائم المعلوماتية وتقنياتها العالية تتطلب من القائمين على البحث الجنائى والتحقيق إلمام كاف بها ، فلا يكفى أن يكون لهم الخلفية القانونية أو أركان العمل الشرطى فقط ، ولكن لا بد من الإلمام بخبرة فنية فى

---

(١)- أنظر د / محمد أبو العلا عقيدة – المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية مركز البحوث والدراسات تاريخ الانعقاد 26 نيسان – 2003 – الانتهاء 28 نيسان 2003 – دبى .

- أنظر - مقال فى مركز بحوث الشرطة عن " نحو استراتيجية دولية لمكافحة الجرائم المعلوماتية " – العدد التاسع 1996 – القاهرة – ص 20 وما بعدها .

(٢)- أنظر د / عبدالفتاح بيومى حجازى – الدليل الجنائى والتزوير فى جرائم الكمبيوتر والإنترنت – دراسة متعمقة فى جرائم الحاسب الآلى والإنترنت – المرجع السابق – ص 122.

مجال الجرائم الإلكترونية والمعلوماتية [١]. ولذلك يستلزم الأمر أن يكون الجهاز المختص بالبحث والتحرى عن الجرائم المعلوماتية يتمتع بمهارات خاصة تتماشى مع التقنية التى يتعامل معها ، وأن يتم تدريبه على استخدام أساليب وتقنيات تحقيق جديدة ومبتكرة وتتماشى مع الجرائم المستحدثة التى تعتمد على التقنية العالية[٢]. بالإ ضافة إلى استقطاب وجذب الكفاءات المهنية المتخصصة فى الحاسب الآلكترونى للاستعانة بهم فى التحقيق فى هذه الجرائم لضبطها واكتشافها وتقديم الأدلة الرقمية ، ولتولى شرح هذه الأدلة أمام المحكمة ، وحتى لا تعطى الفرصة للمتهم للتشكيك فى صحة الدليل الذى يوجد ضده[٣] .

واثبتت الوقائع أن هناك بعض الجرائم المعلوماتية والإلكترونية ارتكبت على مرأى ومسمع من رجال الأمن ، بل وقام بعض رجال الأمن بتقديم يد المساعدة لمرتكبى تلك الجرائم دون قصد وعن جهل [٤] . ويزيد من التحدى الذى يواجه أجهزة العدالة الجنائية فى الجريمة المعلوماتية أن مرتكبى هذه الجرائم لهم المفردات والمصطلحات الخاصة بهم ، لدرجة أنهم يطلقون علىأنفسهم اسم " النخبة " بدعوى أنهم الأكثر معرفة بأسرار

---

(١)- د / عبد الفتاح بيومى حجازى – مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت – دار الفكر الجامعى – الطبعة الأولى – الاسكندرية – 2006 – ص 122 .

(٢)- أنظر د / فتوح عبدالله الشاذلى " المواجهة التشريعية للجرائم المستحدثة " – بحث مقدم إلى مؤتمر الأمن والسلامة – وزارة الداخلية – أبو ظبى من 6- 8 أكتوبر 2003 – ص 35 .

(٣)- د / هشام محمد فريد – الجوانب الإجرائية للجرائم المعلوماتية – المرجع السابق – ص 17.

- د / جميل عبدالباقى الصغير – الجوانب الإجرائية للجرائم المتعلقة بالإنترنت – دار النهضة العربية – 2002 – ص 4 .

(٤)- مثال ذلك : طلبت إحدى دوائر الشرطة بالولايات المتحدة الأمريكية من شركة تعرضت للقرصنة أن تتوقف عن تشغيل جهازها الآلى للتمكن من وضعه تحت المراقبة بهدف كشف مرتكب الجريمة ، وقد حدث نتيجة لذلك أن تسببت دائرة البوليس بدون قصد فى إتلاف ما كان قد سلم من الملفات والبرامج المحتوية على أدلة الإدانة الخاصة بإثبات الجريمة .

- أنظر – مجلة المعارف العربية : قرصنة الكمبيوتر المصرفى – العدد 84 – يناير 2000.

الحاسب الآلى ولغاته المتميزة ، ويطلق على رجال الشرطة والنيابة والقضاة صفة الضعفاء أو القاصرين [١].

لذلك بدأت بعض الدول محاولات جادة فى استيعاب رجال الأمن والقضاء ضمن المتخصصين فى المعلوماتية أو علوم وتطبيقات الحاسب الآلى . فضلاً عن قبول خبراء فى هذا المجال ضمن رجال الضبط والقضاء[٢] ولكن هذه المحاولات لن تأتى ثمارها فى القريب العاجل وذلك للأسباب الآتية : -

١ - الميزانيات المالية لدى اجهزة الأمن والقضاء تكون ضعيفة بالنظر إلى خبرة المتخصصين فى علوم الحاسب الآلى فضلاً عن أنها لا تصل إلى ذات المبالغ التى تسددها مؤسسات وشركات القطاع الخاص[٣].

٢ - كما أن الخبرة العملية لدى سلطات الضبط والتحقيق الجنائى تتأتى من ممارسة أعمال الضبط والتحقيق والاعتياد عليها وذلك يقتضى وقوع هذه الجرائم موضوع الضبط والتحقيق ، ولذلك فالجريمة الإلكترونية والمعلوماتية لم تقع حتى الآن بالعدد والشكل الذى يوازى الجريمة التقليدية كالسرقة أو الضرب أو القتل ، ولذلك فالخبرة الإجرائية فى الضبط والتحقيق لدى أجهزة العدالة بشأن الجريمة المعلوماتية لا زالت حديثة ، إلا أنه مع انتشار الحاسب الآلى وتفشيه فى الحياة الخاصة والعامة ، ولدى الحكومة والقطاع الخاص ، وما يستتبعه من أفعال مخالفة

---

(١)- حسين بن سعيد بن سيف الغافرى – الجهود الدولية فى مواجهة جرائم الإنترنت ص 1 – 61 مقال متوافر على الموقع التالى : http://www.minshawi.com.

(٢)- وقد أوصى المجلس الأوربى رقم (95) فى 11 سبتمبر 1995 فى شأن المشاكل الإجرائية للإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات ضرورة تشكيل وحدات خاصة لمكافحة جرائم الحاسب الآلى وإعداد برامج خاصة لتأهيل العاملين فى مجال العدالة الجنائية لحق المؤلف عبر الإنترنت – المرجع السابق – ص 147.

(٣)- د / محمد الأمين البشرى – التحقيق وجمع الأدلة في مجال الجرائم الإلكترونية – مؤتمر القانون والكمبيوتر والإنترنت – جامعة الإمارات العربية – كلية الشريعة والقانون من 1 – 3 مايو 2000 – المجلد الثالث – ص 1033 – 1082.

– وليست مجرمة – نظراً لعدم وضوح الرؤية فى نصوص التجريم فإن ذلك يثرى عمل الضبط والتحقيق مستقبلاً (١).

٣ - كذلك أدى انتشار الحاسب الآلى على نطاق واسع وتعدد أنظمته وبرامجه وتطورها بشكل سريع ومتلاحق ، يجعل ملاحقتها من حيث إعداد وتدريب رجال الضبط والتحقيق الجنائى عليها أمر يتسم بالصعوبة ، ومع ذلك يجب ألا يكون ذلك سبباً فى عدم التدريب للأجهزة المعنية ، لأن هذه الأجهزة عند تدريبها ستكون قابلة لتحديث وتطوير فيها أول بأول كلما جد جديد .

الفرع الثانى

صعوبات الإثبات الجنائى للجريمة الإلكترونية

تتعلق عملية إثبات الجرائم بصفة عامة بإقامة الدليل ، وذلك بالنظر إلى نوع الجريمة وإلى الإجراءات المتبعة للحصول على الدليل ، والإثبات فى مجال الجرائم المعلوماتية والإلكترونية ينطبق عليه المفهوم العام للإثبات ، إلا أن عملية الحصول على الدليل فى الجرائم الإلكترونية صعبة للغاية ، وذلك نظراً لكون الأدلة فى هذا النوع من الجرائم يتميز بخصوصيته المعنوية بالإضافة إلى ذلك فالإجراءات المتبعة فى إثبات هذه الأدلة أثبتت قصورها ، فإذا كانت ذات فائدة فى الجرائم التقليدية ، فهى غير مجدية فى الجرائم المعلوماتية فى غالب الأحوال خاصة فى ظل الطابع العلمى لهذه الجرائم . وسوف نعرض أهم الصعوبات التى تواجه عملية الإثبات الجنائى للجريمة الإلكترونية وذلك على النحو التالى :-

أولاً : غياب الدليل المرئى :

من الملاحظ أن دليل الإثبات فى الجرائم التقليدية يكون مرئياً كالسلاح النارى أو الأداة الحادة التى تستعمل فى القتل أو الضرب ، وكذلك المادة السامة التى تستعمل فى القتل ، أو المحرر ذاته الذى تم تزويره أو النقود التى زيفت وأدوات تزييفها ، فى كل هذه الأمثلة يستطيع

---

(١)- د / عبدالفتاح بيومى حجازى – الدليل الجنائى والتزوير فى جرائم الكمبيوتر والانترنت – دراسة متعمقة فى جرائم الحاسب الآلى والإنترنت – المرجع السابق – ص 85.

رجل الضبط أو التحقيق الجنائى رؤية الدليل المادى وملامسته بإحدى حواسه[١].

لكن الأمر يختلف فى الجرائم المعلوماتية التى تقع على العمليات الإلكترونية المختلفة ، خاصة التى تتم عبر شبكة الإنترنت ، كالتى تقع على عمليات التجارة الإلكترونية ، أو العمليات الإلكترونية للأعمال المصرفية أو على أعمال الحكومة الإلكترونية ، يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات ، فإذا وقعت جرائم معينة على هذه الجوانب المعنوية ، كجرائم السرقة أو الاختلاس أو الاستيلاء أو الغش أو التزوير أو الإتلاف فإنه قد يصعب إقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذى وقعت عليه الجريمة[٢].

ومما لا شك فيه أن إثبات الأمور المادية التى تترك أثاراً ملحوظة يكون سهلاً ميسوراً بعكس إثبات الأمور المعنوية فإنه يكون فى منتهى الصعوبة بالنظر إلى أنه لا يترك وراءه أى آثار قد تدل عليه أو تشكف عنه ، بحسبان أن أغلب المعلومات والبيانات التى تتداول عبر الحاسبات الآلية والتى من خلالها تتم العمليات الإلكترونية تكن فى هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا من خلال هذه الحاسبات الآلية ، فالجرائم التى ترتكب على العمليات الإلكترونية التى تعتمد فى موضوعها على التشفير والأكوزاد السرية والنبضات والأرقام والتخزين الإلكترونى يصعب أن يخلف وراءها آثاراً مادية قد تكشف عنها او يستدل من خلالها على الحياة .

تعد الطبيعة غير المرئية للأدلة المتحصلة عليها من الوسائل الإلكترونية تلقى بظلالها على الجهات التى تتعامل مع الجرائم التى تقع على شبكة الإنترنت حيث يعتبر كشف وتجميع من هذا النوع لإثبات وقوع الجريمة والتعرف على مرتكبها أحد أبرز المشكلات التى يمكن ان تواجه التحرى والملاحظة كضباط الشرطة . ومن المعلوم أن جهات التحرى

---

(١)- د / عبدالفتاح بيومى حجازى – الدليل الجنائى والتزوير فى جرائم الكمبيوتر – المرجع السابق – ص 36.

(٢)- د / محمد محى الدين عوض – مشكلات السياسة الجنائية المعاصرة فى جرائم نظم المعلومات (الكمبيوتر) – ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائى – القاهرة – 28/25 تشرين الأول 1993 .
- د / على محمود على – المرجع السابق – ص 16.

والتحقيق اعتادت على الاعتماد على الإثبات المادى للجريمة ، ولكن فى محيط الجرائم الإلكترونية فالأمر مختلف ، فالمتحرى أو المحقق لا يستطيع أى منهما تطبيق إجراءات الإثبات التقليدية على المحتويات المعنوية .

ثانياً : سهولة إخفاء الدليل :

تعد من الصعوبات التى يمكن أن تعترض العملية الإثباتية فى مجال الجرائم المعلوماتية أو الإلكترونية سهولة إخفاء الدليل أو محوه ، حيث يقوم المجرم المعلوماتى بمحو أو تدمير أدلة الإدانة بسهولة متناهية ، فضلاً عن تنصله من مسئولية هذا العمل ، بإرجاعه حسبما تشهد وقائع عديدة (١) ، على خطأ فى نظام الحاسب أو الشبكة أو فى الأجهزة (٢). كما أن هناك بعض الأفعال غير المشروعة التى يرتكبها جناة الوسائل الإلكترونية ، يكون أمرها حكراً عليهم كالتجسس على ملفات البيانات المختزنة والوقوف على ما بها من أسرار ، كما انهم قد ينسخون هذه الملفات ويحصلون على نسخ منها بقصد استعمالها تحقيقاً لمصالحهم الخاصة ، كذلك يقومون باختراق قواعد البيانات والتغيير فى محتوياتها تحقيقاً لمآرب خاصة ، وقد يخربون الأنظمة تخريباً منطقياً بحيث يمكن تمويهه ، كما لو كان مصدره خطأ فى البرامج او فى الأجهزة أو فى أنظمة التشغيل او التصميم الكلى للنظام المعالج آلياً للمعلومات ، وقد يدخلون كذلك بيانات غير معتمدة فى نظام الحاسب أو يعدلون برامجه أو

---

(١)- ومن الوقائع الشهيرة قيام مجرم معلوماتى فى ألمانيا حيث برمج نظامه الأمنى لحماية البيانات المخزنة على حاسوبه من محاولات الوصول إليها ، بطريقة تعمل على محو كل هذه البيانات بالكامل ، وذلك إذا ما تم اختراقه من قبل اى شخص غير مرخص له بذلك الولوج ، أنظر – أيمن رمضان محمد احمد – الحماية الجنائية للتوقيع الإلكترونى – رسالة دكتوراه – كلية الحقوق – جامعة عين شمس – 2010 – ص248 .

(٢)- ومن الأمثلة الواقعية حالة شهدتها دولة النمسا تتلخص وقائعها فى قيام مهربى الأسلحة بإدخال تعديلات على الأوامر العادية لنظام تشغيل حاسب صغير يستخدمه فى تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر على الحاسب من خلال لوحة المفاتيح بالنسخ أو الطبع محو وتدمير البيانات كلها : أنظر د / هشام محمد فريد – أصول التحقيق الجنائى الفنى واقتراح إنشاء آلية عربية موحدة للتدريب التخصصى " مؤتمر القانون والكمبيوتر والإنترنت المنعقد من 1 – 3 مارس 2000 – بجامعة الإمارات العربية – كلية الشريعة والقانون – المجلد الثانى – الطبعة الثالثة 2004 – ص 401 – 506 .

يحرقون البيانات المخزنة بداخله دون أن يتخلف من وراء ذلك ما يشير إلى حدوث هذا الإدخال أو التعديل [١] . ومما يؤيد من خطورة الأمر إمكانية وسهولة إخفاء الأدلة المتحصلة من الوسائل الإلكترونية أنه يمكن محو الدليل فى زمن قصير ، فالجانى يمكنه أن يمحو الأدلة التى تكون قائمة ضده أو يدمرها فى زمن قصير جداً ، بحيث لا تتمكن السلطات من كشف جرائمه إذا ما علمت بها ، وفى الحالة التى قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده .

ثالثاً : إعاقة الوصول إلى الدليل :

جناة الجرائم المعلوماتية من فئة المجرمين المحترفين الذين لا يرتكبون جرائمهم بسبب الاستفزاز أو استثارة ، وإنما هم يخططون لما يفعلون ويستخدمون قدراتهم الفنية والعقلية لنجاح هذا التخطيط ولذلك نجد أنهم وهم يرتكبون الجرائم الإلكترونية يحيطون انفسهم بتدابير أمنية تزيد من صعوبة تحديد هويتهم [٢] ويستخدم هؤلاء الجناة مختلف الوسائل الإلكترونية لإعاقة الوصول إليهم ، كاستخدام كلمات سر أو دس تعليمات خفية بينها أو ترميزها [٣] لإعاقة أو منع الاطلاع عليها أو ضبطها ويشكل استخدام تقنيات التشفير لهذا الغرض أكبر العقبات التى تعوق الرقابة على البيانات المخزمة أو المنقولة عبر حدود الدولة ، والتى تحد من قدرة

---

(١)- أنظر د / محمد حماد مرهج – جرائم الحاسوب – المرجع السابق – ص 212.

(٢) - ومثال ذلك نجد المجرمين يستخدمون التشفير وكلمات السر التى تمكنهم من إخفاء الأدلة التى قد تكون قائمة ضدهم ، وقد يدسون تعليمات خفية بين الأدلة لتصبح كالرمز فلا يمكن لغيرهم أن يفهم مقصودها ، وقد يقوم هؤلاء أيضاً بتشفير التعليمات باستخدام طرق وبرامج تشفير البيانات = = المتطورة مما يجعل الوصول إليها فى منتهى الصعوبة ، أنظر د / محمد على حموده – الأدلة المتحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائى – المرجع السابق – ص 18.

(٣)- ويتم البحث عن الدليل الرقمى فى وسط افتراضى يحتويه الجهاز الذى ارتكبت به أو ضده الجريمة الإلكترونية ، وغالباً ما يكون الجهاز مزوداً بنظام حماية ، بحيث لا يمكن تشغيله إلا باستعمال كلمة مرور ملعومة لدى المجرم ، وهو ما يحول دون الحصول على المعلومات من خلاله : أنظر د / طارق محمد الجملى – الدليل الرقمى فى مجالات الإثبات الجنائى " المؤتمر المغاربى الدولى حول المعلوماتية والقانون – أكاديمية الدراسات العليا – طرابلس 28 – 29 /2009/10.

جهات التحرى والتحقيق والملاحقة على قراءتها ، الأمر الذى يجعل صوت حرية البيانات الشخصية المخزنة فى مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والإلكترونية او بتدابير الأمن والدفاع امراً بالغ الصعوبة[١].

رابعاً : ضخامة البيانات المتعين فحصها :

تشكل مجموعة البيانات التى تجرى فى الأنظمة المعلوماتية تداولها أحد الصعوبات التى تعوق تحقيق الجرائم التى تقع عليها أو بواسطتها ، وآية ذلك أن طباعة كل ما يوجد على الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات التى قد لا تثبت كلها تقريباً شيئاً على الإطلاق [٢] . وفى مواجهة هذه الصعوبة يتطلب الأمر من المحقق فى الجريمة المعلوماتية تصفح مئات الآلاف من الصفحات الإلكترونية ، وغير ذلك من البيانات المخزنة على الحاسب الآلى او على ديسكات أو أسطوانات منفصلة والتى قد تكون محاطة بنظام أمنى لمنع الوصول إليها وبذلك لن يتمكن المحقق الجنائى من الوصول إليها لعدم معرفته لكلمة السر أو شفرات المرور والتى يمكن والمؤكد أنها لن تقدم شيئاً مفيداً للتحقيق .بذلك تمثل ضخامة البيانات والمعلومات عائقاً أمام سلطات التحقيق فى تلك الجرائم[٣].

لذلك وفى ظل تواضع المستوى الفنى لرجال الضبط والمحقق الجنائى فيما يتعلق بفنون الحاسب الآلى واستخداماته ، حيث يتطلب كشف الجرائم المعلوماتية والاهتداء إلى مرتكبيها وملاحقتهم قضائياً ندب خبراء فنيين فى مثل هذه الجرائم يتمتعون بمهارات خاصة تسمح لهم بفهم ومواجهة تقنيات الحاسب الإلكترونى المتطورة[٤].

وأساليب التلاعب المحاسبى المعقدة التى تستخدم عادة فى ارتكاب هذه الجرائم ، لذلك وجدت سلطات البحث الجنائى والتحقيق نفسها غير قادرة على التعامل بالوسائل التقليدية مع هذه النوعية من الجرائم ،

---

(١) - د / هشام محمد فريد – المرجع السابق – ص 427.
(٢) - د / هشام محمد فريد – المرجع السابق ص 430.
(٣) - د / أيمن محمد رمضان – الحماية المدنية للتوقيع الإلكترونى – المرجع السابق – ص 248 – 251 .
(٤) - د / على محمود على حمودة – المرجع السابق – ص 119 .

ولنقص الخبرة والتدريب كثيراً ما تحقق أجهزة الشرطة فى تقدير أهمية الجريمة المعلوماتية ، فلا تبذل لكشف غموضها وضبط مرتكبها جهوداً تتناسب مع هذه الأهمية ، لذلك كثيراً ما تفشل جهات التحقيق فى جمع أدلة جرائم نظم المعلومات مثل مخرجات الحاسب وقوائم التشغيل ، بل إن المحقق نتيجة نقص خبرته فى الحاسب الآلى يدمر الدليل بمحو الأسطوانة الصلبة عن طريق الخطأ أو الإهمال أو التعامل بخشونة مع الأقراص المرنة(١).

خامساً : الجريمة الإلكترونية جريمة متعدية الحدود :

الجريمة الإلكترونية تتميز بالطابع الدولى ، ذلك لأن الطابع العالمى لشبكة الإنترنت وما يرتبه من جعل معظم دول العالم فى حالة اتصال دائم على الخط (**on line**) يسهل ارتكاب الجريمة من دولة إلى دولة أخرى فقد ترتكب الجريمة فى دولة ولكن الضرر المترتب على النتيجة الإجرامية يقع فى دولة أخرى مما يزيد من صعوبة كشفها وملاحقتها(٢).

فالجريمة الملعوماتية تعتبر شكلاً جديداً من الجرائم العابرة للحدود الإقليمية بين دول العالم كافة ، إذ يمكن من خلال النظام المعلوماتى ارتكاب العديد من الجرائم مثل جرائم التعدى على قواعد البيانات ، وتزويد وإتلاف المستندات الإلكترونية ، والاحتيال المعلوماتى ، وسرقة بطاقات الائتمان ، والقرصنة وغسيل الأموال . ويثير الطابع الدولى للجرائم المعلوماتية مشكلات عديدة مثل تتبع الاتصالات الإلكترونية عن طريق سلطات التحقيق لأجل إقامة الدليل على الجرائم التى ترتكب فى مجال الإنترنت ، ولا شك أن اختلاف التشريعات فيما بينها فيما يتعلق بشروط قبول الأدلة وتنفيذ بعض الإجراءات مثل التفتيش والمعاينة عبر الحدود يثير مشكلات عديدة قد تعوق اتخاذ الإجراءات اللازمة لضبط هذا النوع من الجرائم العابرة للحدود(٣).

---

(١) - د / عبدالله حسين على محمود – سرقة المعلومات المخزنة فى الحاسب الآلى – دار النهضة العربية – 2002 – ص 351.

(٢) - د / عبدالفتاح بيومى حجازى – المرجع السابق – ص 130 رسالة .

(٣)- لذا أوصى مجلس الدولة الفرنسى فى تقريره المتعلق بالإنترنت والشبكات الرقمية ، بضرورة إلزام مقدمى الخدمات الوسيطة بالتعاون مع الجهات المختصة بالتحقيق عن طريق إمدادها بالبيانات الشخصية الخاصة بالعملاء المشتركين لديهم ، مما يسهل الوصول إلى الجناة .

وبما أن الجريمة الإلكترونية من الجرائم الدولية العابرة للحدود الوطنية الإقليمية والقارية فهى جريمة عالمية عابرة للحدود الجغرافية[١] ، لذلك هناك صعوبات تواجه الحصول على الأدلة الإلكترونية على المستوى الدولى نوضحها فيما يلى :

1- عدم وجود نموذج موحد للنشاط الإجرامى للجريمة الإلكترونية فيعد ذلك من الصعوبات الدولية فى مواجهة الجرائم الإلكترونية فيتامل الأنظمة القانونية القائمةفى الكثير من الدولة لمواجهة الجرائم المعلوماتية ، ومنها الجرائم المتعلقة بشبكة الإنترنت ، يتضح لنا من خلالها عدم وجود اتفاق مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تحريمها ، فما يكون مباحاً فى أحد الأنظمة قد يكون مجرماً وغير مباح فى نظام آخر ، ومن أسباب ذلك اختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر ، وبالتالى اختلاف السياسة التشريعية من مجتمع لآخر[٢].

2- صعوبة تحديد حجم الضرر الناتج عن الجريمة الإلكترونية على المستوى الدولى قياساً بالجرائم التقليدية ، ومحتكريها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم امراً صعباً ، كما أنها تنطوى على سلوكيات غير مألوفة عن المجتمع ، وسهولة إتلاف الأدلة من قبل الجانة ، إضافة إلى انها جريمة عابرة للحدود لا تعترف بعنصر المكان والزمان فهى تتميز بالتباعد الجغرافى واختلاف التوقيتات بين الجانى والمجنى عليه[٣]ولمكافحة الجريمة الملعوماتية دولياً وتفعيل الإبلاغ عن تلك الجرائم

- أنظر د / حسن ابراهيم – الحماية الجنائية لحق المؤلف عير الإنترنت – المرجع السابق – ص 133 .

(١)- د / هدى حامد قشقوش – جرائم الحاسب الآلى فى التشريع المقارن – دار النهضة العربية 0 القاهرة – 1992 – ص 73.

(٢)- د / عبد الفتاح بيومى حجازى – الدليل الجنائى والتزوير فى جرائم الكمبيوتر – المرجع السابق – ص 102 .

(٣)- الجريمة الإلكترونية تختلف فى طبيعتها وأسلوب ارتكابها عن الجريمة العادية ، فمسرح الجريمة هو العالم كله ، حيث يتم ارتكاب جريمة الحاسب عادة عن بعد فلا يتواجد الفاعل فى مكان الجريمة الذى يتطلب انتقال الجانى انتقالاً فيزيقياً ولكن تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجانى ومكان الجريمة حيث تتباعد المسافات بين الفاعل والنتيجة ، وهذه المسافات لا تقف عن حدود الدولة بل تمتد إلى النطاق الإقليمى لدى اخرى مما يضاعف صعوبة كشفها او ملاحقتها - أنظر فى ذلك : د / أيمن عبدالحفيظ – استراتيجية مكافحة جرائم

لتحديد حجم الضرر الناجم عنها طالب البعض في الولايات المتحدة الأمريكية أن تتضمن قوانين المعلوماتية نصوصاً تلزم الجهات المتضررة من تلك الجرائم حتمية الإبلاغ مع تقرير جزاء جنائى لمخالفة ذللك الالتزام [١] وهذا ما دفع المدعين العاملين البلجيكيين إلى التخلى عن ملاحقة القضايا التى يكون التحقيق فيها ذا طابع دولى [٢].

3- اختلاف وتنوع قوانين الإجراءات الجنائية للدول :

بسبب اختلاف وتنوع النظم القانونية والإجرائية ، نجد أن طرق التحرى والتحقيق والمحاكمة التى تثبت فائدتها فى دولة ما ، قد تكون عديمة الفائدة فى دولة اخرى ، أو قد لا يسمح بإجرائها ، كما هو بالنسبة للمراقبة الإلكترونية ، والتسليم المراقب ، والعمليات المستترة ، وغيرها من الإجراءات الشبيهة ، فإذا ما اعتبرت طريقة ما من طرق جمع الاستدلالات أو التحقيق أنها قانونية فى دولة ما ، قد تكون ذات الطريقة غير مشروعة فى دولة أخرى ، لذلك على المشرع الإجرائى الجنائى أن ينشئ قواعد قانونية محددة تكون تحت تصرف السلطة المهيمنة على التحقيق فى مجال الجرائم الإلكترونية[٣].

4- عدم ووجود قنوات اتصال :

أهم الأهداف المرجوة من التعاون الدولى فى مجال الجريمة والمجرمين الحصول على البيانات المتعلقة بالجريمة والمجرمين ، ولتحقيق هذا الهدف كان لزاماً أن يكون هناك نظام اتصال يسمح للجهات القائمة على التحقيق بالاتصال بجهات أجنبية لجمع الأدلة والمعلومات العملية التى غالباً ما تكون مفيدة فى التصدى لجرائم المعلوماتية[٤].

استخدام الحاسب الآلى – دراسة مقارنة – أكاديمية الشرطة – 2004 – ص 239.

(١)- د / فتوح الشاذلى – المواجهة التشريعية للجرائم المستحدثة – بحث مقدم إلى مؤتمر الأمن والسلامة – أبو ظبى من 6 : 8 أكتوبر 2003 –ص 36

(٢)- د / أيمن رمضان محمد – الحماية الجنائية للتوقيع الإلكترونى – المرجع السابق – ص 254.

(٣)- د / فهد عبدالله العبيد – الإجراءات الجنائية المعلوماتية – المرجع السابق – ص 161.

(٤)- د / ايمن عبدالحفيظ – حدود مشروعية دور اجهزة الشرطة فى مواجهة الجرائم المعلوماتية – مجلة مركز بحوث الشرطة – العدد 25 يناير 2004 – ص 215.

5- مشكلة الاختصاص فى الجرائم المعلوماتية :

الجرائم المعلوماتية من أكبر الجرائم التى تثير مسألة الاختصاص على المستوى المحلى أو الدولى ولا توجد أى مشكلة بالنسبة للاختصاص على المستوى الوطنى أو المحلى حيث يتم الرجوع إلى المعايير المحددة قانوناً لذلك ، ولكن المشكلة تثار بالنسبة للاختصاص على المستوى الدولى حيث اختلاف التشريعات والنظم القانونية والتى قد ينجم عنها تنازع فى الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالإنترنت التى تتميز بكونها عابرة للحدود فقد يحدث أن مرتكب الجريمة فى اقليم دولة ميعنة من قبل أجنبي فهنا تكون الجريمة خاضعة للاختصاص الجنائى للدولة الأولى استناداً لمبدأ الإقليمية ، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصى فى جنابه وقد تكون هذه الجريمة من الجرائم التى تهدد أمن وسلامة دولة أخرى فتدخل عندئذ فى اختصاصها استناداً إلى مبدأ العينية [١]. كما تفاد فكرة تنازع الاختصاص القضائى فى حالة تأسيس الاختصاص على مبدأ الإقليمية كما لو قام الجانى ببث الصور الخليعة ذات الطابع الإباحى من اقليم دولة معينة وتم الاطلاع عليها فى دولة أخرى ، ففى هذه الحالة يثبت الاختصاص وفقاً لمبدأ الإقليمية لكل دولة من الدول التى مستها الجريمة .

ويترتب على مشكلة الاختصاص بالجريمة الإلكترونية وكونها جريمة عابرة للحدود تشتيت الجهود وإعاقة التعاون الدولي فى مجال التصدى لهذه الجرائم وذلك لاختلاف الإجراءات الجنائية أو النزاع حول القانون الواجب التطبيق[٢].

---

(١)- د / سلميان أحمد فضل – المواجهة التشريعية والأمنية – المرجع السابق – ص 414.

(٢)- د / محمود احمد عبانية – جرائم الحاسوب وأبعادها الدولية – دار الثقافة والنشر والتوزيع - عمان – 2005 – ص 35.

المبحث الثانى

مضمون الإثبات الجنائى فى الجريمة الإلكترونية

يعد الإثبات الجنائى بالأدلة الرقمية والإلكترونية من أبرز تطورات العصر الحديث فى كافة النظم القانونية ، تلك التطورات التى جاءت لتلائم الثورة العلمية والتكنولوجية والتقنية فى عصرنا الحالى ، والتى تطور معها الفكر الإجرامى فظهر نوع جديد من الجرائم هو ما يعرف بالجرائم المعلوماتية أو الجرائم الإلكترونية ، ما ألقى على عاتق القائمين على مكافحة الجريمة فى الدولة عبئاً شديداً ، ومهاماً جساماً تفوق القدرات المتاحة لهم وفق أسس وقواعد إجراءات البحث الجنائى التقليدية ، نظراً لعدم كفاية وعدم ملائمة هذه النظم التقليدية فى إثبات الجرائم الإلكترونية ، سواء من الناحيتين القانونية والتقنية – وكان حتماً على المشرع أن يستحدث من التشريعات ما يلائم هذا النوع من الجرائم فضلاً عن إنشاء أجهزة فنية متخصصة يناط بها عملية الإثبات العلمى لهذه الجرائم .

وترتكز عملية الإثبات الجنائى للجرائم الإلكترونية على الدليل الجنائى الرقمى باعتباره الوسيلة الوحيدة والرئيسية لإثبات هذه الجرائم ، لذا سوف نتناول من خلال هذا المبحث مفهوم الدليل الرقمى وما يتميز به من خصائص وطرق الحصول على الدليل الرقمى وأشكاله .

المطلب الأول : مفهوم الدليل الإلكترونى وخصائصه .

المطلب الثانى : طرق الحصول على الدليل الإلكترونى.

المطلب الثالث : أشكال الدليل الإلكترونى.

المطلب الأول

مفهوم الدليل الإلكترونى وخصائصه

أولا: تعريف الدليل الإلكترونى :

يعرف البعض الدليل الرقمى أو الالكتروني بأنه " هو الدليل المأخوذ من أجهزة الكمبيوتر ويكون فى شكل مجالات أو نبضات مغناطيسية أو كهربائية ، ممكن تجميعها وتحليلها باستخدام برامج

تطبيقات وتكنولوجيا ، وهى مكون رقمى لتقديم معلومات فى أشكال متنوعة ، مثل النصوص المكتوبة أو الصور أو الصوت أو الأشكال أو الرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون(١).

إلا أن هذا التعريف يقتصر مفهوم الدليل الرقمى على ذلك الذى يتم استخراجه من الحاسب الآلى ، ولاشك أن ذلك فيه تضييق لدائرة الأدلة الرقمية فهى كما يمكن أن تستمد من الحاسب الآلى ، فمن الممكن أن يتحصل عليه من أية آلة رقمية أخرى ، فالهاتف وآلات التصوير وغيرها من الأجهزة التى تعتمد التقنية الرقمية فى تشغيلها يمكن أن تكون مصدراً للدليل الرقمى بالإضافة إلى أن هذا التعريف يخلط بين الدليل الرقمى ومسألة استخلاصه حيث عرف بأنه الدليل المأخوذ من الكمبيوتر ... ، وهذا يعنى أن الدليل الرقمى لا تثبت له هذه الصفة إلا إذا تم أخذه أو استخلاصه من مصدره ويعرف الدليل الرقمى كذلك – بأنه " بيانات يمكن إعدادها وتراسلها وتخزينها رقمياً بحيث تمكن الحاسوب من تأدية مهمة ما ، أو أنه الدليل الذى يجد له أساس فى العالم الافتراضى ويقود إلى الواقعة غير المشروعة ومرتكبها(٢).

وهذا التعريف فى الحقيقة يضع منطق تكوين الدليل الرقمى هو الأساس الذى تبنى عليه معادلة تعريفه ، وبحيث يعترف فقط بالبيانات التى تعد من طبيعة مغناطيسية وإلكترونية ، لذا يجب ملاحظة هنا أن عبارة الرقمى **Digital** لا تشير إلى وضعية مميزة لنوعية أو طبيعة الدليل فى هذا المجال وإنما هى تفسير يجمل على تطوير لمدلول النظام الثنائى الرقمى **Binary code** الذى يتكون منه الدليل وبالتالى أصبح للدليل الرقمى مفهوماًأكثر اتساعاً بحيث يشمل كافة أشكال الرقمية واستخداماتها مثل الهواتف المحمولة والفاكس الرقمى والفيديو الرقمى ... الخ .

ويمكننا أن نعرف الدليل الرقمى بأنه " مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التى يمكن تجميعها وتحليلها باستخدام

---

(١) - د / خالد ممدوح ابراهيم – الدليل الإلكترونى فى الجرائم المعلوماتية – بحث منشور على الإنترنت ص 3.
www.F-B-W.net

(٢) - أنظر د /عمر محمد بن يونس – الدليل الرقمى – دار النهضة العربية – سنة 2007 – ص 25 .

برامج وتطبيقات خاصة لتظهر فى شكل صور أو تسجيلات صوتية أو مرئية ، ترجع تسمية الدليل الرقمى إلى ان البيانات داخل الوسط الافتراضى كانت صوراً او تسجيلات او نصوص ، تأخذ شكل أرقام على هيئة الرقمين (10 و 10) ويتم تحويل هذه الأرقام عند عرضها لتكون فى شكل صورة أو مستند تسجيل[١]

(١)- أنظر د / على محمود على حمودة – الأدلة المتحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائى – المرجع السابق – ص 22.

ثانياً : خصائص الدليل الرقمى :

تقوم خصائص الدليل الرقمى على مدى ارتباطه بالبيئة التى يحيا فيها وهى البيئة الافتراضية ويمكن تعداد خصائص الدليل الرقمى فيما يلى:-

١ -الدليل الرقمى دليل علمى[١]

الدليل الرقمى هو الواقعة التى تبنى عن وقوع جريمة أو عمل غير مشروع ، وهى واقعة مبناها علمى من حيث أن مبنى العالم الرقمى أو الافتراضى هو مبنى علمى شيده العلماء والتقنيين وتفيد هذه الخاصية أنه لا يمكن الحصول على الدليل الرقمى أو الاطلاع علي فحواه سوى باستخدام الأساليب العلمية وتفيد هذه الخصيصة أيضاً حين قيام رجال الضبط القضائى والاستدلال أو سلطات التحقيق أو المحاكمة بالتعامل مع الدليل الرقمى سعياً وراء إثبات الحقيقة (الواقعة بأشخاصها) حيث يجب أن تبنى عملية البحث هنا على أسس علمية فالدليل العلمى يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة .

أيضاً تفيد هذه الخاصية مسألة حفظ الدليل الرقمى حيث يجب أن تبنى عملية حفظ الدليل الرقمى على أسس علمية ، وهذا يتطلب بالضرورة تحديث أسلوب تحرير المحاضر فى هذا الشأن فتحرير محضر يتناول دليلاً علمياً يختلف عن تحرير محضر يتناول اعتراف شخص بجريمة قتل أو سرقة عادية ، ويعنى ذلك فى الحقيقة ضرورة توافر مسلك علمى فى تحريره يتوافق مع ظاهرة الدليل العلمى من حيث الخبرة والتخصص فى هذا المجال .

٢ -الدليل الرقمى دليل تقنى :

التقنية هى بنت العلم ، ولا يمكن أن تتواجد تقنية بدون أسس علمية ، وإذا كنا قد انتهينا إلى التأكيد على أن الدليل الرقمى هو دليل علمى فإن ذلك يثبت بالضرورة أن التقنية هى الخصيصة الثابتة التى يتمتع بها الدليل الرقمى وبحيث يجب لكى يتم التعامل مع الدليل الرقمى أن يكون ذلك من

---

(١)- راجع د / على محمود على حمودة – الأدلة المتحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائى – مقدم ضمن أعمال المؤتمر العملى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية نظمته أكاديمية شرطة دبى فى الفترة من 26 – 28 /4/2003 – ص 22 .

قبل تقنيين متخصصين فى الدليل الرقمى والعالم الافتراضى ككل[١]. فالدليل الرقمى ليس مثل الدليل العادى ، فلا تنتج التقنية سكيناً يتم به اكتشاف القاتل أو اعترافاً مكتوباً أو مالاً فى جريمة الرشوة أو بصمة أصبع ... الخ وإنما ما تنتجه التقنية هو نبضات رقمية تشكل قيمتها فى إمكانية تعاملها مع القطع الصلبة التى تشكل الحاسوب على أية شاكلة يكون عليها .

وللكشف عن الدليل الرقمى لا بد من الاهتمام بأمرين :

الأمر الأول : تقنية البرامج التى تتعامل مع الدليل الرقمى من حيث اكتسابهأو التحفظ عليه وتحليله وتقديمه[٢].

الأمر الثانى : أن هذه البرامج ذاتها والتى تساهم تقنيتها فى الحصول على الدليل يجب أن تكون محل قبول لدى المحكمة وبما يفيد دلالة أنه يجب أن يشاد فى محضر الاستدلال أو التحقيق أو الخبرة الى التقنية البرمجية المستخدمة فى الحصول على الدليل الرقمى .

ويجب أن نلاحظ أن الدليل الرقمى ليس له وجود خارج بيئته التقنية أو الرقمية ، ولكى يكون هناك دليل رقمى أن يكون مستوحى أو مستنبطاً أو حتى مستجلباً من بيئته التى يعيش فيها وهى البيئة الرقمية أو التقنية ، وهى فى إطار جرائم الإنترنت ممثلة فى العالم الرقمى الذى يطلق عليه العالم الافتراضى ، وهو العالم الكامن فى الاقراص والحواسيب والخوادم والمضيفات والشبكات ويتم تداول الحركة فيها عبرها ولذلك يتعين تطوير العمل فى الحقل الجنائى من حيث تطوير أدوات البحث فى الدليل الرقمى ، فعلى سبيل المثال يمكن تحقيق الاستفادة فى إطار التفتيش كقاعدة تقنية من حيث تطوير البحث فى مجاله بحيث يتم تخصيص أفراد تابعين لجهات الاستدلال والتحقيق يتم تطوير قدراتهم باستمرار فى إطار الرقمية كل وفيما يحقق مصلحة الاستدلال والتحقيق .

٣ -الدليل الرقمى دليل متنوع ومتطور :

وتعنى هذه الخاصية للدليل الرقمى أنه على الرغم من أن الدليل الرقمى فى أساسه متحد التكوين بلغة الحوسبة والرقمية ، فإن مع ذلك قد يتخذ أشكال مختلفة . فمصطلح الدليل الرقمى يشمل كافة أشكال وأنواع

---

(١)- د / عمر محمد بن يونس – الدليل الرقمى – المرجع السابق – ص 43 .

(٢) Brian crrier – open source Digital forensics tools . the legal Argunent – oct2002 p.2.

البيانات الرقمية الممكن تداولها رقمياً ، وبحيث يكون بينها وبين الجريمة رابطة من نوع ما ، وتتصل بالضحية على النحو الذى يحقق هذه الرابطة بينها وبين الجانى(١).

ومن حيث التنوع فمن الممكن أن يظهر الدليل الرقمى على هيئة أشكال مختلفة مثل بيانات غير مقروءة من خلال ضبط مصدر الدليل كما هو الشأن حال المراقبة عبر الشبكات أو الخوادم . وقد يكون الدليل مفهوماً للبشر كما لو كان وثيقة معدة بنظام المعالجة الآلية للكلمات **Word processing** بأى نظام ، كما من الممكن أن تكون صورة ثابتة أو متحركة (أفلام رقمية) أو معد بنظام التسجيل السمعى المرئى أو أن تكون مخزنة فى نظام البريد الإلكترونى ، وقد يكون كذلك مرتبطاً بالتشفير .

والتأكيد على أن الدليل الرقمى دليل متطور يعنى أنه من الممكن أن يكون التطور فى تكنولوجيا المعلومات عائقاً أمام الحصول على دليل رقمى يفيد فى كشف الواقعة بأشخاصها (الحقيقة) لذلك يجب مواكبة التطور فى علم تكنولوجيا المعلومات (٢) ويمكن ملاحظة التطور فى إطار البحث فى تطورات التقنية المعلوماتية مثلما هو الحال فى تطور حجم القرص الصلب وتطور سرعات الإدخال والإخراج **out put – in put** والتى لاقت جدلاً كبيراً حول معادلتها .

٤ -الدليل الرقمى يصعب التخلص منه .

وهذه الخاصية يجب إدراكها لتكون عنصراً فى فهم عالم الحوسبة والرقمية (تكنولوجيا المعلومات) فالقاعدة فى هذا الإطار والتى تسرى على كافة ما يتعلق بهيكلة الحوسبة والرقيمة هى أنه كلما حدث اتصال تكنولوجيا المعلومات فى معنى ادخال بيانات إلى ذلك العالم فإنه من الصعب التخلص منها ولو كان ذلك باستخدام أعتى أدوات الإلغاء **Delete** والحذف **Erase** فقد قضى بأنه عندما يتم حذف **Delete** ملف

---

(١) - Eaghancasey ,digital evidence and forensic computer and the internet, computer crianeist, academic press. USA UK 2000 P.9.s

(٢) - أنظر د / عمر محمد بن يونس – الدليل الرقمى –المرجع السابق – ص 46.

حاسوبى فإن محتوى الملف يمكن استرداده[١] . ذلك أن المساحة التى كان يشغلها الملف تظل كما هى متاحة ، وما لم يتم شغلها من قبل ملف آخر فإن الملف الذى تم حذفه يمكن استرداده باستخدام أداة استردادية للملفات المحذوفة ، كذلك يمكن التعرف على تاريخ نشأة الملف وآخر تعديل عليه وآخر مرة تم فتحه منها . فموضوع التخلص من الدليل الرقم باستخدام خصائص التخلص من الملفات فى الحاسوب أو الإنترنت كخاصة **Delete** و **Remove** و **Erase**.... الخ لا تعد من العوائق التى تحيل دون استرجاع الملفات المذكورة، إذ تتوافر برمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التى تم إلغائها أوإزالتها من الحاسب الآلى .

(١)- أنظر د / عمر محمد بن يونس – المبادئ المتعلقة بالإنترنت فى القضاء الأمريكى – دار النهضة العربية – 2005 – ص 47.

المطلب الثانى

طرق الحصول على الدليل الإلكترونى

أنتجت حالة الصراع بين المجتمعات وبين الجريمة فى ثوبها الجديد – الناتجة عن استعمال الإنترنت نظرة جديدة نحو الإثبات الجنائى ، تمثلت فى سؤال يفرض نفسه على دراسات القانون الجنائى وهو مدى إمكانية تجاوب وسائل الإثبات الجنائى التى إن صح تجاوزاً تسميتها بالتقليدية ، مع التقنية الجديدة للإنترنت ؟

وهنا التساؤل يقودنا فى الحقيقة إلى التسليم بأن هناك ظاهرة جديدة ظهرت بجوار المفاهيم التقليدية للأدلة الجنائية ، وهى الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن الحاسوب والإنترنت ، بحيث يصح أن يطلق على الارتباط بين الظاهرة الرقمية الجديدة وبين الإثبات الجنائى تسمية جديدة للدليل هى الدليل الرقمى **Digital evidence** أو الدليل الإلكترونى ، وقد أخذت به المحاكم فى النظم القانونية المقارنة ، سواء من حيث جدواه أو من حيث قيمته القانونية ، فتم إحداث تسوية شبه منطقية بينه وبين الدليل التقليدى المتعارف عليه ، والمستمد من وسائل الحصول عليه المعروفة ، كالتلبس والتفتيش والشهادة والقرائن وأيضاً الاعتراف ، وأساس هذه التسوية المنطقية هنا هى نظرة إلى الواقع الجدى للتقنية الرقمية لكونها ذات مدلول مؤثر وحقيقى فى عالم الإنسان المعاصر والمستقبلى[١] . وسوف نعرض من خلال هذا المطلب مدى إمكانية الحصول على الدليل الإلكترونى أو الرقمى من خلال إجراءات التحقيق التقليدية ، والحصول عليه من خلال الإجراءات الحديثة :-

أولاً : الحصول على الدليل الإلكترونى من خلال إجراءات التحقيق التقليدية :

يقوم الإثبات الجنائى على مبدأ حرية الإثبات الذى يسمح للقاضى بأن يستند فى حكمه إلى الأدلة التى يتم الحصول عليها من خلال الاستدلال والتحقيق ، ويدخل فى هذه الأدلة المعطيات المخزنة فى

---

(١)- أنظر د / جميل عبدالباقى الصغير – الجوانب الإرجائية للجرائم المتعلقة بالإنترنت – دار النهضة العربية – 2002 – ص 5.

الحاسوب ، بما فى ذلك تلك الناتجة عن الاتصال بشبكة الإنترنت ، وأن هذه المعطيات ، التى تدخل فى مجال ما يسمى بالدليل الإلكترونى [١] وسيلة ضرورية لا يمكن تجاوزها لملاحقة الجرائم الإلكترونية المعاقب عليها – ومن الممكن إثبات الجريمة الإلكترونية ، اى الحصول على الأدلة الإلكترونية من خلال إجراءات تقليدية ليستطيع المحقق فى مجال الجرائم الإلكترونية – القيام بالتفتيش فى النظام الحاسوبى ، وضبط المعطيات التى يمكن الحصول عليها ، وأخيراً اعتراض الاتصالات ، فلا تخلو هذه الوسائل التقليدية من أهمية كبيرة فى إثبات الجريمة الإلكترونية ، وذلك على الرغم من الصعوبات والعقبات التى قد تعترض استخدامها فى هذا المجال .

١ -التفتيش والضبط فى الوسط الإلكترونى :

لا يقتصر التفتيش والضبط فى مجال الجرائم المعلوماتية على ذلك الذى يكون محله المكونات المادية للحاسوب ، فتفتيش هذه المكونات يمكن أن يفيد فى الكشف والوصول إلى الحقيقة المتعلقة بالجريمة الإلكترونية ولكنه لا يخرج عن نطاق الشكل التقليدى للتفتيش ، فمحل التفتيش فى مجال الجريمة الإلكترونية يشمل الحاسوب والشبكة بسائر مكوناتها ، كالخادم وموزد الخدمة والمضيف والملحقات التقنية الأخرى .

وفى إطار الجرائم المعلوماتية أو الإلكترونية المرتكبة عبر الإنترنت يقع التفتيش على مضوعين اثنين : القطع الصلبة **had ware** والبيانات **Data** التى يؤخذ مدلولها على القيمة الاستردادية فيها الممثلة فى المعلومات[٢].

---

(١) - ويقصد بالدليل الرقمي أو الإلكترونى – (المعلومات فى شكل نصوص مكتوبة أو رسومات أو أشكال لوجوه أو غيرها من الأشكال) المختزنة فى الحاسوب أو ملحفاته لاسطوانات أو اقراص ممغنطة أو مرنة أو غيرها من وسائل تقنية المعلومات ، أو المنقولة عبر شبكات الاتصال التى يمكن تجميعها وتحليلها بقصد إثبات وقوع الجريمة ونسبتها إلى مرتكبها – أنظر د / طارق الحملى – الدليل الرقمى فى مجال الإثبات الجنائى – ورقة عمل مقدمة للمؤتمر المغربى الأول حول المعلوماتية والقانون المنعقد فى الفترة من 28/ / 29 أكتوبر 2009 منظمة أكاديمية الدراسات العليا – طرابلس – ص 50.

(٢)- والتفتيش فى محيط الجرائم الإلكترونية لا يقتصر على المكونات المادية للحاسوب بل يشمل كذلك للكونات غير المادية والتى تتضمن النبضات والإشارات الإلكترونية الممغنطة أى (المعطيات) فهذه لا تعد من الشياء المادية

والجريمة الإلكترونية تقع فى البيئة الرقمية ، وهى البيئة التى يحيا فيها الدليل الرقمى وهى الحيز الافتراضى (النظام التراسلى ، ونظام التخزين) وهى بيئة المكان الافتراضى **cyberplace** والزمان الافتراضى **cybertime** هذه البيئة ممثلة فى الاقراص بأنواعها بالإضافة إلى معالجات حركة البرامج والذاكرة وكل قطعة يمكن أن تقوم بدور فى هذا الشأن بما فى ذلك القطع المرنة التى لا يعمل الحاسوب بدونها ، مثل نظام التشغيل والبرمجة التى تعمل على تنفيذ أوامر تشغيل الملفات التى وضعها الإنسان [١]، فالبيئة الرقمية والتى تمثل المكان الافتراضى للدليل الرقمى للجرائم الإلكترونية ينعكس ذلك على طبيعة الدليل فى تلك الجرائم ، فيتكون هذا الدليل من نبضات إلكترونية تنساب عبر النظام المعلوماتى الأمر الذى يعنى إمكانية نقل الدليل الإلكترونى عبر شبكات الحاسوب لكى يستقر فى مكان بعيد عن الموقع المادى الذى يجرى فيه التفتيش خصوصاً أن استخدام شبكة الإنترنت يسهل بشكل كبير على الجناة إخفاء الأدلة فى مواقع توجد فى اماكن بعيدة . ومن هذه الناحية يختلف الدليل الإلكترونى عن أدلة الجريمة التقليدية التى تكون فى الغالب فى مكان غير بعيد عن مكان ارتكاب الجريمة .

وإذا كان فى الإمكان من الناحية التقنية الوصول إلى الموقع الذى يوجد فيه الدليل والذى قد يقع فى مكان خارج الاختصاص الإقليمى للقيام بالتفتيش ، سواء داخل الدولة أو فى دولة أخرى ، فهل يكون من الناحية القانونية امتداد التفتيش الذى محله المعطيات الإلكترونية الموجودة فى حاسوب معين ليطال المعطيات الموجودة فى شبكة الحاسوب المرتبطة بالحاسوب المأذون بتفتيشه أصلاً ؟

، وهذا الأمر دفع المشرع الفرنسى إلى تعديل نص المادة 94 من قانون الإجراءات الجنائية بإضافة عبارة " المعطيات المعلوماتية " لهذا النص بحيث يصبح التفتيش ممكنا للربحث عن " أشياء أو معطيات معلوماتية" .

كما أن القانون الإماراتى فى المادة (61) من قانون الإجراءات الجنائية سمحت لمأمورى الضبط القضائى " ضبط كل شئ يفيد فى كشف الحقيقة " مما يدل أن القانون الإماراتى لم يحضر التفتيش فى الأشياء المادية فقط . وهذا ما أكدته المادة 61 إجراءات .

(١) - د / عمر محمد بن يونس – الدليل الرقمى – المرجع السابق – ص 31 وما بعدها.

فى الحقيقة أن تطبيق القواعد التقليدية المتعلقة بالتفتيش لا يسمح بمد التفتيش الواقع على المعطيات المخزنة فى الأجهزة الموجودة بمكان محدد إلى المعطيات الموجودة فى الأجهزة المرتبطة بها ، وذلك لأن التفتيش بالمفهوم التقليدى يرتبط بالمكان المسموح إجراء التفتيش به ، وتجاوز هذا المكان للتفتيش إلى غيره دون أى سند قانونى صريح يعرض التفتيش والضبط الناجم عنه للبطلان ، ويفوت بالتالى إمكانية اللجوء إلى إجراء مهم كالتفتيش فى مكافحة الجريمة الإلكترونية والمعاقبة عليها . الأمر الذى جعل المشرع فى بعض الدول إلى تشريع ما يمكن أن يطلق عليه التفتيش عن بعد(١).

ومن هذه التشريعات التشريع الفرنسى حيث نصت المادة (17) من القانون رقم (239) لسنة 2003 المسمى بقانون الأمن الداخلى على أنه " لضابط الضبط القضائى أو لمن يعملون تحت مسؤليتهم من مأمورى الضبط القضائى ، القيام أثناء تفتيش يجرونه وفقاً لأحكام هذا القانون ، بالدخول من خلال نظام حاسوبى موجود فى الأماكن التى يجرى فيها التفتيش ، إلى معطيات تهم التحقيق مخزنة فى هذا النظام ، او فى نظام حاسوبى آخر ما دام أن هذه المعطيات متاح الدخول إليها من النظام الرئيسى أو من نظام مرتبط بالنظام الرئيسى(٢).

ونرى من الأفضل النص على توسيع نطاق التفتيش والضبط فى الوسط الإلكترونى والمعلوماتى ليشمل التفتيش عن بعد ، وذلك تلافياً لأى صعوبة قد تعترض تطبيق القواعد التقليدية فى هذا الوسط ، حيث أن التفتيش يعد من أهم إجراءات التحقيق فى كشف الحقيقة فهو وسيلة يرجى من خلالها الكشف عن أدلة الجريمة . لذا فإن ضبط الأشياء المتعلقة بإثبات الجريمة هو الأثر المباشر للتفتيش وقد يكون محل الضبط معطيات

---

(١)- تجدر الإشارة إلى أن بعض الدول ما زالت تعتمد تطبيق القواعد التقليدية للتفتيش على التفتيش غير المباشر أو التفتيش عن بعد من هذه الدول ألمانيا – كندا – إسبانيا – إيطاليا – البرتغال . أنظر د / عبدالله حسين محمود – المرجع السابق – ص 510.

(٢)- حيث نصت المادة 19 من الاتفاقية الأوربية لجرائم الإنترنت 2001 بقولها " من حق السلطة القائمة على التفتيش فى الحاسوب الموجود فى دائرة اختصاصهم أن تمتد فى حال الاستعجال نطاق التفتيش إلى أى جهاز، فى حال كان الدخول إلى المعلومات المخزنة يتم من الحاسب الأصلى محل التفتيش"

ذات طبيعة معنوية ، وخاصة عندما يتم ضبط مث هذه المعطيات مجردة من الدعامة المادية المثبتة عليها ، فالضبط لا يرد فحسب إلا على الشئ المادى لكن ما نلاحظه أن بعض التشريعات ومنها التشريع الإماراتى نص فى قانون الإجراءات الجنائية على إجازة ضبط كل ما يفيد فى كشف الحقيقة ، دون أن يحصر الضبط فى الأشياء المادية[١].

ومن الطبيعى أن تختلف طريقة ضبط الأشياء المادية ، كضبط جهاز الحاسوب أو ملحقاته كالأقراص وغيرها عن طريق ضبط المعطيات الإلكترونية . لذا من المنطقى تمكين المحقق فى الجريمة الإلكترونية من النسخ على الدعامة المادية التى يراها مناسبة للمعطيات الإلكترونية التى يسمح له القانون التفتيش فيها ، متى بدأت له أهميتها فى كشف الحقيقة .

وغالباً ما تكون قواعد الضبط التقليدى صالحة للتطبيق فى مجال الجريمة الإلكترونية ، ولهذا لم تقر معظم الدول نظماً تختص " بالضبط الإلكترونى " وإنما اكتفت بتطبيق القواعد التقليدية على ضبط المعطيات الإلكترونية[٢].

وهناك عقبات قد تعترض التفتيش عبر شبكات الحاسوب خاصة عندما يتعلق الأمر بالتفتيش عن بعد فى مجال ضبط المعطيات الإلكترونية ، وفى ظل غياب اشتراط إجراءات خاصة تضمن صدق المعطيات المضبوطة يبقى المجال مفتوحاً للتساؤل حول مصداقية أدلة مستمدة فى الحقيقة من نسخ عن الأصل المخزن فى الوسط الإلكترونى . وفى هذه

---

(١)- أنظر المادتين (61 – 72) من قانون الإجراءات الجنائية الإماراتى .

(٢)- فنلاحظ من التشريعات التى اكتفت بالنص على القواعد التقليدية فى الضبط المشرع الأمانى حيث نص فى المادة (92) وما يليها من قانون الإجراءات الجزائية لم ينص صراحة على ضبط المعطيات الإلكترونية بواسطة النسخ ، وإنما اكتفى بالنص على ضبط أو تسجيل أى معلومات تظهر مفيدة لكشف الحقيقة . ونفس الشئ ذاته القانون الإماراتى حيث يجيز المشرع ضبط كل ما يفيد فى كشف الحقيقة ، فإن الضبط يشمل المعطيات الإلكترونية . أنظر د / هشام محمد فريد – الجوانب الإجرائية للجرائم المعلوماتية – المرجع السابق – ص 59.

الحالة ونظراً لغياب تشريع إجرائى ينظم تلك المسألة ومن أجل المحافظة على الدليل الرقمى يتعين مراعاة ما يلى[١].

١ - أن يكون فى الإمكان الرجوع إلى المعطيات الأصلية التى أخذت عنها ، كلما دعت الضرورة لذلك ، وتظهر ضرورة هذا الاحتياط من خلال إتاحة إمكانية إثبات مطابقة النسخ المضبوط عليها المعطيات الإلكترونية للأصل .

٢ - الأمر الثانى يتعلق بمعالجة المعطيات الإلكترونية المضبوطة فيتعين على المحقق أو الخبير البحث عن المعلومات المطلوبة ضمن المعطيات المضبوطة ، ويتم ذلك من خلال العديد من الإجراءات التى تحتاج إلى تحليل ومعالجة المعطيات ، وعلى المحقق المكلف بالتحقيق فى الدليل الإلكترونى أن يحرص على الحصول على نسخة أخرى إضافية من المعطيات وذلك للعمل بها كدليل على إجراءات المعالجة التى وقعت على المعطيات الإلكترونية .

٣ - هذا بالإضافة إلى كل ما سبق ضرورة مراعاة إجراءات التحرز على الأشياء المضبوطة التى حددها القانون[٢].

٢ -مراقبة البيانات والرسائل الإلكترونية وتسجيلها .

يمثل المساس بسرية البيانات الخاصة اعتداء على الحق فى الخصوصية، ومما لا شك فيه أن هذا الحق أصبح أكثر عرضة للتهديد نتيجة التطور التكنولوجى .

فالخصوصية تكون أكثر عرضة للانتهاك إذا ما استخدمت الوسائل الإلكترونية والوسائل الحديثة لتقنية المعلومات [٣] . لذا تظهر

---

(١) - د / أحمد يوسف الطحطاوى – الأدلة الإلكترونية ودورها فى الإثبات الجنائى – المرجع السابق – ص 96 وما بعدها .

(٢)- أنظر المادة 61 من قانون الإجراءات الجزائية الإماراتى التى تنص على أنه " يجب على مأمور الضبط القضائى أن يضع الأشياء والأوراق المضبوطة فى حرز مغلق مختوم بالشمع الأخمر ويكتب على الحرز تاريخ المحضر ويبط الأشياء ويشار إلى الموضوع الذى حصل الضبط من اجله " أنظر د / حسن الجندى – الكتاب الثانى من قانون الاجراءات الجزائية الإماراتى – ص 145.

(٣) – مبدأ السرية والخصوصية تحرص الدساتير والقوانين الوطنية على احترامه وتأكيده – الدستور المصرى المادة (45) – والدستور الأمريكى القسم الأول والقانون الفرنسى رقم 646 لسنة 1991 ، التوجيه الأوربى الصادر 1995 – ومن ثم لا يجوز للجهات الحكومية مراقبة المراسلات والاتصالات إلا لضرورة

الحاجة إلى حماية البيانات الإلكترونية بصورة أكبر من الحماية التى تتطلبها البيانات العادية ، مما يزيد الاهتمام بسرية وخصوصية المعلومات الشخصية ، أو ما يسمى بالخصوصية الإلكترونية[١].

فالتوسع فى الحماية الجنائية لسرية البيانات الخاصة تشمل صراحة البيانات والرسائل الإلكترونية ، لذلك اشترط قانون مكافحة جرائم تقنية المعلومات الإماراتى رقم (2) لسنة 2006 فى المادة (8) منه على معاقبة أفعال التصنت والالتقاط والاعتراض المتعمد للاتصالات والرسائل الإلكترونية فى حالة وقوع أى من هذه الأفعال دون وجه حق .

لذلك على سلطة التحقيق مراقبة هذا النوع من البيانات إذا اقتضت طرق التحقيق ذلك ، ومن الواضح أن معظم التشريعات لم تنص على إجراءات خاصة لهذه الحالة ، فعلى سلطة التحقيق أن تتبع الإجراءات الخاصة بمراقبة وتسجيل البيانات العادية وأن تراعى الضمانات المقررة عند القيام بهذا الإجراء[٢].

وقد أكدت المادة (75) من قانون الإجراءات الجزائية الإماراتى أن تراعى سلطة التحقيق عند قيامها بضبط المراسلات ومراقبة وتسجيل المحادثات ، الضمانات الآتية :- يدخل الأمر بضبط المراسلات ومراقبة البيانات الإلكترونية وتسجيلها ضمن الصلاحيات التى تملكها النيابة العامة ، فليس لمأمورى الضبط القضائى هذه السلطة ، سواء تعلق التحرى الذى يقوم به هؤلاء بجريمة متلبس بها أم جريمة غير متلبس بها .

تتعلق بالنظام العام ، أو الأمن القومى ، أو للوقاية من الجرائم ، أو لحماية حريات وحقوق الغير ، ولا يتم الكشف عن المعلومة أو الرسالة أو الاتصال إلا عن طريق السطة القضائية أو السلطة الإدارية لأسباب حددها القانون .

(١) - وقد وفر قانون العقوبات الاتحادى الحماية لحرمة الحياة الخاصة من خلال تجريم الاعتداء على الأحاديث الخاصة والاتصالات ، فقد نصت المادة (378) من هذا القانون على أنه يعاقب بالحبس والغرامة كل من :- 1- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت فى مكان خاص أو عن طريق الهاتف أو أى جهاز آخر " وعاقب كذلك هذا القانون الاعتداء الواقع على المراسلات الخاصة التقليدية والمكالمات الهاتفية ، فقد نصت الفقرة الأولى من المادة (380) من قانون العقوبات على أنه " يعاقب بالغرامة التى لا تقل عن ثلاثة آلاف درهم كل من فض رسالة أو برقية بغير رضاء من أرسلت إليه أو استرق السمع فى مكالمة هاتفية .

(٢)- ومن الدول التى اكتفت بتطبيق القواعد التقليدية المتعلقة بمراقبة المراسلات العادية على الاتصالات الالكترونية (فرنسا – ألمانيا – أسبانيا – إيطاليا)

يتطلب اعتراض وضبط المراسلات الإلكترونية صدور إذن من النائب العام . والحقيقة فإنه يتعين التمييز بين اعتراض البيانات والمراسلات الإلكترونية أثناء بثها(**online**) ، أى وقوع الاعتراض أثناء انتقال أطرافه ، أى وقوع الاعتراض أثناء انتقال أطرافه ، واعتراض الاتصالات الإلكترونية المخزنة ، أى وقوع المراقبة والتفتيش على المراسلات الإلكترونية الموجودة فى صندوق البريد الإلكترونى أو الرسائل الصوتية المخزنة لدى مزود الخدمة . ففى الحالة الأولى فقط يتعين إقامة التماثل على المراسلات والمحادثات ، الأمر الذى يؤدى إلى أن يكون تقييد اعتراض الاتصالات الإلكترونيةبالحصول على إذن النائب العام فى هذه الحالة فقط . أما بالنسبة للحالة الثانية فإن قواعد التفتيش العادية هى التى يتعين تطبيقها ، على اعتبار أن هذه الحالة أقرب ما يكون إلى تفتيش الأماكن(١)

ولا شك أن مراقبة البيانات والمرسلات الإلكترونية إن كانت تحمل اعتداء على حرمة الحياة الخاصة ، فإن إباحة هذا الإجراء مقيد فى الحدود الفائدة المرجوة منه ، وهو ضرورته لكشف حقيقة الجريمة والمجرم والوصول لأدلة الجريمة .

والفائدة الأساسية التى يمكن أن تتحقق من مراقبة الاتصالات الإلكترونية تتمثل فى الوصول إلى تحديد هوية مستخدم شبكة الانترنت المشتبه بارتكابه جريمة إلكترونية ، إلا أنه من الصعب فى كثير من الأحيان تحقيق هذ الغاية ، ويعود ذلك إلى مجموعة من أسباب بينها إتاحة مواقع الإنترنت للمستخدم إمكانية إخفاء هويته الحقيقية ، فمراقبة الاتصالات وتسجيلها تتيح للمحقق الوقوف على عناوين المستخدمين من خلالها مطابقتها مع قوائم المشتركين التى يحوزها ، وهذا الأمر تعترضه صعوبات جمة فقد يكون مركز هذا المزور فى دولة أجنبية ، وقد تكون الخدمة التى يكون يقدمها المزود مجانية ، ويترتب على ذلك الحرمان من وسيلة مهمة لتحديد هوية المستخدم والتى تكون فى حيازة مزود الخدمة .

ثانياً : الحصول على الدليل الإلكترونى من خلال إجراءات حديثة .

تسعى الدول فى تطبيق بعض الإجراءات الحديثة المتعلقة باتباع التقاليد التقنية للحصول على الدليل الرقمى أو الإلكترونى ، فهذه التقنية تساهم فى تطوير آلية تفاعل حقوق الإنسان الرقمية مع ضبط الدليل

---

(١) - د / أحمد يوسف الطحطاوى – المرجع السابق – ص 99 وما بعدها .

الرقمى من مصادرة المعروفة او المتعارف عليها . وتقوم بعض الدول بتنفيذ مخطط هام فى هذا الشأن يتمثل فى رصد نظم توجيهية تحتمل التطوير كإعداد مرشد أو نظام عمل لتنفيذ عملية ضبط الدليل الرقمى [١].
مثلما هو الحال فى المرشد الفيدرالى الأمريكى لضبط وتفتيش الحواسيب وصولا إلى الدليل الرقمي ، كما تسمح التقاليد التقنية بتوحيد منهجية العمل فى الشركات والمكاتب الخاصة التى تعمل كبيوت خبرة (خبرة استشارية) فى مجال البحث عن الدليل الرقمى[٢].

ومن الإجراءات الحديثة للحصول على الدليل الرقمى ما يلى :

1- التحفظ على البيانات المخزنة :

يقصد بهذا الإجراء تمكين السلطة المكلفة بالتحقيق من أن تصدر أمراً مستعجلاً لمزود الخدمة بالتحفظ على البيانات الإلكترونية من خلال ما يأتى[٣]:

يبدأ مأمور الضبط سواء بنفسه أو عن طريق خبير له صفة الضبط أو بتكليف لخبير أو لأى شخص على دراية بالحوسبة بالتحفظ ، بضبط القطع الصلبة والمرنة والملحقات كالطابعة والشاشة وغير ذلك . وبمجرد الضبط والتحريز السليم سوف يتولى استلام الحاسوب لتفتيشه . ويجب تقله على وجه السرعة استناداً إلى انه من الممكن أن يكون التأخير فى الكشف عن الدليل يؤدى إلى فقدانه أو إتلافه أو غير ذلك .

---

(١) – أن الإجراءات الحديثة للحصول على الدلي الرقمي ليست محصورة بجرائم محددة بعينها وإنما تشمل التحقيق فى كل الجرائم الإلكترونية التى تقع من خلال نقل الإتصالات عبر نظام الحاسوب ، فقد تكون الجريمة عبارة عن عرض لمواد إباحية تطال الأطفال أو الاتجار بالمخدرات ، والإجراءات المستحدثة ورد تحديداً لها فى اتفاقية (بودابست) المتعلقة بالجريمة الإلكترونية لسنة 2001 حيث خصصت الباب الثانى منها " للقانون الإجرائى " وحددت المواد (16) وما يليها هذه الإجراءات وأخذت بها قوانين بعض الدول كالقانون الفرنسى والأمريكى ومنها إجراءات البحث عن الدليل المستحدثة فى تمكين المختص من أمر مزور الخدمة بالتحفظ على البيانات المخزنة ، وتقديم معلومات تتعلق بالمشترك فى الخدمة ، أنظر د / على حسين الطواليه – التفتيش الجنائى على نظام الحاسوب والإنترنت – دراسة مقارنة – عالم الكتاب الحديث سنة 2004 – ص 205.

(٢)- د / عمر محمد بن يونس – الدليل الرقمى – المرجع السابق – ص 97.

(٣)- أنظر د / عمر محمد بن يونس – الدليل الرقمى – المرجع السابق – ص 98 ، 99 .

يلتزم الخبير المكلف بالقيام بفحص الجهاز والقطع الصلبة المتحفظ عليها وإعداد تقرير بها لتقديمه إلى الجهات المختصة ، وبحيث يشمل التقرير القطع الصلبة والمرنة والملحقات ..الخ .

حين فحص القرص الصلب فى الجهاز يلزم الخبير بعد استخدام ذات الجهاز المتحفظ عليه أو المضبوط ، وإنما يجب ان يعمل الخبير على إعداد جهاز آخر بذات المواصفات فى الحد الأدنى او الاستعانة بأجهزة متطورة حيث الخبير يوضع القرص فيه .

يلزم الخبير بعدم القيام بفحص القرص الصلب المملوك للمتهم أو المشتبه به أو لمزور الخدمة ، وإنما يجب أن يقوم بإعداد نسخة مطابقة له فى قرص صلب آخر من ذات النوعية أو القيام بعمل نسخة باستخدام قرص صلب نموذجى وتتخذ إجراءات إثبات ذلك كتابة ، كرقم القرص التى يتم استنساخ القرص الأصلى .....الخ .

2- الأمر بتقديم بيانات مخزنة :

والمقصود بهذا الأمر تمكين السلطة المختصة بالتحقق من الزام محدودى الخدمة تقديم بيانات بحوزتهم وتحت سيطرتهم تتعلق هذه البيانات باستثناء المعلن منه للجمهور ، بالحق فى الخصوصية ، ويمتد الأمر الذى يمكن للسطة بالتحقيق إصداره ليشمل نوعى البيانات المتعلقة بالمستخدم وهى نوعين .

البيانات المتعلقة بالمرور ، التى تكون فى الغالب فى حيازة مزور الخدمة فقط ، والمقصود بذلك النوع من البيانات تلك التى تعالج الاتصالات التى تمر من خلال نظام معلوماتى ، كأصل ومقصده وخط سيره وتاريخه ووقته ومدته [١] وهذا النوع من البيانات يتضمن بيانات المرور المتعلقة باتصالات سابقة ، فمن خلالها يمكن تحديد خط السير فيتيح إمكانية تحديد هوية من ساهم فى ارتكاب الجريم محل التحقيق .

البيانات المتعلقة بالمحتوى أى الملعومات المنقولة عن الطريق الإلكترونى .

---

(١)- حددت المادة (1) من اتفاقية بودابست بيانات المرور على أنها " أى بيانات كمبيوتر متعلقة باتصال عن طريق منظومة كمبيوتر ، والتى تنشأ عن منظومة تشكل جزءاً فى سلسلة الاتصالات ، توضح مصدر الاتصال ، والوجهة المرسلة إليها والطريق الذى تسلكه ووقت وتاريخ وحجم ومدة وقوع الخدمة المذكورة – أنظر د / هلالى عبد اللاه – اتفاقية بودابست لمكافحة جرائم المعلوماتية – دار النهضة العربية – الطبعة الأولى – ص 160.

نلاحظ أن محل الجريمة الإلكترونية أو المعلوماتية دائماً معطيات الحاسب الإلكترونى أى المحتوى الداخلى ، وتستهدف دائماً هذه الجرائم الحق فى المعلومات المخزنة وأو المعالجة فى نظام الحاسب أو المتبادلة عبر الشبكات، ويمتد تعبير الحق فى المعلومات ليشمل الحق فى انسيابها وتدفقها ، والحق فى الملعومات بذاتها بما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية أو لها قيمة بذاتها كالبرامج بكل أنواعها ، مدخلة ومعالجة ومخزنة ، ومنقولة وتلزم الفقرة (1) من المادة (19) من اتفاقية بودابست الأطراف بتحويل سلطاتها المكلفة بمكافحة الإجرام ، صلاحيات التفتيش والولوج للبيانات المعلوماتية التى تم احتوائها سواء من داخل نظام معلوماتى ، او فى جزء منه أو على دعامة تخزين مستقلة ، وفى بعض الأحيان قد تكون البيانات مخزنة مادياً فى نظام آخر ، او فى جهاز تخزين آخر ، لكن من الممكن الوصول إليها بطريقة قانونية من خلال النظام المعلوماتى الذى يتم تفتيشه ، وذلك بعمل اتصال مع النظم المعلوماتية المنفصلة الأخرى ، وطبقاً لاتفاقية بودابست فإنها تقرر تأهيل سلطة كلية الينا باجراءات الضبط والتفتيش على الأدلة الإلكترونية أو الرقمية .

3- التحفظ على الأدلة الإلكترونية [١]

إن التحفظ على الأدلة داخل الحاسوب من العمليات المعقدة التى تحتاج بداية إلى رصد دقيق لمدى صحة البيانات التى يحتوى عليها الحاسوب . وهذا الأمر يستلزم بالضرورة قيام الخبير التقنى بالكشف بداية على المدى الذى عليه صحة حركة الحاسوب بأساليب سيما من حيث الخلل والعطب وتتم عملية حفظ الأدلة داخل الحاسوب بأساليب متعددة تتشكل فى أبسط مظاهرها باستخدام أسلوب الحفظ العادى وأقوى مظاهرها فى علميات حجز الحاسوب على الدليل الموضوع فيه الدليل الرقمى هو فى العادة ملف يحتوى على بيانات رقمية تعطى مظهراً معلوماتياً محدداً غير قابل للتحويل إلى مظهر آخر .

وعملية حفظ الأدلة فى العالم الرقمى يتطلب من الخبير التقنى القيام برصد موقع على الإنترنت أو المعلومات التى تشير إلى الجريمة ، والتى تكون فمظاهر مختلفة الأشكال ، كما لو كانت الجريمة من جرائم السب والقذف فى غرف المناقشة ، ففى مثل هذه الحالة الأخيرة يتم اللجوء

---

(١)- أنظر د / عمر محمد بن يونس – الدليل الرقمى – المرجع السابق – ص 124.

إلى ذاكرة الخادم الذى يتولى ربط هذه الحالة الأخيرة يتم اللجوء إلى ذاكرة الخادم الذى يتولى ربط هذه الغرف عبر العالم الرقمى لكى يمكن الوصول إلى تحديد موضوع السب والقذف وتاريخه [١] ،وكذلك تستدعى عملية حفظ الأدلة فى العالم الرقم لزوم قيام الخبير بعرض الأدلة على المحكمة أو جهات التحقيق ، وهذا الأمر يتطلب عمل الخبير يستمر لمرحلة المحاكمة وأحياناً يتطلب منه القيام بعمله لمرحلة ما بعد المحاكمة كما هو الشان فى حالة عرض الدليل المقدم إلى محكمة الموضوع أمام جهة قضائية أعلى كالاستئناف أو النقض ومنعاً من المشاكل التى يمكن أن تنجم عن حفظ الأدلة فى العامل الرقمى فإن العديد من المحاكم لجأت إلى ميكنة إدارتها رقمياً ، بحيث يتم تسليم الأدلة إلى الإدارة متخصصة تتولى بدورها حفظ الدلة فى العامل الرقمى لعرضها على القضاء كلما تطلب الأمر ذلك :

وعملية الحصول على مخرجات الحاسوب والانترنت بقصد تقديمها كدليل فى المحكمة تعد من أولى الموضوعات التى تعرض لها الفكر القانونى سواء من حيث قابليتها القانونية أو من حيث منهجية الدليل الذى تم تخريجه ، حتى أن هذه الطريقة تعد فى المرحلة المعاصرة من الأساليب التقليدية فى مجال الحصول على الدليل الرقم [٢] ، إذا يصح فى القانون أن يكون هناك من الأدلة ما هو مخرج من مخرجات الحاسوب والإنترنت ، بحيث تعد هذه المخرجات أدلة أصلية على الرغم من كونها نسخ دليل أصله موجود فى العالم الافتراضى أو فى الحاسوب .

ويقوم الخبير بتخريج هذه المخرجات إلى العالم المادى بطرق مختلفة أبرزها فى العمل هى الطباعة على الطابعة **print out** ، وذلك بتوحيلها إلى نسخ ورقية عوضاً عن كونها رقمية أو نبضية ، والخبير فى ذلك لا يكتفى بمجرد نسخ البعض المعلوماتى وإنما يحتاج أيضاً إلى

---

(١) Hubert Bouchet – lacybervelllance des salaries dans l'entreprise – rapport o'etude etde consulataion publique – mors,2001.p.12

(٢)- د / محمد فتحى محمد انور – تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبار – جامعة عين شمس – 2000 – ص 433 وما بعدها

تخريج النبض البيانى بحيث يقوم بتخريج كافة البيانات الرقمية حين طباعة هذا الدليل[١]

المطلب الثالث

صور وأشكال الدليل الالكتروني

إن الاهتمام الذى يحظى به الدليل الرقمى قياساً بغيره من الأدلة الأخرى المستمدة من الآلة مرده انتشار استخدام تقنية المعلومات الرقمية ، والتى تعاظم دورها مع دخول الإنترنت شتى مجالات الحياة ، وأصبح بذلك هذا الوسط مرتعاً لطائفة من الجناة يطلق عليهم المجرمين المعلوماتيين ، فالجرائم التى يرتكبها هؤلاء المجرمون تقع فى الوسط الافتراضى ، او ما يسمى بالعامل الرقمى ، لذا كان الدليل الرقمى هو الدليل الأفضل لإثبات هذا النوع من الجرائم وهى الجرائم الإلكترونية ، لأنه من طبيعة الوسط الذى ارتكبت فيه ، ومن هنا ظهرت اهمية هذا النوع من الأدلة .

والدليل الرقمي أو الإلكترونى ليس صورة واحدة بل يوجد له العديد من الصور والأشكال سوف نتناولها فيما يلى : -

أولاً : المخرجات الورقية[٢]:

تعتبر مخرجات الكمبيوتر الذى تسجل فيها المعلومات على الورق أحد الأشكال الرئيسية التى تأخذها هذ المخرجات ، ويستخدم فى ذلك الطابعات ، والطابعة ، وهى عبارة عن جهاز يقوم بانتاج نسخ مطبوعة من البيانات مثل التقارير والشيكات وقوائم البيانات والبرامج التى يحتاج إليها المستخدمون ، فتقوم الطابعة بطباعة ما قامت فى فترة زمنية سابقة بطباعته وهو أمر بالضرورة يؤدى إلى الحصول على مخرجات الطابعة **Hard copy** وتتنوع الطابعات الملحقة بأجهزة الكمبيوتر لإنتاج المخرجات الورقية من حيث طريقة تشغيلها ، وسرعة التشغيل والتطبيق المستهدف وخصائص المخرجات الورقية ، فهناك طابعات تصادمية تعمل مثل الآلات الكاتبة ، وطابعات غير تصادمية تستخدم المواد الكيميائية أو

---

(١)- د / عمر محمد بن يونس – الدليل الرقمى – المرجع السابق – ص 126.

(٢)- أنظر د / هلالى عبداللاه أحمد – اتفاقية بودابست لمكافحة الجرائم المعلوماتية – المرجع السابق – ص 165.

أشعة الليزر أو الحرارة ، كما يستخدم أيضاً الرسم فى طباعة الرسومات بدرجات وضوح مختلفة على الورقة ومن أشهر أنواع أجهزة الرسم : راسم الطاولة وراسم الإسطوانات(١).

ثانياً : المخرجات الإلكترونية :

يتم استخراج المخرجات الإلكترونية أو ما يطلق عليها أدلة الحاسب الآلى من خلال أوعية لا ورقية أو غير مطبوعة مثل الأشرطة والأقراص الممغنطة ، أو الضوئية والمصغرات الفيلمية وغيرها من الأشكال غير التقليدية للتكنولوجيا التى تتوفر عن طريق الوصول المباشر ، حيث يقوم المستخدم بإدخال البيانات ويحصل على المخرجات فى نفس الوقت .

وتنحصر المخرجات الإلكترونية أو أدلة الحاسب الآلى فى الأشرطة المغناطيسية ، والأقراص المغناطيسية – والمصغرات الفيلمية للأشرطة المغناطيسية(٢) :

1- الشريط المغناطيسى :

هى عبارة عن شريط بلاستيك مغطى بمادة معدنية قابلة للمغنطة . يبلغ عرضه من ربع إلى نصف بوصة ، والشريط المغناطيسى قد يكون ملفوفاً على بكرة كبيرة مثل التى تستخدم فى أجهزة التسجيل الصوتى وقد يكون داخل علبة على شريط الفيديو أو شريط الكاسيت ، والفكرة التى يبنى عليها تسجيل البيانات على الشريط المغناطيسى هى مماثلة لتلك التى بنى عليها تسجيل الأحاديث على شريط التسجيل الصوتى ، فجميع الأشرطة الممغنطة بها رأس للقراءة والكتابة ، يسجل البيانات على شكل نقطة مغناطيسية على الشريط بشفرة خاصة تدل على البيانات المستخرجة من داخل الحاسب ، كما يستطيع هذا الرأس الاحساس بوجود هذه النقطة ويقوم بارسال النبضات الكهربائية القابلة للشفرة البيانات داخل الحاسب ، ويستخدم الشريط المغناطيسى فى تخزين البرامج والملفات المتتالية ، أى التى يلزم لقراءة البيانات فيها قراءة الشريط من بدايته ، وتنظم المعلومات على الشريط على شكل وحدات خاصة تسمى كل وحدة منها حزمة وحجم

---

(١)- د / هلالى عبداللاه أحمد – حجية المخرجات الكمبيوترية فى المواد الجنائية – دار النهضة العربية –الطبعة الأولى – 1997 – ص 188.

(٢) - راجع د / محمد فهمى طلبة – الموسوعة الشاملة لمصطلحات الحاسب الآلى – موسوعة دلتا كمبيوتر – 1991 – ص 330 : 332.

الحزمة يحدده مستخدم الجهاز ،لذا تعالم الحزمة موحدة متكاملة وذلك عند تخزينها أو إخراجها من الشريط ، وقد جرى العمل على تخصيص الحزمة الأولى والأخيرة من الملف لتسجيل معلومات تعريفية عن الملف .

2- الأقراص المغناطيسية :

وتعتبر الأقراص المغناطيسية من أفضل أنواع الوسائط التى يمكن استخدامها للتخزين المباشر العشوائى ، التى تتميز بقدرتها الاستيعابية العالية ، وسرعة تداول المعلومات المخزنة عليها ، ومن أهم خواص الأقراص المغناطيسية إمكانية القراءة أو التسجيل على أى قطاع من الأسطح ، كذلك يمكن تغيير أو تعديل أى ملف مسجل عليها دون حاجة إلىإنشاء ملف جديد إذ يتم تعديل السجل وهو فى موضعه ، وهناك أنواع عديدة من الأقراص المغناطيسية من أهمها[١]:

- القرص المرن :

يعتبر القرص المرن من أشهر وسائط التخزين للبيانات ، وينتشر استخدامه وتداوله فى الحاسبات الصغيرة والمتوسطة ، وذلك نتيجة سهولة استخدامه ، والقرص المرن دائرى الشكل قطره خمسة وربع بوصة ، يصنع من مادة دقيقة جداً من البلاستيك مغطاه بطبقة من مادة مغناطيسية حساسة من أكسيد الحديد . وتوجد فتحة كبيرة فى القرص تسمى بفتحة القراءة والكتابة بوحدة إدارة الأقراص لتلامس القرص المغناطيسى ، حيث تتم عملية القراءة والكتابة بمعنى اختزان المعلومات واسترجاعها ، ويمكن مسح البيانات من القرص وإعادة تخزينها عدة مرات ، دون أن يفقد القرص المرن كفاءته ، كما توجد على أحد أضلاع القرص فتحة جانبية يطلق عليها فتحة الحماية من الكتابة ، وفى حالة تغطية هذه الفتحة بورق لاصق لا يمكن كتابة أو تسجيل معلومات على القرص ، وبالتالى تتم حماية المعلومات المخزنة عليه ، والتى سبق تسجيلها .

- القرص الصلب : (**Hard Disk**)

ويعد القرص الصلب المحتوى الذى يضم فى داخله مجموع البيانات الرقمية ، وهو عبارة عن قرص معدنى رقيق ومغطى بمادة قابلة

---

(١)- أنظر د / طارق الحملى – الدليل الرقمى فى مجال الإثبات الجنائى – ورقة عمل مقدمة للمؤتمر العربى الأول حول المعلوماتية والقانون المنعقد فى الفترة من 28 / 29 أكتوبر 2009 – تنظمه أكاديمية الدراسات العليا – طرابلس .

للمغنطة ، ويتم من خلال القرص الصلب الكشف على القيمة الاستردادية للبيانات المخزنة فيه سواء أكانت محتويات مكتوبة أو صور أو أصوات ... الخ وكذلك ما تم حذفه **delete** من بيانات وبرامج وبرمجيات [١] .

- المصغرات الفيلمية .

تعبتر من مخرجات الكمبيوتر على الميكروفيلم شكلاً مختلفاً من تكنولوجيا المخرجات ، التى تسجل فيه الملعومات على المصغرات الفيلمية المختلفة ، بدلاً من تسجيلها على الورق . وهى عبارة عن أفلام فوتوغرافية يتم استخدامها فى تصوير صفحات البيانات مع تصغيرها بدرجة متناهية فى الصغر . عن طريق جهاز تحويل للبيانات المسجلة على الأشرطة والأقراص الممغنطة وتتنوع سعة مخرجات الكمبيوتر على الميكروفيلم طبقاً لأنواع المصغرات القيلمية ومعدلات تصغيرها [٢] . فعلى سبيل المثال إذا استخدم الميكروفيش (**micorofich**) ، والواحدة بمعدل تصغير من (1 – 48) فإن بطاقة الميكروفيش تشتمل على معلومات تمثل (270) صفحة من مخرجات الكمبيوتر المطبوعة ، بنفس معدل التصغير فإن لفة الميكروفيلم التى تشتمل على مائة قدم تستوعب ما يعادل (7200) صفحة من صفحات الكمبيوتر المطبوعة .

١ -أدلة العرض المرئى :

بالإضافة إلى مخرجات الطباعة المقروءة بشرياً على الورق أو المخرجات الإلكترونية ، يتوفر مخرج ثالث يتمثل فى عرض مخرجات المعالجة بواسطة الكمبيوتر على الشاشة (**monitor**) الخاصة به [٣] ، وتسمى أيضاً وحدة العرض المرئى ، وهى تعتبر أهم أجزاء الحاسب استخداماً ، إذ عن طريقها يتم استعراض أى بيانات أو معلومات تكتب على لوحة المفاتيح بواسطة المستخدم . كما يتم استعراض البيانات التى تم إدخالها أو المعلومات الناتجة عن معالجة البيانات فى وحدة المعالجة المركزية، وكذلك التعليمات الموجهة للمستخدم بواسطة البرامج

---

(١)- ORINS.KERR. searches and seizures in adigital world.op.at p. 540.

(٢)- أنظر د / محمد فهمى وآخرون – الموسوعة الشاملة لمصطلحات الحاسب الإلكترونى – المرجع السابق – ص 200.

(٣)– أنظر د / محمد محمد المهدى – المرجع السابق – ص 79.

التطبيقية ، ومن أهم أنواع شاشات العرض الشاشة أحادية اللون التى لا تعرض الرسوم ولا الألوان وتلك التى تعرض الرسوم والألوان ، وهذا النوع الأخير هو الأكثر انتشاراً والأقل تكلفة فى نفس الوقت ، ويستطيع ان يتعامل مع الحاسب فى وضعى الكتابة والرسم . كذلك هناك الشاشة الملونة العادية ، وهناك الشاشة الملونة المحسنة ، وفى الفترة الأخيرة تم استخدام تكنولوجيا متطورة لانتاج انواع اكثر تطوراً من شاشات ملونة فائقة الجودة ذات إمكانيات ضخمة من حيث الوضوح وجودة الصورة وعدد الألوان المتاحة .

الفصل الثانى

مدى تأثير الأدلة الرقمية على مبدأ حرية القاضى الجنائى فى تكوين عقيدته

تمهيد :

تعد حرية الإثبات مبدأ من مبادئ الإثبات الجنائى ، فالإثبات يمكن الوصول إليه بأية وسيلة ما دامت مشروعة ، وللقاضى الجنائى مطلق الحرية فى استيفاء أدلة الإثبات ، لا يقيده فى ذلك نوع معين منها ، وله سلطة وحرية كاملة فى سبيل تقصى ثبوت الجرائم أو عدم ثوبتها ، أو الوقوف على حقيقة علاقة المتهمين بها ، ففتح له الباب على مصراعيه فى اختيار ما يراه موصلاً إلى الكشف عن الحقيقة، هذا هو الأصل والذى أقام عليه القانون الجنائى قواعد الإثبات لتكون ملائمة لما تستلزمه طبيعة الأفعال الجنائية وتقتضيه مصلحة المجتمع من وجوب معاقبة كل جان وتبرئة كل برئ ، فالقانون الجنائى لم يحدد للقاضى طرق إثبات خاصة . ومن جهة أخرى للمتهم أن ينفى التهم الموجهة إليه بكافة الوسائل الممكنة له [١].

والقاضى الجنائى يملك حرية واسعة فى تقييم عناصر الإثبات ووزن الأدلة ، وتقديرها بالكيفية التى تمكنه من تكوين عقيدته فى الدعوى المطروحة عليه ، ولا يخضع فى ذلك إلا لصوت ضميره وما يقتنع به شخصياً، ولا يستشير فى ذلك سوى وجدانه ، فهو وحده الذى يملى عليه الحكم الذى يصدره والذى يتوصل إليه ، وله أن يطرح الأدلة التنى لا يطمئن وجدانه إليها ، ومؤدى ذلك أن للقاضى الجنائى الحرية فى تقدير الأدلة المبسوطة بين يديه واستخلاص عناصر اقتناعه من أى دليل يثق به ، طالما فى أوراق الدعوى ، وله السلطة التقديرية الكاملة فى وزن قيمة كل دليل على حده .

وقد ترتب على حالة الصراع بين المجتمعات وبين الجريمة فى ثوبها الجديد والناجمة من استعمال الإنترنت ، نظرة جديدة للإثبات الجنائى من خلال التقنية الجديدة لشبكة المعلومات والاتصالات ، فبرزت ظاهرة جديدة إلى جانب المفاهيم التقليدية للدليل ، هى الظاهرة الرقمية ذات الطبيعة التقنية الناجمة عن الحاسوب والإنترنت ، بحيث يصح ان يطلق على الارتباط بين الظاهرة الرقمية الجديدة وبين الإثبات الجنائى تسمية جديدة للدليل هى الدليل الإلكترونى **Electronic Evidence** أو الدليل الرقمى **DIGITAL Evidence** وقد اعتادت المحاكم فى النظم

---

(١)- أنظر د / حسن صادق المرصفاوى – المرصفاوى فى أصول الإجراءات الجنائية – منشأة المعارف – الاسكندرية – 1996 – ص 726.

القانونية المقارنة ، على إحداث تسوية شبه منطقية بين الدليل الإلكترونى أو الرقمى وبين الدليل التقليدى المتعارف عليه ،والمستمد من وسائل الحصول عليه المعروفة ، كالتلبس والتفتيش والشهادة والقرائن وأيضاً الاعتراف ، وأساس هذه التسوية المنطقية هى نظرة إلى الواقع الجدى للتقنية الرقمية كونها ذات مدلول مؤثر وحقيقى فى عالم الإنسان المعاصر والمستقبلى ، فما تنتجه التقنية الرقمية يؤدى دوراً لا يمكن تجاهله حتى فى المجتمعات يعد نموها بطيئاً فى هذا المجال .

فالدليل الرقمى هو ذلك الدليل الذى يجد له أساساً فى العالم الافتراضى ويقود إلى الجريمة ، فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة التقنية للمعلومات ، والذى يؤدى إلى اقتناع قاضى الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الإنترنت ، فكلما كان هناك مزج فى موضوع الدليل (الفكرة أو المعلومات كبيانات **Data**.. الخ) بالمعالجة الآلية للمعلومات فإنه يعد دليلاً رقمياً [١]. وسوف نتناول من خلال هذا الفصل مشروعية الدليل الإلكترونى أو الرقمى ، وسلطة القاضى الجنائية فى قبول وتقدير الأدلة الإلكترونية أو الرقمية .

المبحث الأول : مشروعية الأدلة الإلكترونية فى الإثبات الجنائى .

المبحث الثانى : سلطة القاضى الجنائى فى قبول وتقدير الأدلة الإلكترونية .

---

(١) – أنظر د / محمد فتحى محمد أنور عزت – تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبار والتى تقع بواسطتها – جامعة عين شمس – 2010 – ص 405 .

المبحث الأول

مشروعية الأدلة الإلكترونية فى الإثبات الجنائى

لقد أضافت ثورة الاتصالات عن بعد بعداً جديداً متطوراً للجريمة المعلوماتية ، بسبب التطور الهائل الذى لحق الوسائل الإلكترونية ، وتعدد استخداماتها فى نواحى الحياة المختلفة فعن طريق استخدام الشبكة الرقمية يمكن عن ذات الطرق الحصول بنجاح على خدمات متعددة يمكن أن تختلف عن تلك التى يقدمها الهاتف ، كنقل البرامج عن طريق الحاسب الآلى ، أضفت عليها طبيعة خاصة مميزة من حيث الطبيعة الخاصة بالجناة الذين يرتكبونها .

فالجريمة وفقاً للفمهوم العام أنها اعتداء على المصالح والقيم التى يحميها المشرع بنصوص التجريم والعقاب ، يمكن أن تندرج تحتها كافة أنواع الجرائم ، وأما القول بأن هناك جرائم معلوماتية ، أو جرائم الكترونية ، فربما يكون السبب فى ذلك النظرة الى الطبيعة الخاصة لهذه الجرائم مكن حيث المحل الذى تقع عليه ، والذى يتمثل فى الوسائط الإلكترونية ذاتها ، بحسبان أنها أصبحت المستودع للقيمة والمصالح المستجدة التى أفرزتها الثورة التكنولوجية ، كالبيانات والبرامج التى تحويها الحاسبات الآلية ، أو التى تنقلها وتتعامل فيها شبكات الإنترنت ، أو بطاقات الوفاء والائتمان المصرفية ، والأعمال الأخرى المصرفية ، فالوسيلة الإلكترونية أصبحت اليوم وسيلة لارتكاب الجريمة وهى أيضاً محلاً لها ، وهو ما جعل البعض من الفقه يعرف الجريمة المعلوماتية بأنها السلوك غير المشروع الذى يرتكب باستخدام الحتاسب الآلى ، وتتميز الجرائم التى تقع على العمليات الإلكترونية بطبيعة خاصة ، هذه الطبيعة انعكست على أدلة إثباتها جنائياً[١] . وسوف نعرض من خلال هذا المبحث مشروعية الأدلة الإلكترونية أو الرقمية المتحصلة عن طريق التفتيش ، ومشروعية تلك الأدلة المتحصلة عن طريق الخبرة وذلك من خلال مطلبين :

---

(١)- أنظر د / هلالى عبداللاه – حجية المخرجات الإلكترونية فى المواد الجنائية – المرجع السابق – ص 9.

المطلب الأول : مشروعية الأدلة الإلكترونية المتحصلة عن طريق التفتيش .
المطلب الثانى : مشروعية الأدلة الإلكترونية المتحصلة عن طريق الخبرة.

المطلب الأول

مشروعية الأدلة الإلكترونية المتحصلة

عن طريق التفتيش

يراد بالتفتيش التقصى والبحث عن الأدلة سعياً وراء ضبطها بقصد الاستعانة القانونية بها لإدانة الجانى وبالتالى ينبغى القيام بضبط ما يترتب عن التفتيش وتحليله بطريقة علمية حتى لا يفقد قيمته القانونية حال تعقده أمام القضاء إذا تطلب الأمر ذلك.

لذا يعد التفتيش من وسائل الإثبات التى ينبثق عنها أدلة تفيد الإدانة حال توافرها ويعد التفتيش من إجراءات التحقيق ذات الخطورة الخاصة ، لكونه من الإجراءات التى تمس حق الإنسان فى الخصوصية وبما يشكل ذلك اتهاماً للحياة الآمنة المستقرة التى تضمنتها الدساتير والمواثيق والإعلانات الأساسية [١].

وسوف نستعرض فيما يتعلق بالأدلة الإلكترونية أو الرقمية المتعلقة عن طريق التفتيش ما يلى :

أولا: ضوابط التفتيش لضبط الأدلة الرقمية أو الإلكترونية فى محتوياتها :

١ - إذن التفتيش :

من ضوابط التفتيش التى يتعين مراعاتها عند ضبط الأدلة الرقيمة أو الإلكترونية ضرورة الحصول على إذن التفتيش ، ويجب أن يتحدد فى إذن التفتيش ذاته الواقعة التى صدر من أجلها الإذن ، وهذا الأمر يمثل قاعدة عامة يجب السير عليها فى هذا الإطار .

---

(١)- أنظر د / حسن صادق المرصفاوى – أصول الإجراءات الجنائية – طبعة 1996 – ص 383 وما بعدها

وقد حص المشرع المقارن على إحاطة التفتيش كإجراء بضمانة الحرص على حقوق الإنسان من ناحيتين : موضوعية ، تتمثل فى الغاية من التفتيش ، وشكلية تتمثل في ضرورة الحصول على إذن التفتيش . كما تضمنت المواثيق الأساسية مثل هذه النصوص التى تلزم الجهات المختصة بهذا الإجراء بضرورة استصدار إذن تفتيش سابق على إجرائه ومحدداً بدقة سببه . على أن عضو سلطة التحقيق لا يكون بحاجة إلى إذن التفتيش أو أمر المحكمة إذا تدخلت إرادة المجنى عليه ، وفى هذه الحالة لا يكون الموضوع متعلقاً بالتفتيش وإنما يطلق عليه الإعلان الإرادى من قبل المجنى عليه . طالما كانت إرادة المجنى عليه واضحة المعالم لا يشوبها شائبة الإكراه أو التحايل أو غير ذلك(١).

ويتعين أيضاً لصحة إذن التفتيش الصادر فى محيط الجرائم التى تقع على الوسائل الإلكترونية أو عن طريقها أن يكون من صدر له الإذن بالتفتيش فى مأمورية الضبط القضائى المختصين بذلك وظيفياً ومكانياًَ ونوعياً، لا يشترط بعد ذلك التزام المحقق بندب مأمور ضبط معين(٢).

ولما كانت الجرائم الإلكترونية ذات طبيعة فنية ، فإنه ينبغى توافر خبرة معينة فى القائمين بالتفتيش فى الوسائل الإلكترونية لكى يتمكن من تأدية عمله ، وفى ذات الوقت يحافظ على سلامة الأدلة المتحصلة من الجريمة المعلوماتية ، ويشترط فى إذن التفتيش أن يكون مكتوباً ومحدداً التاريخ وموقعاً ممن أصدره وأن يكون صريحاً فى الأدلة فى مباشرة التفتيش ، وأن يتضمن من البيانات ما يحدد نوع الجريمة المطلوب جمع الأدلة عنها .

٢ - محل التفتيش

---

(١) - وقد قنن التشريع الأمريكى فكرة الإعلان الإرادى المذكور بمقتضى القانون الوطنى الأمريكى المؤرخ فى The Patuat ACT 2001/10/26 وسمح دون أن يكون فى ذلك صيغة طلب إلزامى المشرع الأمريكى فى القسم 6 صفحة 2702 لمزود الإنترنت بالافصاح الإدارى للسلطات عن محتويات سجلات عضو الإنترنت فى حالة الضرورة التى تتضمن خطراً حالاً مؤدياً إلى موت أو أضرار مادية حقيقية لأى شخص . أنظر د / عمر محمد أبوبكر – المرجع السابق – ص 965 وما بعدها .

(٢) - أنظر / سعيد عبداللطيف حسن – إثبات جرائم الكمبيوتر والجرائم المرتكبة على الإنترنت – الطبعة الأولى – دار النهضة العربية – القاهرة – 1991 – ص 140.

إن المحل الذى يقع عليه التفتيش للحصول على الأدلة الإلكترونية أو الرقمية هو الحاسوب والشبكة التى تشمل فى مكوناتها الخادم والمزود الآلى والمضيف والملحقات التقنية .... الخ .

ومحل التفتيش الذى يرد على المكونات المادية للحاسب الآلى وملحقاته ، وهذه لا خلاف يذكر حول خضوعها للتفتيش والضبط طبقاً للقواعد العامة طبقاً لقواعد قانون الإجراءات الجنائية بما فى ذلك البيانات المخزنة فى أوعية أو وسائط مادية كالأشرطة الممغنطة والأقراص الصلبة والضوئية وذلك تبعاً للمكان أو الحيز الموجودة فيه [١] ومن ثم إذا كانت موجودة بمسكن المتهم أو أحد ملحقاته، فتحكمها القواعد ذاتها التى يخضع لها تفتيش المسكن إذ يجوز تفتيشها وضبطها متى كان تفتيش المسكن جائزاً ، والعكس صحيح وفى حال وجودها فى مكان عام فيحكمها ما يحكم هذا المكان من أحكام . فى حين أنه إذا كان الحاسب فى صورة شخص خارج مسكنه ، فإن تفتيشه يخضع للقواعد ذاتها ، التى يخضع لها تفتيش الشخص بوصفه أحد متعلقاته ، يستوى أن يكون الحائز هو مالك الجهاز أم سواه .

والذى يهمنا فى هذا المكان هو التفتيش الذى يكون فى محله الجانب المنطقى للحاسب الآلى ، المتمثل فى المعلومات والبيانات والمعالجة إلكترونياً . أو ما يسمى بالكيانات المعنوية فى الوسائل الإلكترونية للحاسبات الآلية (الوسط الافتراضى) .

لذلك يثار تساؤل حول مشروعية التفتيش عن الدليل الرقمى وضبطه فى الوسط الافتراضى .

وللإجابة على هذا التساؤل نلاحظ أن الفقه قد اختلف حول مدى جواز تفتيش الوسط الافتراضى وضبطه وما به من محتويات ويرجع منبع الاختلاف إلى أن تحديد المقصود بمصطلح " شئ" الذى يفترض أن يكون محلاً للتفتيش والضبط فإذا كان التفتيش ينصب على شئ فإن التساؤل يثور حول مدى انطباق لفظ شئ على الكيانات المعنوية (الوسط الافتراضى) ولذلك اهمية عملية ، فإذا كانت المكونات المعنوية للحاسب

---

(١)- أنظر د / هشام فريد رستم – الجوانب الإجرائية للجرائم الإجرائية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – 1994 – ص 64 وما بعدها .
- د / أسامه أحمد المناعة – جرائم الحاسب الآلى والإنترنت – دراسة تحليلية مقارنة – الطبعة الأولى – دار الأوائل للنشر – عمان – 2001 – ص 276 وما بعدها .

الآلي لا تكتسب صفة الشئ بالمعنى القانونى ، فإنها لا يمكن أن تكون محلاً للتفتيش ، والأمر لا يقتصر فقط على مشروعية التفتيش وإنما أيضاً تمتد المشروعية لضبط البيانات التى توجد فى الوسط الافتراضى [١]، فإن اختلاف الفقه فى تحديد مفهوم الشئ وهل ينصرف إلى الكيانات المعنوية للحاسب الآلى أو الوسط الافتراض أم لا ينحصر حول ثلاثة اتجاهات :-

الاتجاه الأول : وهو الاتجاه الذى يرى أن المقصود بلفظ شئ هو ما كان مادياً أو ملموساً ، ولذا فإن الوسط الافتراضى والبيانات غير المرئية أو الملموسة لا يمكن اعتبارها شيئاً ، ومن ثم ينحصر عنها النص القانونى الذى استعمل مصطلح شئ ، مما يجعل تفتيش الوسط الافتراضى وضبط محتوياته مخالفاً للقانون ، لذلك يقترح هذا الرأى ، بأنه يجبتعديل النصوص الخاصة بالتفتيش ، وذلك بأن يضاف إليها ما يجعل التفتيش يشمل الوسط الافتراضى وضبط المواد المعالجة عن طريق الحاسب الآلى أو بيانات الحاسب الآلى .

وبهذا الاتجاه أخذت بعض التشريعات المقارنة صراحة على أن إجراءات التفتيش تشمل أنظمة الحاسب الآلى ، بما فى ذلك البيانات والمعلومات التى يشملها الوسط الافتراضى وهو البيئة المعلوماتية لجهاز الحاسوب[٢].

الاتجاه الثانى : يرى هذا الاتجاه إلى أن التفتيش والضبط يقتصران على الأشياء بمفهومها المادى ، لأن الغاية من التفتيش هى البحث عن دليل بشأن جريمة وقعت ، ولذا فإن إعمال قواعد التفسير المنطقى تجعل الكيانات المنطقية ما يمكن تفتيشها وضبط ما بها من محتويات[٣].

الاتجاه الثالث : يرى ضرورة إهمال الجدل الدائر حول مصطلح الشئ والعبرة عند هذا الاتجاه هو بالواقع ، فالضبط لا يمكن وقوعه عملياً إلا على أشياء مادية ، ولذلك فإن المشكلة ليست مشكلة مصطلح عبر عنه

---

(١)- د / على محمود حموده – المرجع السابق – ص 21 وما بعدها .

(٢) - ومن التشريعات التى أقرت أن إجراءات التفتيش تشمل أنظمة الحاسب الآلى – قانون اساءة استخدام الحاسب الآلى الانجليزى الصادر 1990 حيث نص على ان " إجراءات التفتيش تشمل أنظمة الحاسب الآلى " وكذلك ما نصت عليه المادة (119 /1-3) من اتفاقية بوادبست 2001 .

((٣ - د / على محمود على حمودة – المرجع السابق – ص 25.

نص القانون ، وإنما هى تتعلق بإمكانية اتخاذ الإجراء ، وترتيباً على ذلك فإن تفتيش الوسط الافتراضى يكون صحيحاً إذا أسفر عن وجود بيانات اتخذت فيما يعد شكلاً مادياً[١].

ويرى الباحث أنه لا يجب ألا تقف من تفسير لفظ شئ على المعنى الحرفى للكلمة ، وإنما يجب تفسير النص تفسيراً منطقياً ، حيث أن المشرع حينما أجاز التفتيش ، إنما قصد إتاحة الفرصة للبحث عن الدليل الذى يساعد فى كشف الحقيقة بشأن جريمة وقعت فعلاً ، ولا شك أن المشرع حينما استعمل لفظ " شئ " لم يكن يقصد بذلك المفهوم الحرفى للكلمة ، وإنما قصد من ذلك هو البحث عن الدليل فى موضعه ، بصرف النظر عما إذا كان موضع البحث شيئاً مادياً أو معنوياً ، وما إذا كانت الأشياء المراد ضبطها مادية أو معنوية ، غاية الأمر أن المشرع وقت وضع النص لم يكن فى ذهنه الوسط الافتراضى لعدم شيوعه آن ذاك ولذلك نحن نميل إلى الرأى المؤيد لفكرة جواز تفتيش الوسط الافتراضى وضبط محتوياته[٢]

ومن ناحية أخرى فإن مخرجات الحاسب الآلى يمكن اعتمادها كدليل جنائى بالحالة التى ضبطت بها ، ما دامت تصلح لطرحها أمام القضاء ، أى حتى وإن ظلت فى الوسط الذى ضبطت فيه فهى ستتمتع بصفة الدليل . ولذلك فإن الوسط الافتراضى من الممكن أن يكون محلاً للتفتيش ، كما لا يمكن أن تكون محتوياته محلاً للضبط ، ولا يفترض على ذلك بأن القانون يوجب تحريز المضبوطات ، وهو ما لا يتفق وطبيعة المخرجات الرقمية ، فهذا ليس صحيحاً من وجهة نظرنا ذلك أن المخرجات يمكن تحريزها بطريقة تتفق وطبيعتها ، بوضعها فى حالة فصلها عن مصدرها – فى قرص مضغوط **CD** ، وتحريز هذا القرص

---

(١) - ومن التشريعغات التى أخذت بهذا الاتجاه قانون اللإجراءات الألمانى فى القسم (94) حيث نص على أن " الأدلة المضبوطة يجب ان تكون ملموسة ، ولذلك فإن البيانات إذا تمت طباعتها تعد أشياء ملموسة وبالتالى يمكن ضبطها " أنظر د / هلالى عبداللاه أحمد – تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى – الطبعة الأولى – دار النهضة العربية 1979 - ص 202.

(٢)- أنظر فى هذا المعنى د / على محمود على حمودة – المرجع السابق – ص 25.

بالطريقة المنصوص عليها قانوناً ، كما يمكن تحريزها إذا كانت فى شكل نصوص بعد طباعتها وتحويلها للشكل المادى الملموس[١].

ونخلص مما تقدم أن الكيان المعنوى أو الوسط الافتراضى ، والبيانات المتحصلة منه ينطبق عليها لفظ الشئ ، ولذا فإن تفتيش ذلك الوسط يعد صحيحاً وفقاً للقانون ، كما تعد البيانات الموجودة بذلك الوسط أشياء مما يصلح ضبطها[٢].

ثانيا: شروط الدليل الإلكترونى المستمد من التفتيش :

إن الأدلة الرقمية أو الإلكترونية ، كما سبق بيانه إما أن تكون مخرجات ورقية يتم انتاجها عن طريق الطابعات ، أو الراسم ، وإما أن تكون مخرجات غير ورقية أو أن تكون الكترونية كالأشرطة والأقراص الممغنطة واسطوانات الفيديو وغيرها من الأشكال الغير التقليدية أو تتمثل فى مخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به ، أو الإنترنت بواسطة الشاشات أو وحدة القرص المرئى [٣]

ويكون الدليل الإلكترونى أو الرقمى باطلاً إذا تم الحصول عليه عن طريقة مخالفة القانون ، وإذا كان الدليل الباطل هو الدليل الوحيد فلا يصح الاستناد عليه فى إدانة المتهم ، وإذا ما شاب التفتيش الواقع على نظم الحاسوب عيب فإنه يبطله ، والتفتيش الذى يقوم به المحقق بغير

---

(١)- تنص المادة 56 من قانون الإجراءؤا الجنائية المصرى على أنه توضع الأشياء والأوراق التى تضبط فى حرز مغلق وتربط كلما أمكن وتختم ويكتب على شريط ويشار إلى الموضوع الذى حصل الضبط من أجله .

(٢)- وقد أكدت بعض التشريعات الحديثة هذا الاتجاه بحيث أصبحت المكونات المعنوية من ضمن الأشياء التى تصلح لأن تكون محلاً للتفتيش والضبط فالتشريع الأمريكى على سبيل المثال نص فى المادة 34 من القواعد الفيدرالية الخاصة بالاجراءات الجنائية بعد تعديلها بمد نطاق التفتيش ليشمل ما يشمل أجهزة الحاسب الآلى ، وأوعية التخزين والبريد الإلكترونى والصوتى والمنقول عن طريق الفاكس .

- وكذلك اتفاقية بودابست وهى الاتفاقية الأوربية للجرمية المعلوماتية أكدت فى المادة 19 منها على ضرورة تبنى الدول التدابير والإجراءات التشريعية التى تخول السلطات المختصة الولج للبيئة المعلوماتية . أنظر د / هشام فريد رستم – المرجع السابق – ص 80 وما بعدها.

(٣)- أنظر د / هلالى عبداللاه أحمد – حجية المخرجات الكمبيوترية فى الإثبات الجنائى – الطبعة الأولى – دار النهضة العربية 1997 – ص 14 – 22.

الشروط التى نص عليها القانون يعتبر باطلاً بطلاناً مطلقاً ولا يجوز التمسك بما ورد فى محضر التفتيش كما لا يجوز للمحكمة أن تعتمد عليه فى حكمها ، ويشترط لمشروعية الدليل الإلكترونى أو الرقمى توافر الشروط الآتية :

١ - ضرورة الحصول على الدليل الإلكترونى أو الرقمى بطريقة مشروعة :

أكدت الدساتير المدنية على صيانة كرامة الإنسان وحماية حقوقه وهذا ما أكده الدستور المصرى المعدل فى نصوصه فقد نص فى المادة (57) منه على (أن للحياة الخاصة حرمة ، وهى مصونة لا تمس ، وللمراسلات البريدية ، والبرقية والإلكترونية ، والمحادثات الهاتفية ، وغيرها من وسائل الاتصال حرمة ، وسريتها مكفولة ، ولا تجوز مصادرتها أو الاطلاع عليها ، أو رقابتها إلا بأمر قضائى ولمدة محدودة وفى الأحوال التى بينها القانون ....)

وأكد فى نص المادة (58) كذلك بأن (للمنازل حرمة ، وفيما عدا حالات الخطر أو الاستغاثة لا يجوز دخولها ، ولا تفتيشها ، ولا مراقبتها أو التصنت عليها إلا بأمر قضائى مسبب،يحدد المكان، والتوقيت، والغرض منه وذلك كله فى الأحوال المبينة فى القانون ....)

فهذه النصوص الواردة بالدستور تفرض على المشرع عند وضع قواعد الإجراءات الجنائية الالتزام بها وعدم الخروج عنها ، وكذلك فإن إجراءات الحصول على الأدلة الجنائية يجب أن تكن ضمن الإطار العام الذى حدده الدستور ، وإلا فإن الدليل المستمد بطريق مخالف للأحكام الواردة فى الدستور يكون باطلاً بطلاناً مطلقاً لتعلقه بالنظام العام ويجوز لكل ذى مصلحة التمسك به كما أن للمحكمة أن تقضى به من تلقاء نفسها [١] ، ونرى ضرورة أن يقوم المشرع المصرى بتشريع نصوص إجرائية تتكفل بحماية الحياة الخاصة المخزونة فى الحاسوب والإنترنت ، بحيث تمنع اقتحام الملفات الشخصية بدون سند قانونى ، حماية للحقوق

---

(١)- أنظر فى مشروعية الدليل المستمد من التفتيش د / رمزى رياض عوض – مشروعية الدليل الجنائى فى مرحلة المحاكمة وما قبلها – دار النهضة العربية – 1997 – ص 85.

- د / أحمد عوض بلال – قاعدة استبعاد الأدلة المتحصلة بطريق غير مشروعة فى الإجراءات الجنائية المقارنة – دار النهضة العربية – 1994 – ص 16 وما بعدها.

والحريات الفردية التى كفلها الدستور المصرى بالإضافة إلى الموثيق الدولية .

فالدليل الإلكترونى أو الرقمى حتى يكون له قيمة فى الإثبات لا بد أن يتم الحصول عليها من خلال إجراءات مشروعة تتفق مع صحيح القانون . والأدلة الجنائية التى يتم الحصول عليها بطرق غير مشروعة يجب أن تكون مستبعدة سواء كانت تقليدية أم أدلة حاسوب أم أدلة إنترنت[١]ومن أمثلة الطرق غير المشروعة التى يمكن أن تستخدم فى الحصول على الأدلة الناتجة عن الجرائم المعلوماتية الإكراه المادى والمعنوى فى مواجهة المتهم المعلوماتى من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى دائرة حل التشفير أو الوصول إلى ملفات البيانات المخزنة ، وكذلك التحريض على الغش أو التزوير المعلوماتى أو التجسس المعلوماتى والاستخدام غير المصرح به للحاسوب والتصنت والمراقبة الإلكترونية عن بعد[٢] ، وتعد من الطرق غير المشروعة أيضاً استخدام التدليس أو الغش أو الخداع فى الحصول على الأدلة الإلكترونية[٣].

لذلك لا بد أن يكون الحصول على الدليل الإلكترونى جاء من خلال إجراءات مشروعة تحترم فيها الحريات وتؤمن فيها الضمانات التى رسمها القانون[٤].

٢ - يجب أن تكون الأدلة الإلكترونية غير قابلة للشك أى يقينية :

---

(١)- د / هلال عبداللاه أحمد – حجية المخرجات الكمبيوترية فى الإثبات الجنائى – الطبعة الأولى – دار النهضة العربية – 1997 – ص 137.

(٢)- د / جميل عبدالباقى الصغير – أدلة الإثبات الجنائى والتكنولوجيا الحديثة – دراسة مقارنة – دار النهضة العربية – 2001 – ص 111.

(٣)- وقد تضمن قانون الشرطة والإثبات الجنائى الإنجليزى 1984 تحديد الشروط الواجب توافرها فى مخرجات الحاسوب لكى تقبل أمام القضاء ، وتشمل كذلك توجيهات فى كيفية تقدير قيم أو وزن البيان المستخرج عن طريق الحاسوب فأوصت المادة (11) منه على مراعاة كل الظروف عند تقديم البيانات الصادرة عن الحاسوب والمقبولة فى الإثبات طبقاً للمادة (69) من القانون نفسه .
- انظر د / على حسن الطوالية – مشروعية الدليل المستمد من التفتيش الجنائى – دراسة مقارنة – ص 17 .

(٤)- أنظر د / جميل عبدالباقى الصغير – أدلة الإثبات – المرجع السابق – ص16 .

يشترط فى الأدلة المستخرجة من الحاسوب والإنترنت أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة ، ذلك لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضى إلى حد الجزم واليقين ، ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الإلكترونية ، والمصغرات الفيلمية ، وغيرها من الأشكال الإلكترونية التى تتوافر عن طريق الوصول المباشر أم كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به أو على الطرفيات وهكذا يستطيع القاضى من خلال ما يعرض عليه من مخرجات إلكترونية ، وما ينطبع فى ذهنه من تصورات واحتمالات بالنسبة لها ، أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه .

وقد اشترط قانون البوليس والإثبات الإنجليزى 1984 متى تتحقق يقينية الأدلة الإلكترونية أن تكون البيانات حقيقية وناتجة عن الحاسوب بصورة سليمة(١).

ومن التشريعات المقارنة التى أكدت على يقينية الأدلة الإلكترونية بعض قوانين الولايات فى أمريكا ، حيث أكدت على أن النسخ المستخرجة من البيانات التى يحتويها الحاسوب تعد من أفضل الأدلة المتاحة لإثبات البيانات ، وبالتالى يتحقق مبدأ اليقين لهذه الأدلة(٢).

---

(١)– Naughan Bevan Ken Lidstone – Aguide to the police and criminal Evidence Act 1984 – Bulterworthe – London – 1985 – p. 497.

(٢) – كذلك نص قانون الإجراءات الجنائية الشيلى فى المادة 221 على قبول السجلات الممغنطة للحاسوب وكذلك النسخ الناتجة عنها ، ومعنى ذلك أن هذه السجلات وصورها تحقق اليقين المنشود لإصدار الأحكام الجنائية ، كما يتحقق هذا اليقين أيضاً عن طريق تقارير الخبراء الصادرة فى عناصر معالجة البيانات .

- كما يقرر الفقه اليابانى قبول الأدلة المستخرجة من الحاسوب التى تم تحويلها إلى الصورة المرئية سواء أكانت هى الأصل أم كانت نسخاً مستخرجة عن هذا الأصل وذلك استناداً على الاستثناءات التشريعية المنصوص عليها فى المادة (323) من قانون الاجراءات الجنائية اليابانى ، وبالتالى يتحقق اليقين الذى يبنى عليه الحكم الجنائى ، وكذلك يتحقق اليقين لهذه المخرجات من خلال التقارير التى يقدمها الخبراء . أنظر د / هلالى عبداللاه أحمد – حجية المخرجات – المرجع السابق – ص 96.

وتنص القواعد الفيدرالية على أن الشرط الأساسى للتوثيق أو التحقق من صحة أو صدق الدليل ، كشرط سبق لقبوله ، هو أن يفى بأمارة أو بينة كافية لأن تدعم اكتشاف أو الوصول إلى الأمور التى تتصل بالموضوع بما يؤيد الادعاءات أو المطالبة المدعى بها [١]. وقد أكدت محكمة النقض المصرية بأن الأحكام فى المواد الجنائية يجب أن تبنى على الجزم واليقين لا على الظن والاحتمال فإذا كانت المحكمة لم تنته من الأدلة التى ذكرتها إلى الجزم بوقوع الجريمة من المتهم ، بل رجحت وقوعها منه فحكمها بإدانته يكون خاطئاً[٢].

٣ - إمكانية مناقشة الأدلة الإلكترونية المستخرجة من الحاسوب :

يعنى مبدأ مناقشة الدليل الجنائى بصفة عامة أن القاضى لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التى طرحت فى جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى [٣]وهذا يعنى أن الأدلة المتحصلة من جرائم الحاسوب والإنترنت سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب ، أم كانت بيانات مدرجة فى حاملات البيانات ، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فيلمية ، كل هذه ستكون محلاً للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة ، وعلى ذلك فإن كل دليل يتم الحصول عليه من خلال بيئة تكنولوجيا المعلومات ، يجب أن يعرض فى الجلسة ليس من خلال ملف الدعوى فى التحقيق ، لكن بصيغة مباشرة أمام القاضى ، وهذه الأحكام تنطبق على كافة الأدلة المتولدة عن الحاسبات الآلية ، وأيضاً بالنسبة لشهود الجرائم المعلوماتية الذين قد سبق أن سمعت أقوالهم فى

---

(١) – د / معبد عبداللطيف حسن – الإثبات فى جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت – الجرائم الواقعة فى مجال تكنولوجيا المعلومات – دار النهضة العربية – 1999 – ص 159.

(٢)- نقض 15 ابريل 1946 – مجموعة القواعد القانونية – ج 7 – رقم 139 – ص 134.

(٣)- أكد المشرع المصرى على هذا المبدأ فى المادة 302 إجراءات – وكذلك أنظر المادة (2/147) اجراءات أردنى ، والمادة (175 ، 176) إجراءات سورى والمادة 169 إجراءات سويسرى والمادة (151) إجراءات كويتى .

التحقيق الابتدائى ، فإنه يجب أن يعيدوا أقوالهم مرة أخرى من جديد أمام المحكمة[١].

كذلك فإن خبراء الأنظمة المعلوماتية على اختلاف تخصصاتهم [٢] ،ينبغى أن يمثلوا أمام المحاكم لمناقشتهم ، أو مناقشة تقاريرهم التى خلصوا إليها لإظهار الحقيقة وكشفاً للحق .

والأدلة الجنائية الإلكترونية لكونها معدة بعمليات حسابية دقيقة لا بد أن يتم حفظها آلياً بأسلوب علمى يتفق مع التقنية المعلوماتية الحديثة[٣] ، ويثور التساؤل حول إمكانية ضبط الأدلة الإلكترونية أو الرقيمة ومشروعيتها إذا كانت النهاية الطرفية للنظام المعلوماتى فى منزل آخر غير منزل المتهم ؟ فهليمكن تفتيشه فى هذه الحالة ؟ لقد حسمت بعض القوانين هذه المسألة وأجازت التفتيش فى هذه الحالة ، كالقانون الهولندى حيث أجازت المادة (25) منه على إمكانية امتداد تفتيش المسكن إلى تفتيش نظام آلى موجود فى مكان آخر بهدف التوصل إلى بيانات يمكن أن تفيد بشكل معقول فى كشف الحقيقة ، وبالتالى أجاز المشرع للقائم بالتفتيش سلطة تسجيل البيانات الموجودة فى النهاية الطرفية التى يتصل بها النظام المعلوماتى دون التقيد بالحصول على إذن مسبق بذلك من المحقق المختص . إلا أن هذه السلطة غير مطلقة بل هى مقيدة بثلاثة قيود هى [٤]:

---

(١)- الشاهد المعلوماتى : هو الفنى صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الذى تكون لديه معلومات جوهرية لازمة لولوج المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضى التنقيب عن أدلة الجريمة داخله – أنظر د / هلالى عبداللاه أحمد – التزام الشاهد بالاعلام فى الجرائم المعلوماتية – دراسة مقارنة – القاهرة – 2000 – ص 23 وما بعدها .

(٢)- أنظر د / محمد فهمى طلبة وآخرون – دااارة المعارف الحاسب الإلكترونى – مجموعة كتب دلتا – مطابع المكتب المصرى الحديث – 1991 – ص 31 وما بعدها.

(٣)- أنظر د / محمد الأمين البشرى – الأدلة الجنائية الرقمية – مفهومها ودورها فى الإثبات – المجلة العربية للدراسات الأمنية والتدريب – المجلد 17 – العدد 33 – الرياض – 2002 – ص 128 – 129.

(٤) –أنظر د / عفيفى كامل عفيفى – جرائم الحاسب الآلى وحقوق المؤلف والمصنفات الفنية – دراسة مقارنة -0 منشأة المعارف – 2000 – ص 347.

1- ألا تكون النهاية الطرفية المتصل بها الحاسوب موجودة ضمن إقليم دولة أخرى حتى لا يؤدى الاتصال بها إلى انتهاك لسيادة الدولة الإقليمية .
2- أن تحتوى النهاية الطرفية المتصل بها الحاسوب على بيانات ضرورية كافية لظهور الحقيقة .
3- أن يحل قاضى التحقيق محل الشخص صاحب المكان الذى ينبغى تفتيشه بصورة مؤقتة(١)

ويبقى السؤال الأخير ، ما إذا كانت النهاية الطرفية فى إقليم دولة أخرى ، فهل يمكن ضبط الدليل الإلكترونى فى هذه الحالة ، نلاحظ أن المادة (25/أ) من قانون الحاسوب الهولندى استثنت هذه الحالة ، فيمكن الحصول على الأدلة حتى ولو كانت فى إقليم دولة أخرى بواسطة الاتفاقيات الدولية الخاصة بالتعاون الأمنى والقضائى والخاصة بالتفتيش وضبط الأدلة(٢).

وأخيراً فإن متحصلات الجريمة المعلوماتية التى يتم ضبطها يجب أن تعرض على القاضى المختص بكافة مفرداتها وعناصرها(٣) ، ذلك لأن حيادية القاضى توجب عليه أن لا يقيم قضاءه إلا على ما طرح أمامه ، وكان موضوع الفحص والتحقيق والمناقشة . ويترتب على مناقشة أدلة الحاسوب نتيجتان : الأولى : عدم جواز أن يقضى القاضى فى الجرائم المعلوماتية بناء على معلوماته الشخصية ، والثانية : ضرورة التأهل التقنى والفنى للقضاة لمواكبة المناقشة العلمية لأدلة الحاسوب والإنترنت

---

(١) – راجع المادتين 78 ، 18 من قانون الإجراءات الجنائية الليبى .
(٢)- أنظر د / على حسن الطواله – التفتيش الجنائى على نظم الحاسوب والإنترنت – دراسة مقارنة – علام الكتاب الحديثة – 2004 – ص 14 ، 17.
- وفى ظل تبادل المعلومات والمساعدات فيما يتعلق بالجريمة المعلوماتية أكدت إتفاقية بوادبست فى المادة (1/25) بقولها تقوم الدول الأطراف بالاتفاقية بتقديم المساعدات المتبادلة لبعضها البعض إلى أقصى حد ممكن وذلك للأغراض الخاصة بعمليات التحقيق أو الإجراءات المتعلقة بالجرائم التى لها علاقة بنظم وبيانات الكمبيوتر أو بالنسبة لتجميع الأدلة الخاصة بالجريمة فى شكل قانونى) .
(٣)- أنظر د / هلالى عبداللاه أحمد – حجية المخرجات الإلكترونية – المرجع السابق – ص 22

بشكل يتماشى مع التقارير التى تم تقديمها فى المؤتمرات الخاصة بجرائم الحاسوب والإنترنت .

المطلب الثانى

مشروعية الأدلة الإلكترونية المتحصلة عن طريق الخبرة

لقد تعاظم دور الإثبات العملى بالدليل مع ظهور الجرائم المعلوماتية (الرقمية) وضرورة استقاف الآلة الرقمية المطلوبة للإثبات فى هذه الجرائم ، وكشف أنماط الجرائم المرتكبة باستخدام الحاسب الآلى ، وهو الدور الذى يطلع به الخبراء القضائيون ، وأصبح إنشاء المعامل الجنائية الرقمية مطلباً ملحاً لفحص الأدلة الرقمية ، ولتقييم عملية الإثبات الرقمى ، وتحرير الجرائم فى نطاق ما يعرف باسم نظم الخبرة الأمنية[١].

ومما لا شك فيه أن الخبرة التقنية فى مجال الجرائم المعلوماتية أو الإلكترونية تلعب دوراً هاماً ومؤثراً فى الحصول على الأدلة الرقمية والإلكترونية بل اصبحت ضرورية وحتمية فى إثبات الجرائم الإلكترونية ، وسوف نوضح دور الخبرة التقنية فى مجال إثبات الجرائم الإلكترونية من خلال ما يلى :

أولا: الخبرة التقنية فى مجال الجرائم المعلوماتية وأهميتها.

تقوم الخبرة التقنية فى الوقت الحاضر بدور بارز فى عملية الإثبات الجنائى والقضائى نظراً للتطور الهائل الذى أحدثته تكنولوجيا الاتصالات والمعلومات ، فالخبرة ما هى إلا إجراء يتعلق بموضوع يتطلب الإلمام بالمعلومات الفنية لإمكاناستخلاص الدليل منها [٢] ، او هى الاستشارة الفنية التى يستعين بها المحقق أو القاضى فى مجال الإثبات الجنائى لمساعدته فى تقدير المسائل الفنية التى يحتاج تقديرها إلى مساعدة

---

(١) - د / ممدوح عبدالحميد عبدالمطلب – البحث والتحقيق الجنائى فى جرائم الكمبيوتر والإنترنت – دار الكتب الوطنية – 2006 – ص 8.

(٢)- د / مأمون سلامة – الإجراءات الجنائية فى التشريع المصرى – دار الفكر العربى – 1997 – ص645 .

فنية ، أو إدارة لا تتوافر لدى عضو السلطة القضائية المختص بحكم عمله وثقافته [١] ، كما عرفها البعض بأنها الاستشارة الفنية التى يستعين بها القاضى أو المحقق لمساعدته فى تكوين عقيدته نحو المسائل التى يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لديه ، والخبرة الفنية تعتبر إجراء من إجراءات التحقيق بحسب الأصل [٢] والخبرة كدليل فى الإثبات تنصرف إلى رأى الخبير الذى يثبتها فى تقاريره ، وبما أن تقرير الخبير يعتبر من الأدلة الفنية ، وأن إجراء ندب خبير هو من إجراءات جمع الأدلة[٣] والخبير هو كل شخص له دراية بمسألة من المسائل ، وقد يستدعى التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا يشعر المحقق بتوافرها فى نفسه ، فيمكنه أن يستشير فيها خبيراً ، كما هو الحال فى تقرير الصفة التشريحية فى جرائم القتل، أو تحليل المادة المطعومة فى جريمة تسمم ، أو فحص لخطوط الكتابة المدعى بتزويرها[٤].

وتبدو أهمية الخبرة فى أنها تنير الطريق للقاضى الذى يهتدى به لتحقيق العدالة خاصة فى المجال الجنائى ، فقد أجاز قانون الإجراءات الجنائية المصرى فى المادة (29) منه على الاستعانة بالخبراء لكل من مأمورى الضبط القضائى والنيابة العامة وقاضى التحقيق ، وبالتالى لم يحظر قانون الإجراءات الجنائية على المحاكم أن تستعين بالخبراء ، لذلك يجوز دائماً للمحكمة تعيين الخبراء سواء من تلقاء نفسها أو بناء على طلب الخصوم

وإذا كان للخبرة تلك الأهمية فى الجرائم التقليدية ، فإن أهميتها تزداد وتصبح ضرورية وحتمية فى إثبات الجرائم الإلكترونية .

ومنذ ظهور الجرائم المعلوماتية أو الإلكترونية تستعين الشرطة وسلطات التحقيق أو المحكمة بأصحاب الخبرة الفنية والتقنية المميزة فى

---

(١)- د نبيل عبدالمنعم جاد – أسس التحقيق والبحث الجنائى العلمى – كلية الشرطة – ص 196.

(٢)- د / آمال عبدالرحيم عثمان – الخبرة فى المسائل الجنائية – 1964 – جامعة القاهرة – ص 28 وما بعدها.

(٣)- أنظر د / فوزية عبدالستار – شرح قانون الإجراءات الجنائية – دار النهضة العربية – 1986 – ص 176 .

(٤)- د أحمد فتحى سرور – الوسيط فى شرح الإجراءات الجنائية – 1991 – ص 457.

مجال الحاسب الآلى ، بغرض كشف غموض الجريمة ، لتجميع أدلتها والتحفظ عليها ، او مساعدة المحقق فى إجلاء جوانب الغموض فى العمليات الإلكترونية الدقيقة ذاتالصلة بالجريمة محل التحقيق . ويجوز طبقاً للتشريع المصرى لمأمورى الضبط القضائى اسلاتعانة بالخبراء وتحليفهم اليمين إذا خيف ألا يستطيع فيما بعد سماع شهادتهم باليمين [١].

وأهمية الاستعانة بخبير فى مجال الجرائم الإلكترونية قد تعجز الشرطة عن كشف غموض الجريمة ، فقد تعجز هى أو أجهزة التحقيق عن جمع الأدلة حول الجريمة ، وقد تدمر الدليل أو تمحوه بسبب الجهل أو الإهمال عند التعامل معه [٢] ، ولذلك لا بد من الاهتمام بالخبرة التقنية لدورها البارز والمهم فى الحصول على الأدلة الإلكترونية أو الرقمية .

ثانيا: ضرورة توافرشروط خاصة فى الخبير المعلوماتى.

إن الخبرة التقنية فى مجال الجرائم المعلوماتية أو الإلكترونية لا تشمل بالضرورة تلك النوعية من الخبرة الدراسية التى (رغم عدم وجود نص يفيد القضاء بضرورة الاستعانة بها تحديداً) . وينبغى التقرير بأن دراسات الحاسوب والإنترنت لا ترتبط بمنهج دراسى أو بحثى معين أو حتى مدة زمنية يقضيها المرء دارساً فى الجامعات والمعاهد المتخصصة ، وإنما ترتبط بمهارات خاصة وأفضلية استخدام الحاسوب والإنترنت والتعامل مع تقنية المعلومات[٣].

لذلك من الممكن أن يكون أمهر مبرمجى نظم التشغيل لم يتجاوز تحصيله العلمى المرحلة الثانوية ، وذات الأمر ينطبق على عتاة الهكرة ومحترفى الأنظمة فإن أعمارهم لا تتجاوز مرحلة التعليم الثانوى والسنوات الجامعية الولى فى أحسن الأحوال ، ومع الوقت تتطور قدراتهم وإمكاناتهم ما لم يردعها ... القانون ومن هذا المنطلق تتميز الخبرة فى مجال تكنولوجيا المعلومات عن الخبرة فى أى نوع آخر من الفروع التى يمكن أن تكون محلاً للخبرة أمام القضاء . ولذلك تقتضى فاعلية الخبرة ضرورة الجمع بين التعمق لى كل من الدراسة العلمية والنظرية

---

(١)- أنظر نص المادة (29 / 2) إجراءات مصرى ، والمادة 40 من قانون الإجراءات الإماراتى .

٢Robet taylor ; computer crine0in criminal investigation edited by charpes . swanson , n, chanmeleion and territory hill , ine .5editian1992 p 1

(٣)- انظر د / عمر محمد بن يونس – الدليل الرقمى – المرجع السابق – ص 106.

والممارسة العملية للتخصص العلمى والنظرى ، وكذا متابعة مستمرة للتطورات التى تلحق بفروع التخصص ، غير أن ذلك ليس شرطاً لازماً فى بعضفقد يقتصر دور الخبير على مجرد الخبرة العلمية فى فرع التخصص دون أن يكون هناك رضصيد من الدراسة العلمية والنظرية وهو الأمر الذى تلاحظه فى مجالات الخبرة فى الفروع المهنية المختلفة[١]منها فى مجال الحاسب الآلى ، حيث يتعين عفى خبراء الحاسب الآلى المنتدبين للتحقيق أن تتوافر لديهم القدرة الفنية والإمكانات العلمية فى المسألة موضوع الخبرة ، ولا يكفى فى ذلك حصول الخبير على شهادة علمية ، بل يجب مراعاة الخبرة العملية لأنها هى التى تحقق الكفاءة الفنية . ولذلك لا وجود لخبير لديه معرفة متعمقة فى سائر أنواع الحاسبات وبرمجياتها وشبكاتها ، أو لديه القدرة على التعامل مع كل أنواع الجريمة المرتكبة عن الإنترنت[٢].

وتتطلب طبيعة الجرائم الإلكترونية توافر شروط خاصة فى الخبير الذى يندب لبحث مسائل فنية وعلمية تتعلق بالأدلة الإلكترونية أو الرقمية وذلك على النحو التالى :

1- الإلمام بتركيب الحاسب الآلى وصناعته وطرازه ونظم تشغيله الرئيسية والفرعية ، والأجهزة الطرفية الملحقة به ، وكلمات المرور أو السر وأكواد التشفير .

2- طبيعة البيئة التى يعمل فى ظلها الحاسب من حيث تنظيم ومدى تركيز او توزيع عمل المعالجة الآلية ، وتحديد أماكن التخزين والوسائل المستخدمة فى ذلك .

3- قدرة الخبير على إتقان مأموريته دون أن يترتب على ذلك أعطاب أو تدمير الأدلة المتحصلة من الوسائل الإلكترونية .

4- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة أو المحافظة على دعاماتها لحين القيام بأعمال الخبرة بعير أن

---

(١)- د / محمد فاروق عبدالحميد – القواعد الفنية الشرطة للتحقيق والبحث الجنائى – الطبعة الأولى – اكاديمة نايف العربية للعلوم الأمنية – الرياض – 1999 – ص 286.

(٢)- أنظر د / عبدالفتاح بيومى حجازى – مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت – الطبعة الأولى – دار الفكر الجامعى – الاسكندرية – 2006 – ص 138.

يلحقها تدمير أو إتلاف ، مع إثبات أن المخرجات الورقية لهذه الأدلة تطابق ما هو مسجل على الحاسب أو النظام أو الشبكة[١].

بالإضافة إلى ما سبق يتعين على الخبير فى الجرائم الإلكترونية التنسيق مع المحقق الجنائى قبل محاكمة الجانى فى هذه الجريمة ، على أن يشمل اللقاء كافة الخبراء الذين ساهموا مع سلطات الضبط أو التحقيق فى تلقى البلاغ أو إجراءات الضبط والتفتيش أو فحص البرامج وجمع الأدلة الجنائية على أن يتم فى هذا اللقاء حصر الأدلة المتوفرة وترتيبها وفقاً لأهمية كل دليل أو بينة أو قرين .

وإذا كانت المحكمة تمتلك سلطة تقديرية بالنبسبة لتقرير الخبير الذى يرد إليها ، إلا أن ذلك لا يمتد إلى المسائل الفنية فلا يجوز بلها تقديرها إلا بأسانيد فنية تخضع للتقدير المطلق لمحكمة الموضوع . ومن ثم لا تستطيع المحكمة أن تفندها وترد عليها إلا بأسانيد فنية قد يصعب عليها أن تشق طريقها فيها إلا عن طريق خبرة فنية أخرى[٢].

أساليب عمل الخبير المعلوماتى لاستخلاص الأدلة الإلكترونية :

بداية ينعقد الاختصاص للخبير التقنى أو المعلوماتى فى أحد شكلين : إما ان يكون مكلفاً بذاك قبل إحدى جهات التحقيق (الأصلية أو الاستثنائية) ، وإما ان يقوم بعمله بناء على أمر من محكمة الموضوع ، وفى الحالتين يعد الأمر الصادر عليه قضائياً . فإذا لم تتوافر الصفة القضائية للأمر الصادر إلى الخبير فإن ما ينتج من دليل عند عمل الخبير يعد دليلاً غير مشروع ومن ثم يحق لمحكمة الموضوع ألا تأخذ ببه .

وهناك حالة ثالثة يمكن أن تضاف إلى ما سبق وهى التى يشير إليها القانون لحق المتهم (فقط) فى الاستعانة بخبير استشارى حيث يجوز له استخدامه وقتما يشاء أثناء التحقيق [٣]. وطبقاً للتشريع المصرى فإن المتهم يمكنه استخدام هذا الحق فى أية مرحلة من مراحل التقاضى وكذلك يمكن أن يستخدم هذا الحق ولو لم يكن هناك وجه لإقامة الدعوى أو تم حفظها ، وموضوع الخبير الاستشارى يظل من حقوق الدفاع

---

(١)- د / عبدالفتاح بيومى حجازى – الدليل الجنائى والتزوير فى جرائم الكمبيوتر – دراسة متعمقة فى جرائم الحاسب الآلى والإنترنت – 2009 – ص98.

(٢)- أنظر د / على محمود على حمودة – المرجع السابق – 2 53.

(٣)- د / مأمون سلامة – الإجراءات الجنائية فى التشريع الليبى – الطبعة الثانية – ليبيا – 2000 – ص 608.

الجوهرية التى يملكها المتهم لا يجوز حرمانه منها شريطة ألا يترتب على الاستعانة بالخبير الاستشارى تعطيلاً فى سير الدعوى[١].

وللخبير التقنى فى سبيل تحرى الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها وهو فى إطار القيام بعمله أن يتسخدم الأساليب لالعلمية التي قوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب ما يكون رفضها لها مسبباً بشكل منطقى وإلا تعرض حكمها للنقض .

وهناك أسلوبان لعمل الخبير التقنى أو المعلوماتى :

الأول : القيام بتجميع وتحصيل لمجموعة المواقع التى تشكل جريمة فى ذاتها ، كما هو الشأن فى التهديد أو النصب أو السب أو جرائم النسخ وبث صور إباحية فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعارة والرقيق ودعارة الأطفال وغيرها . ثم القيام بعملية تحليل رقمى لها لمعرفة كيفية إعدادها البرمجى ونسبتها إلى مسارها الذى أعدت فيه ، وتحديد عناصر حركتها ، وكيف تم التوصل إلى معرفتها ، ومن ثم التوصل فى النهاية إلى معرفة بروتوكول الإنترنت **IP** الذى ينسب إلى جهاز الحاسوب الذ صدر عنه هذه المواقع .

الثانى : القيام بتجميع وتحصيل لمجموعة من المواقع التى لا يشكل موضوعها جريمة فى ذاته ، وإنما تؤدى حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم . كما هو الحال فى المواقع التى تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية التى تناسب وزن الإنسان بإدعاء أنه إذا تتبع التعلميات الواردة فيها فلن يصاب الشخص بحالة إدمان ، وأيضاً كيفية زراعة المخدرات بعيداً عن أعين الناس (ويطلق عليه فى هذه الحالة الفضولى) وأيضاً كيفية إعداد القنابل وتخزينها ، وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها[٢] وكذلك القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بالدخول من مكان ثابت ، ومثل هذا الأمر جائز الحدوث كما لو كان مرتكب الجريمة مشتركاً لدى مزود فى مدينة مختلفة

---

(١)- أنظر نص المادة 88 من قانون الإجراءات الجنائية المصرى - ونص المادة 73 إجراءات ليبى .

(٢) - POTRICK S. CHEN – An Automatic system for collection crine in formation on the internet – 31 october 2000 – Journal of information low and technology available on line in Jan 2001 at http//elj. Worwick .ac .uk / jit00 – 3 / chen .htnl.

عن تلك التى يقيم فيها بالولوج إلى الإنترنت من محل إقامته . وهذا الأخير من الدفوع التى تلزم محكمة الموضوع بالرد عليها . ويتم فى إطار تصنيف المواقع المذكورة استخدام برمجيات متطورة مهمتها الكشف عن مثل هذه المواقع باستمرار ومعرفة الجديد فيها .

ولما كانت عملية تجميع الأدلة العلمية الجنائية فى الجرائم المعلوماتية أو الرقمية تعد من أهم وأصعب الأمور التى تواجه عملية الإثبات الجنائى لذا كان لزاماً أن يتم اللجوء إلى الخبير المعلوماتى والتقنى ، ويكون متخصص لاستقاف الدليل العملى الفنى الجنائى .

والخبير المعلوماتى هو الخبير المتخصص والمدرب على معالجة جميع أنواع الأدلة الرقمية وحصرها وتحليلها[١].

ويرى بعض المتخصصين أن عملية تجميع الأدلة الرقمية فى الجرائم الرقمية التى تتم عبر الشبكة العالمية (الإنترنت) تتم عبر ثلاثة مراحل[٢]:

المرحلة الأولى : مرحلة تجميع المعلومات المخزنة لدى الطرف مقدم الخدمة (**third – party services**) حيث تتبع الحاسبات الخوادم التى دخل المجرم منها ومحاولة إيجاد أى أثر له .

المرحلة الثانية : مرحلة المراقبة (**surveillance – prospective**) من خلال هذه المرحلة يتم مراقبة المجرم لأن هناك حقيقة شبه مؤكدة بأن المجرم لا بد وأن يعود أو يحوم حول مسرح جريمته ، وتنوع أساليب مراقبة الحاسب الآلى منها على سبيل المثال :

- استخدام برامج مراقبة يمكن تحميلها للبحث عن المعلومات المشتبه فيها وحصر تسجيل بيانات كل دخول وخروج بالموقع .
- استخدام ما يعرف بالحشرات (**bugs**) وهى أجزاء توضع فى الحاسب لمراقبته .
- استخدام كاميرات مراقبة لشاشة الحاسب الآلى معدة للاستخدام التجارى وأبسط الطرق لمراقبة الحاسب الآلى هى الدخول لمكان وجوده وزرعه .

---

(١)- أنظر د / محمد أمين البشرى – التحقيق فى الجرائم المستحدثة – المرجع السابق – ص 243.

(٢)- Orin S. Kerr , digital evidence and the new criminal procedure . coeumbia low review (vol – 105 : 279) – 2005 .

المرحلة الثالثة : ضبط الأجهزة المشتبه فيها وفحصها فحصاً فنياً وشرعياً ، حيث يبدأ فى هذه المرحلة عمل الخبير المعلوماتى فى فحص النظام الحاسوبى المشتبه فيه بمكوناته المادية ومكوناته البرمجية ، سعياً لاستقاف الدليل المادى لتقديمه لجهة التحقيق أو الحكم ، لتقرير مدى وقوع الجريمة باستخدام النظام المضبوط من عدمه .

ولتقرير إدانة المتهم أو تأكيد براءته ، وذلك كله وفق الأسس والقواعد الفنية المتعارف عليها والمتبعة فى مجال الخبرة المعلوماتية ، مع مراعاة القواعد القانونية ، أعلاء لمبدأ المشروعية .

وأن عملية تحويل الدليل الرقمى إلى هيئة مادية ، وذلك عن طريق طباعة الملفات او تصوير محتواها إذا كانت صور أو نصوص ، أو وضعها فى أى وعاء آخر حسب نوع البيانات والمعلومات المكونة للدليل ، يحتاج بالضرورة إلى الخبير التقنى والمعلوماتى الذى يستخدم الأساليب التقنية والتى تساعد على ضبط الدليل والتحفظ عليه داخل الحاسوب ورصد موقع الإنترنت أو المعلومات التى تشير إلى الجريمة وإعدادها من مخرجات العالم المادى بدلاً من الرقمى وذلك بتحويلها إلى نسخ ورقية لعرضها على سلطات التحقيق والحكم .

المبحث الثانى

سلطة القاضى الجنائى فى قبول وتقدير الأدلة الإلكترونية

يقوم القاضى الجنائى بدور هام تجاه الدليل الجنائى ، فلا يقتصر دوره على مجرد الموازنة بين الأدلة المقدمة من الخصوم ، أو النيابة العامة (المثبتة أو النافية) للجريمة ، وإنما دوره إيجابى يفرض عليه التحرى عن الحقيقة والبحث عنها ، وهذا الدور الإيجابى للقاضى الجنائى هو الذى جعل المشرع يجرده من قيود الإثبات التى قيد بها القاضى المدنى ، وتستوجب قيام القاضى الجنائى بدور هام فيها يتولى المبادرة وتوجيه عمليات الإثبات ، فللقاضى الجنائى أن يقبل جميع الأدلة التى يقدمها أطراف الدعوى الجنائية[١] ، وله أن يستبعد ما لا يطمئن إليه منها ، فلا وجود لأدلة يلزمه بها القانون مقدماً بقبولها ، أو يحظر عليه مقدماً قبولها ، أما القاضى المدنى فملتزم باستبعاد الشهادة أو القرائن إذا جاوزت قيمة التصرف حد معيناً .

وقد فرض نظام حرية الإثبات للأطراف فى اختيار وسيلة الإثبات ، هذا الدور الإيجابى للقاضى الجنائى الذى يتمثل فى سلطة فى تقدير قيمة الأدلة المقدمة إليه واستخلاص عناصر اقتناعه منها دون تقيده بدليل معين ، وأن له أن يعتمد على أى دليل ما دام يؤدى إلى النتيجة التى انتهى إليها سواء بطريق مباشر أو غير مباشر ، فله أن يكمل الدليل من المنطق ، ويستخلص منه ما هو مؤداه إليه حتماً ، فالقاضى الجنائى أن يستمد اقتناعه من أى دليل يطمئن إليه ما دام لهذا الدليل أصل ثابت فى الأوراق .

وسوف نتناول بالشرح سلطة القاضى الجنائى قبول وتقدير الأدلة الرقمية أو الإلكترونية من خلال مطلبين :

المطلب الأول : سلطة القاضى الجنائى فى البحث عن الأدلة الإلكترونية وتقديرها.

المطلب الثانى : حجية الأدلة الرقمية فى الإثبات أمامالقاضى الجنائى.

---

(١) - د / أحمد عوض بلال – قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة من الإجراءات الجنائية – دار انهضة العربية – 1994 – ص 35 .

المطلب الأول

سلطة القاضى الجنائى فى البحث

عن الأدلة الإلكترونية وتقديرها

أولا: سلطة القاضى الجنائى فى البحث عن الأدلة الإلكترونية وقبولها .

إن القاضى الجنائى حر فى أن يستعين بكافة طرق الإثبات للبحث عن الحقيقة والكشف عنها إذ لا يجوز أن يقنع بفحص الأدلة التى يقدمها إليه أطراف الدعوى ، وإنما يتعين عليه أن يتحرى بنفسه الأدلة ، وأن يستشير الأطراف إلى تقديم عناصر الإثبات اللازمة لظهور الحقيقة .

وهكذا فإن القاضى الجنائى سواء بناء على طلبات الأطراف أو بموجب مقتضيات وظيفته ، أن يأمر باتخاذ الإجراء الذى يراه مناسباً أو ضرورياً للفصل فى الدعوى . وقد أكدت محكمة النقض المصرية فى حكم لها " للمحكمة متى رأت أن الفصل فى الدعوى يتطلب تحقيق دليل معين بعينه . فإن عليها تحقيقه طالما كان ممكنا بغض النظر عن مسلك المتهم من شأنه هذا الدليل [١]

كما اكدت على ان تحقيق الإدانة فى المواد الجنائية لا يتوقف على مشيئة المتهم[٢]

فالقاضى الجنائى عليه من تلقاء نفسه وفاء لمهمته – طلب أطراف الدعوى منه أو لم يطلبوا – أن يحقق بنفسه كل دليل يتطلبه الفصل فى الدعوى باعتباره دفاعاً جوهرياً ، أو ترسمه الوقائع ، أو يشهد به الواقع ويسانده ظاهر الحال .

وقد أكد المشرع المصرى فى قانون الإجراءات الجنائية فى المادة 291 هذا المعنى بقولها " أن للمحكمة أن تأمر من تلقاء نفسها أثناء نظر

---

(١)- أنظر نقض 3 ديسمبر 1980 – مجموعة الأحكام – س 50 – ق 330 – ص 512 .

(٢)- نقض 24 ابريل 1978 – مجموعة أحكام النقض – س 29 – ق 84 – ص 442.

الدعوى تقديم أى دليل تراه لازماً لظهور الحقيقة . وكذلك للمحكمة سواء من تلقاء نفسها أو بناء على طلب الخصوم أن تعين خبيراً واحداً أو أكثر فى الدعوى"[١].

وللمحكمة مطلق الحرية فى القيام بأى إجراء من إجراءات التحقيق تراه لازماً لتكوين عقيدتها ، وتكملة أى نقص وسداً لأى فراغ فى إجراءات التحقيق أو الاستدلال الذى سبق وأن قامت به سلطة الاستدلال أو سلطة التحقيق ، كالنيابة العامة أو قاضى التحقيق .

وقد أكدت محكمة النقض المصرية بأنه لم يعين القانون للمحاكم الجنائية طرقاً مخصصة للاستدلال لا بد منها ، فلم يوجب عليها تعيين خبير لكشف أمور وضحت لديها ، بل جعل للقاضى مطلق الحرية فى أن يقرر بنفسه الحقيقة التى يقتنع بها استمداداً من الأدلة المقدمة فى الدعوى ، ما دام لقضائه وجه محتمل ومأخذ صحيح ، فله أن يرفض طلب الخبرة إذا ما رأى أنه فى غنى عنها بما يستخلصه من الوقائع التى تثبت لديه [٢].

وكذلك أنه إذا ندبت المحكمة خبير فى الدعوى لا يسلب المحكمة سلطتها فى تقدير وقائعها وما قام فيها من أدلة الثبوت [٣] ، وللمحكمة كامل الحرية فى تقدير القوى التدليلية لتقرير الخبير المقدم إليها دون أن تلتزم بندب خبير آخر ، ولا بإعادة الدعوى إلى الخبير ، ما دام إسنادها إلى الرأى الذى انتهى إليها هو إسناد سليم ، لا يجافى المنطقية ولا القانون[٤].

ويترتب على ظهور الأدلة العلمية فى مجال الإثبات الجنائى تعاظم دور الخبراء[٥] فى القيام بدور فعال فى إبداء خبرتهم الفنية فيما يعرض عليهم من قضايا تتعلق باستخدام الحاسب الآلى وتقنية الملعومات فى الإثبات الجنائى ، والتطور العلمى الذى يشهده مجال الإثبات الجنائى فى مجال الجرائم الإلكترونية لا يتعارض مع مبدأ حرية القاضى الجنائى فى تكوين عقيدته ، وأن الأمر لا يعدو من اتساع مجل الاستفادة بأعمال

---

(١)- أنظر المواد 26 ، 293 ، 294 من قانون الإجراءات الجنائية المصرى .
(٢)- نقض 3 ديسمبر 1968- مجموعة القواعد القانونية – س 19 – ق 211 – ص 1041.
(٣)- نقض 17 أكتوبر 1996 – مجموعة أحكام النقض – س 17 – ق 180 – ص 971.
(٤)- نقض 20 فبراير 1968 – مجموعة الأحكام – س 19 – ق 47 – ص 260.
(٥)- أنظر/ آمال عبدالرحيم عثمان – المرجع السابق – ص 309 .

الخبرة التقنية فى إطار السلطة التقديرية للقاضى حسبما يستريح ضميره ، ولا يختلف دور القاضى الجنائى فى البحث عن الدليل الجنائى التقليدى عن دوره فى البحث عن الدليل الإلكترونى ، إلا أنه بالنسبة للأخير يقتضى الاستعانة بأهل الخبرة فى هذا الشأن حتى لا يتم فقد الدليل أو العبث بمخرجاته .

أما عن سلطة القاضى الجنائى فى قبول الأدلة الرقمية :

فإن الدليل الرقمى يختلف كلية عن الدليل الجنائى المادى ، لأنه يكون فى وسط افتراضى [١] ، ولذلك فإن مجرد الحصول على الدليل الرقمى وتقديمه للقضاء لا يكفى لاعتماده كدليل للإدانة ، إذ الطبيعة الخاصة للدليل الرقمى تمكن من العبث بمضمونه على نحو يحرف الحقيقة ، دون أن يكون فى قدرة غير المتخصصين إدراك ذلك العبث ، فضلاً عن ذلك فإن نسبة الخطأ فى إجراءات الحصول على دليل صادق فى الإخبار عن الحقيقة تبدو عالية فى مثل هذا النوع من الأدلة ، ولذلك تثور فكرة الشك فى مصداقية الدلة الرقمية كأدلة للإثبات الجنائى ، فهل تعنى ذلك استبعاد الدليل الرقمى من دائرة أدلة الإثبات الجنائى؟

لا شك أن النظم القانونية التى تعتمد النظام اللاتينى فى الإثبات كالتشريع الفرنسى والمصرى[٢]، فإن القاضى الجنائى يملك سلطة واسعة فى تقييم الدليل من حيث قيمته التدليلية ، فللقاضى قبول الدليل أو رفضه وهو يعتمد فى ذلك على مدى اقتناعه الشخصى بذلك الدليل [٣] وبناء على ذلك فهل يمكن للقاضى الجنائى وفقاً لهذا النظام أن يعمل سلطته التقديرية لقبوله أو رفضه بما يمكنه من استبعاد الدليل الرقمى لعدم الاقتناع به أو للشك فى مصداقيته؟

لا شك أن الدليل الرقمى يعد من الأدلة العلمية عموماً وأن هذا الدليل يتمتع من حيث قوته التدليلية بقيمة اثباتية قد تصل إلى حد اليقين ، كما ان معظم التشريعات الحديثة منحت القاضى الجنائى سلطة تقديرية

---

(١) - د / عمر محمد بن يونس – الدليل الرقمى – المرجع السابق – ص 33 .

(٢) - أنظر نصوص المواد 353 ، 304 ، 427 من قانون الإجراءات الفرنسى والمادة 302 ، 291 من قانون الإجراءات المصرى ، والمادة 147 إجراءات أردنى ، والمادة 175 ، 176 إجراءات سورى .

(٣) - د / طارق الحملى – الدليل الرقمى فى مجال الإثبات الجنائى – المرجع السابق – ص 25.

واسعة فى تكوين اقتناعه بالاستناد إلى دليل يطمئن إليه ، فأصبح الاقتناع الذاتى للقاضى الجنائى هو أساس العدالة لأن إطلاق سلطة القاضى فى تكوين عقيدته يدفع عنه العوائق فى سبيل الوصول للحقيقة . فالقاضى الجنائى يملك سلطة قبول الدليل الرقمى متى تأكد من سلامته وصحته ، وهذا القول لا يناقض القول بأن الدليل الرقمى هو موضع للشك من حيث سلامته من العبث من ناحية ، وصحة الإجراءات المتبعة فى الحصول عليه من ناحية أخرى حيث يشكلك فى الدليل الرقمى من ناحيتين :

الأولى : الدليل الرقمى من الممكن خضوعه للعبث ، للخروج به على نحو يخالف الحقيقة ، ومن ثم فقد يقدم هذا الدليل بعداً عن واقعة معينة ، صنع أساساً لأجل التعبير عنها خلافاً للحقيقة ، وذلك دون أن يكون فى استطاعة غير المتخصصين إدراك ذلك العبث فالتقنية الحديثة تمكن من العبث بالدليل الرقمى بسهولة ويسر ، بحيث يظهر وكأنه نسخة أصلية فى تعبيرها عن الحقيقة .

الثانية : وإن كانت نسبة الخطأ الفنى فى الحصول على الدليل الرقمى نادرة للغاية إلا أنها تظل ممكنة ، ويرجع الخطأ فى الحصول على الدليل الرقمى لسببين[١]:

الأول : الخطأ فى استخدام الأداة المناسبة فى الحصول على الدليل الرقمى ويرجع ذلك للخلل فى الشفرة المستخدمة ، أو لسبب استخدام مواصفات خاطئة .

والثانى : الخطأ فى استخلاص الدليل ويرجع ذلك إلى اتخاذ قرارات لاستخدام تقل نسبة صوابها عن (100%) ويحدث ذلك بسبب وسائل اختزال البيانات أو بسبب معالجة البيانات بطريقة تختلف عن الطريقة الأصلية التى تم تقييمها.

والخلاصة أن الشك فى الدليل الرقمى لا يتعلق بمضمونه كدليل وإنما بعوامل مستقلة عنه ولكنها تؤثر فى مصداقيته.

ثانيا: سلطة القاضى الجنائى فى تقدير الأدلة الإلكترونية وأثر ذلك على الإثبات الجنائى :

إن أساس الأحكام الجنائية إنما هى حرية القاضى الجنائى فى تقدير الأدلة الناتجة فى الدعوى ، وأنه لم يقضى بالبراءة أو الإدانة إلا بعد

---

(١)- د / سيد عتيق – المحاكمة وطرق النقض – الكتاب الثانى – دار النهضة العربية – ص 182.

أن يلم بكل الأدلة المطروحة أمامه فى الدعوى ووزنها ، فالقاضى يعتمد على المنطق ، وعلى وعيه وإدراكهبكافة أدلة الدعوى الجنائية ، وتمحيصها ثم استنتاج ما تحتويه من أدلة قادرة على خلق اليقين له .و قد نصت المادة المادة (320) من قانون الإجراءات الجنائية على أنه يحكم القاضى فى الدعوى حسب العقيدة التى تكونت لديه بكامل حريته ومع ذلك لا يجوز له أن يبنى حكمه على دليل لم يطرح أمامه فى الجلسة ، وتقدير الأدلة وترجيح بعضها على بعض من أخص خصائص محكمة الموضوع(١).

ويثور التساؤل حول الوضع بالنسبة للدليل الإلكترونى هل التثبت من سلامة الدليل الرقمى من حيث العيوب ؟

الدليل الرقمى يخضع لقواعد معينة تحكم طرق الحصول عليه كذلك فى نفس الوقت يخضع لقواعد أخرى للحكم على قيمته التدليلية ، والسبب فى ذلك هو الطبيعة الفنية لهذا الدليل فهناك وسائل فنية من طبيعته هذا تمكن من فحصه للتأكد من سلامته وصحة الإجراءات فى الحصول عليه .

وهناك طرق مختلفة للتأكد من سلامة الدليل الرقمى من العبث تتخل فيما يلى(٢) :

١ - فكرة التحليل التناظرى الرقمى ، تعد من الوسائل المهمة للكشف عن مصداقية الدليل الرقمى ، ومن خلالها تتم مقارنة الدليل الرقمى المقدم للقضاء بالأصل المدرج بالآلة الرقمية ، ومن خلال ذلك يتم التأكد من مدى حصول عبث فى النسخة المستخرجة أم لا .

٢ - فى حالة عدم الحصول على النسخة الأصلية للدليل الرقمى ، أو فى حالة أن العبث قد وقع على النسخة الأصلية ، ففى الإمكان التأكد من سلامة الدليل الرقمى من التبديل أو العبث من خلال استخدام عمليات حسابية خاصة تسمى بالخوارزميات .

---

(١) - د / ممدوح عبدالحميد عبداللطيف – زبيدة محمد القاسم – عبدالله عبدالعزيز – المرجع السابق – ص 2241.

(٢)- أنظر د / ممدوح عبد المطلب ، زبيدة محمد قاسم ، عبدالله عبدالعزيز ، نموذج مقترح لقواعد الدليل الرقمى للإثبات فى جرائم الكمبيوتر – منشور ضمن أعمال المؤتمر – الأعمال المصرفية والإلكترونية – نظمته كلية الشريعة والقانون – جامعة الإمارات فى الفترة 9-2003/5/12 – المجلد الخامس – ص 2241 – 2247.

٣ - هناك نوع من الأدلة الرقمية يسمى بالدجليل المحايد ، هو دليل لا علاقة له بموضوع الجريمة ، ولكنه يساهم في التأكد من سلامة الدليل الرقمى المقصود من حيث عدم حصول تبديل أو تغيير فى النظام (الحاسب الآلى) .

ونخلص من ذلك إلى أنه يمكن الوقوف على سلامة الدليل الرقمى إذا توافرت فى الدليل الرقمى الشروط العامة فى الدليل ، فالدليل الرقمى بوصفه دليلاً علمياً ، فإن دلالته قاطعة بشأن الواقعة المستشهد عنها ، فإذا سلمنا سابقاً بإمكانية التشكيك فى سلامة الدليل الرقمي بسبب قابليته للعبث ونسبة الخطأ فى إجراءات الحصول عليه ، فتلك مسألة فنية لا يمكن للقاضى أن يقطع فى شأنها برأى حاسم ، وإن لم يقطع به أهل الاختصاص ، ولذلك فإذا توافرت فى الدليل لا يمكن رده استناداً لفكرة الشك يلزم لإعمالها أن يكون هناك ما يرقى لمستوى التشكيك فى الدليل ، وهو ما لا يستطيع القاضى الجزم به متى توافرت فى هذا الدليل شروط السلامة ، بحيث يقتصر دور القاضى على بحث صلة الدليل بالجريمة[١].

ولا شك أن الخبرة فيما يتعلق بالتثبت من صلاحية الدليل الرقمى ، كأساس لتكوين عقيدة القاضى ، فبحث مصداقية هذا الدليل من صميم فن الخبير لا القاضى ، ويجب التنويه إلى أنه لا يمكن اعتبار هذه القيمة التى تدعيها للدليل الرقمى بمثابة خروج مستحدث عن القواعد العامة للإثبات الجنائى فى القانون المصرى ، حيث إن هناك من الأدلة ما لا يستطيع القاضى الجنائى تقديرها وفقاً لسلطته ، كمحاضر المخالفات مثلاً .

وهناك فرق بين الشك الذى يشوب الدليل ، بسبب إمكانية العبث به ، أو لوجود خطأ فى الحصول عليه ، وبين القيمة الإقناعية لهذا الدليل ، فالحالة الأولى لا يملك القاضى الفصل فيها لأنها مسألة فنية ، فالقول فيها قول أهل الخبرة ، فإن سلم الدليل من العبث والخطأ فإنه لن يكون للقاضى سوى القبول بهذا الدليل ، ولا يمكنه التشكيك فى قيمته التدليلية ، لكونه وبحكم طبيعته الفنية يمثل إخباراً صادقاً عن الواقع ، ما لم يثبت عدم صلة الدليل بالجريمة المراد إثباتها .

وفيما يتعلق بتأثير ظهور الأدلة الإلكترونية أو الرقمية على الإثبات الجنائى ، لا شك أن التطور العلمىقد يؤثر بلا شك على نظام الاقتناع القضائى ، فقد يُعلى هذا التطورمن تقارير الخبراء بالنظر إلى

---

(١)- د / أحمد يوسف الطحطاوى – الأدلة الإلكترونية – ودورها فى الإثبات الجنائى – المرجع السابق – ص 238.

كثرة المسائل الفنية البحتة التى تفرزها تطبيقات ثورة المعلومات والاتصالات عن بعد ، فهذا التطور قد يزيد من دور الخبرة فى المسائل الجنائية بالنظر إلى أن الكثير من الجرائم التى ترتكب كنتيجة لهذه الثورة المعلوماتية ستقع على مسائل الكترونية ذات طبيعة فنية معقدة ، أو قد تستخدم هذه الوسائل ف ارتكابها ، وبالنظر إلى تطور مجالات الخبرة فقد توفر التقنية العملية طرقاً دقيقة لجمع الأدلة بحيث يساهم العلم فى صنع الدليل بحيث أن هذا الدليل قد يتمتع بقوة علمية يصعب إثبات عكسها(١).

والثورة العلمية فى الاتصالات لم تؤثر فقط فى نوعية الجرائم التى ترتبت عليها ، وفى نوعية الجناة الذين يرتكبون هذه الجرائم وإنما أثرت تأثيراً كبيراً على الإثبات الجنائى ، وعلى طرق هذا الإثبات ، بحيث يمكن القول أن طرق الإثبات التقليدية قد أصبحت عقيمة بالنسبة لإثبات الجرائم الإلكترونية ، وأن الطرق العلمية والفنية للحصول على الدليل قد أصبحت هى المناسبة لإثبات هذا النوع من الجرائم(٢).

وفى ظل هذا التطور العلمى لثورة الاتصالات والمعلومات ، فإن الغلبة بالنسبة لإثبات الجرائم الإلكترونية ستكون للإثبات بالقرائن والخبرة ، وذلك يزيد من أهمية الدليل العلمى فى الإثبات الجنائى وفى ذات الوقت يزيد من أهمية دور القاضى فى هذا الإثبات ، فيظل القاضى متمتعاً بسلطة تقديرية واسعة فى تقدير هذه الأدلة . بحسب ما إذا كانت مؤكدة على سبيل القطع ، أو قد تكون مجرد إمارات أو دلالات ، أو قد يحوطها الشك فهنا تظهر أهمية هذه السلطة التقديرية التى يجب أن يظل القاضى متمتعاً بها لأنه من خلال هذه السلطة يستطيع إظهار مواطن الضعف فى الأدلة ويستطيع كذلك تفسير الشك لصالح المتهم .

المطلب الثانى

حجية الدليل الإلكترونى فى الإثبات الجنائى

في الأنظمة القانونية

أولا: حجية الدليل الإلكترونى فى النظم اللاتينية .

---

(١)- أنظر د / أحمد يوسف الطحطاوى – المرجع السابق – ص 249.

(٢)- د / طارق الحملى – الدليل الرقمى فى مجالات الإثبات الجنائى – ورقة عمل مقدمة للمؤتمر المغربى الأول حول المعلوماتية والقانون – المنعقد فى الفترة من 29/28 أكتوبر 2009 – طرابلس – ص 30.

إن القوانين اللاتينية والتى تشمل القانون الفرنسى والمصرى والسورى واللبنانى وغيرها من القوانين التى تأثرت بها[١] ، حيث أن هذه القوانين تعتمد على نظام الإثبات الحر أو نظام الأدلة المعنوية والتى يتمتع فيها القاضى بسلطة تقديرية واسعة فى تقدير أدلة الإثبات الجنائى ، وقد منح هذا النظام لقاضى سلطة مطلقة فى تكوين اقتناعه بالاستناد إلى أى دليل يطمئن إليه ، فهو غير ملزم بالحكم بالإدانة إذا لم يكن مقتنعاً بكفاية الأدلة لهذا الحكم ، حتى لو كانت هناك أدلة ضد المتهم ، وهو كذلك غير ملزم بالبراءة ولو لم تتوافر الأدلة الكاملة للحكم بالإدانة إذا ما استخلص من أحد هذه الأدلة إدانته ، وأدى هذا الدليل إلى اقتناعه بعدم البراءة . وقد خصص المشرع الإجرائى المصرى المادة (291) لحرية القاضى فى الإثبات، والمادة (302) لحرية القاضى فى الاقتناع وإذا كان مبدأ الثبوت المعنوى يشمل كل جهات القضاء الجنائى فإنه يمتد أيضاً لكل مراحل الدعوى الجنائية ، سواء فى مرحلة التحقيق الابتدائى أو التحقيق النهائى ، وهكذا فإن هذا المبدأ إن كان يطبق أمام جهات التحقيق النهائى فإنه يطبق أيضاً أمام قضاء التحقيق والإحالة ، وبالتالى فإن حجية المخرجات الإلكترونية أو الرقمية فى ظل الأنظمة اللاتينية تخضع كذلك لمبدأ حرية الإثبات والاقتناع فإن حجية هذه المخرجات لا تثير صعوبات سواء بالنسبة لمدى حرية تقديم المخرجات الإلكترونية لإثبات جرائم الحاسب ، أما بالنسبة لمدى حرية القاضى الجنائى فى تقديرالمخرجات الإلكترونية باعتباره أداة إثبات فى الموادالجنائية فالأساس فيه هو حريـة القاضى فى تقدير هذه الأدلة [٢] ولا شك أن مخرجات الحاسب الآلى ما هى إلا من

---

(١) - ومن القوانين التى تأثرت بالصيغة اللاتينية القانون الألمانى والقانون التركى واليونانى وقانون لوكسمبرج والقانون البرازيلى فهذه القوانين تخضع الأدلة الإلكترونية لحرية القاضى فى الاقتناع القضائى بحيث تكون مقدرة بطرح مثل هذه الأدلة رغم قطعيتها العلمية – ذلك عندما يجد أن الدليل الإلكترونى لا يتفق منطقياً مع ظروف الواقع وملابساتها .
- أنظر د / هلالى عبداللاه احمد – حجية المخرجات الكمبيوترية – المرجع السابق – ص 43.

(٢)- الفقه الفرنسى يدرس حجية المخرجات الإلكترونية فى المواد الجنائية ضمن مسألة أوسع وأعم ، هى مسألة قبول الأدلة الناشئة عن الأدلة ، أو الأدلة العلمية مثل الرادارات والأجهزة السينمائية وأجهزة التصوير وأشرطة التسجيل وأجهزة

تطبيقات الدليل العلمى[١]

وما يتميز به من موضوعية وحياد وكفاءة فى اقتناع القاضى الجنائى ، وهذه السمات التى ربما تؤدى إلى اعتقاد البعض أن التطور العلمى وما يترتب عليه من ظهور للأدلة العلمية ومن بينها المخرجات الإلكترونية أن يطغى على نظام الاقتناع القضائى فيجعل للخبير القول الفصل ، ولا يبقى للقاضى بعد ذلك الإذعان لرأى الخبير دون أى تقدير من جانبه[٢]. إلا أنه لا يمكن التسليم بهذا الرأى ، حيث أن التطور العلمى لا يتعارض مع مبدأ حرية القاضى فى تكوين اقتناعه وإن الأمر لا يعدو سوى اتساع مجال الاستفادة بالقرائن وأعمال الخبرة فى إطار السلطة التقديرية للقاضى حسبما يستريح ضميره[٣].

ولا بد أن نشير إلى أن تقدير القاضى لا يتناول فيما يتعلق بالمخرجات الإلكترونية القيمة العلمية للدليل الرقمى أو الإلكترونى حيث أنها تقوم على أسس علمية دقيقة ، ولكن أما الظروف والملابسات التى

التنصت تلك الآلة التي أخذ بها المشرع وقبله القضاء فى إطار مجموعة من الشروط ، من أهمها أن يتم الحصول عليها بطريقة شرعية ونزيهة ، وأن يتم مناقشتها حضورياً عن طريق الأطراف ، وعلى ذلك حكمت محكمة النقض الفرنسية " أن أشرطة التسجيل الممغنطة التى يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائى ، ولا يختلف الأمر بالنسبة لقبول مخرجات الحاسب الآلى ، حيث لم يتضمن قانون (5) يناير 1988 أية أوضاع خاصة بهذا الصدد .

- أنظر د / هلالى عبداللاه – حجية المخرجات الكمبيوترية – المرجع السابق – ص 251.

(١) - د / محمد محمد الهادى ، د / نشأت خميس الغياطى أحمد – نحو مستقبل أفضل لتكنولوجيا المعلومات فى مصر – أبحاث ودراسات المؤتمر العلمى الأول لنظم المعلومات وتكنولوجيا الحاسبات الذى نظمته الجمعية المصرية لنظم المعلومات وتكنولوجيا الحاسبات – القاهرة – المكتبة الأكاديمية 1995.

(٢)- د / حسين محمود ابراهيم – الوسائل العلمية الحديثة فى الإثبات الجنائى – دار النهضة العربية 1981 – ص 79 .

- أنظر د / محمد فتحى محمد أنور – تفتيش الإنترنت جرائم الاعتداء على الآداب العامة والشرف والاعتبار – المرجع السابق – ص 331.

(٣)- د / محمود نجيب حسنى – شرح قانون الإجراءات الجنائية – المرجع السابق – رقم 780 – ص 722.

وجد منها الدليل فإنها تدخل فى نطاق تقديره الذاتى فهذا من طبيعة عمله[١] .

وبالتالى إن كانت الأدلة العلمية بما فيها المخرجات الإلكترونية تخضع لحرية القاضى فى الاقناع ، فإنه ليس معنى ذلك أن ينازع القاضى فى قيمة ما يتمتع به الدليل العلمى من قوة استدلالية قد استقرت بالنسبة له وتأكدت من الناحية العلمية ، ولكن تقديره يكون للظروف والملابسات التى أحاطت به بحيث يكون فى إمكان القاضى أن يطرح هذا الدليل – رغم قطعيته من الناحية العملية ، وذلك عندما يجد أن وجوده لا يتسق منطقياً مع ظروف الواقعة وملابساتها .

فبمجرد توافر الدليل العلمى لا يعنى أن القاضى ملزم بالحكم مباشرة – دون بحث الظروف والملابسات – بالإدانة أو البراءة ، فالدليل العلمى ليس آلية معدة لتقدير اقتناع القاضى بخصوص مسألة غير مؤكدة[٢] ولذلك فالوسائل العلمية وإن كانت تفيد فى تسهيل مهمة الكشف عن الحقيقة القضائية ، إلا أنها قد تعصف بحريات وحقوق الأفراد إذا لم يحسن استخدامها . وعلى ذلك إذا واجهت المحكمة مسألة فنية وجب عليها أن تتخذ من الوسائل ما تراه لتحقيقها بلوغاً إلى غاية الأمر منه[٣].

ويرى البعض وبحق – لقبول الدليل العلمى بما يشمله من مخرجات إلكترونية أو رقمية [٤] ، أن يصل قيمة الدليل إلى درجة القطع من الناحية العملية البحتة . وألا يكون فى الأخذ بهذا الدليل المساس بحريات وحقوق الأفراد بالقدر المسموح به قانوناً . واستناداً إلى ذلك يمكن البت فى موضوع قبول أو عدم قبول ما ينتج عن الحاسب الآلى من أدلة تفيد الإثبات الجنائى.

ثانيا: حجية الدليل الإلكترونى أو الرقمى فى النظم الأنجلوسكونية :

هذه الأنظمة فى مقدمتها القانون الإنجليزى الذى يعتنق نظام الإثبات القانونى أو المقيد ، وفى هذا النظام يحدد المشرع أدلة إثبات ويقدر قيمتها الاقتناعية . ومقتضى ذلك أن يتقيد القاضى فى حكمه بالإدانة أو البراءة بأنواع معينة من الأدلة أو يعدد منها طبقاً لما يرسمه التشريع

---

(١)- د / عطية بوحيش – حجية الدليل الرقمى فى إثبات الجرائم المعلوماتية – أكاديمية الدراسات العليا - طرابلس – 2009 – ص 101.
(٢)- د / هلالى عبداللاه أحمد – المرجع السابق – ص 41.
(٣)- نقض 17 مايو 1990 – مجموعة أحكام النقض – س 41 – ص 727.
(٤)- د / أحمد يوسف الطحطاوى – المرجع السابق – ص 205.

المطبق ، إذ يقوم المشرع بصحة الإسناد أو عدم صحته مقام اقتناع القاضى ، وبالتالى فإن اليقين القانونى يقوم أساساً على افتراض صحة الدليل بصرف النظر عن حقيقة الواقع أو اختلاف ظروف الدعاوى [١] أما دور القاضى فلا يتعدى مراعاة تطبيق القانون من حيث توافر الدليل أو شروطه ، بحيث إذا لم تتوافر هذه الشروط وتلك الشكليات ، فإن القاضى لا يستطيع أن يحكم بالإدانة بصرف النظر عن اعتقاده الشخصى ، أى ولو اقتنع يقينياً بأن المتهم مدان فى الجريمة المسندة إليه .

ولذلك فإنه طبقاً لنظام الإثبات القانونى أو المقيد فإن المشرع هو الذى ينظم قبول الأدلة سواء بطريق تعيين الأدلة المقبولة للحكم بالإدانة ، أو باستبعاد أدلة أخرى ، أو بإخضاع كل دليل بأن يضفى حجية دامغة على بعض الأدلة ، أما دور القاضى فى ظل هذا النظام فهو دور آلى ، لا يتعدى مراعاة توافر الأدلة وشرائطها القانونية ، بحيث إذا لم تتوافر لا يجوز له أن يحكم بالإدانة بل يحكم باستبعاد الدليل حتى ولو اقتنع بأن المتهم مدان فنظام الأدلة القانونية هو السائد فى القوانين ذات الصياغة الأنجلوسكونية ومنها القانون الإنجليزى الذى أصدر عام 1990 قانون إساءة استخدام الحاسب الآلى إلا أن هذا القانون لم يتناول الأدلة الناتجة عن الحاسوب ، وربما كان السبب فى ذلك هو وجود قانون البوليس والإثبات الجنائى الصادر سنة 1984 والذى حوى تنظيماً محدداً لمسألة قبول مخرجات الحاسوب والإنترنت كأدلة إثبات فى المواد الجنائية[٢].

فإذا نظرنا إلى قانون البوليس والإثبات الإنجليزى لوجدنا أن المستند الناتج عن الحاسب الآلى لا يقبل كدليل . وقد اعتبر بعض الفقهاء الانجليز أن الأدلة الناتجة عن الحاسب بطريقة معينة تعد غير مقبولة ، بالإضافة إلى أنه فى حالة ما إذا كان الحاسب موضوعاً للاستخدام غير المصرح به فإن أى أدلة صادرة عنه تكون غير مقبولة ، لأن سواء

---

(١)- د / حسين رؤوف عبيد – مبادئ الإجراءات الجنائية فى القانون المصرى – الطبعة السابعة – مطبعة نهضة مصر 1968– ص 672.
- أنظر د / مأمون محمد سلامة – الإجراءات الجنائية فى التشريع المصرى – دار الفكر العربى – 1977 – ص 170.

(٢)- لقد صدر تشريع الإثبات بالحاسوب فى انجلترا 1983 وقد أكد بصفة أساسية على قبول مخرجات الحاسوب كدليل لإثبات أية حقيقة فيه والتى تزود بشهادة شفوية تكون مقبولة والتى يتم تقديرها من قبل المحكمة المختصة . أنظر د / سعيد عبدالمطلب حسن – الحماية الجنائية للسرية المصرفية – دار النهضة العربية – الطبعة الأولى 2004 – ص 194.

استخدام الحاسب فى حد ذاته أدى إلى أن الجهاز نفسه لا يعمل كما ينبغى[١].

وفى الولايات المتحدة الأمريكية تناولت بعض القوانين حجية الأدلة الإلكترونية ، ومن ذلك على سبيل المثال ما نص عليه قانون الحاسوب 1984 ، الصادر فى ولاية (ايوا) من أن مخرجات الحاسوب تكون مقبولة بوصفها أدلة إثبات بالنسبة للبرامج والبيانات المخزنة فيه (المادة 716 / أ / 16) ، كما يتضح من قانون الإثبات الصادر 1983 فى ولاية (كاليفورنيا) من أن النسخ المستخرجة من البيانات التى يحويها الحاسوب تكون مقبولة بوصفها أفضل الأدلة المتاحة لإثبات هذه البيانات ، وبالنسبة لمدى قبول الأدلة الناتجة عن الحاسب ، وأكد الفقه الأمريكى أن الصعوبات الحقيقية فى الولايات المتحدة الأمريكية نابعة من عدم الألفة مع تكنولوجيا الحاسب الآلى ، أكثر من العصوبات القانونية ، لذلك من غير المعقول أن تكون هناك حاجة ماسة إلى سن تشريعات بخصوص التعامل مع مدى قبول السجلات المعالجة بواسطة الحاسب [٢].

وفى كندا يمكن قبول السجلات الناجمة عن الحاسوب إذا توافرت شروط معينة ، وتنص المادة (29) من قانون الإثبات الكندى على عدد من الشروط التى يجب توافرها قبل عمل صورة (**copy**) من السجل الذى يضاف إلى الأدلة ، ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلى ، وقد قضت محكمة استئناف (أونتاريو) الكندية فى قضية مكميلان (**MCMULLEN**) بأنه يشترط لكى تكون سجلات الحاسوب مقبولة بصفها نسخاً حقيقية من السجلات الإلكترونية ، وأن تكون محتوية على وصف كامل لنظام حفظ السجلات السائد فى المؤسسات المالية ، كما يمكن أن يتضمن ذلك وصفاً للإجراءات والعمليات المتعلقة بإدخال البيانات وتخزينها واسترجاعها ، حتى يتبين أن المخرج المتحصل من الحاسوب موثوق به بشكل كاف [٣]. وتنص قواعد الإثبات الفيدرالية الأمريكية ، على أن النسخة المطابقة للأصل لها ذات حجية الأصل ، أياً

---

(١)- د / عمر محمد أبو بكر يونس – الجرائم الناشئة عن استخدام الإنترنت – دار النهضة العربية 2004 – ص 835.

(٢)- أنظر د / هلالى عبداللاه أحمد – حجية المخرجات الكمبيوترية – المرجع السابق – ص212.

(٣)- أنظر د / عطية بوحوش – حجية الدليل الرقمى فى إثبات الجرائم المعلوماتية – المرجع السابق – ص 119.

كانت الطريقة أو الوسيلة المستخدمة فى النسخ كالطباعة ، والتصوير ، والتسجيل الميكانيكى والتسجيل الإلكترونى ، بما يسمح بقبول مخرجات الحاسوب فى الإثبات ، والغالب الأعم فى القضاء الأمريكى يُعول على قبول دليل السجلات الممغنط بها على الحاسوب[١].

ثالثا: حجية الأدلة الإلكترونية فى القوانين ذات الاتجاه المختلط :

وهذه الأنظمة تجمع بين النظامين اللاتينى والأنجلوسكونى ، فيعتمد النظام المختلط على أن عدد القانون أدلة معينة لإثبات بعض الوقائع دون بعضها الآخر ، أو يشترط فى الدليل شروطاً فى بعض الأحوال ، أو يعطى القاضى الحرية فى تقدير الأدلة القانونية ، مثل القانون الإجرائى اليابانى ، وقد حصر المشرع اليابانى طرق الإثبات المقبولة فى ما يلى : (أقوال المتهم ، وأقوال الشهود ، والقرائن والخبرة) أما بالنسبة لأدلة الحاسوب والإنترنت ، فيقرر الفقه اليابانى ، أن السجلات الإلكترومغناطيسية تكون غير مرئية فى حد ذاتها ، ولذلك لا يمكن أن تستخدم كدليل فى المحكمة ، إلا إذا تم تحويلها إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات ، وفى مثل هذه الحالة يتم قبول الأدلة الناتجة عن الحاسوب والإنترنت سواء كانت هى الأصل أم كانت نسخة من الأصل[٢].

ومن القوانين ذات الصياغة المختلطة أيضاً قانون الإجراءات الشيلى وتنص المادة (113) من قانون الإجراءات الجنائية الشيلى على إمكانية استخدام الأفلام السينمائية ، والحاكى(الفوتوغراف) ، والنظم الأخرى الخاصة بانتاج الصورة والصوت والاختزال ، وبصفة عامة أية وسائل أخرى قد تكون ملائمة ، ووثيقة الصلة ، وتقضى إلى استخلاص المصداقية ، يمكن أن تكون مقبولة كدليل إثبات[٣] ويرى الفقه الشيلى ، أن الدليل الناتج عن الحاسوب والإنترنت يمكن أن يكون مقبولاً فى المحكمة ، كدليل كتابى أو مستندى ، مثل النظم الحديثة الأخرى لجمع وتسجيل المعلومات ، تسجيل وإنتاج الحقائق ، التصوير الفوتوغرافى ، والتصوير بالأقمار الصناعية ، التصوير بالأشعة ، الهاتف اللاسلكى ، تسجيل

---

(١)- أنظر د / سعيد عبداللطيف حسن – المرجع السابق – ص 165.

(٢)- أنظر د / هلالى عبداللاه أحمد – حجية المخرجات الكمبيوترية – المرجع السابق – ص 62.

(٣)- د / هلالى عبداللاه احمد – حجية المخرجات الكمبيوترية – المرجع السابق – ص 64 – 66 .

الصوت ، جميع تسجيلات الصوت والصورة ، فهذه الوسائل العلمية جميعاً يمكن اعتبارها مستندات بالمعنى الواسع ، فالتقدم العلمى والفنى قد تجاوز المفهوم التقليدى للمستند الذى يعرفه على أنه مجرد ورقة مكتوبة ، وأصبح يسمح بالحصول على وسائل أخرى من التسجلات التى تمثل فكرة أو حقيقة أكثر دقة وبأسلوب موثوق به ، ويثور التساؤل حول القوة الإثباتية للتسجلات الصوتية المسجلة إلكترونياً ؟ فالصوت عند تسجيله الكترونياً ، لا يحتمل الخطأ ، ويصعب التلاعب به ، ويمكن للخبراء أن يكتشفو أى تلاعب أو خداع بوسائل تقنية عالية الكفاءة ، ومن ثم يمكن القول بأن التسجيل الصوتى الممغنط يمكن أن يكون حجة دامغة فى الإثبات[١].

والأدلة الناتجة عن الحاسب الآلى يمكن الاعتراف بها كدليل يستند على تقرير الخبير الصادر فى عنصر معالجة البيانات فطبقاً للمادة (221) من قانون الإجراءات الجنائية التشيلى ، للقاضى أن يطلب تقارير الخبراء فى القضايا التى يشترط فيها القانون ذلك[٢].

---

(١)- أنظر د / سعيد عبداللطيف – المرجع السابق – ص 211.

(٢)- د / ممدوح عبدالحميد عبدالمطلب – البحث والتحقيق الجنائى الرقمى فى جرائم الحاسب الآلى والإنترنت – المرجع السابق – ص 87.

الخاتمــة والتوصيات

شهد العالم ثورة هائلة فى مجال تقنية المعلومات والاتصالات أثرت فى شتى أوجه الحياة والعلوم والميادين ، وعلى كافة القطاعات الاقتصادية ، والاجتماعية ، والسياسية ، والتعليمية ، والطبية ، والدبلوماسية ، وغيرها من قطاعات الأعمال المختلفة بما فى ذلك بما فى ذلك قواعد ونظم المعلومات والشبكات القومية والعالمية ونتيجة لهذا التطور وإساءة استخدام العلم ظهرت الجريمة المعلوماتية بما أحدثته من خروج على مقتضيات القانون والنظام والأمن العام وبالرغم من مزايا التقنية المعلوماتية فى شتى مجالات الحياة ، إلا أنه كما هو شأن كل اكتشاف أو اختراع جديد ، أدى إلى ظهور مشاكل قانونية ، دعت الدول إلى البحث عما إذا كانت القوانين القائمة تكفى لمواجهة بعض الاستخدامات غير المأمونة للإنترنت أم أنه يتعين مواجهة هذه الأعمال بنصوص قانونية وإجرائية تجريمية جديدة والجريمة الإلكترونية أو المعلوماتية مشكلة معقدة تؤرق الدول والأفراد ،وتشيع فقدان الثقة بالتقنية وتهدد إبداع العقل البشرى ،ولم يكن لارتباط الجريمة الإلكترونية بالحاسب الآلى أثره فى تمييز الجريمة الإلكترونية عن غيرها من الجرائم التقليدية فحسب وإنما كان له أثره فى تمييز المجرم الإلكترونى عن غيره من المجرمين الذين جنحوا إلى السلوك الإجرامى النمطى ، وفى تمييز القوانين التى وضعتها الحكومة لمكافحة الإجرام الإلكترونى ومعاقبة المجرم الإلكترونى .

ومع التطور الكبير والمتزايد لتكنولوجيا المعلومات انتشرت الجريمة الإلكترونية واعتمدت فى موضوعها على التشفير والأكواد السرية والنبضات والأرقام والتخزين الإلكترونى ، وأصبح من الصعب أن تخلف ورائها آثاراً مرئية قد تكشف عنها أو تستدل من خلالها على الحياة ، وأن خطر هذه الجرائم يكمن فى أنها فى طبيعتها تجمع بين الذكاء الاصطناعى والذكاء البشرى مما يجعل إثباتها جنائياً يمثل صعوبة لأجهزة إنفاذ القانون .

ويلاحظ أنه من خلال رصد ظاهرة الإجرام فى عالمنا الحديث اليوم ، أن ثمة صراعاً محتدماً بين المجتمع من جهة والخارجين عن القانون من جهة أخرى ، ويسعى المجرمون من جانبهم إلى اللجوء إلى كافة الوسائل الإلكترونية الحديثة فى ارتكاب جرائمهم وتمكنهم من الإفلات من العقاب عما اقترفوه من جرائم . فضلاً عن ذلك صار المجرمون اليوم أكثر خطورة ودهاء من مجرمى الأمس ، وفى سبيل الوصول إلى أغراضهم

الإجرامية ، أصبحوا يلجأون إلى تسخير العلم إلى أبعد الحدود ، وذلك باستخدام التقنية العالية والوسائل الفنية المتطورة التى فاقت فى بعض الأحيان إمكانيات الأجهزة المعنية بمكافحة الجريمة ذاتها .

الأمر الذى مكنهم من إخفاء جرائمهم وطمس آثارها مما ضاعف من صعوبة كشفها واستجلاء غموضها .

فإذا تخلف الدليل لم يعد مجال للحديث عن المسئولية الجنائية ، وبالتالى لا محل لإنزال العقاب بشخص الجانى ، إذ لا إدانة ولا عقوبة بدون إثبات ، فقواعد الإثبات الجنائى تهدف للوصول إلى الحقيقة الواقعية والذى لن يتأتى إلا من خلال العملية الإثباتية المتمثلة فى البحث عن الدليل الجنائى وتقديمه للقضاء ليقول كلمته على أساسه إما بالإدانة أو بالراءة.

وقد خول المشرع القاضى الجنائى سلطة واسعة من حيث قبول الدليل وتقدير قيمته الإثباتية ، حيث فسح المجال أمامه لكى يستلهم عقيدته من أية وسيلة أو دليل يطمئن إليه وجدانه ويرتاح إليه ضميره .

وقد كشفت معظم الدراسات والأبحاث الحديثة عن حدوث تطور كبير فى ميدان الإثبات الجنائى ، ولا شك أن الأدلة الإلكترونية أو الرقمية أصبحت جزء لا يتجزأ من البحث الجنائى والجرائم الإلكترونية باتت فرعاً مهماً من فروع الجريمة ، ولا يمكن اكتشاف الجريمة إلا بوجود الأدلة الرقمية . لذا فإن العلم اليوم فى تطور مستمر لاكتشاف المزيد من الأدلة التى تساعد على الحد من الجريمة الإلكترونية .

من خلال بحثنا الإثبات الجنائى فى الجريمة الإلكترونية توصلنالعدد من التوصيات والنتائج نذكر منها ما يلى :-

١ - يجب تعديل قانون العقوبات بحيث ينص صراحة على تجريم الجرائم الإلكترونية ووضع العقاب الرادع لها ، أو إصدار قوانين خاصة تتضمن عقوبات للجرائم الإلكترونية ، وذلك إعلاء لمبدأ شرعية الجرائم والعقوبات.

٢ - تعديل قانون الإجراءات الجنائية كذلك ، وغيره من التشريعات ذات الصلة بما يتوافق مع طبيعة الجرائم الإلكترونية ، وبما يساعد فى الضبط والتحقيق ، والعمل مع طبيعة الجريمة الإلكترونية والعمل على كشف تلك الجرائم وتعقب مرتكبها .

٣ - حتى يكون للقاضى الجنائى السيادة والهيمنة على الدعوى الجنائية فى الجرائم الإلكترونية لا بد أن يكون مدرباً تدريباً فنياً خاصاً على كيفية التعامل مع تقنية المعلومات وأنظمة معالجة

البيانات المعقدة ، ومع الأدلة الناتجة عن الحاسب الآلى بشكل واف ودقيق .

٤ - تتسم الجرائم الإلكترونية بخصائص تقنية خاصة وبصعوبة اكتشافها وإثباتها ، وخاصة السرعة الفائقة فى ارتكابها وسهولة طمس معالمها ومحو آثارها دون أثر ملموس لذا يتطلب الأمر توافر الخبرة والمهارة التقنية لكشف الأدلة الناتجة عن الجرائم الإلكترونية من جانب رجال الضبط والنيابة والقضاة، مع الاستعانة بخبراء استشاريين فى مجال الجرائم الإلكترونية .

٥ - يجب أن تتصدى الجمعية العربية للقانون الجنائى لوضع مشروع عربى موحد حول ضرورة تطوير وسائل الإثبات بتطور وسائل الإجرام .

٦ - الاهتمام بأعمال الخبرة الفنية القضائية المتخصصة بالإثبات العلمى والفنى للجرائم الرقمية وإقامة علاقات التبادل والتكامل فى هذا المجال بين الدول العربية من جانبها ، وبينها وبين غيرها من الدول المتقدمة من جانب آخر .

٧ - إنشاء أكاديميات فنية وقضائية لإعداد وتأهيل وتخريج الخبراء القضائيين فى كافة التخصصات العلمية ، وخاصة مجال الجرائم المستحدثة ، وعلى رأسها الجرائم الإلكترونية ، والجرائم ذات الصلة .

٨ - ضرورة إصدار دليل إرشادى تقنى وقانونى حول صور الجرائم الإلكترونية والأصول العلمية لكشفها والتحقيق فيها ، وأساليب التعامل مع الأدلة الرقمية ومواصلة تحديث هذا الدليل بشكل دورى ، وكلما دعت الحاجة لذلك وتعميمه على العاملين فى مجال التحقيق فى الميدان وعلى أجهزة القضاء والاستفادة من الدليل الصادر عن المنظمة العالمية للشرطة الجنائية (الانتربول) .

٩ - العمل على إقامة التوازن العادل فيما يتعلق بالإجراءات المتبعة فى الضبط والتحقيق والمحاكمة للجرائم الإلكترونية وبين حقوق الإنسان وحرياته الأساسية المنصوص عليها فى القوانين والدساتير والمواثيق الدولية ، وذلك بتطبيق مبدأ تناسب الإجراءات مع طبيعة وظروف ومقتضيات الجريمة .

١٠ توعية مستخدمة الإنترنت والحاسب الآلى والمراكز العلمية حول خطورة الجرائم الملعوماتية ، وضرورة الحماية منها من جانب وأهمية الإبلاغ عنها والإرشاد عن مرتكبها من جانب آخر .

١١ إمكانية مناقشة الأدلة الإلكترونية المستخرجة من الحاسب الآلى والإنترنت عند الأخذ بها كأدلة إثبات أمام المحاكم .

١٢ الجرائم الإلكترونية أو المعلوماتية لا تقتصر على دولة معينة ، وإنما تتخذ العالم كله مسرحاً لها ، ولذلك فإن عولمة الجريمة المعلوماتية تقتضى عولمة المواجهة وأهمية التعاون الدولى ، فلم تعد السلطات القضائية فى دولة ما قادرة على التصدى لهذه الجرائم دون مساندة أو مشاركة غيرها من السلطات فى الدول الأخرى .

١٣ ضرورة العمل على إنشاء مركز قومى لأمن الحاسب الإلكترونى والملعومات ، فالأمن المعلوماتى هو جزء حيوى من الأمن القومى ، وإن المسئولية يجب أن يتعاون فيها كل الجهات التقنية والأمنية والقضائية ، ويكون من اختصاصاته اقتراح القواعد والتشريعات الخاصة بالمعلوماتية والإنترنت ، وإعداد تقارير إحصائية ، ومتابعة ما تم فى عالمنا فى هذا المجال ، واستقبال الشكاوى من الأفراد والمؤسسات وإرسال الشكاوى إلى إدارة الاتصال بالشرطة الدولية ، ووضع معايير سياسات أمن المعلومات والإنترنت ، وتحديد المسئولية بين الجهات المعنية.

قائمة المراجع

أولا:المراجع العربية .

1- المراجع العامة :

د / حسن صادق المرصفاوى – المرصفاوى فى أصول الإجراءات الجنائية – منشأة المعارف – الاسكندرية – 1996 .

د / حسين رؤوف عبيد – مبادئ الإجراءات الجنائية فى القانون المصرى – الطبعة السابعة – مطبعة نهضة مصر 1968.

د / فهد عبدالله العبيد – الإجراءات الجنائية المعلوماتية – جامعة عين شمس – 2012.
د / فوزية عبدالستار – شرح قانون الإجراءات الجنائية – دار النهضة العربية – 1986.
د / مأمون سلامة – الإجراءات الجنائية فى التشريع الليبى – الطبعة الثانية – ليبيا – 2000 .
د / مأمون سلامة – الإجراءات الجنائية فى التشريع المصرى – دار الفكر العربى – 1997.
د / مأمون سلامة – قانون الإجراءات الجنائية معلقاً عليه بالفقه والقضاء – دار الفكر العربى1981.
د / محمود نجيب حسنى – شرح قانون الإجراءات الجنائية – الطبعة الثالثة - دار النهضة العربية – 1998.

2- المراجع الخاصة :

د / أحمد حسام طه تمام – الجرائم الناشئة عن استخدام الحاسب الآلى – دار النهضة العربية – سنة 2000 .
د / أحمد خليفة الملط – الجرائم المعلوماتية – دار الفكر العربى – 2005 .
د/ أحمد ضياء الدين محمد خليل – مشروعية الدليل فى المواد الجنائية كلية الحقوق – جامعة عين شمس 1984.
د / أحمد عوض بلال – التطبيقات المعاصرة للنظام الاتهامى فى القانون الانجلوأمريكى – دار النهضة العربية 1992.
د / أحمد عوض بلال – قاعدة استبعاد الأدلة المتحصلة بطريق غير مشروعة فى الإجراءات الجنائية المقارنة – دار النهضة العربية – 1994 .
د / أحمد فتحى سرور – الوسيط فى شرح الإجراءات الجنائية – 1991 .
د / أحمد يوسف الطحطاوى – الأدلة الإلكترونية ودورها فى الإثبات الجنائى – دراسة مقارنة – دار النهضة العربية – 2015 .
د / أسامه أحمد المناعة – جرائم الحاسب الآلى والإنترنت – دراسة تحليلية مقارنة – الطبعة الأولى – دار الأوائل للنشر – عمان – 2001 .
د / اسامه عبدالله فايد – الحماية الجنائية للحياة الخاصة – وبنوك المعلومات – دار النهضة العربية – 1994 .
د / جميل عبدالباقى الصغير – أدلة الإثبات الجنائى والتكنولوجيا الحديثة – دراسة مقارنة – دار النهضة العربية – 2001 .
د / جميل عبدالباقى الصغير – الجوانب الإجرائية للجرائم المتعلقة بالإنترنت – دار النهضة العربية – 2002.
د / جميل عبدالباقى الصغير – القانون الجنائى والتكنولوجيا الحديثة – الكتاب الأول – دار النهضة العربية – 1992 .
د / حسن طاهر داوود – جرائم نظم المعلومات – أكاديمية نايف العربية للعلوم الأمنية – الرياض – الطبعة الأولى – 2000.

د / حسين بن سعيد بن سيف الغافرى – الجهود الدولية فى مواجهة جرائم الإنترنت .
د / حسين محمود ابراهيم – الوسائل العلمية الحديثة فى الإثبات الجنائى – دار النهضة العربية 1981 .
د / خالد ممدوح ابراهيم – التقاضى الإلكترونى – الدعوى الإلكترونية وإجراءاتها أمام المحاكم – دار الفكر الجامعى – الاسكندرية – 2008 .
د / خالد ممدوح ابراهيم – الدليل الإلكترونى فى الجرائم المعلوماتية – بحث منشور على الإنترنت .
د / خالد ممدوح ابراهيم – أمن الجريمة الإلكترونية – الدار الجامعية – الاسكندرية – 2010 .
د / رمزى رياض عوض – مشروعية الدليل الجنائى فى مرحلة المحاكمة وما قبلها – دار النهضة العربية – 1997 .
د / سامى على حامد عياد – الجريمة المعلوماتية وإجرام الإنترنت ، دار الفكر الجامعى – الاسكندرية – 2007 .
د / سعيد عبداللطيف حسن – إثبات جرائم الكمبيوتر والجرائم المرتكبة على الإنترنت – الطبعة الأولى – دار النهضة العربية – القاهرة – 1991.
د / سعيد عبداللطيف حسن – الحماية الجنائية للسرية المصرفية – دار النهضة العربية – الطبعة الأولى 2004 .
د / سليمان أحمد فضل – المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت) – دار النهضة العربية – 2007.
د / سيد عتيق – المحاكمة وطرق النقض – الكتاب الثانى – دار النهضة العربية.
د / صغير يوسف – الجريمة المرتكبة عبر الإنترنت – جامعة مولود محمدى – 2013 .
د / طارق ابراهيم الدسوقى – الأمن المعلوماتى (النظام القانونى لحماية المعلومات) دار الجامعة الجديدة للنشر – 2009.

د / عبد الفتاح بيومى حجازى – مبادئ الإجراءات الجنائية فى جرائم الكمبيوتر والإنترنت – دار الفكر الجامعى – الطبعة الأولى – الاسكندرية – 2006.
د / عبدالفتاح بيومى حجازى – الدليل الجنائى والتزوير فى جرائم الكمبيوتر – دراسة متعمقة فى جرائم الحاسب الآلى والإنترنت – بهجات للطباعة والتجليد – مصر 1995.
د / عبدالفتاح بيومى حجازى – صراع الكمبيوتر والإنترنت – فى القانون العربى النموذجى – دار الكتب القانونية – القاهرة 2007.
د / عبدالله حسين على محمود – سرقة المعلومات المخزنة فى الحاسب الآلى – دار النهضة العربية – 2002.
د / عطية بوحيش – حجية الدليل الرقمى فى إثبات الجرائم المعلوماتية – أكاديمية الدراسات العليا - طرابلس – 2009.
د / عفيفى كامل عفيفى – جرائم الحاسب الآلى وحقوق المؤلف والمصنفات الفنية – دراسة مقارنة - منشأة المعارف – 2000.
د / على حسن الطواليه – التفتيش الجنائى على نظم الحاسوب والإنترنت – دراسة مقارنة – عالم الكتاب الحديثة – 2004.
د / على حسن الطوالية – مشروعية الدليل المستمد من التفتيش الجنائى – دراسة مقارنة .
د / على سليمان احمد فضل – المواجهة التشريعية للجرائم الناشئة عن استخدام شبكة المعلومات الجولية والإنترنت - دار النهضة العربية – 2007.
د / عمر محمد بن يونس – الجرائم الناشئة عن استخدام الإنترنت – دار النهضة العربية 2004 .
د /عمر محمد بن يونس – الدليل الرقمى – دار النهضة العربية – سنة 2007.
د / عمرو عيسى الفقى - الجرائم المعلوماتية – جرائم الحاسب الآلى والانترنت فى مصر والدول العربية ، المكتب الجامعى الحديث – الاسكندرية – 2006.

د / محمد بن عبدالله بن على المنشاوى – جرائم الإنترنت فى المجتمع السعودى – أكاديمية نايف للعلوم الأمنية – الرياض – 2003.
د / محمد حماد مرهج البهينى – جرائم الحاسوب – موضوعها – ماهيتها – اهم صورها والصعوبات الى تواجهها – دراسة تحليلية – الطبعة الأولى – دار المناهج للنشر والتوزيع – عمان – 2006 .
د / محمد فاروق عبدالحميد – القواعد الفنية الشرطة للتحقيق والبحث الجنائى – الطبعة الأولى – اكاديمة نايف العربية للعلوم الأمنية – الرياض – 1999.
د / محمد فتحى محمد أنور عزت – تفتيش شبكة الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبار والتى تقع بواسطتها – جامعة عين شمس – 2010.
د / محمود احمد عبنيه – جرائم الحاسوب وأبعادها الدولية – دار الثقافة والنشر والتوزيع - عمان – 2005.
د / محمد فهمى طلبة – الموسوعة الشاملة لمصطلحات الحاسب الآلى – موسوعة دلتا كمبيوتر – 1991.
د / محمود محمود مصطفى – الإثبات فى المواد الجنائية .
د / محمود نجيب حسنى – الاختصاص والإثبات فى قانون الإجراءات الجنائية – دار النهضة العربية – 1992.
د / مصطفى حمد موسى – أساليب إجرامية بالتقنية الرقمية (ماهيتها ، مكافحتها) – دار الكتب القانونية – مصر 2005 .
د / معبد عبداللطيف حسن – الإثبات فى جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت – الجرائم الواقعة فى مجال تكنولوجيا المعلومات – دار النهضة العربية – 1999.
د / ممدوح خليل عمر – حماية الحياة الخاصة والقانون الجنائى – دار النهضة العربية 1982 .
د / ممدوح عبدالحميد عبدالمطلب – البحث والتحقيق الجنائى فى جرائم الكمبيوتر والإنترنت – دار الكتب الوطنية – 2006.
د / منير الجنبهى – البنوك الإلكنرونية – الطبعة الثانية – دار الفكر الجامعى الاسكندرية – 2006 .

د / نائلة عادل محمد فريد – جرائم الحاسب الآلى الاقتصادية – منشورات الحلبى الحقوقية – 2005 .
د / نبيل عبدالمنعم جاد – أسس التحقيق والبحث الجنائى العلمى – كلية الشرطة.
د / هدى حامد قشقوش – تزوير المستندات المعالجة الآلية – بحث مقدم حول الكمبيوتر والقانون – كلية الحقوق – جامعة عين شمس – 1994 .
د / هدى حامد قشقوش – جرائم الحاسب الإلكترونى فى التشريع المقارن – دار النهضة العربية 1992.
د / هشام فريد رستم – الجوانب الإجرائية للجرائم الإجرائية – دراسة مقارنة – مكتبة الآلات الحديثة – أسيوط – 1994 .
د / هشام فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات وميكنة الآلات الحديثة – أسيوط - 1992.
د /هشام محمد فريد رستم – الجوانب الإجرائية المعلوماتية مكتب الآلات الحديثة – 1994.
د / هلال بن محمد بن حارب البورسعيدى – الحماية القانونية والفنية لقواعد المعلومات المحوسبة – دراسة قانونية وفنية مقارنة – دار النهضة العربية – 2009.
د / هلال عبداللاه أحمد – حجية المخرجات الكمبيوترية فى الإثبات الجنائى – الطبعة الأولى – دار النهضة العربية – 1997.
د / هلالى عبد اللاه – اتفاقية بودابست لمكافحة جرائم المعلوماتية – دار النهضة العربية – الطبعة الأولى .
د / هلالى عبداللاه أحمد – التزام الشاهد بالاعلام فى الجرائم المعلوماتية – دراسة مقارنة – القاهرة – 2000.
د / يونس العزب المحامى – بحث بعنوان جرائم الكمبيوتر والإنترنت – المعنى والخصائص والصور واستراتيجية المواجهة القانونية – الطبعة الأولى – 2003.

3- الرسائل

د / آمال عبدالرحيم عثمان – الخبرة فى المسائل الجنائية – 1964 – جامعة القاهرة .

د/ بدر سليمان يونس – أثر التطور التكنولوجى مع الحريات الشخصية فى النظم السياسية – رسالة دكتوراه – جامعة القاهرة 1982 .
د / حسن ابراهيم – الحماية الجنائية لحق المؤلف عبر الإنترنت – رسالة دكتوراه – دار النهضة العربية – 2006 .

4- المؤتمرات والأبحاث والندوات

د / أحمد شوقى أوخطوة – جريمة الاحتيال ماهيتها وخصائصها " دورة عمل حول جرائم الاحتيال والإجرام المنتظم – جامعة نايف العربية للعلوم الأمنية ، من 18 – 20 جوان 2007 – الرياض الطبعة الأولى 2008 .

د / أيمن عبدالحفيظ – حدود مشروعية دور اجهزة الشرة فى مواجهة الجرائم المعلوماتية – مجلة مركز بحوث الشرطة – العدد 25 يناير 2004 .

د / راشد حمد البلوشى – ورقة عمل حول الدليل فى الجريمة المعلوماتية – مقدمة إلى المؤتمر الدولى الأول حول حماية أمن المعلومات والخصوصية فى قانون الإنترنت برعاية الجمعية الدولية لمكافحة الإجرام بفرنسا – فى الفترة من 2 : 2 يونيو 2008 – القاهرة .

د / طارق الحملى – الدليل الرقمى فى مجال الإثبات الجنائى – ورقة عمل مقدمة للمؤتمر العربى الأول حول المعلوماتية والقانون المنعقد فى الفترة من 28 / 29 أكتوبر 2009 – تنظمه أكاديمية الدراسات العليا – طرابلس .

د / على عبدالقادر القهوجى – الحماية الجنائية لبرامج الحاسب – بحث منشور بمجلة الحقوق للبحوث القانونية والاقتصادية – كلية الحقوق – جامعة الاسكندرية – العدد 24 سنة 1992.

د / على محمود على حمودة – الأدلة المتحصلة من الوسائل الإلكترونية فى إطار نظرية الإثبات الجنائى – مقدم ضمن أعمال المؤتمر العملى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية نظمته أكاديمية شرطة دبى فى الفترة من 26 – 28 /4/2003 .

د / عمر الشيخ الأصم – البطاقات الائتمانية المستخدمة الأكثر انتشاراً فى البلاد العربية " أعمال ندوة تزوير البطاقات الائتمانية – أكاديمية نايف العربية للعلوم الأمنية – الرياض – الطبعة الأولى – 2002 .

د / فتوح الشاذلى – المواجهة التشريعية للجرائم المستحدثة – بحث مقدم إلى مؤتمر الأمن والسلامة – أبو ظبى من 6 : 8 أكتوبر 2003 .

د / محمد ابراهيم محمد الشافعى – النقود الإلكترونية – مجلة الأمن والحياة – أكاديمية شرطة دبى س 12 ، ع 1 – يناير 2004.
د / محمد أبو العلا عقيدة – المؤتمر العلمى الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية مركز البحوث والدراسات تاريخ الانعقاد 26 نيسان – 2003 – الانتهاء 28 نيسان 2003 – دبى .
د / محمد الأمين البشرى – الأدلة الجنائية الرقمية – مفهومها ودورها فى الإثبات – المجلة العربية للدراسات الأمنية والتدريب – المجلد 17 – العدد 33 – الرياض – 2002.
د / محمد الأمين البشرى – التحقيق وجمع الأدلة فى مجال الجرائم الإلكترونية – مؤتمر القانون والكمبيوتر والإنترنت – جامعة الإمارات العربية – كلية الشريعة والقانون من 1 – 3 مايو 2000 – المجلد الثالث.
د/ محمد سامى الشوا – الغش المعلوماتى كظاهرة إجرامية مستحدثة ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائى – القاهرة – 25 – 28 – أكتوبر 1993 .
د / محمد عبدالرسول خياط " عمليات تزوير البطاقات الائتمانية – أعمال ندوة تزوير البطاقات الائتمانية أكاديمية نايف العربية للعلوم الأمنية الرياض 2002.
د / محمد محمد الهادى ، د / نشأت خميس الغياطى أحمد – نحو مستقبل أفضل لتكنولوجيا المعلومات فى مصر – أبحاث ودراسات المؤتمر العلمى الأول لنظم المعلومات وتكنولوجيا الحاسبات الذى نظمته الجمعية المصرية لنظم المعلومات وتكنولوجيا الحاسبات – القاهرة – المكتبة الأكاديمية 1995.
د / محمد محى الدين عوض – مشكلات السياسة الجنائية المعاصرة فى جرائم نظم المعلومات (الكمبيوتر) – ورقة عمل مقدمة إلى المؤتمر السادس للجمعية المصرية للقانون الجنائى – القاهرة – 28/25 تشرين الأول 1993 .
د / ممدوح عبد المطلب ، زبيدة محمد قاسم ، عبدالله عبدالعزيز ، نموذج مقترح لقواعد الدليل الرقمى للإثبات فى جرائم الكمبيوتر – منشور ضمن

أعمال المؤتمر – الأعمال المصرفية والإلكترونية – نظمته كلية الشريعة والقانون – جامعة الإمارات فى الفترة 9-2003/5/12 – المجلد الخامس .
د / هشام محمد فريد رستم – بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت والذى عقد بدولة الإمارات العربية المتحدة خلال الفترة من 1-3 مايو 2000.

ثانيا:المراجع الأجنبية .

Brian crrier – open source Digital forensics tools .the legal Argument – oct2002 p.2.

Eaghancasey ,digital evidence and forensic computer and the internet, computer creamiest, academic press. USA UK 2000 P.9.s

GELBSTEIN Eduardo , Governance de l,internet enjeux – acteurs et fractures, publie por diplofoundation et global knawledge partnership suisse 2005 , p 98.

Hubert Bouchet – lacybervelllance des salaries dans l'entreprise – rapport o'etude etde consolation publique – mors,2001.p.12

John Eaton jermysmithirs.Amanagers guide to information technology, London , Philip Appan 1982 p. 263.

MASCALA corinne" eriminalite et contract electronique " le contract electronique , travaux de l'association CAPLTANT Henri, Journos motional, Paris 2000 p. 118.

Naughan Bevan Ken Lidstone – A guide to the police and criminal Evidence Act 1984 – Butterworth – London – 1985 – p. 497.

Orin S. Kerr , digital evidence and the new criminal procedure . coeumbia low review (vol – 105 : 279) – 2005 .

ORINS.KERR. searches and seizures in a digital world.op.at p. 540.

POTRICK S. CHEN – An Automatic system for collection crime in formation on the internet – 31

October 2000 – Journal of information low and technology available on line in Jan 2001 at http//elj. Warwick .ac .uk / jit00 – 3 / chen .htnl.

Robet taylor, computer crine0in criminal investigation edited by charges . Swanson , n, chameleon and territory hill , ine 5editian1992 p 1.

SEDALLAN Valerie Drait de l'internetReglementation – Responsibilities – contrat ,Edilion Net press, paris, 1997,p149.

TOM forester , Essential problems to hig-tech society first mitpres edition , cambridge Massachusetts , 1989.p.104.