الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

كلية الحقوق والعلوم السياسية

قسم الحقوق

الإثبات الجنائي في الجرائم الالكترونية

مذكرة ضمن متطلبات

نيل شهادة الماستر في شعبة الحقوق تخصص قانون جنائي

اعداد الطالب :

- صكصك محمد

إشراف الاستاذ :

- بن جاري عمر

لجنة المناقشة

أ/د ضيفي نعاس	رئيسا
أ/ بن جاري عمر	مشرفا و مقررا
أ/ طعيبة عيسى	ممتحنا

الموسم الجامعي 2022/2021

الشكر و العرفان

الحمد لله والشكر من لا يشكر الناس فلا يشكر الله

الشكر الموصول الى الأساتذة الكرام

الأستاذ المشرف بن جاري عمر على مساندته وتصحيحه وتسهيله وتشجيعه ومتابعته للمذكرة

والأستاذان طعيبة عيسى وضيفي نعاس على الإرشادات والتوجيهات ولهما مني فائق الشكر والاحترام والتقدير

الاهداء

أهدي هذه المذكرة بكل حرف فيها الى من كان سبب الوجود لوالدي الحبيبان وبالأخص لأبي وان يجعلها في ميزان حسناتهما والى العائلة الكريمة وأخواتي واخوتي وبالأخص احمد الأخ والصاحب الطيب والى الدكتورة والزوجة الوفية والراقية والغالية الحنونة فاطمة الزهراء والى بنيتي سيرين وقرة عيني علي وأحمد حفظهم الله

مقدمـــــــــة

مقدمة:

لم يكن أحد يتصور بأن البشرية ستدخل عصرا اسمه عصر المعلوماتية، فقد استفاق العالم فجأة على ثورة المعلومات مجالها الحاسوب والانترنت وهي شبكة ممتدة عبر العالم ومرتبطة. حولت العالم وبسرعة إلى قرية صغيرة، فقد مكنت هذه التقنية من توفير قفزة نوعية بسرت المعاملات وسهلت الاتصالات بل الأكثر من ذلك أنها باتت مجالا واسعا للولوج الى عالم شاسع من المعلومات. و بقدر ما يتصوره البعض عالما افتراضيا فقد بات حقيقة ملموسة من خلال المعاملات التي أضحى الحاسوب مجالا لها مثل التجارة الالكترونية والتحويلات المالية الافتراضية بدلا من النقود الورقية وزاد التطور إلى حد الاستغناء على الإدارة الورقية فتشكل ما يسمى بالحكومة الالكتروني.

ان هذا التطور التكنولوجي المذهل صاحبته ظاهرة أخرى حيرت رجال القانون وهي الجريمة المعلوماتية هذه الظاهرة الإجرامية الحديثة سرعان ما أخذت في التطور والتنوع وازدادت خطورتها كلما توسع استعمال الحاسوب والانترنت بل أن خطورة هذه الظاهرة تكمن في كونها عابرة للحدود ولا تنحصر في إقليم محدد أو داخل حدود الوطن، كما أن محترفوها أو ما يسمى بالمجرم الالكتروني هم بمواصفات خاصة يتمتعون بقدر كبير من المعرفة والذكاء كل ذلك دفع المجتمعات والحكومات إلى الاجتهاد في إصدار قوانين ردعية المواجهة هذه الظاهرة.

بات واضحا أن الجريمة المعلوماتية فرضت نفسها بقوة وازدادت خطورتها بتزايد الاستعمالات اليومية لشبكة الانترنت سيما في مجال الاقتصاد فازدادت ظاهرة سرقة الأموال واختراق المواقع وسرقة البيانات والاعتداء على الحياة الخاصة كل ذلك سرع من إصدار تشريعات متخصصة للحد من هذه الجريمة ومجابهتها لكن الصعوبة تظل قائمة في كيفية ملاحقة المجرمين وتقفي آثارهم والوصول إليهم فإذا كانت التشريعات المختلفة قد أوجدت النص القانوني للتعريف بالجريمة الالكترونية وتحديد العقاب المسلط على مرتكبيها فإن الوصول إلى هذه النتيجة يظل من الصعوبة بمكان ذلك أنه من البديهي جدا أن إثبات قيام أية جريمة لا بد من توفر الدليل بشأنها وهنا تكمن الصعوبة إذ أن الوصول إلى الدليل في مثل هذا النوع من الجرائم صعب المنال وبسبب بسيط هو أن الدخول إلى الحاسوب بغية التفتيش عن الدليل أو تعقب آثار المجرم المعلوماتي يصطدم بعوائق هامة

وخطيرة تميزها عمليات التشفير للبيانات أو تخزينها عن طريق جهاز مرتبط بالخارج بواسطة شبكات الاتصال ثم أنه إذا كان توقيع العقاب سهلا وميسرا فإن جمع الأدلة وإثبات الجريمة المرتكبة عبر الانترنت ومدى صحة وصلاحية الدليل الرقمي يطرح العديد من الصعوبات والإشكالات القانونية وهنا تكمن أهمية الموضوع.

كما أن أهمية الموضوع تبرز أيضا في البحث في مدى جدية وفعالية النصوص القانونية الجنائية والإجرائية لمساعدة المحققين وفسح المجال أمامهم للبحث عن الدليل والحصول عليه وجعله وسيلة اقتناع اللقاضي الجنائي في مجال الجريمة المعلوماتية.

لقد أثبت الواقع العملي أن الجرائم الالكترونية تعرف تطورا مذهلا وأصبحت تشكل تحديا كبيرا وتتطلب جهودا متظافرة من طرف مختلف الأجهزة الأمنية والقضائية بغية إيجاد السبل الكفيلة لمواجهتها سيما وأنها تتميز بتعدد اشكالها وصورها ويتضح بأن الوصول إلى كشف هذا النوع من الجرائم يعد تحديا كبيرا أمام صعوبة الوصول إلى الدليل أو الحصول عليه.

لأن الأمر هنا يتجاوز الوسائل التقليدية ويرتكز فقط على الوسائل التقنية والعلمية الحديثة وهو ما يثير الرغبة والفضول للغوص في الموضوع لمعرفة طبيعة هذه الأدلة وكيفية الوصول إليها وتحديد طابعها القانوني ومدى حجيتها في الإثبات الجنائي وكل ذلك كان الدافع لاختيار هذا الموضوع.

ان الفراغ القانوني لا يزال قائما رغم ان الجهود المبذولة على مختلف الأصعدة إلى حد الآن لمواجهة الجريمة الالكترونية و بالأخص ما يتصل بالجوانب الاجرائية في مجال الوصول الى الدليل و تقفي آثار المجرم المعلوماتي، لذلك فإننا نصبو من خلال البحث الى ابراز الأهداف التالية :

- التعريف أكثر بالأدلة الجنائية الحديثة على اختلاف أنواعها.

- إبراز الأعمال الإجرائية المعتمدة للوصول إلى الدليل الرقمي والتعريف بهذه الإجراءات، ثم تحديد المعيار الضامن لمشروعية هذه الأعمال الإجرائية والغاية من كل ذلك هو وضع لبنة أمام المهتمين والمساهمة ولو بقدر بسيط في إثراء الموضوع.

من الواضح أن رصد الأدلة الالكترونية وضبطها بغية الوصول إلى إثبات الجريمة الكترونية يعد من الصعوبة بمكان نظرا لطابع الجريمة في حد ذاتها ومن ثم فإن الإشكالية

التي تطرح في هذا البحث هيكيف يتم الحصول على الدليل الجنائي ووضع اليد عليه في غياب الدليل المرئي أو المادي، وما مدى الصعوبة التي تواجه ذلك على اعتبار أن الأفعال المجرمة سيما التي تقع على الكيانات المعنوية للحاسوب تبقى في شكل نبضات أو ذبذبات، وفي حال ما إذا تحولت تلك البيانات إلى مستخرجات أو مستندات وأضحت كيان مادي ملموس فكيف يمكن الوصول إليها لضبطها لتقديمها كدليل إدانة ضد المجرم المعلوماتي , وما مدى حجيتها أمام القاضي الجنائي.ثم كيف يمكن إضفاء المشروعية على الأعمال الإجرائية للوصول إلى الدليل أو بمعنى آخر كيف يتم التوفيق بين مبدأ عدم انتهاك حرمة الحياة الخاصة المكرس دستوريا وحتمية الوصول إلى الدليل.

كل ذلك يحتم إيجاد الإجابات السديدة والتوضيحات المناسبة من خلال عناصر البحث والذي اخترت بأن اتبع فيه المنهج التحليلي نظرا لما يتسم به الموضوع من جوانب تقنية وقانونية ومحاولة الوصول إلى التوفيق والربط بينها لاستجلاء الأسس التي يمكن الاعتماد عليها في معرفة الدليل والوصول إليه وتعزيز حجيته وجعله وسيلة لتشكيل قناعة القاضي.

ومن أجل الإلمام بالموضوع والتصدي لهذه الإشكالات أفردنا للبحث فصلين كاملين تناولت في الفصل الأول مفهوم الجريمة المعلوماتية. و وسائل الحصول على الدليل الرقمي بشأنها و ماهية هذا الدليل بشكل عام . ثم خصصت الفصل الثاني للتعريف بالطبيعة القانونية للدليل الالكتروني و كيفية الوصول اليه. ثم مدى حجيته .

الفصل الاول

مفهوم الجريمة الالكترونية و وسائل الحصول على الدليل الالكتروني.

تمهيد:

يجب التأكيد ومنذ البداية أنه لا وجود لجريمة معلوماتية أو الكترونية بدون وجود جهاز حاسوب بمكوناته المادية والمعنوية أو البرامجية ذلك أن الحاسوب قد يكون هدفا للجريمة أو أداة لها وبيئة لها و اما أداة للكشف عنها، ومجابهتها ومن هنا يمكننا القول بأن التطور السريع والمستمر في استخدام الحاسوب، صاحبته ظاهرة تعد خطيرة للغاية وهي الجريمة المعلوماتية وهي ظاهرة اجرامية جديدة ومما يزيد من خطورتها أنها تطال الحياة الخاصة للأشخاص وتستهدف المعلومات لذلك فإن تحديد مفهومها وإدراك ماهية هذه الجريمة بمختلف صورها، يتطلب استقراء أراء الفقهاء والوقوف على التعريف المستنبط لها، بما تتخذه من المصطلحات الدالة عليها ذلك أن هذا النوع من الجرائم يتميز بتعدد الأشكال منها جرائم اختراق شبكات المعلومات، واتلاف البيانات وتدمير البرمجيات وسرقة المعلومات وغير ذلك كثير. واذا كانت الجريمة المعلوماتية ظاهرة قائمة ومتفاقمة الآن فإن الجهود المتواصلة لمجابهتها تصطدم بعدة عراقيل، سيما على مستوى النص الإجرائي للوصول إلى مرتكبي هذه الجرائم وتقديمهم للعدالة نظرا الخصوصية هذا النوع من الجرائم وطابعها الخاص ومن هنا تثار الصعوبة حول إمكانية الحصول على الدليل الرقمي وهو أمر يشكل بحد ذاته تحديا كبيرا, وعلى ضوء ذلك سنتناول في هذا الفصل ماهية الجريمة الالكترونية في المبحث الاول و مفهوم الاثبات الجنائي في الجريمة الالكترونية و وسائله الحديثة في المبحث الثاني .

المبحث الأول: ماهية الجريمة الالكترونية

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

المطلب الأول: تعريف الجريمة الالكترونية

قبل التطرق إلى تعريف الجريمة الالكترونية أو المعلوماتية نشير إلى توضيح بعض المصطلحات في مجال المعلوماتية ، فهذه الكلمة كما يبدو مشتقة من معلومة والمعلومات يستخدمها البعض كألفاظ مترادفة للبيانات. بينما يرى مختصون بأن هذه الأخيرة مجموعة من الحقائق أو المشاهدات أو القياسات التي تكون عادة في شكل حروف أو أرقام أو اشكال خاصة توصف أو تمثل فكرة. و تمثل هذه البيانات المادة الخام التي يتم تجهيزها للحصول على المعلومات[1].

وقد أصبحت المعلومات تشكل قيمة اقتصادية هائلة نظرا لضخامة حجمها وقيمتها وتوصف بكونها تشكل في الوقت الراهن سلعة تباع وتشترى[2]. وبذلك أضحت محل اهتمام عالمي تحظى بالحماية، ولذلك نلاحظ أن التشريعات العالمية سارعت إلى إصدار نصوص تشريعية في الجريمة المعلوماتية. وضع اطر قانونية ملائمة لتحديد شروط استعمال المعلوماتية وتكنولوجيات الإعلام والاتصال في مختلف المعاملات وحماية الأنظمة المعلوماتية وتجدر الإشارة إلى أن كثير من الدول أصدرت قوانين في الإطار المذكور ونذكر منها:

---

[1] جميل عبد الباقي الصغير . الانترنت و القانون الجنائي" الأحكام الموضوعية للجرائم المتعلقة بالانترنت. الطبعة الأولى. دار النهضة العربية :مصر. 2001. ص 03.

[2] كوثر مازوني. الشبكة الرقمية وعلاقتها بالملكية الفكرية.دط. دار هومة للطباعة والنشر : الجزائر. 2008. ص115.

- السويد: أصدرت سنة 1977 أول تشريع فدرالي خاص بجرام الحاسوب.
فرنسا: أصدرت عام 1988 قانون Godfrain الخاص بجرائم المساس بأنظمة المعالجة الآلية للمعطيات وقبل ذلك أصدرت سنة 1978 قانون الحريات والمعلوماتية .
-اليابان: أصدرت سنة 1988 قانون حماية المعطيات الشخصية وفي سنة 1999 قانون يجرم الدخول غير المشروع للحاسوب.
بلجيكا: عدلت سنة 2000 قانون العقوبات وأدخلت جرائم المساس بأنظمة المعالجة الآلية للمعطيات.

يضاف إلى كل ذلك تبني المجلس الأوروبي اتفاقية حماية المعطيات الشخصية لسنة 1981[1] ثم تلى ذلك اتفاقية المجلس الأوروبي لمكافحة الجريمة الافتراضية والتي انضمت إليها الولايات المتحدة الأمريكية وكندا واليابان وجنوب أفريقيا[2]. ويمكن الإشارة أيضا إلى صدور قوانين عديدة في الولايات المتحدة الأمريكية منها القانون الفدرالي الخاص بحماية أنظمة الكمبيوتر الصادر سنة 1977 وفي مصر صدر القانون رقم 10 سنة 2003 ، المتعلق بتنظيم الاتصالات وقانون حماية الملكية الفكرية.[3] وقد حاول المشرع الجزائري مواكبة هذا التطور فبادر بتعديل قانون العقوبات بموجب القانون 06-23 المؤرخ في 20/12/ 2006 ، ثم تلاه القانون رقم 09-04 المؤرخ في 05/08/2009[4] والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ويمكن القول بأن مختلف هذه التشريعات تكاد تجمع بان مصطلح المعلومات يكاد ينحصر في أنها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تكون محلا للتبادل أو الاتصال أوللمعالجة بواسطة الأشخاص أو الأنظمة الالكترونية.[5]

في حين أفرد لها المشرع الجزائري تعريفا في القانون رقم 09/04 المادة 2 بالقول : "بان المنظومة المعلوماتية هي أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين

[1] مدحت رمضان جرائم الاعتداء على الاشخاص و الانترنت. دط. دار النهضة العربية: مصر. 2000. ص 109.

[2] مختار الاخضري بحث بعنوان الإطار القانوني لمواجهة جرائم المعلوماتية وجرائم الفضاء الافتراضي." نشرة القضاة" :العدد 66. 2010.ص 53.

[3] زيدان زيبحة. الجريمة المعلوماتية في التشريع الجزائري والدولي. الطبعة الأولى.مطبعة دار الهدى: الجزائر. 2011. ص 20.

[4] القانون رقم 09-04 المؤرخ في 05/08/2009. صدر بالجريدة الرسمية للجمهورية الجزائرية العدد 47.

[5] نائلة عادل محمد فريد قورة . جرائم الحاسب الآلي الاقتصادية. الطبعة الأولى. منشورات الحلبي: لبنان 2005. ص 97.

" و الملاحظ أن هناك فرق بين البيانات والتي هي مجرد معطيات تتم معالجتها لتحول إلى معلومات.

فالمعطيات هي المادة الخام التي تستخرج منها المعلومات[1]. وقد ذهب المشرع الجزائري إلى تعريف المعطيات في المادة 2 فقرة 3 من القانون رقم: 09/04 المشار له بما يلي: "بأنها أي عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها". وقد أكدت بعض الآراء بأن المعلومات يجب أن تتوفر فيها شروط قانونية لكي تتمتع بالحماية القانونية ومنها أن تكون محددة تحديدا دقيقا وأن تتوفر فيها السرية والاستئثار أي أنه إذا كانت شائعة فإنها تكون بعيدة عن حيازة شخص بعينه وهو لا يستأثر بها كالرقم السري مثلا [2].

كما أن بعض الآراء الفقهية ذهبت الى التفريق بين المعلومة وبرامج الحاسب الآلي، والذي وجد لمساعدة مستخدميه في معالجة البيانات وإجراء العمليات وفق مجموعة من المهام مثل تخزين البيانات ولكي يتم حل أية مسألة بواسطة الحاسوب يجب تغذيته بمجموعة من التعليمات أو الأوامر والبيانات اللازمة للحل وتسمى مجموعة هذه التعليمات بالبرامج Programes؟[3]

فبرنامج الحاسوب يعد من العناصر الأساسية للكيان المنطقي لأي حاسوب فالحاسوب بدون برنامج يبقى مجرد ألة ويعرف الكيان المنطقي في حد ذاته بأنه " مجموعة البرامج والأساليب والقواعد وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات[4].

والكيان المنطقي هو مصطلح أعم و أشمل من البرنامج و بعنى آخر تعرف البرمجية بأنها « :مجموعة التعليمات المعبر عنها بمفردات أو بدائل أو مخططات أو بأي شكل أخر، والتي تمكن من القيام بنشاط علمي أو نوع أخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بألة وتترجم باندفاعات الكترونية وهي أسلوب الكتروني أو ما يشبه

---

[1] انتصار نوري الغريب. أمن الكمبيوتر والقانون . الطبعة الأولى مدار الراتب الجامعية:بيروت.1994. ص 81.

[2] محمد صادق اسماعيل. الجرائمالالكترونية "دراسة قانونية قضائية مقارنة"، الطبعة الأولى. المركز القومي اللاصدارات القانونية :مصر.2012.ص 45.

[3] هدى حامد قشقوش. جرائم الحاسب الالكتروني والتشريع المقارن .دط. دار النهضة العربية: القاهرة.مصر.1992 .ص 6.

[4] رشا مصطفى أبو الغيط . الحماية القانونية للكيانات المنطقية برنامج الحاسوب" دط. ملتقى الفكر للطباعة : الاسكندرية.مصر. 2000. ص 05.

ذلك بشرط أن يكون صالحا لمعالجة الإعلام» [1].وعلى خلاف تعريف البرمجيات فإن هناك تعريفات أخرى لبرنامج الحاسوب منها أنه: « جميع العناصر غير المادية وغير الملموسة اللازمة لتشغيل اجهزة الكمبيوتر فهو بمثابة مجموعة أوامر وتعليمات قابلة للتنفيذ عبد العال الديربيي .

[2]كما أعطي له تعريفا أخر هو أنه: مجموعة من الأوامر و الإرشادات التي تحدد الجهاز الحاسوب العمليات التي يقوم بتنفيذها بتسلسل و خطوات محددة و تحمل هذه العمليات على وسيط معين يمكن قراءاته عن طريق الآلة، و يمكن للبرنامج عن طريق معالجة المعطيات أن يؤدي وظائف معينة ويحقق النتائج المطلوبة»[3]. كما أن برنامج الحاسوب يختلف عن قاعدة البيانات والتي هي بمثابة بنك معلومات وهي مجموعة البيانات التي تخزن وتسترجع وتعطي المعرفة أو ما يسمى بالمعلومة وبقدر ما هي نتاج فكري مرتبط بصاحبه فهي بمثابة مصنف يحميه القانون بما في ذلك مواقع الويب والمعبر عنها بشبكة المعلومات الدولية « World wideWEB »، التي يرمز لها اختصارا WWW وهي تتضمن مختلف المعلومات في مختلف المجالات وتشمل مجموعة هامة من المواقع (Site internet) سواء عامة المؤسسات أو شركات أو خاصة بالأشخاص ويبدو أن أغلب التشريعات أضفت على البرمجيات والمواقع حماية قانونية باعتبارها مصنفات محمية إذ أصدرت دول الاتحاد الأوروبي قرار توجيهيا بشأن حماية قواعد البيانات في 11/03/1996[4].

وقد أورد المشرع الجزائري ضمن قانون حق المؤلف والحقوق المجاورة الصادر بالأمر رقم 03-05 في 2003 نص المادة 04 من هذا الأمر والتي تدرج برنامج الحاسوب ضمن المصنفات الأدبية المحمية.

---

[1] محي الدين عكاشة . محاضرات في الملكية الأدبية والفنية. ط. ديوان المطبوعات الجامعية:الجزائر. 2001. ص48.

[2] محمد الهادي بن زيطة .حماية برنامج الحاسوب في التشريع الجزائري. الطبعة الأولى . دار الخلدونية: الجزائر.2007. ص 34

[3]هاني محمد دويدار.نطاق احتكار التكنولوجية بواسطة المعرفة السرية..ط. دار الجامعة الجديدة للنشر:مصر. 1996ص: 41.

[4]عفيفي كمال عفيفي. فتوحالشادلي. جرائم الكمبيوتر. دط. منشورات الحلبي الحقوقية:لبنان. 2003، ص 27.

وإذا كان الموقع « Site »كما يعرف بأنه عبارة عن عقل الكتروني متسع يمكن من الربط المباشر المجموعة من شبكات الانترنت عن طريق استقبال المعلومات وتخزينها وتوزيعها.[1]

فان المشرع الجزائري عرف الموقع في المادة 03 من المرسوم رقم 98-257 المتعلق بشروط اقامة خدمات الانترنت بأنه أي مكان يحتوي موزعا أو عدة موزعات للمعطيات الضرورية لتقديم خدمات الانترنت[2]..

وفي سياق المصطلحات المتداولة في مجال المفاهيم المتعلقة بالجريمة المعلوماتية أو الرقمية (مصطلح الرقمية) فيقال الجريمة الرقمية أو الدليل الرقمي وقد يتصور البعض أن الجريمة تنصب على الأرقام وهذا غير صحيح إذ أن المقصود هو أن المصطلح المذكور مرجعه استخدام النظام الرقمي الثنائي (0-1) وهي الصيغة التي تسجل بها كل البيانات (اشكال وحروف ورموز وغيرها داخل الحاسب الآلي) إذ يمثل (0) وضع الإغلاق OFF والواحد (1) وضع التشغيل ON ويمثل الرقم صفر (0) أو الرقم (1) ما يعرف بالبايت *Bit.[3]

و مثلما جرى الاختلاف في تعريف المعلومة في حد ذاتها فقد تعددت وتنوعت التعاريف التي تناولت الجريمة المعلوماتية إذا لا يوجد هناك تعريف جامع ومحدد يحظى باتفاق فقهاء القانون وقد ذهب البعض إلى القول بعدم إعطاء تعريف لها بحجة أن هذا النوع من الإجرام ما هو الا جريمة تقليدية ترتكب بأسلوب الكتروني ويمكن القول بأنه من الصعوبة وضع تعريف مانع جامع لها، فهي بطبعها تأبي التعريف بل وصعبة التعريف ومستعصية عليه ونظرا للتطور المتلاحق الذي تمر به وسرعة بروز اشكالجديد مستحدثة

---

[1] زيدان زيبحة . مرجع سابق. ص 36.

[2] –المادة 03 من المرسوم رقم 98–257 المتعلق بشروط اقامة خدمات الانترنت.

[3] محمد عبيد سيف سعيد المسماري. عبد الناصر محمد محمود فرغلي. الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والطب الشرعي. بحث مقدم للمؤتمر الشرعي":12– 14/11/2007.جامعة نايف العربية للعلوم الأمنية: الرياض – السعودية. ص 05.

لها[1] . ويمكن تصنيف التعريفات إلى أربعة اتجاهات، فالاتجاه الأول يستند في تعريف الجريمة إلى وسيلة ارتكاب الجريمة فيشترطون وجوب ارتكابها بواسطة الحاسب الألي.

أما الاتجاه الثاني فيستند إلى موضوع الجريمة فيشرط أن يكون الحاسب الالي هو محل الجريمة أي بمعنى أن يتم الاعتداء على الحاسب الالي أو على نظامه [2]، أما الاتجاه الثالث فيستند إلى معيار شخصي فيشترط أن يكون مرتكب هذا النوع من الجرائم ملما بتقنية المعلومات ولديه مهارة استخدام الحاسوب حتى يمكن اعتبار الفعل من جرائم الحاسب الألي.

ويذهب اتجاه أخر إلى تصنيف الجرائم المعلوماتية إلى أربعة أصناف وهي :

1- جرائم استغلال البيانات

المخزنة على الحاسب الألي بشكل

غير قانوني مثل سرقة البيانات

والمعلومات، التجسس الالكتروني .... الخ.

2- جرائم اختراق الحاسب الألي بغير تدمير البرنامج والبيانات الموجودة في الملفات المخزنة فيه من خلال بث الفيروسات والتي تؤدي إلى تعطيل نظام التشغيل أو اتلاف البرامج.[3]

3- جرائم استخدام الحاسب للتخطيط أو ارتكاب جرائم تقليدية كاستخدامه في تزوير مستندات والمحررات

الرسمية أو العرفية.

4- جرائم استخدام الحاسب الألي بشكل غير قانوني من قبل المعهود لهم باستعماله، كسرقة المعلومات أو افشائها وما أشبه ذلك، وفي كل ذلك يستخلص بأن المجرم المعلوماتي أخذ هو الأخر تعريفات مختلفة

---

[1] محمد سامي الشوا. ثورة المعلومات و انعكاساتها على قانون العقوبات. الطبعة الأولى. دار النهضة العربية: مصر 1994، ص 05.

[2] عفيفي كمال عفيفي.فتوحالشادلي. مرجع سابق.ص 30. –عفيفي كمال عفيفي .

[3] فتوح الشادلي . المرجع نفسه. ص 31.

بالنظر إلى كونه يختلف عن مرتكبي الجرائم التقليدية ، فمن أهم مميزاته أنه يتمتع بقدر من المعرفة والمهارة، إذ أن مجال ممارسة أفعاله الإجرامية هي الحاسوب الألي لذلك فهو يمتلك المهارة في المجال التكنولوجي ومعرفة انظمة الكومبيوتر [1].

ومن سماته أيضا أنه مجرم غيرعنيف فهو يعتمد على الذكاء ويعمد إلى أسلوب الحيلة ولا يستعمل العنف ويصنف البعض هؤلاء المجرمين إلى ثلاثة أنواع أو أصناف وهي:

1- فئة الفضولين أو الهواة أو العابثين ويطلق عليه مصطلح « الهاكرز» ، وقد أطلق هذا المصطلح لأول مرة في الستينات عن طريق مجموعة من الطلبة الذين يدرسون في الجامعات الأمريكية ممن يتميزون بقدر كبير من الكفاءة التقنية ويتفاخرون بإلمامهم بعلوم الحاسوب وبقدرتهم على اختراق شبكات الحاسب الآلي وبجهدهم الذاتي وأغلب هؤلاء من صغر السن أو المراهقين المولعين بالشبكة العنكبوتية، حيث يدفعهم الفضول إلى معرفة كلمة سر بعض الأشخاص والدخول إلى نظامهم المعلوماتي وهؤلاء لا يشكلون خطرا[2]، وذهب البعض الأخر إلى اعتبار هؤلاء في رتبة أقل من المجرمين لأن سلوكهم بسيط وبدافع المغامرة والتحدي وأنهم لا يهدفون إلى الحصول على المعلومات بخلاف المحترفون الذين يهدفون إلى الاستلاء على البيانات.

2- أما الطائفة الثانية فهم المحترفون من مرتكبي جرائم الحاسب الآلي، ويطلق عليهم مصطلح الكراكز Crackers ويتمتع هؤلاء بالتخصص العالي في مجال الحاسب الألي وأغلبهم ممن يعلمون في منشآت تستخدم الحاسب الآلي وهم بذلك مطلعون باستمرار على محتوياته وأسراره[3]، ويصفهم الفقه بالقول"

بأن محترفي ارتكاب جرائم الحاسب الألي يتميزون بأنهم أفراد لهم مكانة عالية في المجتمع ويتمتعون بقدر ليس بقليل من العلم كون أن هذه الجرائم تستلزم الماما كافيا بالمهارات والمعارف الفنية المتصلة بالحاسب الآلي وتشغيله"[4]. ويقال عنهم" بأنهم

---

[1] داود حسن طاهر . نظم المعلومات..ط. اكادمية نايف الامنية: الرياض – السعودية.1420 هجري . ص 65.

[2] فاروقحسين. معجم مصطلحات الحاسب الألي. ط. دار الراتب الجامعية: بيروت.لبنان. 1999، ص 80

[3] فاروق حسين. المرجع نفسه . ص84

[4] جميل عبد الباقي الصغير. مرجع سابق. ص 15.

أشخاص متسللون يتابعون عن كثب أخر الأخبار وبرامج الحماية الأمنية للأجهزة والمعلومات و ينشؤون أحيانا نوادي لتبادل المعلومات"[1].

وبالعودة إلى تعريف الجريمة الالكترونية فقد ذهبت آراء بعض الفقهاء إلى تعرفيها بأنها الفعل غير المشروع الذي يساهم الحاسوب في ارتكابه أو هي: الفعل غير المشرع الذي يكون الحاسب الألي أداة رئيسية في ارتكابه أو هي كذلك مختلف صور السلوك الإجرامي التي ترتكب باستخدام المعالجة الألية للبيانات أو هي أيضا عمل أو امتناع عن عمل يأتيه الإنسان أضرارا بمكونات الحاسب وشبكات الاتصال

الخاصة به التي يحميها قانون العقوبات ويفرد لها عقابا[2].

كما تعرف بأنها فعل أو أفعال غير مشروعة تتم بواسطة أو تستهدف النظم البرامجية أو نظم المعالجة الالكترونية للحاسب الألي أو الشبكات الحاسوبية أو شبكة الانترنت أو ما على شاكلتها[3]، وفي تعريف أخر يبدو أقرب إلى الفهم كما أورده الدكتور عبد الفتاح بيومي حجازي بالقول بأن الجريمة المعلوماتية عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الألي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي [4]»

وعلى خلاف هذه التعريفات فإن هناك من يقتصر على مجالين في تعريف الجريمة المعلوماتية ومنها التعريف الضيق والتعريف الموسع فالأول يربطها باستخدام الحاسب الألي كأداة رئيسية ويدخل في نطاق تعريف مفهوم الجريمة المعلوماتية الضيقة التعريف الصادر عن مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية بأنها الجرائم التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسيا[5]. وإلى جانب ذلك فإن التعريفات الموسعة لمفهوم الجريمة المعلوماتية تذهب إلى القول بأنها تشمل إلى جانب الحاسوب كأداة لارتكاب الجريمة استهداف الحاسوب في حد ذاته بسرقته أو الولوج إلى مكوناته.[6]

---

[1] داود حسن طاهر، مرجع سابق، ص 65

[2] داود حسن طاهر. المرجع نفسه.ص 68

[3] محمد عبيد سيف سعيد المسماري. عبد الناصر محمد محمود فرغلي . مرجع سابق، ص 43.

[4] عبد الفتاح بيومي حجازي. الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت. ط. دار الكتب القانونية :مصر. 2002. ص28

[5] عبد الفتاح بيومي حجازي. الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت. مرجعسابق. ص68

[6] أحمد خليفة الملط. الجرائم المعلوماتية . الطبعة الثانية. دار الفكر الجامعي الاسكندرية.مصر. 2006. ص 167

ويمكن في خلاصة الأمر تبني التعريف الذي أقره مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي عرف الجريمة المعلوماتية بأنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوب وتشتمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية".[1]

المطلب الثاني: خصائص الجريمة الالكترونية

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

1- أنها تتم في بيئة رقمية الكترونية مجالها الحاسب الألي بمكوناته المادية من أجهزة ومعدات وتجهيزات

الحاسب الألي ومكوناته المعنوية من النظم البرامجية.[2]

2- سرعة التنفيذ : إذا يمكن ارتكابها وبضغطة واحدة على لوحة المفاتيح فهي جريمة تتم في وقت ضئيل

قد لا يتعدى ثانية واحدة .

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

4- أنها جريمة ناعمة تخلوا من أي عنف فنقل البيانات من جهاز حاسب إلى أخر يجري بطريقة ألية سهلة.

5- أنها جريمة صعبة الأثبات وذلك راجع إلى صعوبة الوصول إلى الدليل اوأثار مادية يتركها المجرم كما هو الشأن في الجريمة التقليدية إذ يمكن وبسهولة محو الدليل أوتدميره في زمن قياسي[3]، ولما كانت الجريمة المعلوماتية تكتسي هذا الطابع الخاص بها والمميز عن الجريمة التقليدية فقد كان من الضروري أن يوضع لها إطار خاص من حيث الطبيعة القانونية لهذه الخصوصية ومن هنا أوجدت التشريعات نصوصا خاصة لمواجهة الإشكالات القانونية التي قد تثار لا سيما بخصوص جمع الأدلة ومدى قبولها من طرف

---

[1] محمد سامي الشوا. مرجع سابق، ص 10.

[2] محمد سامي الشوا . المرجع نفسه. ص 18.

[3] يونس خالد عرب. العالم الالكتروني "الوسائل و المحتوى و المزايا و السلبيات" .منشورات اتحاد المصاريف العربية: الأردن. 2001. ص 72

الجهات القضائية ثم تحديد الجهة القضائية التي يؤول إليها الاختصاص في محاكمة مرتكب هذا النوع من الجرائم.[1]

وقد سعت مختلف التشريعات إلى توسيع مجال التعاون الدولي والتقارب في المفاهيم القانونية حول الجريمة المعلوماتية، إذ أنها وبهذا الشكل لا تعترف بالحدود بين الدول ولعل ذلك لا يقتصر على نوع أو التبادل واحد من هذه الجرائم كزرع الفيروسات أو اختراق عمليات التحويل الالكتروني للأموال الالكتروني للمعلومات.[2]

وقد سارت مختلف التشريعات في إطار التبادل الدولي على وضع الأطر القانونية لحماية الحياة الخاصة للأفراد وقد أثارت هذه النقطة اهتمام المنظمات العالمية والاقليمية ويبرز هنا موقف منظمة الأمم المتحدة والمجلس الأوروبي ومنظمة التعاون الاقتصادي فمنظمة الأمم المتحدة كانت سباقة في ميدان حماية الحياة الخاصة في مواجهة التقدم التقني منذ تبنيها لتوصيات مؤتمر طهران سنة 1968 والتي جاء فيها بأن الحاسبات الالكترونية تمثل أكبر تهديد للحياة الخاصة والحرية الشخصية سيما إذا تم تخزين البيانات الشخصية على الحاسب الآلي وتحليلها.[3]

تم تلا ذلك توقيع اتفاقية مجلس أروبا والخاصة بحماية الأشخاص من مخاطر المعالجة الألية للبيانات ذات الطابع الشخصي والذي ظهرت في 17/9/1980 وبدأ سريانها الفعلي في أكتوبر 1985 إضافة إلى التوصيات العديدة التي صدرت فيما بعد[4].

ومن بينها أيضا التوصية الصادرة عن منظمة التعاون الاقتصادي والتنمية في 26/11/1992 والخاصة بحماية الحاسوب وشبكة المعلومات.

ويبدوا أن المشرع الجزائري بادر إلى مواكبة الجهود الدولية بوضعه لأطر قانونية للإحاطة بموضوع الجريمة المعلوماتية بشكل عام وحماية الحياة الخاصة للأفراد، والتي هي مكرسة في الدستور الجزائري إذ بادر المشرع الجزائري بتعديل قانون العقوبات بموجب القانون رقم 04/15 المؤرخ في 10/11/2004 وكذا القانون رقم 23-06 المؤرخ

---

[1] على حمودة الأدلة المتحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي الجزء الاول. "مجلة أكاديمية شرطه دبي": العدد 01. 2003 . دبي. ص 197

[2] نائلة عادل محمد فريد قورة . مرجعسابق. ص 54

[3] يونس خالد عرب. مرجعسابق.ص 125

[4] يونس خالد عرب. المرجع نفسه. ص128.

في 20/12/2006 أفرد له قسما خاصا وهو القسم السابع مكرر تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات ثم تلاه صدور القانون رقم 09-04 المؤرخ في 5/8/2009

والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والذي أعقبه فيما بعد المرسوم الرئاسي رقم 15-261 في 8/10/2015 يحدد تشكيله وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته[1].

ويبدو أنه وبالرغم من إصدار ترسانة من القوانين والتشريعات على المستوى المحلي والدولي فإن الأثار السلبية للثورة المعلوماتية ما فتئت تتزايد من خلال ارتفاع نسبة الجرائم المستحدثة التي ترتكب عن طريق الوسائل التقنية الحديثة وبالذات الحاسوب الانترنت[2].

المطلب الثالث: أساليب الجريمة الالكترونية والأثار الناجمة عنها

إن اشكال و أنواع الجرائم الالكترونية متعددة ومتنوعة ولكنها في الغالب لا تخرج عن نطاق الحاسب الألي ومكوناته وهي تتخذ أساليب وصور منها الاعتداء على أنظمة الحاسوب فتكون هذه الأخيرة هدفا أو محلا للجريمة أما الصورة الثانية فتتعلق بالاستعمال غير المشروع لنظم المعالجة الألية للمعلومات[3].

ويلاحظ بأن الصورة الأولى يستخدم فيها الجاني الحاسب الألي كوسيلة لارتكاب الجريمة ويكون ذلك بأي فعل يؤدي إلى تعطيل نظام المعالجة الألية عن القيام بوظائفه ويتم ذلك بالاختراق أو الدخول غير المشروع في كل جزء من منظومة المعالجة الألية للمعطيات وقد يتم ذلك بعدة طرق احتيالية منها.

---

[1] زيدان زيبحة. المرجع السابق .ص22

[2] عبد الفتاح بيومي حجازي. التجارة الالكترونية و حمايتها القانونية..ط. دار الفكر الجامعي الاسكندرية.مصر.2004. ص 14.

[3] عبد الله عبد الكريم عبد الله. جرائم المعلوماتية و الانترنت الجرائمالالكترونية دراسة مقارنة"، الطبعة الأولى. منشورات الحلبي الحقوقية:بيروت.لبنان.2007. ص 52.

استعمال رمز الدخول Code d'accesبصفة غير عادية أو باستعمال برامج أخرى مثل البرنامج المسمى حصان طروادة Cheval de troi'.[1]

وهو برنامج خادع يخفي ظاهرة غرضها غير مشروع ويظهر كبرنامج عادي يؤدي بعض المهام المفيدة والمألوفة لمستخدميه بينما يكون بداخله وبطريقة خفية بعض الأوامر أو التعليمات التي تؤدي عند تشغليه مهاما ضارة غير متوقعة تمثل أغراضه الحقيقة المضرة وقد بدأ هذا البرنامج في أمريكا في أواخر السبعينات نتيجة انتشار استخدام اللوحات الالكترونية للبيانات التي تنتج تخفيف أو زيادة تحميل البرامج وهذا النوع من البرامج يبدو عند تشغيله كأحد العاب التسلية ثم يقوم بعد ذلك بمحو أقراص النظام.[2]

وهناك من البرامج الخبيثة كذلك ما يتخذ صورا عديدة وتستهدف أغراضا عديدة منها ما يهدف إلى الاحتيال والاستيلاء بواسطة الحاسوب على الأموال وسرقة المعلومات أو تدمير البيانات ومنها بالإضافة إلى برنامج حصان طروادة برنامج ما يسمى بالقنابل الموقوتة أو المنطقية وبرنامج الدودة وهي برنامج تشغيل تندمج في نظم التشغيل[3].

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

أما المشرع الجزائري فقد انتهج نفس النهج كذلك حين بادر بتعديل قانون العقوبات بموجب القانون 04/15 المؤرخ في 10/11/2004 والذي تضمن ثماني مواد من المادة 394 مكرر إلى المادة 394 مكرر 7 ونص في ذلك على عدة جرائم منها :[4]

[1] هشام مُحَّد فريد رستم قانون العقوبات و مخاطر تقنية المعلومات .دط. مكتبة الآلات الحديثة: أسيوط.مصر.1994 ص 2

[2] جميل عبد الباقي الصغير. مرجعسابق. ص 23.

[3] هدى حامد قشقوش. مرجعسابق. ص 568

[4] مدحت رمضان .مرجعسابق. ص 98.

1- الدخول عن طريق الغش في كل أو جزء من منظومة المعالجة الألية للمعطيات .[1]

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

3- عرقلة السير العادي للمنظومة المعلوماتية .

4- تكوين جمعية الأشرار في عالم الانترنت.

أما الصورة الثانية والمتعلقة بالاستعمال غير المشروع لنظم المعالجة الآلية للمعلومات فتتجلى هذه الحالة في وضعيتين او صورتين منها الدخول أو البقاء غير المشروع، ونظام المعالجة الآلية الحالة الثانية هي سرقة منفعة الحاسب الآلي أو المال المعلوماتي[2]، كالدخول إلى نظام الحاسوب والوصول إلى محتوياته أو البقاء فيه بصورة غير مسموح بها ومثال على ذلك العامل المرخص له قانونا للدخول إلى المنظومة المعلوماتية في إطار عمله يقوم وباستعمال رموز الدخول المزيفة للإطلاع على معطيات لا تدخل في نطاق مهامه العادية ومن أمثلة ذلك أيضا قيام فريق مكون من خمسة أشخاص في شيكاغو بالولايات المتحدة الأمريكية يعملون بإحدى المراكز التعليمية باستغلال الحاسب الآلي التابع للمركز لبرمجة أعمال عملائهم الخاصة بشركة خاصة أخرى لهم[3]، ومثال أخر أنه تم اكتشاف استخدام الحاسب الآلي في أكبر معامل انتاج الصواريخ النووية وقاعدة FBI بالولايات المتحدة الأمريكية من قبل مئتي مستخدم وذلك لأغراضهم الشخصية.

وفي نفس السياق أكدت احصائيات قام بها مكتب التحقيق الفيدرالي بان خسائر الشركات من الهجمات الفيروسية وغيرها من الخروقات غير القانونية، يبلغ ما يقارب 68.2 مليون دولار سنويا، قد شملت هذه الإحصائيات أكثر من 2066 مؤسسة أو شركة متضررة من هذه الهجمات[4].

ويبدو أن اتساع رقعة انتشار المعلومات وعولمتها بسرعة أدى إلى ازدياد الجرائم الالكترونية سبب جرائم سرقة المعلومات والتي يعتبرها البعض أموالا منقولة وأنه يمكن

---

[1] زيدان زيبحة. مرجع سابق، ص 47

[2] محمد رمضان بازة. قانون العقوبات الليبي "جرائم الاعتداء على الأموال".دط. القسم الخاص . الجزء الثاني. منشورات جامعة ناصر: طرابلس. ليبيا 1992. ص 44.

[3] محمد سامي الشوا. مرجع سابق. ص 221. 4- هدى حامد قشقوش . مرجعسابق. ص 82.

[4] عبد الله عبد الكريم عبد الله. مرجع سابق، ص36

تقويمها بالمال انطلاقا من القيمة الاقتصادية لها[1]. وقد بات من السهولة بمكان لمحترفي الإجرام المعلوماتي إجراء تحويلات لهذه الأموال من أي مكان في العالم من خلال الولوج الى الملفات المدرجة في أنظمة الحاسوب بمجرد الحصول على الكلمة السر [2].

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

أما في الولايات المتحدة الأمريكية فإن احصائيات مكتب التحقيقات الفدرالي أكدت بأن الخسائر المترتبة عن الجريمة الالكترونية تفوق 150 مرة الجريمة العادية[4].

أما في الجزائر فإن الاحصائيات المتوصل إليها من سنة 2005 إلى 2010أكدت بأن جرائم الدخول غير المشروع مع اتلاف المعطيات أو تعديلها بلغ عدد 13 بمعدل 34% في حين بلغت نسبة ادخال المعطيات خلسة 21% وبالمقابل كانت المؤسسات المستهدفة 60% بالنسبة للإدارات العمومية والمؤسسات ذات الطابع الصناعي والتجاري وبنسبة 20% للشركات الخاصة ونسبة 11% بالنسبة للشركات الخاصة الأجنبية، وكانت الدوافع المادية تشكل نسبة 65% ودوافع الفضول 15%و التحدي 05% [5]وعلى العموم فإنه يصعب تقدير حجم الخسائر الناجمة عن الجرائم المعلوماتية كما تشير إليه الأبحاث التي

---

[1] عمر الفاروق الحسيني. المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية. الطبعة الثانية. دار النهضة العربية :مصر. 1995. ص 103. – نائلة محمد فريد قورة. مرجع سابق ، ص 80

[2] ميل عبد الباقي الصغير. مرجع سابق، ص 164. – جميل عبد الباقي الصغير. مرجعسابق. ص 165.

[3] علي القهوجي. الحماية الجنائية لبرنامج الحاسب الألي.دط. الدار الجامعية للنشر: بيروت. 1999. ص 157.

[4] عبد الله عبد الكريم عبد الله .مرجعسابق. ص 21.

[5] مختار الاخضري . مرجعسابق. ص 39 .

أجريت بشأنها في معظم الدول الغربية، سيما فرنسا والولايات المتحدة الامريكية وانجلترا، كما أصدر المكتب الجنائي الاتحادي في المانيا في السنوات الأخيرة تقريرا يحذر فيه من خطورة استعمال الوسائل المعلوماتية من طرف الارهابيين لأنها أصبحت تشكل أهم وسية لهم.[1]

[1] عبد الله عبد الكريم عبد الله. مرجع سابق، ص28

المبحث الثاني: مفهوم الاثبات الجنائي في الجريمة الالكترونية ووسائله الحديثة:

من المعلوم أن إثبات الجريمة يكتسي أهمية بالغة إذا أن الغاية في الإثبات هي الوصول إلى الحقيقة ، فالجريمة واقعة من الماضي وليس بالإمكان معاينتها والتعرف على حقيقتها واسنادها للمتهم و

القضاء بشأنها لا يتم إلا بالاستعانة بوسائل تجسد صورتها كما حدثت وهذه الوسائل هي ما يسمى بأدلة الإثبات فالاهتمام يبدأ في صورة الشك والقاضي يمحص هذا الشك بأدلة الإثبات فيصل بالشك إلى اليقين.

والملاحظ أن الإثبات يختلف بين أحكام القانون المدني والجنائي كلية ففي الجانب المدني عرفه الدكتور

عبد الرزاق السنهوري في كتابة «الوسيط في شرح القانون المدني بقوله «الإثبات بمعناه القانوني، هو إقامة الدليل أمام القضاء بالطرق التي حددها القانون على وجود واقعة قانونية ترتبت أثارها»[1]. فيقوم على مبدأ البينة على من ادعى أن الاثبات الجنائي سيقع على عاتق النيابة التي حركت الدعوى.

هذا فضلا على أن أوجه الاختلاف بين الإثبات الجنائي و المدني أن مبدأ الحياد للقاضي المدني دون أن يتدخل في توجيه الأطراف على عكس القاضي الجزائي الذي هو ملزم بالبحث والتحري للوصول إلى الحقيقة. و لتحديد مفهوم الاثبات الجنائي في الجريمة الالكترونية يجب أن نتوقف عند تعريف الاثبات الجنائي و المعلوماتي في المطلب الأول و ماهية الوسائل الحديثة للاثبات الجنائي في المطلب الثاني وبعد ذلك نتطرق إلى المبادئ العامة للاثبات الجنائي للجريمة الالكترونية في المطلب الثالث.

[1] عبد الرزاق السنهوري. الوسيط في شرح القانوني المدني. ط. الجزء الثاني. دار احياء التراث العربي: بيروت. لبنان.1952. ص 67

المطلب الأول: تعريف الإثبات الجنائي والالكتروني

أطلقت على الإثبات الجنائي تعاريف عديدة منها ما أوردها الدكتور هلالي عبد اللاه أحمد، بأن" الإثبات هو التنقيب على الدليل وتقديمه وتقديره لاستخلاص السند القانوني للفصل في الدعوى وأضاف بأن الإثبات أعم وأشمل من كلمة دليل "[1].

والدليل الجنائي هو الأخر يعرف بأنه: «كل وسيلة مرخص بها أو جائزة قانونا لإثبات أو نفي الواقعة المرتكبة» ، أو هو الوسيلة التي يستعين بها القاضي للوصول إلى اليقين القضائي الذي يقيم عليه حكمه في ثبوت الاتهام المعروض عليه، أو " هو ببساطة كل ما يؤدي إلى كشف الحقيقة المبحوث عنها في جريمة معينة[2]، وهناك شروط من الواجب أن تتوفر في الدليل الجنائي وأولها المشروعية بمعنى أن يكون الحصول عليه وفقا للإجراءات القانونية وأن يكون له أصلا في الدعوى ولا يشوبه غموض[3]..

أما الإثبات الالكتروني فيأخذ مفهوما مختلف عن سابقه باختلاف طبيعة كل منهما فالأدلة الالكترونية إما أن تكون مخرجات ورقية يتم انتاجها عن طريق الطابعات أو الرسم وإما أن تكون مخرجات غير ورقية مثل الأشرطة ، الاقراص المضغوطة، اسطوانات الفيديو[4]، وهي عبارة عن دعائم أو وسائط لحفظ المعلومات بمعنى أن البيانات قد تم تخزينها في الأشرطة أو على القرص الصلب أو القرص المضغوط أو فلاش ديسك وذلك على شكل رقمي[5].

يضاف إلى ذلك أن تطور المعاملات عن طريق استعمال الحاسوب في البيع والشراء بظهور التجارة الالكترونية، وتداول حركة رؤوس الأموال وما صاحب ذلك من جرائم تستخدم الشبكة المعلوماتية كوسيلة لها أو تلك التي يكون الحاسوب مجالا لها، فقد صاحب ذلك ظهور أدلة إثبات أخرى قد تصلح في الإثبات الالكتروني أمام القضاء المدني مثل الشبكات الالكترونية والمحفظة الالكترونية ، استعمال بطاقات الائتمان الالكترونية والممغنطة يضاف لها الكتابة الالكترونية والتوقيع الالكتروني والبريد الالكتروني وعلى

---

[1] عبد اللاه أحمد هلالي. النظرية العامة للإثبات في المواد الجنائية. الطبعة الأولى. دار النهضة العربية: القاهرة مصر . 1987. ص 340

[2] اعمار عباس الحسيني. التحقيق الجنائي والوسائل الحديثة في كشف الجريمة الطبعة الأولى. منشورات دار الحلبي :لبنان. 2015. ص 146

[3] عبد الله أوهايبية. شرح الإجراءات الجزائية الجزائري. التحري والتحقيق .دط. دار هومة: الجزائر. 2008. ص 279

[4] عبد اللاه أحمد هلالي. حجية المخرجات الالكترونية. الطبعة الأولى. دار النهضة العربية: القاهرة .مصر. 1997. ص. 22.

[5] فراح منانى.ادلة الإثبات الحديثة في القانون. ط. دار الهدى : الجزائر .2008. ص262

العموم فإن الإثبات الالكتروني يتم عن طريق جمع وحفظ وتحليل الأدلة الرقمية من أية دعامة للتخزين تعمل بواسطة الإعلام الآلي لعرضها أمام القضاء قصد إثبات التهمة أو نفيها عن شخص ما[1].

ويظل الحصول على الدليل بخصوص الجريمة المعلوماتية صعبا جدا ويطرح اشكالات عدة فالدليل هنا غير مرئي ويمكن محوه وطمسه في ثواني عديدة، فالجريمة المعلوماتية تتسم بالسرعة[2]، بمجرد النقر على رز الفأرة أو على أحد مفاتيح اللوح.

المطلب الثاني: ماهية الوسائل الحديثة في الإثبات الجنائي

أصبح المجتمع المعلوماتي في الوقت الراهن حقيقة واقعة فالمجتمعات المعاصرة تسير شؤونها بواسطة تقنيات الحاسب الألي والمعلوماتية وبالمقابل أصبحت هذه المجتمعات ملزمة لإن تواجه ظاهرة الإجرام الجديدة التي صاحبت ثورة المعلوماتية وأن تتعامل في ممارسة وتنفيذ هذا المجتمع في الدفاع عن كيانه ضد الإجرام وفق أشكال جديدة ومستخدمة من الأدلة غير المادية أمام اندثار الدور التقليدي للوثائق الورقية في الإثبات[3].

إذ أن هناك تطور كبير قد برزفي مجال الإثبات سواء منه المدني أو الجنائي فظهر ما يسمى بالوثائق الرقمية التي ستحل محل المستندات والوثائق الورقية[4]، وبالموازاة مع ذلك ومدى حجيتها في الإثبات[5] والملاحظ أن بعض التشريعات الحديثة اخذت في الاعتماد بالسندات الالكترونية والتوقيع الالكتروني سيما في ظل إزدهار ما يعرف التجارة الالكترونية[6].

فقد صدر في فرنسا القانون رقم 230 لسنة 2000 في 13 مارس 2000 والذي عدل نص المادة 1316 من القانون المدني ليتم الأخذ بالسندات الالكترونية والتوقيع الالكتروني ويضاف إلى ذلك أن القانون المدني الكندي لعام 1991 يسوي في الإثبات بين الأدلة

---

[1] فراح مناني. المرجع نفسه. ص 264.

[2] هشام مُحَّد فريد رستم. مرجع سابق، ص 23.

[3] فراح مناني. مرجع سابق. ص 56.

[4] امال قارة. الحماية الجزائية للمعلوماتية في التشريع الجزائري. الطبعة الثانية. دار هومة : الجزائر .2007. ص 134

[5] فراح مناني. مرجع سابق، ص 46.

[6] سليم سعداوي. عقود التجارة الالكترونية. دراسة مقارنة . الطبعة الأولى. دار الخلدونية: الجزائر. 2008. ص

الالكترونية والأدلة الورقية المكتوبة"[1]، وكذلك عمل المشرع الجزائري بإدراج التوقيع الالكتروني والاعتداد به كوسيلة إثبات وذلك عندما عدل القانون المدني بموجب القانون رقم 05-10 المؤرخ في 20/06/2005 ، باستحداث المادة 323 مكرر والتي تفيد بأن الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق [2]، ولقد خرجت التشريعات في المجال الجنائي على توسيع نطاق البحث عن الدليل الالكتروني فضبط الدليل لا يتوقف فقط على تحريز جهاز الكمبيوتر بل يمتد وموازاة مع ضبط المكونات المادية إلى مختلف أجراء النظام فيشمل المعطيات والبيانات والبرامج المخزنة في النظام أو النظم المرتبطة به المثبتة فيه أو إلى أدوات رفع الكترونية سهولة التغيير أو الاتلاف[3].

إذ أن الدليل الجنائي لإثبات الجريمة الالكترونية يختلف تماما عن الدليل الجنائي في الجريمة التقليدية من حيث البيانات المدونة في جهاز الحاسوب وكيفية إثباتها من حيث وسيلة الإثبات أو من حيث القائم بالإثبات ومدى خبرته في هذا المجال بالمقارنة مع طبيعة المجرم المعلوماتي الذي يتسم بالمعرفة و الذكاء[4]، وإذا كان من الممكن إثبات الجريمة المعلومات بالأدلة المستعملة في الجريمة التقليدية مثل: سماع الشهود، والانتقال للمعاينة وانتداب الخبراء والتفتيش والاستجواب والمواجهة[5]، فإن الدليل في الجريمة المعلوماتية يكتسي طابعا خاصا ولا يمكن الوصول إليه بسهولة فالجريمة الالكترونية ذاتها غير مرئية وبالتالي ينعدم فيها الدليل المرئي فهي تتم في بيئة لا علاقة لها بالأوراق أو المستندات بل أن قيام هذه الجريمة يرتبط بوجود جهاز حاسب ألي[6]، وهو يحتوي على المعلومات أو البيانات والتي هي عبارة عن نبضات الكترونية غير مرئية تنساب عبر أجهزة غير مرئية[7].

---

[1] اسامة أحمد بدر. حماية المستهلك في التعاقد الالكتروني" دراسة مقارنة" .دط. دار الجامعة الجديدة للنشر: الإسكندرية. مصر.2005. ص 50.

[2] زيدان زيبحة . مرجعسابق. ص 23.

[3] عبد الفتاح بيومي حجازي . مكافحة جرائم الكمبيوتر والانترنت" دراسة معمقة للقانون المعلوماتي". الطبعة الأولى. دار الفكر الجامعي: الاسكندرية.مصر.2006. ص 14.

[4] محمود سامي الشوا . مرجعسابق. ص 35

[5] رمزي رياض عوض.مشروعية الدليل الجنائي في مرحلة المحاكمة. ط. دار النهضة العربية : مصر.1997. ص 09.

[6] عبد الفتاح بيومي حجازي. الدليل الجنائي والتزوير في جرائم الكومبيوتر والانترنت. مرجعسابق. ص 33

[7] هشام مُحَمَّد فريدرستم. الجوانب الاجرامية الجرائم المعلوماتية" دراسة مقارنة". مكتبة اللات الحديثة : اسيوط . 1994.ص 28

فالبيانات أو المعطيات المخزنة في ذاكرة الحاسوب إما أن تكون مرصودة ومثبتة على دعامة أو حامل كالأقراص أو اشرطة ممغنطة فهذه الأخيرة تعد من حكم الأشياء المادية يجوز ضبطها بسهولة، أما البيانات الالكترونية فإنه لا يمكن ضبطها لانتفاء الكيان المادي إلا بعد نقلها على كيان مادي ملموس عن طريق التصوير الفوتوغرافي.

أو بنقلنا على دعامة كحامل الأقراص أو اشرطة ممغنطة ففي هذه الحالة الأخيرة يمكن ضبط وحجز هذه الأشياء بسهولة لأنها أصبحت أشياء مادية و يبقى الأمر صعبا بخصوص المعلومات في حد ذاتها.

إذ أنها تعتبر في ألأصل شيء معنوي ويطلق عليها مصطلح الأموال المعنوية[1]، وتعتبرها مختلف التشريعات غير قابلة للضبط إلا بعد تحويلها إلى كيان مادي كما ذهب إليه التشريع الألماني وكذا التشريع الفرنسي[2]،

غير أن المشرع الجزائري إنحاز إلى الرأي القائل بإمكانية حجز المعلومات إذ ورد في المادة 06 من القانون 09-04- بأنه يمكن حجز المنظومة المعلوماتية برمتها إذا كان ضروريا لمصلحة التحقيق وذلك بعد نسخها على دعامة مادية"[3]، وواقع الحال أن الوصول إلى الجرائم المعلوماتية لا يزال يصطدم بصعوبات كبيرة ويتطلب ضوابط قانونية وتقنية[4].

المطلب الثالث: المبادئ العامة للإثبات الجنائي في الجريمة الالكترونية

يعتبر الإثبات بمثابة المحور الرئيسي الذي تدور حوله قواعد الإجراءات الجنائية منذ لحظة وقوع الجريمة إلى غاية صدور الحكم النهائي بشأنها، وهذا الحكم نفسه تبنى نتائجه على مسار واحد وهو قناعة القاضي والتي يشكلها وفقا لسلطته التقديرية في تقدير الأدلة وموازاتها وترجيح ما يبدو مفيدا منها وبما يخوله التشريع السائد في ذلك للقاضي الجزائي أو بمعنى أخر حسب نوع نظام الإثبات الذي يتبناه المشرع[5].

---

[1] هشام مُحَّد فريد رستم ، مرجع سابق، ص: 41.

[2] زيدان زيبحة.مرجع سابق .ص 150

[3] زيدان زيبحة. المرجع نفسه. ص 151

[4] فاضل زيدان مُحَّد سلطة القاضي الجنائي في تقدير الأدلة "دراسة مقارنة". دط. دار الثقافة للنشر والتوزيع: عمان. 2006. ص 116

[5] ماروك نصرالدين . محاضرات في الإثبات الجنائي. ط. الجزء الأول. دار هومة : الجزائر. 2003. ص625

ومن أهم هذه المبادئ مبدأ الاقتناع الشخصي للقاضي الجزائي والذي يطلق عليه أيضا مبدأ القناعة الوجدانية ليصل في النهاية إلى نتيجة منطقية وهي البراءة أو الإدانة، وبملاحظة مختلف التشريعات نجدها لا تخرج عن أنظمة الإثبات الثلاثة وهي: نظام الإثبات القانوني أو المقيد ونظام الإثبات المعنوي أو المطلق، ونظام الإثبات المختلط[1].

ومما يستدعي توضيحه هو أن مبادئ الإثبات الجزائي هي مبادئ مسقرة تقوم عليها نظرية الإثبات سواء في الجريمة التقليدية أو الالكترونية لذلك فإن هذه المبادئ هي أربعة كما يلي:

1- مبدأ الاقتناع الشخصي.

2- مبدأ عبء الإثبات.

3- مبدأ قرينة البراءة.

4- مبدأ المشروعية أي مشروعية الدليل[2].

- مبدأ الإقناع الشخصي يختلف فيما يتعلق بالإثبات بين القاضي المدني والقاضي الجنائي، فالقاضي المدني مقيد بطرق محددة للإثبات بينما القاضي الجنائي يملك سلطة واسعة في تشكيل قناعته من خلال قبول أو رفض أي دليل إذا أن القانون لم يحدد للقاضي الطريقة التي ينتهجها لتكوين قناعته ومن هنا جاءت فكرة حرية الإثبات الذي يقوم عليه الاقتناع الشخصي للقاضي الجنائي وقد أخذت به مختلف التشريعات المعاصرة فقد أخذ به المشرع الفرنسي في المادة 335 من قانون الإجراءات الجزائية الفرنسي[3].

أما بالنسبة لمشرع الجزائري فقد نصت المادة 212 من قانون الإجراءات الجزائية الجزائري بالقول بأنه القاضي أن يصدر حكمهبناءا على اقتناعه الشخصي وأن عليه أن يبني قراره على الأدلة المقدمة له في معرض المرافعة وحصلت مناقشتها حضوريا أمامه غير أنه وباستقراء نص المادة 212 المشار لها يتضح بأن مبدأ الاقتناع الشخصي للقاضي

[1] فاضل زيدان محمد. مرجع سابق، ص 129

[2] محمد مروان .نظام الإثبات في المواد الجنائية في القانون الوصفي الجزائري .دط. ديوان المطبوعات الجامعية : بن عكنون. الجزائر. 1999،ص64

[3] اسامة احمد بدر. مرجع سابق .ص50

الجنائي تحكمه ضوابط ومنها أن يكون الدليل ضمن أوراق الدعوى و مرتبط بها ويطرح في جلسة المحاكمة ويكون مستخلص من إجراء صحيح[1] .

- مبدأ عبء الإثبات وهو ما يعرف بالفرنسية « La charge de la preuve » وهو جمع الأدلة وتقديمها ويقع عبء الإثبات على الجهة التي حركت الدعوى العمومية وهي النيابة ، وينصرف الإثبات هنا إلى الركنين المادي والمعنوي للجريمة .

فإثبات الركن المادي على عاتق جهة المتابعة وعليها أن تقدم الدليل بأن الفعل والامتناع موجود وأن الشخص المتابع هو من قام به غير أنه وفي بعض الحالات يمنح المشرع قوة الإثبات تلقائية للمحاضر ولا يمكن استبعادها إلا بالطعن فيها بالتزوير مثل المحاضر المثبتة بمخالفات المرور ومحاضر المعاينات المادية للجمارك، أما فيما يتعلق بالركن المعنوي ويسمى أيضا بالقصد الجنائي ويعني ذلك أن الجاني يقوم بالفعل الإجرامي وهو عالم ومدرك بما يفعل ويستخلص القاضي هذا الركن من ملابسات القضية[2].

- مبدأ قرينة البراءة وهو مبدأ مهم وقد تطور إلى أن أصبح مبدأ دستوري في غالبية الدساتير الحديثة ومنها الدستور الجزائري الذي نص في المادة 56 منه[3] اعلى قرينة البراءة إذ يعتبر كل شخص بريء حتى تثبت جهة قضائية رسمية أدانته. وقد سبق ذلك الإعلان العالمي لحقوق الإنسان المعتمد من قبل الجمعية العامة للأمم المتحدة بتاريخ: 10/12/1948 الذي نص في المادة 11 منه على أن كل شخص متهم بجريمة يعتبر بريئا إلى أن تثبت إدانته قانونا بمحاكمة علنية تؤمن له فيها الضمانات الضرورية للدفاع عنه[4]، إذا أن الأصل هو براءة الذمة ومن نتائج قرينة البراءة أن الشك يفسر لصالح المتهم وتجد هذه القاعدة مصدرها كذلك في الشريعة الإسلامية فيقوله تعالى: «وما يتبع أكثرهم إلا ظنا أن الظن لا يغني من الحق شيئا»[5]

---

[1] زبدة مسعود. الاقتناع الشخصي للقاضي الجزائي الطبعة الأولى. المؤسسة الوطنية للكتاب : الجزائر .1989. ص 08.

[2] محمود أحمد طه. عبء إثبات الأحوال الأصلح للمتهم .دط. منشأة المعارف: الاسكندرية.مصر.2003. ص 10

[3] المادة 56 من الدستور الجزائري المعدل بالقانون رقم 16-01 المؤرخ في 06 مارس 2016 الجريدة الرسمية رقم 14 في 7 مارس 2016

[4] تبنت الجزائر على هذا الإعلان بموجب المادة 11 من دستور 1963 بالنص: توافق الجمهورية على الإعلان العالمي لحقوق الإنسان وتنظم إلى كل منظمة دولية تستجيب لمطامح الشعب الجزائري وذلك اقتناعا منها بضرورة التعاون الدولي.

[5] سورة يونس الآية رقم 36

- مبدأ شرعية الحصول على أدلة الإثبات:

يعد مبدأ المشروعية أو مبدأ سيادة القانون من أهم المبادئ الدستورية في العالم ذلك أنه من غير الممكن أن يؤسس حكما قانونيا على دليل متحصل عليه، بطرق غير مشروعة ويرى الدكتور محمد زكي أبو عامر بأن "مبدأ المشروعية أو الشرعية الجزائية يتكون من شقين يكملان بعضهما وهما: لا جريمة ولا عقوبة دون نص، ولا عقوبة دون حكم قضائي صادر من محكمة مختصة وفقا للقانون[1].

[1] محمد زكي أبوعامر.الإجراءات الجنائية. الطبعة السابعة دار الجامعة الجديدة للنشر :الإسكندرية. مصر. 2005. ص23

خلاصة الفصل الأول:

لقد تناولنا في هذا الفصل أهمية المعلومة في حد ذاتها وبينا الفرق بينها وبين البيانات والتي تعد المادة الخام التي يتم تجهيزها ومعالجتها لتتحول إلى معلومة فتصبح ذات قيمة اقتصادية بمثابة سلعة تباع وتشري وباتت تحظى بحماية قانونية، ثم عرجنا على تناول أهم التعريفات التي تناولت الجريمة الالكترونية في التشريع والفقه المقارن، ثم بينا خصائص هذه الجريمة ومميزاتها وكذا الأساليب المنتهجة في ارتكابها والمتسمة بتقنيات دقيقة وحديثة مبرزين في ذلك موقف المشرع الجزائري من خلال النصوص التشريعية التي بادر بها لمواكبة مختلف التشريعات العالمية بغية مواجهة ظاهرة الجريمة الالكترونية، والتي تركت وإلى حد الآن آثارا وخيمة في مجالات عديدة من خلال الإحصائيات التي أوردناها، ثم تطرقنا بعد ذلك وبشيء من التفصيل إلى تعريف الإثبات الجنائي المعلوماتي ووسائله الحديثة وذيلنا ذلك بشرح وتوضيح للمبادئ العامة للإثبات الجنائي في الجريمة الالكترونية.

الفصل الثانى

اجراءات التحقيق و جمع الأدلة في الجريمة الالكترون

تمهيد

يقصد بالتحقيق الجنائي أو التحقيق من أجل جمع الأدلة بشكل عام هو مجموعة الإجراءات التي تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت، وتجميعها ثم تقديمها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة ويتضح بأن إجراءات التحقيق الابتدائي خاصة هي نوعان : إجراءات تستهدف البحث عن الأدلة وجمعها وتوفير شروط صحتها، أما النوع الثاني فيقتصر على مجرد المحافظة على الأدلة وفق الإجراءات المقررة لذلك .ويبدوا الأمر سهلا في هذا المجال بالنسبة للجرائم العادية أما في الجريمة المعلوماتية فإن هذه الإجراءات بنوعيها تعترضها صعوبات كبيرة جدا . ولذلك فإن مسار التحقيق من أجل الحصول على الدليل في الجريمة الالكترونية يتم وفق أساليب إجرائية تخضع لضوابط وقواعد يحددها القانون.

ولكي نبين ذلك بوضوح سنتطرق إلى القواعد الإجرائية للتحقيق في المبحث الأول ثم إلى إجراءات ضبط وتحريز الأدلة في الحاسوب والانترنت في المبحث الثاني.

المبحث الأول: القواعد الإجرائية للتحقيق في الجريمة الالكترونية.

لقد تبين من خلال التعرف على الجريمة الالكترونية أنها تتسم بطابع خاص فهي غير مقيدة بمكان أو زمان محددين فضلا على أنها تقع في بيئة افتراضية وهذا ما أوجد إشكالات بخصوص إثبات هذه الجريمة، إذ أن الوصول إلى الدليل المعلوماتي يطرح مشكلات قانونية وتقنية، لذلك فإن القواعد الإجرائية للتحقيق وجمع الأدلة تخضع لتدابير محددة يتعين على المحقق التقيد بها . ومن أجل توضيح ذلك سنتطرق في هذا المبحث إلى التفتيش في المطلب الأول ثم المعاينة والشهادة في المطلب الثاني، والخبرة الفنية في المطلب الثالث.

المطلب الأول: التفتيش.

يعد التفتيش من أهم الإجراءات الرامية إلى جمع الأدلة والبحث عن المتهمين، و لمعرفة ما اذا كان التفتيش الواقع على نظم الحاسوب والانترنت يختلف عن بقية الإجراءات التحقيقية الأخرى سنتطرق الى تعريف التفتيش وطبيعته القانونية وإلى القواعد العامة لتفتيش نظم الحاسوب.

أولا: تعريف التفتيش:

يعرف التفتيش بوجه عام بأنه "الإطلاع على محل منحه القانون حرمة خاصة باعتباره مستودع سر لصاحبه لضبط ما عسى أن يوجد فيه ما يفيد في كشف الحقيقة عن جريمة معينة[1] وفي الجرائم الالكترونية نجد أن الدخول غير المشروع إلى الأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزنة عما قد يتصل بجريمة وقعت، إجراء يفيد في كشف الحقيقة عنها وعن مرتكبها[2]، وتقتضيه مصلحة وظروف التحقيق في الجرائم الالكترونية هو إجراء جائر قانونا. وقد عرف المجلس الأوروبي التفتيش في المنظومة المعلوماتية بأنه "إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل الكتروني"[3] ويمكن تعريفه أنه: "الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه يستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الانترنت[4].

ثانيا: شروط تفتيش المنظومة المعلوماتية :تقسم شروط تفتيش نظم الحاسبا لالكتروني إلى نوعين:

1/ الشروط الموضوعية لتفتيش المنظومة المعلوماتية:

---

[1] عمار عباس الحسيني مرجع سابق .ص 199.

[2] على عدنان الفيل .اجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية " دراسة مقارنة".دط. المكتب الجامعي الحديث : الاسكندرية. مصر. 2012. ص 38

[3] على عدنان الفيل. مرجع سابق ، ص 39.

[4] علي حسن مُحَمَّد الطوالبة. التفتيش الجنائي على نظم الحاسوب و الانترنت "دراسة مقارنة"، الطبعة الأولى. عالم الكتاب الحديث للنشر: الأردن .2004.ص 13.

أ- وقوع جريمة معلوماتية، سواء كانت جنحة أو جناية، وذلك حسب أحكام المادة 44 من قانون الإجراءات الجزائية الجزائري[1].

ب- بتورط شخص أو أشخاص معينين في ارتكاب الجريمة المعلوماتية أو الاشتراك فيها

ت- توافر إشارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة.

ث- توجيه الاتهام لشخص أو مجموعة من الأشخاص: نرى أن التشريع الجزائري خرج عن هذه القواعد العامة بخصوص الجريمة الالكترونية وجعل من التفتيش المنصب عليها إجراء وقائي، أي يمكن أن يكون سابقا لارتكاب أي جرم أو حتى دون توجيه الاتهام لأي شخص.

ج- ومحل التفتيش هي كل مكونات الحاسب سواء كانت مادية أو معنوية أو شبكات الاتصال

الخاصة بها بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الالكتروني محل التفتيش[2].

2/ الشروط الشكلية لتفتيش المنظومة المعلوماتية:

و يستخلص من نص المادة 5 من القانون 09-04[3] بأن المشرع الجزائري قد أدرج التفتيش في مجال الجرائم المعلوماتية في قانون الإجراءات الجزائية. ويتبين لنا بوضوح بأن التفتيش يكون في الأصل بصفة مباشرة بالانتقال إلى مسكن المتهم أو المكان الذي تتواجد فيه الأجهزة المقصودة أو في الأماكن العامة[4]، ولعل أهم عناصر التفتيش التي نصت عليها المدة 44 من قانون الإجراءات الجزائرية:

- وجود إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق.
- الاستظهار بالإذن قبل دخول المنزل المراد تفتيشه.

---

[1] الأمر رقم 66-155 المؤرخ في 8/6/1966 المعدل و المتمم بالأمر رقم 69-73 في 16/9/1969 و المتعلق بقانون الاجراءات الجزائية الجزائري.

[2] على عدنان الفيل. مرجع سابق، ص 4-50

[3] القانون رقم 09-04 المؤرخ في 5/8/2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها.

[4] زيدان زيبحة. مرجع سابق، ص 133.

- أن يتضمن الإذن بيان وصف الجريمة، موضوع البحث عن الدليل بشأنها وعنوان الأماكن المقصودة بالتفتيش.

- حضور الشخص المعني بتفتيش مسكنه أو من ينوب عنه.

- في حالة رفض الحضور يستدعي ضابط الشرطة القضائية شاهدين من غير الموظفين الخاضعين السلطته.

ثالثا: مدى خضوع شبكات الحاسب الآلي للتفتيش :

يمكن التمييز بين ثلاثة احتمالات:

- الاحتمال الأول: اتصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر داخل الدولة: ويرى الفقه الألماني بشأن مدى إمكانية امتداد الحق في التفتيش إذا تبين أن الحاسب أو النهاية الطرفية في منزل المتهم متصلة بجهاز أو طرفيه في مكان آخر مملوك لشخص غير المتهم، أنه يمكن أن يمتد التفتيش في هذه الحالة إلى سجلات البيانات التي تكون في موقع آخر استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجزائية الألماني[1]، كما نص المشرع الجزائري في القانون 09-04 المؤرخ في 05/08/09 والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها على تمديد تفتيش المنظومة المعلوماتية.[2] وقد نصت المادة 05 من القانون 09-04 على أنه: "في الحالة المنصوص عليها في الفقرة -1 -من هذه المادة إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك".

- الاحتمال الثاني: اتصال حاسب المتهم بحاسب أو نهاية خارجية موجودة في مكان آخر خارج الدولة: من المتصور طبقا لهذا الاحتمال أن يقوم مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية المعلومات خارج الدولة عن طريق شبكات الاتصالات الرقمية بهدف عرقلة سلطات التحري و التحقيق في جمع الأدلة[3]، ولمواجهة هذا الاحتمال نص المشرع

[1] عبد العال الديربي. محمد صادق اسماعيل. مرجع سابق. ص 303 .

[2] زيدان زيبحة. مرجعسابق ص 121.

[3] عبد العال الديربي. محمد صادق اسماعيل. مرجع سابق. ص 303.

في قانون جريمة الحاسب الآلي بهولندا" أنه يجوز لجهات التحقيق مباشرة التفتيش داخل الأماكن ولما ينطوي عليه تفتيش نظم الحاسب المرتبطة حتى إذا كانت موجودة في دول أخرى[1]، وأكد القانون 09-04 في المادة 16 منه على أنه وفي إطار التحقيقات والتحريات يمكن تبادل المساعدة القضائية في المستوى الدولي، ويمكن أن يكون بواسطة الدخول إلى المنظومة المعلوماتية المشكوك في تخزينها المعلومات المبحوث عنها.

- الاحتمال الثالث: يسمح بالتنصت والأشكال الأخرى للمراقبة التيلفونية في العديد من الدول: حيث يجيز القانون الفرنسي الصادر في 10 يوليو سنة 1991 اعتراض الاتصالات البعدية بما في ذلك شبكات تبادل المعلومات[2]، وقد أجاز القانون الجزائري كذلك مراقبة الاتصالات الالكترونية وعرفته المادة 2 فقرة "2" من القانون 09-04 بأنها "تراسل أو إرسال أو استقبال علامات واشارات أو كتابات أو صور أو معلومات مختلفة بواسطة وسيلة الكترونية" وبالتالي فإن الاتصالات الالكترونية تشمل الاتصالات السلكية والخلوية بالفاكس والبريد الالكتروني وغيرها .وقد نص عليها المشرع الجزائري في قانون الإجراءات الجزائرية وذلك في المادة 65 مكرر 05 منه على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور وامكانية إجراء هذه المراقبة وتتجسد مراقبة شبكة الاتصالات باستخدام التقنية الالكترونية لجمع المعطيات والمعلومات عن المشتبه فيه سواء كان شخصا أو مكانا أو شيئا[3] .. ولكن هذه المراقبة تتم في حالات نص عليها المشرع صراحة في المادة 04 قانون 09-04 وهي:

. الوقاية من الأفعال الموصوفة بجرائم إرهابية أو تخريبية أو ماسة بأمن الدولة.

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

. لمقتضيات التحريات والتحقيقات عندما يكون من الصعب الوصول إلى نتيجة الأبحاث دون اللجوء إلى مراقبة الاتصالات الالكترونية.

. في إطار تنفيذ طلبات المساعدة القضائية الدولية.

المطلب الثاني: المعاينة والشهادة:

[1] عبد العال الديربي. محمد صادق اسماعيل. مرجع سابق. ص 303.

[2] على عدنان الفيل . مرجع سابق. ص 31.

[3] زيدان زيبحة. مرجع سابق، ص122.

تعتبر المعاينة والشهادة أو سماع الشهود من إجراءات التحقيق التي تهدف إلى الحصول على الدليل، وليس على المحقق التزام بإتباع ترتيب معين عند مباشرة هذه الإجراءات بل هو غير ملزم أساسا المباشرتها جميعا[1] وإنما يباشر منها ما تمليه مصلحة التحقيق وظروفه ويرتبها وفقا لما تقتضيه هذه المصلحة وما تسمح به هذه الظروف.

أولا: المعاينة

1/ تعريفها:

يقصد بالمعاينة إثبات الآثار المادية وحالة الأماكن والأشياء التي يمكن أن تساعد في كشف الحقيقة والمعاينة من إجراءات التحقيق الابتدائي، ويجوز للمحقق اللجوء إليها متى رأي لذلك ضرورة لذلك[2]، والأصل في المعاينة أن يحضر أطراف الدعوى الجزائية، وقد يقرر المحقق أن يجريها في غيابهم[3]، ولا يلتزم المحقق بدعوة محامي المتهم للحضور[4].

2/ أهمية المعاينة:

مع التسليم بأهمية المعاينة في كشف غموض الكثير من الجرائم التقليدية وجدارتها بتبوء مكان الصدارة والأولوية، إلا أن أهميتها تتضاءل في بعض الجرائم دون غيرها مثل الجرائم الالكترونية، ويعود ذلك السببين:

- أن الجريمة الالكترونية قلما تخلف آثارا مادية.

- أن كثيرا من الأشخاص قد يترددون على مسرح الجريمة خلال الفترة من زمان وقوع الجريمة وحتى اكتشافها، مما يعطي الفرصة لحدوث إتلاف أو تغيير بالآثار المادية الأمر الذي يورث الشك في دلالة الأدلة المستقاة من المعاينة في الجريمة الاكترونية[5].

و في كل الاحوال فان مسرح الجريمة يختلف عن مسرح الجريمة التقليدية، ولذلك يجب مراعاة وفي كل الأحوال، فإن مسرح الجريمة الالكترونية يختلف الآتي قبل التحرك إلى مسرح الجريمة :

---

[1] عمار عباس الحسيني. مرجع سابق، ص 265.

[2] على عدنان الفيل. مرجع سابق. ص 32.

[3] عبد الفتاح بيومي حجازي. الاثبات الجنائي في جرائم الكمبيوتر و الانترنت . مرجع سابق، ص142.

[4] على عدنان الفيل. مرجع سابق، ص 32

[5] عبد العال الديربي. مُحَمَّد صادق اسماعيل. مرجع سابق، ص 312. د. عبد الفتاح بيومي حجازي. الاثبات الجنائي في جرائم الكمبيوتر و الانترنت. مرجع سابق، ص144-145.

- وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوبة معاينتها وشبكاتها.

- وجود خريطة توضح الموقع الذي ستتم معاينته، وتفاصيل المبنى أو الطابق موضوع البلاغ.

- تحديد الأجهزة المحتمل تورطها في الجريمة حتى يتم تحديد كيفية التعامل معها فنيا قبل المعاينة

- تأمين الأجهزة والمعدات التي سيتم الاستعانة بها في عملية المعاينة .

- إعداد الفريق المتخصص الذي يتولى المعاينة من الخبراء ورجال الضبط والأمن.

- إخطار الفريق الذي سيتولى المعاينة قبل إتمامها بوقت كاف حتى يستعد من الناحية الفنية والعملية، وذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.

- تحديد البيانات والمهام والاختصاصات المطلوبة من كل عضو في فريق المعاينة على حدى،

- أن تتم كل هذه الإجراءات وفق مبدأ المشروعية وفي إطار ما تنص عليها القوانين الجنائية.

- تأمين عدم انقطاع التيار الكهربائي.

الضوابط التي يجب إتباعها في مسرح الجريمة:

1- تصوير الحاسب الالكتروني والأجهزة الطرفية المتصلة به والمحتويات والأوضاع العامة مع التركيز بوجه خاص على تصوير الأجزاء الخلفية للحاسب وملحقاته[1] .

2- ملاحظة الطريقة المعد بها النظام المعلوماتي والآثار التي يخلفها، ومعرفة السجلات الالكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع، وبروتوكولات الاتصال عبر الانترنت وإن تعلقت الجريمة بهذه الشبكة والتي تعرف اختصارا ب (IP 2[2]).

[1] جميل عبد الباقي الصغير . مرجع سابق، ص 28.

[2] عبد الفتاح بيومي حجازي. الاثبات الجنائي في جرائم الكمبيوتر و الانترنت. مرجع سابق، ص 146.

3- عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسب من مجالات القوى المغناطيسية.

4- التحفظ على محتويات سلة المهملات وما فيها من أوراق ممزقة وأقراص ممغنطة غير سليمة ورفع البصمات التي تكون عليها.

5- التحفظ على مستندات الإدخال والمخرجات الورقية للحاسب ذات الصلة بالجريمة

6- قصر المعاينة على الباحثين والمحققين الذين ليدهم كفاءة علمية وخبرة فنية في مجال الحاسبات

والشبكات واسترجاع المعلومات، وأن يكونوا قد تلقوا تدريبا جيدا على ذلك[1] .

ثانيا: الشهادة:

تعد الشهادة من أهم الأدلة الكاشفة عن حقيقة الجريمة، وقد وردت مفردة الشهادة ومشتقاتها اللغوية في القرآن الكريم في مواد متعددة منها قوله تعالى: "...وشهد شاهد من أهلها إن كان قميصه قد من دبر..."[2] وقوله تعالى: "وشهد شاهد من بني إسرائيل ...[3]

1/ تعريف الشهادة في الجريمة الالكترونية:

الشهادة هي الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى متهم أو براءته منها[4]، لذلك فالشهود يتقسمون إلى شهود نفي وشهود إثبات، وللشهادة في مجال الإجراءات الجنائية أهمية بالغة. وتتركز الشهادة على ما يلي:

- طبع ملفات البيانات المخزنة في ذاكرة الحاسوب أو الدعامات الأخرى على أن يقوم بتسليمها إلى سلطات التحقيق.

- الإفصاح عن كلمات المرور.

- الكشف عن الشفرات المدونة بها الأوامر الخاصة بتنفيذ البرامج المختلفة.

2/ الشاهد في الجريمة المعلوماتية:

[1] على عدنان الفيل. مرجع سابق.ص 33

[2] القران الكريم. سورة يوسف. الاية 26.

[3] القران الكريم. سورة الأنفال. الاية 10.

[4] عمار عباس الحسيني.مرجعسابق. ص 245.

- الشاهد في الجريمة المعلوماتية هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي والاتصالات بحيث تكون له معلومات جوهرية وهامة لازمة للدخول إلى نظام المعالجة الآلية للمعطيات، ويسمى بالشاهد المعلوماتي وذلك من أجل تمييزه عن الشاهد العادي، ويلزم الشاهد المعلوماتي أو الالكتروني متى كان حائزا على معلومات تفيد سير التحقيق بأن يعلم بها جهات التحقيق القضائي وإلا تعرض للعقوبات المقررة عن الامتناع عن الإدلاء بالشهادة. ويشتمل الشاهد المعلوماتي على عدة طوائف:

* القائم على تشغيل الحاسب الالكتروني: وهو المسؤول عن تشغيل الحاسب الالكتروني والمعدات المتصلة به ويجب أن تكون له خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج [1].

* المبرمجون: وهم الأشخاص المتخصصون في كتابة البرامج[2].

* المحللون: المحلل هو ذلك الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات مفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات[3]،.

* مهندسو الصيانة والاتصالات: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسبة بمكونات وشبكات الاتصال المتعلقة به .

مديرو النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية. التزامات الشاهد المعلوماتي :

يجب على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، و هناك اتجاهين بصدد امكانية الزام الشاهد على طبع الملفات و الافصاح عن كلمات المرور:

- الاتجاه الأول: يرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة،

---

[1] على عدنان الفيل. مرجع سابق ، ص 62.

[2] عبد العال الديربي. محمد صادق اسماعيل. مرجع سابق. ص314

[3] على عدنان الفيل. مرجعسابق. ص 63.

ويميل الفقه الألماني إلى هذا الاتجاه حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسبة على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب[1].

- الاتجاه الثاني: يرى أنصار هذا الاتجاه أن من التزامات الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة[2].

الضوابط التي تخضع لها الشهادة في مجال الجرائم المعلوماتية:

يرى جانب من الفقه الجنائي أن تقديم الشهادة في جرائم الحاسب الآلي والانترنت يجب تقديمه وفقا لضوابط محددة ، وهذه الضوابط تخضع لممثل الاتهام النيابة العامة - وهي:[3]

1. حصر الشهادة في النقاط التي يجب إثباتها أمام المحكمة.
2. وضع أسئلة نموذجية وإجابات محددة لها من قبل الشاهد.
3. تحديد الشهود الذين سوف توجه إليهم الأسئلة.
4. ترتيب الأسئلة حسب ترتيب الوقائع.
5. السيطرة على شهود الاتهام أي شهود الإثبات - منعا لانفلاتهم.

المطلب الثالث: الخبرة الفنية:

الخبرة إجراء يهدف إلى الكشف عن بعض الدلائل وتحديد مدلولها التقني والعلمي وآثارها لأن هذه المعلومات العلمية قد لا تتوفر لدى المحقق ولهذا للخبرة في مجال الجريمة المعلوماتية أهمية بالغة.

أولا: ماهية الخبرة:

تعرف الخبرة بأنها تقدير مادي أو ذهني يبديه أصحاب الفن أو الاختصاص في مسألة فنية لا يستطيع القائم بالتحقيق في الجريمة معرفتها بمعلوماته الخاصة. كما عرفها البعض بأنها "الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة إدارية علمية خاصة لا تتوفر لديه"[4].. والخبير هو كل شخص له دراية خاصة بمسألة من المسائل وقد يستدعي التحقيق فحص مسألة يستلزم لفحصها كفاءة خاصة فنية أو علمية لا تتوفر في المحقق، فالخبرة

[1] على عدنان الفيل. مرجع سابق. ص 64.

[2] امير فرج يوسف. الجرائم المعلوماتية على شبكة الانترنت. دط. دار المطبوعات الجامعية: الاسكندرية.مصر. 2009.ص 238.

[3] عبد الفتاح بيومي حجازي. الاثبات الجنائي في جرائم الكمبيوتر و الانترنت. مرجع سابق ص 241.

[4] اعمار عباس الحسيني.مرجع سابق.ص 134.

الالكترونية وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الأدلة[1].والأصل أن يباشر الخبير عمله في حضور المحقق وتحت إشرافه والاستثناء أن يتم ذلك في غيابه. وللخصوم حق الحضور أثناء عمل الخبير ويجوز أن يمنعهم كذلك من الحضور إذا كان للمنع سبب.[2]

ثانيا: أهمية الخبرة:

وتكمن أهمية الخبرة في البحث عن الدليل الرقمي في أنها تنير الطريق لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجزائية لذلك فقد اهتم المشرع الجزائري بتنظيم أعمال الخبرة من المواد 143 إلى 156 من قانون الإجراءات الجزائية واعتبرها من إجراءات البحث عن الدليل حيث نصت المادة 143[3] أنه يمكن لجهات التحقيق أو الحكم أن تأمر بندب خبير عندما تعرض لها مسألة ذات طابع فني إما من تلقاء نفسها أو بناء على طلب من النيابة العامة وإما بطلب من الخصوم. وإذا كان للخبرة أهمية في الجرائم التقليدية فإن أهميتها تزداد وتصبح حتمية في إثبات الجرائم الالكترونية التي تقوم على نظم وبرمجيات الحاسب الآلي وإثبات الحاسوبية وشبكات الاتصالات العالمية، كأعمال التجارة الالكترونية والمصارف والأعمال المصرفية الالكترونية، والإدارة الالكترونية مما ترتب عليه أن تتنوع الجرائم التي تقع على هذه العمليات وفقا لنوع الوسائل الالكترونية المستخدمة في ارتكابها. ومن أهم المسائل التي يستعان فيها بالخبرة في مجال الجرائم المعلوماتية هي:[4]

1. تركيب الحواسيب وصناعتها وطرازها، ونوع نظام التشغيل وأهم الأنظمة الفرعية التي تستخدمها بالإضافة إلى الأجهزة الطرفية الملحقة به وكلمات المرور أو السر ونظام التشفير.

2. طبيعة بيئة الحاسب الالكتروني أو الشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائط الاتصالات وتردد موجات البث وأمكنة اختزانها.

3. الموضع المحتمل لأدلة الإثبات والشكل أو الهيئة التي تكون عليها .

---

[1] عبد الناصر محمد محمود فرغلي . محمد عبيد سيف المسماري. مرجع سابق .ص د

[2] على عدنان الفيل. مرجع سابق. ص 28.

[3] المادة 143 من قانون الاجراءات الجزائية الجزائري.

[4] على عدنان الفيل. مرجع سابق. ص 29-30.

4. أثر التحقيق من الوجهة الاقتصادية والمالية على المشاركين في استخدام النظام.

5. كيف يمكن عند الاقتضاء عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق الضرر بالأجهزة.

6. كيف يمكن عند الاقتضاء نقل أدلة الإثبات إلى أوعية ملائمة بغير أن يلحقها تلف.

رابعا: شروط صحة الخبرة ومدى حجيتها:

نظرا للأهمية البالغة للخبرة فقد حرصت معظم التشريعات على تنظيمها ووضع شروط وضوابط لها. ومن الشروط التي حرصت أغلب التشريعات على تحديدها منها ما يتعلق بالخبير ومنها ما يتعلق بتقرير الخبرة[1].

1. شروط تتعلق بالخبير:

أ- اختياره من قائمة الخبراء المحددة أسماؤهم ضمن الجدول المعد مسبقا، وفق ما نصت عليه المادة 144 من قانون الإجراءات الجزائية الجزائرية[2].

144 من قانون الإجراءات الجزائية الجزائرية.

ب حلف اليمين القانونية، حسب ما نصت عليه المادة 145 من قانون الإجراءات الجزائية[3].

2. شروط تتعلق بتقرير الخبرة: بعد انتهاء الخبير من أبحاثه وفحوصاته يقدم تقريرا كتابيا ويجب مراعاة أن يقدمه في المدة المحددة، ما لم تتطلب طبيعة الفحص وقتا أطول، ويرفق هذا التقرير بملف الدعوى[4].

المبحث الثاني: إجراءات ضبط وتحريز الأدلة في الحاسوب والانترنت.

ان البحث عن الدليل يجب أن يكون في إطار احترام حقوق الأفراد وكرامتهم ومحققا للعدالة. وقد سعت الجهود الدولية إلى تنظيم قانون مكافحة الجريمة الالكترونية وإلى التعاون على مكافحتها باعتبارها من الجرائم العابرة للحدود. ويطرح التساءل عن إمكانية ضبط الحاسوب ونظمه وشبكة الانترنت؟ وهل من الممكن مخالفة قواعد التفتيش وضبط نظم الحاسوب والانترنت؟ وهل ينعكس البطلان كجزاء لمخالفة إجراءات التفتيش على

[1] عمار عباس الحسيني. مرجع سابق.ص 193.

[2] في المادة 44 من قانون الاجراءات الجزائية الجزائري

[3] المادة 145 من قانون الاجراءات الجزائية الجزائري

[4] عمار عباس الحسيني. مرجع سابق. ص 194.

الدليل المستمد منه؟ وما هي حجية الدليل المعلوماتي أمام القضاء؟ وما هو دور التعاون الدولي في مكافحة الجريمة الالكترونية؟ وسوف نجيب عن كل هذه التساؤلات في هذا المبحث عن طريق التطرق إلى ضبط الكيانات المادية والمعنوية للحاسوب في المطلب الأول، والقيمة القانونية الدليل الالكتروني ومدى حجيته في المطلب الثاني و دور التعاون الدولي في الإنابة القضائية ومكافحة الجريمة المعلوماتية في المطلب الثالث.

المطلب الأول: ضبط الكيانات المادية والمعنوية للحاسوب.

يهدف التفتيش إلى ضبط الأدلة المادية التي تفيد في كشف الحقيقة، فالضبط هو الغاية من التفتيش أي الأثر المباشر لهذا الإجراء، فإذا ما بطل إجراء التفتيش بطل الضبط.ويقع الضبط في القواعد العامة على الأشياء المادية فقط، فهل يمكن أن ينطبق على الكيانات المنطقية للحاسوب والانترنت؟

أولا: تعريف الضبط وطبيعته:

يقصد بالضبط في قانون الإجراءات الجزائية وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها"[1] وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال والتحقيق.وتحدد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط فإذا كان الشيء وقت ضبطه في حيازة شخص واقتضى الأمر تجريده من حيازته يكون الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليها دون الاعتداء على حيازة قائمة فإنه يكون بمثابة إجراء استدلال[2].

ثانيا: محل الضبط:

الضبط بطبيعته وبحسب تنظيمه القانوني وغايته لا يرد إلا على الأشياء أما الأشخاص فلا يصلحون محلا للضبط بالمعنى الدقيق، وإذا كان قانون الإجراءات الجزائية يتحدث في بعض النصوص عن ضبط الأشخاص وإحضارهم فإنه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف تماما عن ضبط الأشياء. ولا يفرق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه فإنه يستوي أن يكون الشيء المضبوط مملوكا

[1] عبد العال الديربي. محمد صادق اسماعيل. مرجع سابق. ص 320.

[2] على عدنان الفيل. مرجعسابق. ص54.

للمتهم أو لغيره[1] . فالضبط بحسب الأصل لا يرد إلى على أشياء مادية، فلا صعوبة بالتالي بضبط أدلة الجريمة الواقعة على المكونات المادية للكمبيوتر [2]، ولكن تكمن الصعوبة في ضبط الكيانات المعنوية.

اولا : ضبط الكيانات المادية

الأشياء المادية التي يجوز ضبطها في الجريمة المعلوماتية والتي لها قيمة خاصة في إثبات جرائم الحاسب الالكتروني ونسبتها إلى المتهم هي:

1- الورق: كثير من الجرائم الواقعة على المال أو على جسم الإنسان تترك خلفها قدرا كبيرا من الأوراق والمستندات الرسمية منها والخاصة، إلا أن وجود أجهزة الحاسبة يجعل كثيرا من المعلومات يتم حفظها في الحاسب الالكترونية، مما قلل حجم الأوراق ومع ذلك نجد أن الكثيرين يقومون بطباعة المعلومات لأغراض المراجعة أو التأكد من الشكل العام للمستندات أو الرسالة أو الرسومات موضوع الجريمة . والورق أربعة أنواع:[3]

أ- أوراق تحضيرية يتم إعدادها بخط اليد كمسودة تصور العملية التي يتم برمجتها .

ب- أوراق تالفة تتم طباعتها للتأكد، ومن ثم إلقاؤها في سلة المهملات.

ت- أوراق أصلية تتم طباعتها والاحتفاظ بها كمرجع أو لأغراض تنفيذ الجريمة.

ث- أوراق أساسية وقانونية محفوظة في الملفات العادية أو دفاتر الحسابات وتكون لها علاقة بالجريمة خاصة عند تقليدها أو تزوير بياناتها لتنفيذ جريمة الحاسب الآلي.

2- جهاز الحاسب وملحقاته: وجود جهاز الحاسب مهم للقول بأن هناك جريمة ولأجهزة الحاسب الالكتروني أشكال وأحجام وألوان مختلفة وخبير الحاسب الالكتروني يستطيع أن يتعرف على الحاسب الالكتروني ومواصفاته بسرعة فائقة، كما يستطيع تمييزه عن الأجهزة الالكترونية الأخرى وتحديد أسلوب التعامل معه في حالة الضبط و التحريزا [4].

---

[1] على عدنان الفيل. المرجع نفسه. ص 55

[2] امير فرج يوسف. مرجع سابق. ص237.

[3] علي حسن محمد الطوالبة. مرجع سابق، ص 141.

[4] عبد الفتاح بيومي حجازي. الاثبات الجنائي في جرائم الكمبيوتر و الانترنت. مرجع سابق، ص 2

3- أقراص الليزر: مع أي جهاز شخصي عادي نجد قدرا كبيرا من أقراص الليزر علاوة على أن مراكز الحاسب الآلي في الشركات والبنوك نجد فيها الآلاف من الأقراص، وقد تكون على غلاف القرص بيانات توضح محتويات القرص إلا أن ذلك لا يعتد به في التحقيق الذي يتطلب بيانات دقيقة عن محتويات كل قرص

وبمعرفة خبير يقدم الدليل إلى المحكمة[1].

4- الشرائط الممغنطة: تستعمل الشرائط الممغنطة عادة للحفظ الاحتياطي وقد تكون في مكان بعيد آمن كما يقوم البعض بإيداعها في خزائن البنوك التجارية أو مراكز التوثيق الحكومية الآمنة[2].

5- لوحة الدوائر. 99.

- المودم: هي الوسيلة التي تمكن أجهزة الحاسب الآلي من الاتصال مع بعضها البعض عبر خطوط الهاتف وقد تطور المودم إلى أجهزة إرسال الفاكس والرد على المكالمات الهاتفية و تبادل البيانات وتعديلها.

7- الطابعات: للطابعات أنواع منها العادية ومنها الطابعات الليزرية.

8- البرامج اللينة والمراشد: المراشد المصاحبة للحاسب الآلي مفيدة للتعرف على الجهاز والبرامج المستعملة فيه.

9- البطاقات الممغنطة وبطاقات الائتمان القديمة: و المواد البلاستيكية المستعملة في إعداد تلك البطاقات تعتبر قرائن في إثبات الجرائم الالكترونية.

كل ذلك يعد أثرا أو جزءا من جسم الجريمة ينبغي البحث عنها وفحصها والاستفادة منها في التحقيق[3]..

ثانيا : ضبط الكيانات المعنوية

قد يكون محل الضبط في الجرائد المعلوماتية بيانات معالجة الكترونيا، واختلف الفقه حول إمكانية أن تكون هذه البيانات محلا للضبط. ويرى الاتجاه الأول أن بيانات الحاسب

[1] عبد العال الديربي. محمد صادق اسماعيل. مرجع سابق .ص322

[2] على عدنان الفيل . مرجع سابق. ص 55.

[3] عبد الفتاح بيومي حجازي. الاثبات الجنائي في جرائم الكمبيوتر و الانترنت. مرجع سابق. ص 100.

الالكتروني لا تصلح لأن تكون محلا للضبط، ولا سبيل لضبطها إلا بعد نقلها على كيان مادي ملموس"[1].

ويرى الاتجاه الثاني "أن البيانات المعالجة الكترونيا إن هي إلا ذبذبات الكترونية، أي موجات كهرومغناطيسية وهي غير مرئية في حد ذاتها ولكن يمكن تحويلها إلى صورة مادية محسوسة عبر نقلها وبثها واستقبالها وطبعها وإعادة إنتاجها، فوجودها المادي لا يمكن إنكاره"[2].

كيفية وصول الجريمة الالكترونية إلى علم سلطات الضبط:

الجريمة التقليدية تصل إلى علم سلطات الضبط عن طريق الشكوى أو الإبلاغ، أو في حالة ضبط الجريمة متلبسا بوقوعها، بينما الجريمة الالكترونية، تصل أخبارها إلى سلطات الضبط بإحدى الطرق التالية:

1- تلقي سلطات الضبط أو أجهزة التحقيق معلومات مفادها أن أشخاصا معروفين أو غير معروفين يمارسون أنشطة تندرج تحت تعريف الجريمة الالكترونية، وذلك في مكان معروف وعلى أجهزة محددة، ووفق لغات برمجية معلومة[3].

2- ضبط شخص معين وبحوزته أموال مشبوهة أو بطاقات مزورة أو بطاقات تعريف مشبوهة.

3- بلاغ إلى سلطات الضبط أو التحقيق من المجني عليه يفيد تلاعب أو ممارسات خاطئة في حقه أو حقوق الآخرين، سواء تمثل ذلك في صورة عجز مالي في حسابات مؤسسة مالية أو ضياع حقوق أو تغييرات في الودائع[4].

4- توافر معلومات عن نشر فيروسات تخريبية عبر شبكة الانترنت سيما وأن تطبيق القانون في مجال مكافحة الفيروسات المعلوماتية يواجه صعوبات، وموانع كثيرة.

الصعوبات المرتبطة بإجراءات الضبط:

---

[1] على عدنان الفيل. مرجع سابق. ص 57.

[2] د. علي حسن محمد الطوالبة. مرجع سابق. ص 165.

[3] عبد الفتاح بيومي حجازي. الاثبات الجنائي في جرائم الكمبيوتر و الانترنت. مرجع سابق. ص153.

[4] عبد الفتاح بيومي حجازي. الاثبات الجنائي في جرائم الكمبيوتر و الانترنت. المرجع نفسه. ص 154.

الضبط بحسب الأصل لا يرد إلا على أشياء مادية فلا صعوبة بالتالي بضبط أدلة الجريمة الواقعة على المكونات المادية للكمبيوتر كرفع البصمات مثلا عنها . ولذلك فلا صعوبة أيضا في ضبط الدعامة المادية للبرنامج أو الوسائل المادية المستخدمة في النسخة غير المشروع أو إتلافها وسائل تقليدية كالكسر أو الحرق .ولكن تكمن أهمية الصعوبة في ضبط الوسائل الفنية المستخدمة في إتلاف البرامج[1] ، مثل: الفيروس وفي ضبط بيانات الكمبيوتر DATA لعدم وجود أي دليل مرئي في هذه الحالات ولسهولة تدمير الدليل في ثوان معدودة ولعدم معرفة كلمات السر أو شفرات المرور أو ترميز البيانات، ومن الصعوبات التي تواجه إجراء الضبط وعملية استخلاص الدليل في الجريمة الالكترونية كذلك نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن، كذلك لدى أجهزة العدالة الجنائية الممثلة في سلطة الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بشفافية الحاسب الآلي والإلمام بعناصر المعلوماتية وكيفية التعامل معها، لذلك كخطوة أولى يتعين منح الضبطية القضائية لأولئك العاملين في مجال المعلومات الأمنية سواء كانوا من أفراد الأمن أو في القطاعات ذات العلاقة بجهاز الحاسب الآلي سواء كانوا فنيين أو خبراء.

المطلب الثاني: القيمة القانونية للدليل الالكتروني ومدى حجيته:

إن الأدلة الالكترونية إما أن تكون مخرجات ورقية يتم إنتاجها عن طريق الطابعات، أو الراسم، وإما أن تكون مخرجات غير ورقية أو أن تكون الكترونية: كالأشرطة والأقراص الممغنطة وأسطوانات الفيديو وغيرها من الأشكال الالكترونية غير التقليدية، أو تتمثل في عرض مخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به، أو الانترنت بواسطة الشاشات او وحدة العرض المرئي، ويكون الدليل باطلا إذا تحصل عليه عن طريق مخالفة القانون .ولذلك يجب أن يتم الحصول على الدليل وفق الإجراءات والشروط المنصوص عليها قانونا، وذلك لأجل أن يكتسب حجيته في إثبات الجرائم الالكترونية.

[1] امير فرج يوسف . مرجع سابق. ص 237. 2 عبد الله عبد الكريم عبد الله. مرجع سابق.ص 38..

ولتبين ذلك بوضوح سنتطرق في هذا المطلب إلى شروط الدليل الالكتروني ثم إلى حجية الدليل الالكتروني في إثبات الجرائم الالكترونية.

أولا: شروط الدليل الالكتروني:

الشرط الأول:

يجب الحصول على الدليل بصورة مشروعة وغير مخالفة لأحكام الدستور ولا لقانون العقوبات: إن أهم أهداف الدستور هو صيانة كرامة الإنسان وحماية حقوقه لذلك تتضمن الدساتير والقوانين الحديثة نصوص تنظيم القواعد الأساسية في الاستجواب والتوقيف والحبس والتفتيش وغيرها[1] ، فقد نص الدستور الأردني في المادة 10 منه على أن: "للمساكن حرمة فلا يجوز دخولها إلا في الأحوال المبنية في القانون، وبالكيفية المنصوص عليها فيه"[2] وكذلك القانون الجزائري رقم 200-03 المتعلق بالبريد والمواصلات السلكية واللاسلكية فقد كان حريصا على إضفاء حماية خاصة على الاتصالات الورقية أو اللاسلكية بين الأشخاص تماشيا مع المبادئ الدستورية والمواثيق الدولية فيما يتعلق بحماية الحياة الخاصة للأفراد، وكذلك المشرع الجزائري في التعديل الذي أدخله على قانون الإجراءات الجزائية بموجب القانون رقم 06 22 في 20/11/2006 فإنه بادر بإجراء جديد منصوص عليه في المادة 65[3] فهذه النصوص وغيرها تفرض أن تكون إجراءات الحصول على الأدلة الجنائية ضمن الإطار العام الذي حدده القانون، بمعنى أنه لكي تتوفر المشروعية في الدليل الالكتروني يجب أن يكون مستخلص بطريقة موافقة لأحكام القانون ومبادئ الدستور خاصة ما تعلق منها بحماية الحريات الأساسية. ونرى أن الآراء الفقهية لرجال القانون في الدول المتطورة في أوروبا وأمريكا تتجه كلها إلى تكريس مبدأ المشروعية في الدليل الالكتروني والمتحصل من الحاسوب بطريقة شريفة ونزيهة وبعيدة عن أساليب الغش والتدليس، وتجمع كلها على: أن تكون الأدلة المضبوطة دقيقة وصحيحة ومستمدة بطريقة شرعية"[4]. أما جزاء مخالفة القانون في الحصول على الأدلة فيترتب عليه جزاءات جنائية أو إدارية فضلا عن الحكم

---

[1] زيدان زيبحة . المرجع نفسه.ص 157.

[2] علي حسن مُحَّد الطوالبة. مرجع سابق.ص 184

[3] : المادة 65 من قانون الاجراءات الجزائية الجزائري.

[4] زيدان زيبحة . مرجع سابق.ص 173.

بالتعويض، فالموظف الذي يعهد إليه القانون بعمل فيتصرف على وجه مخالف يعد مقصرا في عمله ومخالفا لواجباته فيستحق المؤاخذة[1] . والمهم هنا هو الجزاء الإجرائي إذ لا شك أن الدليل المستخلص عن طريق ارتكاب جريمة يكون باطلا بطلانا مطلقا لأنه متعلق بالنظام العام. ومن الطرق غير المشروعة في الحصول على الأدلة الناتجة عن الجرائم المعلوماتية:

- الإكراه المادي والمعنوي في مواجهة المشتكى منه المعلوماتي من أجل فك شفرة نظام من النظم المعلوماتية أو الوصول إلى ملفات البيانات المخزنة[2].

- التحريض على ارتكاب الجريمة الالكترونية من قبل أعضاء الضبطية القضائية، كالتحريض على الغش أو التزوير المعلوماتي أو التجسس المعلوماتي، والاستخدام غير المصرح به للحاسوب، والتنصت والمراقبة الالكترونية عن بعد.

- استخدام التدليس أو الغش أو الخداع في الحصول على الأدلة الالكترونية.

الشرط الثاني:

يجب أن تكون الأدلة الالكترونية غير قابلة للشك أي يقينية:

يشترط في الأدلة المستخرجة من الحاسوب والانترنت أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه لا مجال لدحض قرينة البراءة وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين، ولذلك فإن القاضي الجنائي ملزم بفحص الدليل الالكتروني أو الدليل الجنائي كقاعدة عامة لكي يتوصل إلى تشكيل قناعته انطلاقا من عرض هذا الدليل على مناقشة الأطراف وهو ما تنص عليه المواد 212 و 234 من قانون الإجراءات الجزائية الجزائري[3].

ويمكن التوصل إلى ذلك من خلال ما يعرض من الأدلة الالكترونية، والأشرطة الفيلمية أو غيرها من الأشكال الالكترونية التي تتوافر عن طريق الوصول المباشر، أم كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الحاسوب على الشاشة الخاصة به أو على الطرفيات[4]، وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات

---

[1] علي حسن محمد الطوالبة. مرجع سابق. 185.

[2] عبد الفتاح بيومي حجازي. الاثبات الجنائي في جرائم الكمبيوتر و الانترنت. مرجع سابق. ص 115.

[3] المواد 212. 234 من قانون الإجراءات الجزائية الجزائري.

[4] علي حسن محمد الطوالبة. مرجع سابق. ص 191.

الكترونية وما يتطبع في ذهنه من تصورات واحتمالات بالنسبة لها أن يحدد قوتها الاستدلالية على صدق نسبة الجريمة الالكترونية إلى شخص معين من عدمه.

الشرط الثالث: إمكانية مناقشة الأدلة الالكترونية المستخرجة من الحاسوب والانترنت:

يعني مبدأ وجوب مناقشة الدليل الجنائي بصفة عامة أن القاضي لا يمكن أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحكمة وخضعت لحرية مناقشة أطراف الدعوى، وهذا يعني أن الأدلة المتحصلة من جرائم الحاسوب والانترنت تكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة[1]

ثانيا: حجية الدليل:

إن حجية المخرجات المتحصلة من الحاسوب هي قوته الاستدلالية على صدق نسبة الفعل إلى شخص معين أو كذبه، أو هي قيمة ما يتمتع به المخرج المتحصل من الكمبيوتر من قوة استدلالية في كشف الحقيقة. لقد اختلفت أنظمة الإثبات في تقديرها لحجية المخرجات ففي القوانين ذات الصياغة اللاتينية، ومنها القانون الأردني والفرنسي والمصري والسوري واللبناني"[2]، فإن حجية الأدلة الالكترونية لا تثير صعوبات لمدى حرية تقديم هذه الأدلة لإثبات جرائم الحاسوب والانترنت. أما في النظم الانجلوساكسونية التي تأتي في طليعتها بريطانيا فالمشرع يحدد فيها أدلة الإثبات ويقدر قيمتها الإقتناعية"[3]. أما في القوانين ذات الاتجاه المختلط، وهي التي تجمع بين النظامين اللاتيني والانجلوساكسوني، فيعتمد النظام المختلط على أن يحدد القانون أدلة معينة لإثبات بعض الوقائع دون بعضها الآخر[4].

حجية الدليل المستمد من المراقبة والتسجيل لأن الصوت عند تسجيله الكترونيا لا يحتمل الخطأ، ويصعب التلاعب به، يمكن القول بأن التسجيل الصوتي الممغنط يمكن أن تكون له حجية دامغة في الإثبات . وكذلك يمكن أن يستخدم تسجيل الفيديو لإثبات تهم استعمال القوي أو إساءة استعمال السلطة من قبل أعضاء الضبطية القضائية ضد المواطنين.

---

[1] عبد الله عبد الكريم عبد الله. مرجع سابق.ص 169.

[2] امير فرج يوسف. مرجع سابق. ص 286.

[3] علي حسن محمد الطوالبة . مرجع سابق. ص 196.

[4] على عدنان الفيل. مرجع سابق. ص 198.

ويستخدم التوقيع الالكتروني دليلا للإثبات، إذا توافرت فيه الشروط التي تجعل له الحجية المطلقة في الإثبات، والمتمثلة في:" أن يكون الدليل مقروءا ومستمرا وغير قابل للتعديل أو التغيير"[1].

المطلب الثالث: دور التعاون الدولي في الإنابة القضائية ومكافحة الجريمة الالكترونية:

مع أن التشريعات الداخلية لمعظم الدول حاولت جاهدة أن تحد من الجريمة المعلوماتية ولكنها عجزت عن ذلك، لأن الجريمة الالكترونية هي جريمة عابرة للحدود. و بعد أن شعرت هذه الدول بمدى خطورتها و التي لا تنحصر على إقليم الدولة الواحدة سعت الى تبادل المعلومات المشفرة فيما بينها، ويلاحظ أن الجريمة الالكترونية في تزايد مستمر ونتجت عنها خسائرهامة لذلك اعتبرها البعض من الجرائم المنظمة و تستلزم وجود تعاون دولي قوي وفعال بين الدول لمجابها فعمدت بعض التشريعات الداخلية إلى إصدار قوانين تهدف إلى تحديد الإجراءات الخاصة بالإنابة القضائية، فضلا عن سعي الهيئات الدولية وفي مقدمتها منظمة الأمم المتحدة إلى إبرام اتفاقيات دولية لتكريس تعاون دولي لمواجهة الجرائم الالكترونية و هذا ما سنوضحه في هذا المطلب.

الإنابة القضائية الدولية في مجال الجريمة الالكترونية:

لاحظنا بصدد الحديث عن مشكلة استخلاص الدليل في الجريمة المعلوماتية أن هناك صعوبات هامة تعترض هذا المسعى بسبب الترابط بين شبكات المعلومات، إذ أن هذه الجريمة قد تقع في مكان معين وتنتج آثارها في مكان آخر خارج إقليم الدولة، فهنا يصبح الأمر بحاجة إلى اتفاقيات دولية ثنائية أوجماعية[2] والتي من شأنها تسهيل وتفعيل التواصل الأدائي وتسريع الإنابة القضائية لإنجاز الإجراءات المطلوبة.وتأخذ الإنابة القضائية تعريفات عديدة في الفقه القانوني ومن بينها ما أورده الدكتور أحمد فتحي سرور "بأنها كل تصرف إجرائي يصدر ممن له سلطة التحقيق بموجبه يفوض أحد مأموري الضبط القضائي ليقوم به بدلا منه"[3]. وفي مجال الجريمة الالكترونية تكتسي الإنابة القضائية والمساعدة الدولية بشكل عام أهمية بالغة لذلك أولى لها المشرع الجزائري عناية خاصة

[1] سليم سعداوي. عقود التجارة الالكترونية "دراسة مقارنة". الطبعة الأولى. دار الخلدونية: الجزائر .2008.

[2] عبد الفتاح بيومي حجازي .الاثبات الجنائي في جرائم الكمبيوتر و الانترنت. مرجع سابق. ص 13.

[3] . احمد فتحي سرور. الوسيط في قانون الإجراءات الجزائية. دط. دار النهضة العربية : مصر. ص 507.

فأوكل مهمة تنفيذها إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إلى جانب الهيئات القضائية والمنشأة بموجب المرسوم الرئاسي رقم 15-261 المؤرخ في 08/11/2015[1] وقد جعل من مهامها أيضا تبادل المعلومات مع نظيراتها في الخارج، وهو ما أكدته المادة 14 من القانون رقم 09-04 المؤرخ في 05/08/2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وقد نص في المادة 16 منه على انه وفي حالة الاستعجال قبول طلبات المساعدة القضائية الواردة في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون الواردة عن طريق وسائل الاتصال السريعة بما فيها الفاكس والبريد الالكتروني غير أن اللجوء إلى الإنابة القضائية ليست مطلقة بل أنها مقيدة بشروط[2]. ومن أهمها :أن المشرع الجزائري حدد معالمها في المادة 17 من القانون 09-04 بالقول "لتتم الاستجابة لطلبات المساعدة القضائية الرامية بتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل" وقد حصرت الاتفاقيات الدولية على هذا الاتجاه بالتأكيد على مبدأ السيادة وعدم التدخل في الشؤون الداخلية فقد نصت على سبيل المثال المادة 04 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من طرف الجمعية العامة لمنظمة الأمم المتحدة بتاريخ 15/11/2000[3] على ما يلي: اليس في الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية المنوطة بسلطات تلك الدولة الأخرى بغض النظر عن قانونها الداخلي". ومن أهم القيود المشار لها أيضا ما تضمنته الاتفاقية الدولية لمنظمة الأمم المتحدة في 14/09/05 والخاصة بقمع أعمال الإرهاب النووي وبإلزام الدول الأطراف باتخاذ التدابير لحماية المعلومات التي يتم الحصول عليها سرا بموجب هذه الاتفاقية من دولة أخرى[4]، والحاصل أن الجهود الدولية قطعت شوطا كبيرا في إرساء تعاون وثيق من خلال المؤتمرات التي تشرف عليها الأمم المتحدة أو التي تمت تحت رعاية الجمعية الدولية لقانون العقوبات أو ما ورد في الإعلان العالمي المنبثق

[1] المرسوم الرئاسي رقم 15-261 الصادر بالجريدة الرسمية للجمهورية الجزائرية. العدد 53 سنة 2015.

[2] زيدان زيبحة. مرجع سابق.ص 145.

[3] صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05/02/2002

[4] صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 10-270 في 03/11/2010

بسويسرا في 10-12 ديسمبر2003 ، ففي المؤتمر الثامن للأمم المتحدة المنعقد بهافانا بكوبا عام 1990 تم حث الدول الأعضاء لتكثيف جهودها لمكافحة إساءة استعمال الحاسوب والتصدي لهذا الشكل الجديد من الإجرام بإصدار قوانين ملائمة، كما أن المجلس الأوروبي أصدر العديد من التوصيات في إطار الحد من الجرائم المعلوماتية منها التوصية (رقم 95/13) والتي أكدت أن ما يقتضيه التدخل السريع لمد الإجراءات إلى أنظمة حواسب قد تكون موجودة خارج الدولة، وحتى لا يشكل هذا الإجراء اعتداء على سيادة دولة أو على القانون الدولي، يجب وضع قاعدة قانونية صريحة تسمح بمثل هذا الإجراء[1]، وقد عملت اللجنة الأوروبية بشأن مشاكل الجريمة ولجنة خبراء في مجال جرائم الكمبيوتر على إعداد اتفاقيات منها الاتفاقية رقم 19" أعلنها المجلس الأوروبي في 27/04/2000 والملاحظ أن اهتمام التشريعات الأوروبية بمشكل الجرائم المعلوماتية بدأ في مطلع الثمانينات حيث تبنى المجلس الأوروبي اتفاقية حماية المعطيات الشخصية لسنة 1981 .ويتضح بأن الاتفاقية المعلنة سنة 2000 والمشار لها تعد حاليا بمثابة الاتفاقية الدولية المرجعية بعد أن انضمت إليها كل من الولايات المتحدة الأمريكية وكندا واليابان وجنوب إفريقيا وقد تمت تكملتها ببروتوكول إضافي يتعلق بتجريم الأفعال ذات الطابع العنصري والمعادي للأجانبالمرتكبة عن طريق الأنظمة المعلوماتية والموقع في ستراسبورغ بتاريخ 28/09/2003[2]

أما عن الجهود العربية في إطار الحماية من الجرائم المعلوماتية فإنه يمكن الإشارة إلى القانون العربي الاسترشادي لمكافحة جرائم تقنية المعلومات وما في حكمها والذي اعتمده مجلس وزراء العدل العرب في دورته التاسعة عشر بالقرار رقم 19.495 في 08/10/2003 وكذا مجلس وزراء الداخلية العرب في دورته الحادية والعشرين بالقرار رقم 417-د. في 21/04/2004[3] . وعلى العموم يمكن أن نخلص إلى القول بأنه وأمام تطور وتنوع الجريمة المعلوماتية وتعدد أشكالها وصورها فإن المجهود الدولي لا يزال

[1] مدحت عبد الحليم رمضان. مرجع سابق. ص 31

[2] د. محمد سامي الشوا. مرجع سابق. ص164.

[3] د. محمود احمد عبابنة. مرجع سابق. ص 171

غير كاف مما يستدعي بالضرورة إيجاد آليات إجراءات من شأنها الإحاطة بالظاهرة والحيلولة دون المزيد من تفاقمها.

خلاصة الفصل الثاني:

تطرقنا في الفصل الثاني إلى إجراءات التحقيق وجمع الأدلة في مجال الجريمة المعلوماتية ووقفنا على مدى الصعوبة التي تعترض هذه العملية نظرا للطبيعة التي يتسم بها الدليل الرقمي وطبيعته البيئية التي يتواجد فيها وقد بينا القواعد الإجرائية التقليدية التي يمكن اعتمادها لاستخلاص الدليل الرقمي أو المعلوماتي كالتفتيش والمعاينة والشهادة والخبرة الفنية ثم ركزنا على التفتيش في البيئة الرقمية والذي يمكن أن يكون عن بعد من خلال الدخول إلى المنظومة المعلوماتية أو جزء منها وكذا المعطيات المخزنة فيها ووضحنا شروط التفتيش وإجراءاته في هذه المنظومة، ثم خلصنا إلى التدابير الخاصة بضبط وتحريز الأدلة في الحاسوب والانترنت من خلال ضبط الكيانات المادية أو المعنوية للحاسوب مبرزين كل نوع منها وطبيعه ومدى الصعوبة المرتبطة بإجراءات

الضبط هذه، ثم حددنا القيمة القانونية للدليل الالكتروني من خلال تحديد شروطه ثم الوقوف على مدى حجته لننتهي إلى تعريف الإنابة القضائية المتاحة في إطار التعاون الدولي لملاحقة الجريمة الالكترونية وأشرنا في ذلك إلى الجهود الدولية والإقليمية في هذا المجال وأهم الاتفاقيات الدولية التي شكلت مرجعا ومنهلا لمختلف
التشريعات المستحدثة لمكافحة الجريمة الالكترونية.

الخاتمـــــــــــة

الخاتمة

ليس من الصدفة أن أتناول موضوع الاثبات الجنائي في الجريمة الالكترونية, بل بدا لنا لأول وهلة من الأهمية بمكان . بعد أن اتسعت دائرة الجريمة الالكترونية اذ لم تعد مقتصرة على النفاذ غير المصرح به الى نظم الحاسوب وبياناته و الاقدام على استعمالها دون اذن. بل امتدت و بشكل واضح الى الاعتداء على الحياة الخاصة للإنسان و حقوقه الاساسية و الاكثر من ذلك أن هذه الجريمة اصبحت تهدد كيان الدول في اختراق مواقع مؤسساتها و خاصة المالية منها , و قد لاحظنا أن هذه الجريمة تتسم بطابع خاص و مميز كونها تتم في عالم افتراضي و مرتكبوها هم اشخاص لهم مواصفات خاصة اهمها الذكاء و الدهاء و من هنا طرحت اشكالية الدليل , و كيفية الوصول اليه.

و من اجل ذلك تناولنا في البحث اهم التعريفات التي سلطت الضوء على الجريمة الالكترونية و استجلاء حقيقتها و ماهيتها ثم تطرقنا الى الاثبات الجنائي في الجريمة الالكترونية و تعريف مبادئه و وسائله الحديثة .

ثم تناولنا اجراءات التحقيق و جمع الأدلة في مجال الجريمة الالكترونية و وقفنا على الصعوبة التي تعترض هذه العملية و ذلك بالنظر إلى طبيعة الدليل الرقمي في حد ذاته و الطابع المميز للبيئة التي يتواجد فيها , ثم بينت اهم الوسائل التقليدية التي يمكن اعتمادها للوصول الى الدليل مثل التفتيش و المعاينة و الشهادة و وضحنا بان التفتيش و ان كانت غايته ضبط أدلة الجريمة موضوع التحقيق او كل ما يفيد في كشف الحقيقة بشانها فانه يختلف بالنسبة للمنظومة المعلوماتية و توقفنا عند الضوابط التي اوردها بشان ذلك المشرع الجزائري في القانون 09_04 في المادة 5 منه سيما فيما يتعلق بالدخول عن بعد بغرض تفتيش المنظومة المعلوماتية او المعطيات المخزنة فيها و وقفنا على مدى الصعوبة و العوائق التي تثار عندما ينصب التفتيش على مكونات الحاسوب المعنوية أو المنطقية كالبرامج و قواعد البيانات و الذي يتطلب الكشف عن الرقم السري الكود " cod " للمرور إلى الملفات , و قد اوردنا شروط التفتيش و اجراءاته و كذلك الشأن بالنسبة للوصول الى ضبط و تحريز الأدلة و ما تعلق منها بالكيانات المادية و المعنوية للحاسوب .

ثم بينا القيمة القانونية للدليل الرقمي و مدى حجيتة و انتهينا إلى تعريف الانابة القضائية الدولية و الجهود الدولية في مكافحة الجريمة الالكترونية بشكل عام و اهم الاتفاقيات المبرمة بهذا الشان. النتائج او من خلال الإجابة عن الاشكالات المطروحة و التي أبرزتها الدراسة خلصنا الى جملة من النتائج اهمها:

_ أن الجريمة الالكترونية ظاهرة جديدة و خطيرة و هي تمثل الوجه السلبي للثورة المعلوماتية و التطور التكنولوجي كونها تتخذ نظام الحاسوب كوسيلة لها . آن صعوبة الحصول على الدليل في الجريمة الالكترونية يظل من الصعوبة بمكان و ان الاجراءات التي اقرها المشرع الجزائري في هذا المجال بموجب أحكام القانون 09_04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها , تعد غير كافية .

- ان الصعوبة تظل قائمة في التوفيق بين فكرة حماية النظام العام و مبدا الحفاظ على الحياة الخاصة و ذلك من الناحية العملية و ما يصاحب ذلك من اشكالات وتضارب النصوص كما هو الشان في مراقبة الاتصالات الالكترونية التي تنظمها المادة 3 من القانون 09_04 و تجيزها في حين تحظرها المادة105 الفقرة الأخيرة من القانون رقم 2000/03 المؤرخ في 05/08/2000 الذي يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية و التي تنص على أنه "لا يمكن بأي حال من الأحوال انتهاك سرية المراسلات ".

التوصيات

و في الاخير وعلى ضوء ما انتهينا اليه فضلنا بان ندرج جملة من التوصيات و المقترحات فيما يلي :

1_ اصدار المزيد من النصوص الخاصة من شانها الاحاطة بالوسائل العلمية و بتيسير استعمالها في اطار التحقيق و التحريات لملاحقة المجرم المعلوماتي و استخلاص الدليل الرقمي بما في ذلك تقنية البصمة الوراثية ADN.

2 _ العمل على تدريب رجال القضاء و اعداد رجال امن متخصصين في مجال الحاسوب و الانترنت .

3- وضع ضوابط خاصة تحكم عمل مقاهي الانترنت و منها وضع استمارة خاصة تتضمن هوية و رقم
الجهاز المستعمل للزبون...
4_ انشاء تخصصات جديدة بكليات الحقوق بالجامعات لتدريس الحماية القانونية للمعلومات على غرار
الملكية الفكرية و برامج اخلاقيات الاستخدام العقلاني للأنترنت. وفي النهاية أمل أن أكون قد وفقت بعون الله.

قائمة المراجع و المصادر

قائمة المصادر و المراجع

المصادر

1_ القران الكريم

2_دستور 1663.

3_دستور 1996 المعدل و المتمم بالقانون رقم 16-01 المؤرخ في 06 مارس 2016 الجريدة

الرسمية رقم 14 المؤرخة في 7 مارس 2016.

4_ الاعلان العالمي لحقوق الانسان المعتمد من قبل الجمعية العامة للامم المتحدة بتاريخ 10/12/1948

تبنته الجزائر بموجب نص المادة 11 من دستور 1963 .

5_ اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من قبل الجمعية العامة المنظمة الأمم المتحدة بتاريخ 15/11/2000 . صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 02-55.

6_ الاتفاقية الدولية لمنظمة الأمم المتحدة في 14/09/2005 و الخاصة بقمع اعمال الارهاب النووي. صادقت عليها الجزائر بتحفظ بموجب المرسوم الرئاسي رقم 10-270 في تاريخ 2010/11/3.

7_ الأمر رقم 66-155 المؤرخ في 8/6/1966 المعدل و المتمم المتعلق بقانون الاجراءات الجزائية الجزائري.

8_ القانون رقم 2000/03 المؤرخ في 05/08/2000 يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلكية و اللاسلكية.

_ القانون رقم 09-04 المؤرخ في 05/08/2009 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال ومكافحتها صدر بالجريدة الرسمية للجمهورية الجزائرية العدد 47.

10_ مرسوم رقم 04-183 المؤرخ في 26/06/2004 يتضمن أحداث المعهد الوطني للأدلة الجنائية و

علم الاجرام للدرك الوطني و تحديد قانونه الأساسي.

11_ المرسوم الرئاسي رقم 15-261 الصادر بالجريدة الرسمية الجزائية . العدد 53 سنة 2015.

المراجع

الكتب

1_ اسامة أحمد بدر. حماية المستهلك في التعاقد الالكتروني "دراسة مقارنة ". ط. دار الجامعة الجديدة للنشر: الاسكندرية.مصر.2005.

2_ انتصار نوري الغريب. أمن الكمبيوتر والقانون "دراسة مقارنة". الطبعة الأولى.دار الراتب الجامعية: بيروت. لبنان.1994.

3_ احمد خليفة الملط. الجرائم المعلوماتية. الطبعة الثانية. دار الفكر الجامعي: الاسكندرية. مصر .2006.

4_ امال قارة. الحماية الجزائية للمعلوماتية في التشريع الجزائري. الطبعة الثانية.دار هومة: الجزائر .2007.

5- احمد فتحي سرور. الوسيط في الاجراءات الجزائية. ط. دار النهضة العربية: مصر 1999.

6_ جميل عبد الباقي الصغير. الانترت و القانون الجنائي." الأحكام الموضوعية للجرائم المتعلقة بالانترنت". الطبعة الأولى. دار النهضة العربية: مصر. 2001.

7_ داود حسن طاهر. نظم المعلومات.دط. اكادمية نايف الامنية: الرياض. السعودية. 1420هجري.

8_ هشام محمد فريد رستم. قانون العقوبات و مخاطر تقنية المعلومات.دط. مكتبة الآلات الحديثة: اسيوط. مصر. 1994.

9_ هشام محمد فريد رستم. الجوانب الاجرائية للجرائم المعلوماتية. "دراسة مقارنة". دط. مكتبة اللات الحديثة: اسيوط. 1994.

10_ هاني محمد دويدار. نطاق احتكار التكنولوجيا بواسطة المعرفة السرية.دط. دار الجامعة الجديدة: مصر. 1996.

11_ هدى حامد قشقوش. جرائم الحاسب الالكتروني و التشريع المقارن.دط. دار النهضة العربية: القاهرة. مصر.1992.

12_ زيدان زيبحة. الجريمة المعلوماتية في التشريع الجزائري و الدولي. الطبعة الأولى. دار الهدى: الجزائر. 2011.

13_ يونس خالد عرب. العالم الالكتروني. "الوسائل و المحتوى و المزايا و السلبيات". دط. منشورات اتحاد المصاريف العربية: الأردن. 2001.

14_ كوثر مازوني. الشبكة الرقمية و علاقتها بالملكية الفكرية.دط. دار هومة: الجزائر .2008.

15_ مدحت رمضان. جرائم الاعتداء على الأشخاص و الانترنت.دط. دار النهضة العربية: مصر.2000.

16_ محي الدين عكاشة. محاضرات في الملكية الادبية و الفنية.دط.ديوان المطبوعات الجامعية: الجزائر. 2001.

17_ محمد الهادي بن زيطة. حماية برنامج الحاسوب في التشريع الجزائري. الطبعة الأولى. دار الخلدونية: الجزائر 2007.

18_ محمد سامي الشوا. ثورة المعلومات و انعكاساتها على قانون العقوبات. الطبعة الأولى. دار النهضة العربية: مصر. 1994.

19_ ماروك نصر الدين. محاضرات في الاثبات الجنائي .دط. الجزء الأول. دار هومة: الجزائر.2003.

20_ محمد مروان. نظام الاثبات في المواد الجنائية في القانون الوصفي الجزائري.دط. ديوان المطبوعات الجامعية: بن عكنون. الجزائر 1999.

21_ محمود احمد طه. عبئ اثبات الأحوال الأصلح للمتهم. دط.منشاة المعارف: الاسكندرية. مصر.2003.

22_ مسعود زبدة. الاقتناع الشخصي للقاضي الجزائي. الطبعة الأولى. المؤسسة الوطنية للكتاب : الجزائر. 1989 .

23_ محمد رمضان بازة. قانون العقوبات الليبي" جرائم الاعتداء على الأموال . القسم الخاص". دط. الجزء الثاني. منشورات جامعة ناصر: طرابلس. ليبيا. 1992.

24_ محمد زكي أبو عامر. الاجراءات الجنائية. الطبعة السابعة. دار الجامعة الجديدة للنشر: الاسكندرية. مصر .2005.

25_ نائلة عادل محمد فريد قديورة. جرائم الحاسب الالي الاقتصادية. الطبعة الأولى. منشورات الحلبي: لبنان. 2005.

26_ سليم سعداوي. عقود التجارة الالكترونية. "دراسة مقارنة". الطبعة الأولى. دار الخلدونية: الجزائر. 2008.

27_ عبد العال الديربي. محمد صادق اسماعيل. الجرائم الالكترونية." دراسة قانونية مقارنة"، الطبعة الأولى. المركز القومي للاصدارات القانونية: مصر. 2012.

28_ عفيفي كمال عفيفي. فتوح الشادلي. جرائم الكمبيوتر.دط. منشورات الحلبي الحقوقية: لبنان.2003.

29_ عمار عباس الحسيني. التحقيق الجنائي و الوسائل الحديثة في كشف الجريمة. الطبعة الأولى. منشورات دار الحلبي: لبنان. 2015.

30_ عبد الله اوهابية. شرح قانون الاجراءات الجزائية الجزائري." التحري والتحقيق" .دط. دار هومة: الجزائر. 2008.

31_ عبد الفتاح بيومي حجازي.لدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت .دط. دار الكتب القانونية: مصر .2002

32_ عبد الفتاح بيومي حجازي. التجارة الالكترونية و حمايتها القانونية.دط. دار الفكر الجامعي: الاسكندرية. مصر.2004.

33_ عبد الفتاح بيومي حجازي. مكافحة جرائم الكمبيوتر و الانترنت. "دراسة معقمة للقانون المعلوماتي". الطبعة الأولى. دار الفكر الجامعي: الاسكندرية. مصر. 2006.

34_عبد الفتاح بيومي حجازي. الدليل الجنائي والاثبات في جرائم الكمبيوتر و الانترنت في القانون العربي النموذجي. الطبعة الأولى. دار الفكر الجامعي: الاسكندرية. مصر. 2006.

35_ عبد الله الكريم عبد الله. جرائم المعلوماتية و الانترنت "الجرائم الاكترونية. دراسة مقارنة". الطبعة الاولى. منشورات الحلبي الحقوقية: بيروت. لبنان. 2007.

36_ عمر الفاروق الحسيني. المشكلات الهامة في الجرائم المتصلة بالحاسب الالي و ابعادها الدولية. الطبعة الثانية. دار النهضة العربية: مصر. 1995.

37_ علي القهوجي. الحماية الجنائية لبرامج الحاسب الالي .دط. الدار الجامعية: بيروت. لبنان.1999.

38_ عبد الرزاق السنهوري. الوسيط في شرح القانون المدني. الجزء الثاني -دار احياء التراث العربي: بيروت. لبنان. 1952. ص 67.

39_ عبد اللاه احمد هلالي. النظرية العامة للإثبات في المواد الجنائية. الطبعة الأولى. دار النهضة العربية: القاهرة . مصر. 1987.

40_ عبد اللاه احمد هلالي. حجية المخرجات الالكترونية. الطبعة الأولى. دار النهضة العربية: القاهرة. مصر 1997.

41_ علي حسن محمد الطوالبة. التفتيش الجنائي على نظم الحاسوب و الانترنت"دراسة مقارنة". الطبعة الأولى. المركز القومي للاصدارات القانونية: مصر. 2012.

42_ فاروق حسين. معجم مصطلحات الحاسب الالي .دط. دار الراتب الجامعية: بيروت، لبنان. 1999.

43_ فراح مناني. أدلة الإثبات الحديثة في القانون .دط. دار الهدى للطباعة و النشر : الجزائر. 2008.

44_ فاضل زيدان محمد. سلطة القاضي الجنائي في تقدير الادلة" دراسة مقارنة" . دار الثقافة للنشر : عمان. 2006. عوض. مشروعية الدليل الجنائي في مرحلة المحاكمة.دط. دار النهضة العربية:

45_ رمزي رياض مصر. 1997.

46 رشا مصطفى ابو الغيظ. الحماية القانونية للكيانات المنطقية" برنامج الحاسوب. ملتقى الفكر للطباعة : الاسكندرية. مصر.2000.

المقالات في المجالات المتخصصة :

1_ مختار الأخضري. بحث بعنوان الاطار القانوني لمواجهة جرائم المعلوماتية و جرائم الفضاء الافتراضي. "نشرة القضاة": العدد 2010.66.

2_ محمد عبيد سيف سعيد المسماري. عبيد الناصر محمد محمود فرغلي. الاثبات الجنائي بالادلة الرقمية من الناحيتين القانونية و الطب الشرعي." بحث مقدم للمؤتمر الشرعي". من 12 الى 14/11/2007. جامعة نايف العربية للعلوم الأمنية: الرياض. السعودية.2007.

3_ علي حمودة. الأدلة المتحصلة من الوسائل الالكترونية في اطار نظرية الاثبات الجنائي. الجز الاول. "مجلة أكاديمية شرطة دبي": دبي. عدد 01. 2003.

الفـــــــهرس