آليات الحصول على الأدلة الرقمية كوسائل إثبات في الجرائم الإلكترونية

Mechanisms for obtaining digital evidence as evidence in Electronic Crimes.

- **فلاك مراد،** تسجيل سادس دكتوراه علوم في القانون العام، حي محمد بوضياف الجنوبي بلدية برهوم ولاية المسيلة.

تاريخ إرسال المقال: 2019/05/03 **تاريخ قبول المقال:** 2019/05/11 **تاريخ نشر المقال:** 2019/06/12

ملخص:

تهدف الدراسة إلى فهم نوع مستحدث من الجرائم يعرف بالجرائم الالكترونية, مرتكب من طرف أصناف يعرفون بالمجرمين المعلوماتيين الذين يتميزون بالذكاء والفطنة. ورأينا أن هذه الجريمة يتولد عنها نوع جديد من الأدلة الجنائية , وهو الدليل الرقمي ذو هيئة الكترونية غير ملموسة لا تدرك بالحواس, وهذه أهم خاصية تميز الدليل الالكتروني عن غيره من الأدلة الجنائية.

ولإثبات الجريمة الالكترونية لابد من إتباع طرق الإثبات المتعارف عليها , والتي تخضع للقواعد العامة للإثبات الجنائي. ولكن ما يميز هذه الجرائم أنه عند تطبيق طرق الإثبات في مجالها ينتج دليل خاص بها وهو الدليل الالكتروني, والدي يتميز بكونه دليل دو هيئة الكترونية غير ملموسة, ويخضع شأنه شأن الأدلة الجنائية الأخرى للسلطة التقديرية للقاضي الجزائي .

الكلمات المفتاحية:

الأدلة الرقمية– الجرائم الالكترونية– الجريمة المعلوماتية– وسائل الإثبات .

Abstract:

The study aims at understanding an innovative type of crime known as cybercrime, committed by categories known to intelligence criminals who are intelligent and discerning. We have seen that this crime generates a new type of forensic evidence A digital guide with an intangible electronic body that is not aware of the senses, and this is the most important characteristic of the electronic evidence of other forensic evidence.

In order to prove the electronic crime, it is necessary to follow the usual methods of proof, which are subject to the general rules of criminal evidence. However, it is characteristic of these crimes that when the methods of proof are applied in their field, a manual is produced which is the electronic evidence. My father is characterized by evidence as an electronic body and is subject, like other criminal evidence, to the discretion of the criminal judge.

Key words

Digital evidence - Electronic Crimes - Information crime - Means of proof.

مقدمة:

إن التطور المدهش للإنترنيت، أدى إلى نشوء جرائم ناتجة عن ذلك الاستخدام، و هذه الجرائم قد تقع على الإنترنيت نفسه أو قد تقع بواسطته، بحيث يصبح أداة في يد الجاني يستخدمه ليحقق أغراضه الإجرامية نظرا لظهور مشكلة جرائم الكمبيوتر كمشكلة أمنية، وقانونية واجتماعية، فإن خبراء الأمن المعلوماتي وصانعي السياسات الحكومية ومسوقي الكمبيوتر، والأفراد المهتمين بهذا الموضوع في حاجة إلى تغيير نظرتهم تجاه جرائم الكمبيوتر، لا لأنها مشكلة وطنية فقط، وإنما كمشكلة عالمية، وتتطلب الإجراءات الوطنية تعاونا في مجالي القطاع العام والخاص، فبخصوص القطاع الخاص الالتزام بإجراءات الوقاية، وبخصوص القطاع العام تنفيذ الإجراءات اللازمة لمكافحة الجريمة وبوجه عام.

واعتبارا لهذا الازدياد السريع للجرائم الإلكترونية، فقد ذهبت جل الدول إلى وضع تشريعات جنائية خاصة لمكافحة الجرائم الإلكترونية، هذه الظاهرة المستحدثة في علم الإجرام ومن هذه الدول الولايات المتحدة الأمريكية و فرنسا وهولندا و الاتحاد الأوروبي؛ هذا الأخير الذي وضع اتفاقية حول جرائم الكمبيوتر سنة 2000.

وكما هو الحال في كل دول العالم استفحلت الجريمة الإلكترونية في الجزائر خلال العقود الأخيرة، وأصبح القضاء الجزائري في محك حقيقي، عندما وضعت أمامه قضايا تتعلق بالجرائم الإلكترونية.

ونظرا لهذا التطور الذي عرفته الجريمة في الجزائر، قام المشرع الجزائري بتعديل قانون بموجب قانون العقوبات رقم 04-15المؤرخ في 10نوفمبر2004المتمم للأمر رقم 66-156 المتضمن قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات, ويتضمن هذا القسم ثمانية مواد من المادة 394 مكرر إلى المادة 394 مكرر7.

لكل هذه الأسباب كان لابد من الاشتغال على و سائل الإثبات و تطويرها، بحيث أصبح ما يعرف بالإثبات الإلكتروني أو الرقمي، متجاوزا تلك الإثباتات التقليدية و استبدال الملفات الورقية بالأسطوانات الضوئية أو الأقراص الممغنطة.

هنا يمكن طرح الإشكال على الشكل التالي: ما هي آليات الحصول على الدليل الرقمي في الجرائم الإلكترونية؟ و إلى أي حد يمكن قبول الأدلة الرقمية كوسائل إثبات؟ و ما هي الصعوبات التي يطرحها الحصول على الدليل الإلكتروني ؟

وللإجابة عن الإشكال سوف نتبع التصميم التالي:

المطلب الأول: ماهية الدليل الرقمي في الجريمة الإلكترونية.

المطلب الثاني : الإجراءات التقليدية للحصول على الدليل الإلكتروني.

المطلب الأول: ماهية الدليل الرقمي في الجريمة الإلكتروني .

يعد الإثبات الجنائي بالأدلة الرقمية من أبرز تطورات العصر الحديث، و التي جاءت لتلائم الثورة العلمية و التكنولوجية و التقنية في عصرنا الحالي، و التي تطور معها الفكر الإجرامي الذي صاحب ظهور ما يعرف بالجريمة الإلكترونية ألقى على عاتق القائمين على مكافحة الجريمة في الدولة عبئا شديدا و مهاما جسيمة تفوق القدرات المتاحة لهم و فق أسس و قواعد و إجراءات البحث الجنائي و الإثبات الجنائي التقليدي ، نظرا لعدم كفاية و عدم ملائمة هذه النظم التقليدية في إثبات تلك الجرائم سواء من الناحيتين القانونية أو التقنية، الشيء الذي ألزم على المشرع أن يتدخل بقوانين تتناسب مع مثل هذه الجرائم.

فكانت هذه التطورات التي عرفتها المعلوميات كفيلة لتجعل الإثبات الجنائي يتأثر من جراء الجرائم التي أفرزتها هذه الثورة المعلوماتية، الأمر الذي جعل من طبيعة الإثبات بالوسائل التقليدية أمر متجاوز, ولعل هذه الطبيعة غير المرئية للأدلة المتحصلة من الوسائل الإلكترونية تلقى بظلالها على الجهات التي تتعامل مع الجرائم التي تقع بالوسائل الإلكترونية حيث تصعب قدرتهم على فحص واختبار البيانات محل الاشتباه خاصة في حالات التلاعب في برامج الحاسوب، ومن ثم فقد يستحيل عليهم الوصول إلى الجناة[1]. فمن المعلوم أن جهات التحري والتحقيق اعتادت على الاعتماد في جمع الدليل على الوسائل التقليدية للإثبات الجنائي التي تعتمد على الإثبات المادي للجريمة ولكن في محيط الإلكترونيات فالأمر مختلف، فالمتحري أو المحقق لا يستطيع أي منهما تطبيق إجراءات الإثبات التقليدية على المعلومات المعنوية.

أولا : ماهية الدليل الرقمي

يقصد بالإثبات إقامة الدليل على وقوع الجريمة و على نسبتها إلى المتهم، أي إثبات الوقائع، فليس هناك من شك في أن وصول القاضي الجنائي إلى حكم يعبر عن الحقيقة في الواقعة المطروحة عليه، ليس بالأمر الهين, لذلك فالقاضي ملزم بإقامة الدليل على وقوع هذه الجريمة و على مسؤولية المتهم عنها. وهذا يستلزم على القاضي أن يستعين بوسائل تعيد أمامه تفاصيل حدوث الجريمة، وهذه الوسائل هي وسائل الإثبات، ومن هنا تأتي مسؤولية الدليل في المسائل الجنائية هذا من ناحية, أما من ناحية أخرى فعملية الإثبات الجنائي في الجرائم الرقمية ترتكز على الدليل الرقمي باعتباره الوسيلة الوحيدة و الرئيسية لإثبات الجريمة، و هو محور اهتمام بحثنا.

بداية نشير إلى أن الأدلة الإلكترونية المستخرجة من الأنترنيت، قد تكون مستخرجات ورقية يتم إنتاجها عن طريق الطابعات (les imprimantes)،أو مستخرجات لا ورقية لكنها إلكترونية كالأقراص

[1] - أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الإنترنت ، دار المطبوعات الجامعية الإسكندرية ، 2009,ص25

الممغنطة أو أسطوانات الفيديو أو الأقراص الضوئية و غيرها من الأشكال غير التقليدية ،إضافة أن هناك نوع ثالث يتمثل في عرض المستخرجات المعالجة بواسطة الحاسوب[2].

وعموما يُعرِّف الدليل الرقمي بأنه: هو الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج تطبيقات وتكنولوجيا وهى مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ و تطبيق القانون [3].

كما يمكن تعريف الدليل الإلكتروني بأنه:هو تلك المعلومات التي يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية و علمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي و ملحقاتها و شبكات الاتصال، و يمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة[4].

ولذا بالاستفادة مما سبق يمكن تعريف الدليل الرقمي بأنـه: مجموعة المجالات أو النبضات المغناطيسية أو الكهربائية التي يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات خاصة لتظهر في شكل صور أو تسجيلات صوتية أو مرئية .

ثانيا : أنواع الدليل الإلكتروني

إن التعريف بالدليل الرقمي يحتم علينا تحديد أنواعه و أشكاله حتى يتسنى فهم الهيأة التي يتخذها للحكم على قيمته القانونية فيما بعد، بحيث يمكن تقسيم الدليل الرقمي لنوعين رئيسين هما:

1 - أدلة أعدت لتكون وسيلة إثبات

وهذا النوع من الأدلة الرقمية يمكن إجماله فيما يلي :

-السجلات التي تم أنشاؤها بواسطة الآلة تلقائياً، وتعتبر هذه السجلات من مخرجات الآلة التي لم يساهم الإنسان في إنشائها مثل سجلات الهاتف وفواتير أجهزة الحاسب الآلي.

-السجلات التي جزء منها تم حفظه بالإدخال وجزء تم إنشاؤه بواسطة الآلة ومن أمثلة ذلك البيانات التي يتم إدخالها إلى الآلة و تتمُّ معالجتها من خلال برنامج خاص ، كإجراء العمليات الحسابية على تلك البيانات .

2- أدلة لم تعد لتكون وسيلة إثبات

وهذا النوع من الأدلة الرقمية نشأ دون إرادة الشخص، أي أنها أثر يتركه الجاني دون أن يكون راغباً في وجوده ، ويسمى هذا النوع من الأدلة بالبصمة الرقمية، وهى ما يمكن تسميته أيضاً بالآثار

2- عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر و الانترنت ، دار الكتب القانونية مصر 2006 [2] .، ص 81.

[3] - أمير فرج يوسف ، مرجع سابق ,ص29.

[4] - هشام محمد رستم : الجوانب الإجرائية للجرائم المعلوماتية ـ مكتبة الآلات الحديثة- أسيوط 1994، ص 31

المعلوماتية الرقمية، وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وكافه الاتصالات التي تمت من خلال الآلة أو شبكة المعلومات العالمية[5].

وتبدو أهمية التمييز بين هذين النوعين فيما يلي :

– النوع الثاني من الأدلة الرقمية هو الأكثر أهمية من النوع الأول لكونه لم يُعد أصلاً ليكون أثراً لمن صدر عنه، ولذا فهو في العادة سيتضمن معلومات تفيد في الكشف عن الجريمة ومرتكبها.

– يتميز النوع الأول من الأدلة الرقمية بسهولة الحصول عليه لأنه أُعد أصلاً لأن يكون دليلاً على الوقائع التي يتضمنها، في حين يكون الحصول علي النوع الثاني من الأدلة بإتباع تقنية خاصة لا تخلو من صعوبة وتعقيد.

– لأن النوع الأول قد أُعدَّ كوسيلة إثبات لبعض الوقائع فإنه عادة ما يُعمد إلى حفظه للاحتجاج به لاحقاً وهو ما يقلل من إمكانية فقدانه، و على عكس النوع الثاني حيث لم يُعد ليحفظ ما يجعله عرض للفقدان لأسباب منها فصل التيار الكهربائي عن الجهاز مثلا .

ثالثا :أشكال الدليل الإلكتروني

يتخذ الدليل الرقمي ثلاثة أشكال رئيسة هي :

1 – **الصور الرقمية:** وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفى العادة تقدم الصورة إما في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنولوجيا بديلة للصورة الفوتوغرافية التقليدية وهي قد تبدو أكثر تطوراً ولكنها ليست بالصورة أفضل من الصور التقليدية .

2 – التسجيلات الصوتية: وهى التسجيلات التي يتم ضبط وتخزينها بواسطة الآلة الرقمية ، وتشمل المحادثات الصوتية على الانترنت والهاتف.... الخ .

3– النصوص المكتوبة: وتشمل النصوص التي يتم كتابها بواسطة الآلة الرقمية، ومنها الرسائل عبر البريد الالكتروني، والهاتف المحمول، والبيانات المسجلة بأجهزة الحاسب الآلي،.... الخ .

رابعا :خصائص الدليل الإلكتروني

يتميز الدليل الجنائي الإلكتروني عن الدليل الجنائي التقليدي بعدة خصائص يمكن رصد مجملها فيما يلي:

– الأدلة الرقمية تتكون من بيانات و معلومات ذات هيئة إلكترونية غير ملموسة،لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بالأجهزة و المعدات و الأدوات الآلية(hardware) ، و استخدام نظم برامجية حاسوبية (software)[6].

[5] - عبد الفتاح بيومي حجازي , مرجع سابق , ص 84.

[6] - محمد عادل ريان ، جرائم الحاسب الآلي وأمن البيانات،بيروت،2002،ص 43.

– الأدلة الرقمية ليست أقل من الدليل المادي فحسب،بل تصل إلى درجة التخيلية في شكلها و حجمها و مكان تواجدها غير المعلن.

– يمكن استخراج من الأدلة الرقمية الجنائية نسخ مطابقة للأصل ولها ذات القيمة العلمية و الحجية الثبوتية الشيء الذي لا يتوفر في أنواع الأدلة(الأخرى التقليدية)،مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد، والتلف، و التغيير، عن طريق نسخ طبق الأصل من الدليل[7].

– يتميز الدليل الرقمي بصعوبة محوه أو تحطيمه، إذ حتى في حالة محاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلة التي تحتوى ذلك الدليل.

المطلب الثاني: الإجراءات التقليدية للحصول على الدليل الإلكتروني.

على الرغم من وجود تشابه كبير بين التحقيق في جرائم الإنترنت وبين التحقيق في الجرائم الأخرى فهي جميعاً تحتاج إلى إجراءات تتشابه في عمومها مثل المعاينة والتفتيش والشهادة و الخبرة بالإضافة إلى جمع الأدلة، كما أنها تشترك في كونها تسعى إلى الإجابة على الأسئلة المشهورة لدي المحقق، ماذا حدث؟ وأين؟ ومتى؟ وكيف؟ ومن؟ ولماذا؟.

وتظل الجرائم المتعلقة بشبكة الإنترنت تمتاز عن غيرها من الجرائم ببعض الخصائص وهذا بالطبع يستدعي تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع هذه الخصوصية، وتمكن المحقق من كشف الجريمة والتعرف على مرتكبيها بالسرعة والدقة اللازمين فالتحقيق في هذا النوع من الجرائم يستدعي الرجوع إلى عدد كبير من السجلات التي يجب الاطلاع عليها مثل الكتيبات الخاصة بأجهزة الحاسب الآلي، وملفات تسجيل العمليات الحاسوبية، بالإضافة إلى الاطلاع على كم كبير من السجلات عن خلفية المنظمة وموظفيها.

ومما لا شك فيه أن هذه الجرائم غيرت أسلوب عمل أجهزة البحث و التحقيق، وفرضت عليه التعامل مع مسرح جريمة غير معتاد يقع في عالم افتراضي، وفي بيئة تقنية تتطلب مهارات و قدرات و تقنيات خاصة قد لا تتوفر معظم هذه الأجهزة مما فرض عليها كذلك تخصيص فرق متخصصة و متكونة في مجال تقنيات المعلوميات ورصدها لمكافحة هذه الجرائم.

فعلى المستوى الإجرائي تشكل الإجراءات التقليدية من معاينة وتفتيش والاستماع إلى الشهود وندب الخبراء أساس عمل أجهزة البحث و الحقيق قصد الحصول على الأدلة الجنائية، للتثبت من الجريمة و ضبط مرتكبيها و تقديمهم للمحاكمة.

ويعد كل من المعاينة والتفتيش و الشهادة من أحد وسائل جمع الأدلة ولكل منها قواعده يتم إتباعها، وسنتناول كل واحدة على النحو التالي:

[7] -هشام محمد رستم , مرجع سابق , ص 36.

أولا: المعاينة

يرى البعض أن أهمية المعاينة تتضاءل في الجريمة المعلوماتية، وذلك لندرة تخلف أثار مادية عند ارتكاب الجريمة المعلوماتية، كما أن طول فترة الوقوع بين وقوع الجريمة و ارتكابها و بين اكتشافها يكون له تأثير السلبي على الآثار الناجمة عنها سواء بسبب العبث أو المحو أو التلف لتلك الآثار[8].

ويقصد بالمعاينة أنها "رؤية العين لمكان أو شخص أو أي شيء لإثبات حالته و ضبط كل ما يلزم لكشف الحقيقة" "،و يقصد بها كذلك أنها "إثبات مادي و مباشر لحالة الشخص و الأشياء والأمكنة ذات صلة بالحادث[9].

كما يقصد بالمعاينة الكشف الحسي المباشر لإثبات حالة شيء أو شخص، وتتم إما بانتقال المحقق إلى مكان أخر أو بجلب موضوع المعاينة إلى مقره كما في معاينة العملات المزورة أو الأشياء و الأسلحة و الأوراق التي استخدمت في اقتراف الجريمة أو مكان و أثار الجريمة أو الكشف عن المجني عليه لإثبات أثار الجريمة من ضرب أو جرح أو قتل أو فحص المدعى عليه لإثبات حالته المرضية أو ما تعرض له من ضرب و تعذيب

فالمعاينة وسيلة بواسطتها يتمكن القاضي من الإدراك المباشر للجريمة ومرتكبها وقد تشمل النتائج المادية التي تخلفت عنها أو إثبات حالة الأماكن أو الأشياء أو الأشخاص التي لها علاقة بالجريمة أو إثبات الوسيلة التي استخدمت في ارتكابها أو المكان الذي وقعت فيه الجريمة[10].

وتتم المعاينة بأية حاسة من الحواس، مثل المس و السمع و البصر و الشم والتذوق. والمعاينة قد تكون شخصية فتنصب الملاحظة على شخص، ويستوي أن تتناول المعاينة المجني عليه أو المتهم كما إذا كان الغرض منها إثبات أثار الإكراه بالمجني عليه في جريمة السرقة، وقد يكون موضوع المعاينة شخصا على قيد الحياة. وفي الجرائم المعلوماتية تكون فرصة الحصول على الدليل الإلكتروني ضئيلة مقارنة مع الجرائم الأخرى.

أما الجهة التي أسندت إليها المهمة الخاصة بإجراء المعاينة فهي الشرطة القضائية التي عليها في حال علمها بارتكاب جناية أو جنحة أن تخبر بها النيابة العامة و أن تنتقل في الحال إلى مكان ارتكاب الجريمة من أجل إجراء المعاينة كما ينبغي على الشرطة القضائية أن تحافظ على الأدلة القابلة للاندثار و التحفظ على مكان الجريمة و المحافظة على كل ما قد يوصل إلى الحقيقة [11].

[8] - عبد الفتاح مراد , شرح جرائم الكمبيوتر و الانترنت , دار الكتب والوثائق المصرية , 2005 ،ص65.
[9] - هشام محمد رستم , مرجع سابق , ص 39.
[10] - عبد الفتاح بيومي حجازي , مرجع سابق , ص 92.
[11] -محمد عادل ريان , مرجع سابق , ص 46.

وفي كل الأحوال عند تلقي بلاغ عن وقوع جريمة إحدى الجرائم الإلكترونية و التأكد من صحة الخبر و البيانات المتضمنة في الخبر، يتم الانتقال إلى مسرح الجريمة من أجل المعاينة، ومسرح الجريمة المعلوماتية يختلف عن المسرح الخاص بالجريمة التقليدية كالقتل و السرقة.

وإن كانت الجريمة واردة في كل الجرائم، إلا أن أهميتها تتضاءل في بعض الجرائم مثل جريمة التزوير المعنوي و جريمة السب فإن المعاينة فيها غير ذات جدوى، أما معاينة الجريمة التقليدية و الاطلاع على مسرح الجريمة فيها فيكون ذات أهمية متمثلة في تصور كيفية و قوع الجريمة و ظروف ملابسات ارتكابها، إلا أن إجراء المعاينة في الجريمة الإلكترونية يتقيد بعدة ضوابط أهمها[12]:

– تصوير الحاسب الآلي والأجهزة الطرفية المتصلة به، على أن يتم تسجيل وقت وتاريخ و مكان التقاطها.

– قطع التيار الكهربائي من موقع المعاينة لشل فاعلية الجاني من القيام بأي فعل من شأنه التأثير أو محو الآثار.

– إخطار الفريق الذي سيتولى المعاينة قبل موعدها بوقت كافي حتى يستعد من الناحية الفنية و العملية، و ذلك لكي يضع الخطة المناسبة لضبط أدلة الجريمة حال معاينتها.

– التحفظ على مستندات الإدخال و المخرجات الورقية للحاسب ذات صلة بالجريمة.

– عدم نقل أي مادة معلوماتية مسرح الجريمة قبل إجراء اختبار التأكد من خلو المحيط الخارجي لموقع الحاسب من أي مجال لقوى مغناطيسية يمكن أن يتسبب في محو البيانات المسجلة.

ثانيا: التفتيش

عرفت الأنظمة الجنائية في مراحل تطورها أنواعاً من الإجراءات تنطوي على انتهاك لحقوق الفرد الأولية في سبيل تتبع الجناة ومحاكمتهم ومنها القبض والتفتيش فإذا ما تخلت يد العدالة عن التعرض لحقوق الأفراد أصبحنا إزاء فوضى إجرامية.

ويعتبر التفتيش إجراء من إجراءات التحقيق، يهدف إلى البحث عن أشياء تتعلق بالجريمة، وكل ما يفيد بصفة عامة في كشف الحقيقة، سواء تعلق بالأشخاص أو بالأماكن. وللتفتيش شروط موضوعية تتعلق ب[13]:

أ– بسببه: وقوع جريمة بالفعل تعد جناية أو جنحة، وان يوجه اتهام إلى الشخص المراد تفتيشه أو تفتيش مسكنه.

ب– الغاية منه: ضبط أشياء تفيد في كشف الحقيقة.

والشروط الشكلية تتحدد بـ :

[12] - عبد الفتاح بيومي حجازي , مرجع سابق , ص 93.

[13] -منى الأشقر ، القانون والانترنت " تحدي التكيف والضبط " ، بيروت ، الناشر ش م م مصر, 2008 ,ص 70 .

أ- أن يكون الأمر بالتفتيش مسببا.

ب- حضور المتهم أو من ينيبه أو الغير أو من ينيبه التفتيش.

ج- تحرير محضر بالتفتيش.

ويثور السؤال عن إمكانية التفتيش وفقا للضوابط السابقة والغاية منه في مجال الجرائم الإلكترونية ؟ والغرض من هذا السؤال يتضح من أن التفتيش بالمعنى التقليدي يهدف إلى حفظ أشياء مادية تتعلق بالجريمة وتفيد في كشف الحقيقة، بينما البيانات الإلكترونية ليس لها بحسب جوهرها مظهر مادي ملموس في العالم الخارجي. ومع ذلك فيمكن أن يرد التفتيش على هذه البيانات غير المحسوسة عن طريق الوسائط الإلكترونية لحفظها وتخزينها كالأسطوانات والأقراص الممغنطة، ومخرجات الحاسب.

ولهذا فقد أجاز الفقه والتشريعات التي صدرت في هذا المجال إمكانية أن يكون محل لتفتيش البيانات المعالجة آليا، والمخزنة بالحاسب الآلي، ثم ضبطها والتحفظ عليها، أو ضبط الوسائط الإلكترونية التي سجلت عليها هذه البيانات .والتفتيش في هذه الحالة يخضع لما يخضع له التفتيش بمعناه التقليدي من ضوابط وأحكام. فالتفتيش أو البحث في الشبكات الإلكترونية يسمح باستخدام الوسائل الإلكترونية للبحث في أي مكان عن البيانات أو الأدِّلة المطلوبة[14].

ومحل التفتيش وما يتبعه من ضبط يشمل: البرامج أو الكيانات المنطقيةLes logiciels ، البيانات المسجلة في ذاكرة الحاسب أو في مخرجاته – السجلات المثبتة الاستخدام نظام المعالجة الآلية للبيانات – دفتر يومية التشغيل وسجل المعاملات – السجلات الخاصة بعمليات الدخول إلى نظام المعالجة الآلية للبيانات، ويتعلق بها من سجلات كلمات السر، ومفاتيح الدخول، ومفاتيح فك الشفرة. ونظرا لكون التفتيش يتضمن تقييداً للحرية الفردية ويمثل اعتداء على حرمة الحياة الخاصة فيجب أن تتوافر فيه الضمانات القانونية اللازمة لصحته ومنها أن يتم صدور أمر قضائي مسبب بشأنه وأن يباشره الشخص أو الجهة المختصة (النيابة العامة، أو الشرطة القضائية).

وبحسب الأصل يجب أن يصدر إذن التفتيش مكتوباً إلا أن هذا الشرط يحمل بعض المخاطر أحيانا وذلك في حالة ما إذا كان البحث عن أدلة الجريمة يستدعي أن يتم التفتيش في مكان آخر في نظام معلوماتي آخر غير الذي صدر بشأن الإذن المكتوب. صدر والمخاطر تتمثل في إمكانية قيام الجاني بتدمير، أو محو البيانات، أو نقلها، أو تعديلها، خلال الفترة التي يراد الحصول على إذن مكتوب بشأنها. ولمواجهة هذه المخاطر، يرى البعض أن الإذن الأول بالتفتيش في مكان ما يجب أن يتضمن الإذن بتفتيش أي نظام معلوماتي آخر يوجد في أي مكان غير مكان البحث[15].

[14] - أمير فرج يوسف ، مرجع سابق ,ص33.

[15] - سامي جلال فقي حسين , الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي, د.ط ,دار الكتب القانونية مصر, 2012,ص113.

ويثير امتداد الإذن بالتفتيش إلى أماكن أو أنظمة أخرى، غير الواردة في الإذن الأول بعض المشكلات، يتعلق أولها برفض صاحب المكان أو النظام الآخر مباشرة التفتيش لديه، يرى البعض في هذه الحالة عدم استمرار أو امتداد البحث لديه إلا في حالتي التلبس، أو رضائه بالتفتيش.

ويرى البعض أنه في حالة امتداد الاختصاص، فيمكن أن يصدر الأمر بالإمداد شفويا من قاضي التحقيق، تحقيقا للسرعة المطلوبة، ثم يصدر فيما بعد الإذن المكتوب، وفي جميع الأحوال يجب أن يكون الإذن مسببا، لتتمكن الجهة القضائية من مراقبة مدى مشروعيته[16].

وعموما فالتفتيش في الجرائم المعلوماتية يكون محله كل مكونات الحاسب الآلي سواء كانت مادية أو معنوية، و كذلك شبكات الاتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش و تشمل جميع مكوناته، ويستلزم تفتيش الحاسب الآلي مجموعة من الأشخاص لديهم الخبرة والمهارة التقنية .

ثالثا: الخبرة

الخبرة هي الوسيلة التي من خلالها تستطيع سلطة التحقيق أو المحكمة تحديد التفسير الفني للأدلة أو الدلائل بالاستعانة بالمعلومات العلمية ، فهي في حقيقتها ليست دليلا مستقلا عن الدليل القولي أو المادي وإنما هي تقييم فني لهذا الدليل. فهي في مجملها تقرير صادر عن الخبير في أمر من الأمور المتعلقة بالجريمة.

والعنصر المميز للخبرة عن غيرها من إجراءات الإثبات كالمعاينة والشهادة والتفتيش هو الرأي الفني للخبير في كشف الدلائل أو تحديد قيمتها التدليلية في الإثبات والذي يتطلب معارف علمية أو فنية خاصة لا تتوافر سواء لدى المحقق أو القاضي[17].

وإذا كان القانون قد أخذ في الاعتبار ضرورة توافر الأركان الشكلية والموضوعية في الخبرة فإن الأمر يستدعي أن يقوم القضاء بالاستعانة بخبراء مصنفين في هذا الشأن مما هو مندرج في قائمة المحكمة، وهو ما يطلق عليه نظام جدول الخبراء الذي يتميز به النظام القانوني الفرانكفوني، دون نظيره الأنجلوفوني، فحين يندب القاضي في هذا النظام خبيرا فإنه يقوم بذلك مستعينا بجدول الخبرة المعد في كل محكمة.

على إن هذا الأمر غير مقيد للقاضي، وإنما يجوز للقاضي ندب خبير من خارج الجدول، وإن كان القضاء الفرنسي يستلزم في هذه الحالة ضرورة أن يقوم القاضي بتسبيب قراره هنا وإلا ترتب البطلان على قرار ندب الخبير. أضف إن القانون يتطلب إجراءات شكلية أخرى في الخبير ينبغي توافرها كحلف الخبير اليمين ... الخ ، وهذه كلها إجراءات يترتب على مخالفتها البطلان إن لم يقم الخبير بمراعاتها.

[16] - عائشة بن قارة مصطفى , حجية الدليل الالكتروني في مجال الإثبات الجنائي , دار الجامعة الإسكندرية , 2010, ص76.
[17]- سامي جلال حسين , مرجع سابق ,ص 114.

ولكن السؤال المطروح هنا يتمثل في مدى إمكانية قيام القضاء باللجوء إلى الخبرة حين اعتراض قضائه موضوعا من موضوعات الانترنت ؟لا سيما وهو يواجه قاعدة خطرة تتمثل في حداثة موضوع العالم الافتراضي أو الرقمي ككل ، مما يعني إن ما يمكن أن يردد كنتيجة للخبرة يمكن أن يكون غير الذي سوف يتقرر مستقبلا ، ناهيك عن كونه يمكن أن يكون مثار جدل في الفترة المعاصرة. على إن مثل هذا القول لا يعفي في الحقيقة القضاء من ضرورة الاستعانة بالخبرة التقنية بحسب ما هو متاح .

إن الخبرة التقنية في مجال الانترنت والعالم الافتراضي لا تشمل بالضرورة تلك النوعية من الخبرة الدارسة، فدراسات الحاسب الآلي والانترنت لا ترتبط بمنهج دراسي أو بحثي معين أو حتى مدة زمنية يقضيها المرء دارسا في الجامعات والمعاهد المتخصصة، وإنما ترتبط بمهارات خاصة وبموهبة استعمال الحاسوب والانترنت والتعامل مع تقنية المعلومات، إذ إن أمهر مبرمجي نظم التشغيل حتى الآن مثل Bill Gatesلم يكن تحصيله العلمي يتجاوز المرحلة الثانوية، وذات الأمر ينطبق على عتاة الهاكرز ومخترقي الأنظمة فإن أعمارهم لا تتجاوز مرحلة التعلم الثانوي والسنوات الجامعية الأولى في أحسن الأحوال[18].

ومن هذا المنطلق تتميز الخبرة في مجال تكنولوجيا المعلومات عن الخبرة في أي فرع آخر من الفروع التي يمكن أن تكون محلا للخبرة أمام القضاء. وللخبرة في المجال التقني أنواع أهمها [19]:

1 –الخبرة الخاصة: وهذه تعد أقوى أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنظمات الخاصة. وهي تضم في جنباتها الخبرة الفردية التي تعد أقوى وأهم مظاهر الخبرة السائدة في مجال تكنولوجيا المعلومات/الانترنت، ويكفي هنا أن نذكر إن المؤسسات الكبرى المتخصصة في الحاسب الآلي والانترنت تسعى بكل جهودها إلى الاستعانة العقدية بأشخاص اثبتوا كفاءاتهم في مجال الحاسوب الانترنت. حتى عصاة القانون منهم فهناك اتجاه اقتصادي يحاول جاهدا إثبات عدم جدوى التخلص من هؤلاء بمعاقبتهم وفقا للقانون، وإنما يلزم اللجوء إلى الحلول الاقتصادية لكي يمكن أن يظلوا عاملين في إطار الأهداف الاقتصادية ، بل إن من الدول ما تسعى جاهدة إلى محاولة التعرف على قراصنة تحولوا مع مرور الوقت إلى رموز وطنية جراء تحركاتهم عبر الانترنت.

2 –المؤسسات التعليمية: لما كانت الانترنت تعد أحد منتجات العلم في حركته التقنية ، فإنه يمكن القول وبحق إن أقوى مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة في العالم الافتراضي يمكن أن تكون من خلال المؤسسات التعليمية، فهذه الأخيرة تعد مصدر دعم متكامل لمؤسسات الدولة ككل , وهذه المؤسسات تعتمد منهج علمي غير تجاري هدفها بالتأكيد تطوير العلم ليقضي على المشكلات التي تواجه البشرية، كما إن التفكير العلمي لا يمكن تجنبه في رصده للظاهرة الإنسانية.

---

[18] – عائشة بن قارة مصطفى , مرجع سابق , ص 78.

[19] – سامي جلال حسين , مرجع سابق ,ص 115.

ولقد قامت عدة مؤسسات تعليمية بتكوين قاعدة خبرة كبيرة فيها لتكون على أهبة الاستعداد لمواجهة الجريمة عبر الانترنت ، ومن ذلك دراسات الحاسب الآلي التي تتطور بشكل فائق في جامعة ستانفورد، كذلك معهد التكنولوجيا في ماساشوستس الذي قدم للبشرية خبراء على درجة عالية من التفوق.

3 –جهات الضبط القضائي: شرعت بعض الدول في إعداد أجهزة متخصصة للخبرة في الإجرام عبر الانترنت. وعلى رأس تلك الدول الولايات المتحدة التي تجاوز نشاطها في هذا المجال الإطار الدولي الممثل في منظمة الإنتربول. وكان آخر نشاط مؤسسي في هذا الإطار هو ذلك الفرع الجديد الذي تأسس في المباحث الفيدرالية الأمريكية FBI أطلق عليه المعمل الإقليمي الشرعي للحاسوب.

أساليب عمل الخبير التقني:

للخبير التقني في سبيل تحري الحقيقة أن يقوم بكل ما يمكنه من التوصل إليها . وهو في إطار القيام بعمله عليه أن يستخدم الأساليب العلمية التي يقوم عليها تخصصه وليس للمحكمة أن ترفض تلك الأساليب ما لم يكن رفضها لها مسببا بشكل منطقي وإلا تعرض حكمها للنقض. وهناك أسلوبان لعمل الخبير التقني[20]:

الأول: القيام بتجميع وتحصيل لمجموعة المواقع التي تشكل جريمة في ذاتها ،كما هو الشأن في التهديد Intimidationأو النصبFraudأو السبDefamationأو جرائم النسخ Infringement of copyrights وبث صور فاضحة بقصد الدعاية للتحريض على ارتكاب جرائم الدعارة والرقيق الأبيض ودعارة الأطفال وغيرها. ثم القيام بعملية تحليل رقمي لها لمعرفة كيفية إعدادها البرمجي ونسبتها إلى مسارها الذي أُعدت فيه، وتحديد عناصر حركتها ، وكيف تم التوصل إلى معرفتها ، ومن ثم التوصل في النهاية إلى معرفة بروتوكول الانترنت IP الذي ينسب إلى جهاز الحاسوب الذي صدر عنه هذه المواقع.

الثاني: القيام بتجميع وتحصيل لمجموعة المواقع التي لا يشكل موضوعها جريمة في ذاته، وإنما تؤدي حال تتبع موضوعها إلى قيام الأفراد بارتكاب جرائم . كما هو الحال في المواقع التي تساعد الغير على التعرف على جرعات المخدرات والمؤثرات العقلية التي تناسب وزن الإنسان بادعاء أنه إذا تم تتبع التعليمات الواردة فيها فلن يصاب الشخص بحالة إدمان، وأيضا كيفية زراعة المخدرات بعيدا عن أعين الغير (ويطلق عليه في هذه الحالة الفضولي) وأيضا كيفية أعداد القنابل وتخزينها، وكيفية التعامل مع القنابل الزمنية وتركيبها والقيام بفكها وحفظها ، وكذلك القيام بتحديد مسار الدخول على مواقع دعارة من أماكن متفرقة دون لزوم القيام بالدخول من مكان ثابت، ومثل هذا الأمر جائز الحدوث كما لو كان مرتكب الجريمة مشتركا لدى مزود في مدينة مختلفة عن تلك التي يقيم فيها ويقوم بالولوج إلى الانترنت من محل أقامته .

[20] - مني الأشقر , مرجع سابق , ص 78.

كذلك يحق للخبير أن يطلع على شهادات وأقوال الجناة في الصحف وأمام الجهات الرسمية والشعبية، إذ أن كثيرا ما يكون في مثل هذه الأقوال عوامل مساعدة لخبرته، فيمكن من خلالها التعرف على أسلوب عمل مرتكب الجريمة المعلوماتية والتعامل معه على أساس أقواله، ومعلوم إن الكونجرس الأمريكي قد استدعى أحد كبار هكرة العالم الافتراضي، بل أخطرهم على الإطلاق، وهو "كيفين ميتنيك"، لكي يدلي بشهادته كهاكر عن كيفية ارتكابه للاختراق ورأيه في إعداد تشريع يحظر الاختراق. ولقد تضمنت شهادته العديد من الأمور التي كانت خافية على رجال التشريع والقانون[21].

رابعا :الشهادة

يقصد بالشهادة بأنها: "تقرير الشخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بالحواس ويقصد بالشاهد في جرائم المعلوماتية بأنه الشخص الفني صاحب الخبرة المعلوماتية و التخصص في تقنية وعلوم الحاسب الآلي و شبكاته، و يطلق على هذا النوع من الشهود مصطلح الشاهد المعلوماتي "témoin informatique le" تمييزا له عن الشاهد التقليدي . ويشمل الشاهد في الجرائم المعلوماتية عدة طوائف أهمها [22]:

1- القائم على تشغيل الحاسب الآلي : و هو المسئول عن تشغيل الحاسب الآلي و المعدات المتصلة به و يجب أن تكون لديه الخبرة الكبيرة في استخدام الجهاز ،كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج.

2 – المبرمجون: و هم الأشخاص الذين يأخذون على عاتقهم كتابة البرامج، وينقسمون إلى فئتين:
*الفئة الأولى: هم مخططو البرامج التطبيقية و يقومون بالحصول على خصائص النظام المطلوب.
*الفئة الثانية: وهم مخططو برامج النظم و يقومون باختيار و تعديل و تصحيح برامج النظام الحاسب الداخلية و إدخال أي تعديلات أو إضافات لها.

3- مهندسو الصيانة و الاتصالات: و هم المسئولون عن أعمال الصيانة الخاصة بتقنيات الحاسب و بمكوناته و شبكات الاتصال المتعلقة به.

4- المحللون : وهم الأشخاص الذين تأتي على عاتقهم مهمة التحليل الخاصة ببيانات نظام معين إلى وحدات مفصلة و استنتاج العلاقة الوظيفية منها، كما يقومون كذلك بتتبع البيانات داخل النظام عن طريق ما يسمى بمخطط تدفق البيانات و استنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب الآلي.

5- مديرو النظم: وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية.

6- طاقم عمليات البيانات :الذي يعد البيانات بالصورة التي يستطيع الكمبيوتر قراءتها (شريط أو اسطوانة).

[21] - عائشة بن قارة مصطفى , مرجع سابق , ص 80.
[22] - سامي جلال حسين , مرجع سابق ,ص 118.

7- مهندس الصيانة الإلكترونية: الذي يقوم على صيانة الجهاز الأصلي والتأكد من عمله بصورة صحيحة.

يتعين على الشاهد المعلوماتي أن يقدم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في نظام المعالجة الآلية للبيانات سعيا عن أدلة الجريمة بداخله، والسؤال الذي يطرح نفسه هل يلتزم الشاهد بطبع الملفات والإفصاح عن كلمات المرور والشفرات؟ هناك اتجاهان في هذا الصدد:

الاتجاه الأول: ويرى أنه ليس من واجب الشاهد وفقا للالتزامات التقليدية للشهادة أن يقوم بطبع ملف البيانات أو الإفصاح عن كلمة المرور أو الشفرات الخاصة بالبرامج المختلفة ويميل إلى هذا الاتجاه الفقه الألماني حيث يرى عدم التزام الشاهد بطبع البيانات المخزنة في ذاكرة الحاسب على أساس أن الالتزام بأداء الشهادة لا يتضمن هذا الواجب , وكذلك لا يجوز في تركيا إكراه الشاهد لحمله على الإفصاح عن كلمات المرور السرية أو كشف شفرات تشغيل البرامج المختلفة[23].

الاتجاه الثاني: ويرى أنصار هذا الاتجاه أن من بين الالتزامات التي يتحمل بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة حيث يرى اتجاه في الفقه الفرنسي أن القواعد العامة في مجال الإجراءات تحتفظ بسلطانها في مجال الإجراءات المعلوماتية ومن ثم يتعين على الشهود من حيث المبدأ الالتزام بتقديم شهادتهم (المواد 62، 109، 138 من قانون الإجراءات الجنائية الفرنسية) ومن ثم يجب عليهم الإفصاح عن كلمات المرور السرية التي يعلمونها، ولكن رفض إعطاء المعلومات المطلوبة غير معاقب عليه جنائيا إلا في مرحلة التحقيق والمحاكمة[24] .

الخاتمة

ختاما يكمن القول أن تسارع إيقاع التقدم التكنولوجي والتقني الهائل ، وظهور الفضاء الإلكتروني ووسائل الاتصالات الحديثة كالفاكس والإنترنيت وسائر صور الاتصال الإلكتروني عبر الأقمار الصناعية كانوا وسيلة استغلها مرتكبو الجرائم الإلكترونية، في تنفيذ جرائمهم التي لم تعد تقتصر على إقليم دولة واحدة، بل تجاوزت حدود الدول ، وهي جرائم مبتكرة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية.

ومن حيث ما يرتبط بهشاشة نظام الملاحقة الإجرائية التي تبدو قاصرة على استيعاب هذه الظاهرة الإجرامية الجديدة، سواء على صعيد الملاحقة الجنائية في إطار القوانين الوطنية أم على صعيد الملاحقة الجنائية الدولية، مما أوجب تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة علي المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة، بما يضمن في الأحوال كافة

[23] - أمير فرج يوسف ، مرجع سابق ,ص41.
[24] - محمد عادل ريان , مرجع سابق , ص 58.

احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى ، وتتكامل فيه في الدور والهدف مع المعاهدات الدولية.

النتائج :

هناك العديد من النتائج التي توصلت إليها الدراسة ,علما أن ماتم التوصل إليه من نتائج الآن ربما يتغير مستقبلا بحكم طبيعة الجريمة الالكترونية المرتبطة بالتقنية التي تتطور بشكل كبير, والنتائج هي :

1- يعد الإثبات من أهم التحديات التي تواجه الأجهزة الأمنية ويزداد الإثبات صعوبة في الجرائم المعلوماتية , وفي حال اكتشاف وقوع هذه الجريمة والإبلاغ عنها فان إثباتها أمر يحيط به الكثير من الصعاب , مما يستلزم الكثير من الجهد والخبرة الفنية.

2- تواجه طرق التحقيق في إثبات الجريمة الالكترونية صعوبات متعددة ,حيث تستدعي في المقام الأول اكتشاف الجريمة الالكترونية ومحلها وبيئتها ثم الإبلاغ عنها ,واخذ إذن الجهات المختصة قبل القيام بالمعاينات والتفتيش للمواقع , ودلك للبحث عن الدليل الرقمي الالكتروني بالطرق الفنية .

3- تمثل الشهادة أهمية كبيرة في إثبات الجريمة الالكترونية في المواد الجزائية فهي ترد على وقائع مادية وترشد القاضي إلى تحري قيمتها , حيث يكون للشهادة أثناء التحقيق اثر كبير فيما يتعلق بالبراءة والإدانة , كما لها أهميتها في الكشف عن الأدلة التي تساعد على إثبات الجريمة الالكترونية.

4-لم تنص اغلب التشريعات والقوانين على الدليل الالكتروني أو الرقمي ومنهم المشرع الجزائري ,الذي بدوره لم ينص على الدليل الالكتروني في قوانينه, علما انه يعتبر المساهم الأول في سبيل مواجهة الجرائم الالكترونية ,وهدا يعتبر قصورا من طرف مختلف التشريعات والقوانين.

التوصيات :

على ضوء هده النتائج المتوصل إليها يمكن وضع جملة من التوصيات أهمها :

1- فيما يتعلق بمعاينة الجريمة الالكترونية ,فيجب تحديد أجهزة الحاسب الآلي الموجودة في مكان المعاينة وتحديد موقعها بأسرع وقت ممكن ,وفي حالة وجود شبكة اتصالات يجب البحث عن خادم الملفات بهدف تعطيل الاتصالات لمنع تخريب الأدلة المتحصل عليها ,مع تصوير الأجهزة الموجودة و خاصة الأجهزة الخلفية

2- على الدولة أن تعمل على تبني جهازاً خاصاً للخبرة الجنائية للجريمة المعلوماتية ، يتكون أعضاؤه من فريق متخصص فنياً في التقنية المعلوماتية ، على أن يتم إعادة النظر في القواعد التقليدية للخبرة ، لأن إثبات الجريمة المعلوماتية يتطلب قواعد خاصة للتعامل مع الأدلة في هذه الجرائم ، لأن البحث عنها يتم داخل نظام اليكتروني معقد ، يسهل فيه محو الأدلة إذا ما تم التعامل الأولي مع الجهاز بشكل خاطئ.

3- يجب فحص كل ما تحويه سلة المهملات في الجهاز ورفع البصمات التي قد تكون لها دلالة على مرتكب الجريمة ,بالإضافة إلى ضرورة القيام بحفظ كل المستندات الخاصة بالإدخال والإخراج والتي قد تكون على صلة بالجريمة .

4- أهمية التنسيق المستمر بين الجهات القضائية والأمنية من جهة والجهات ذات العلاقة بالتكنولوجيا من جهة أخرى لمسايرة ما يستجد في هدا المجال .

5- ضرورة النص صراحة على الأدلة الالكترونية كأدلة إثبات في المجال الجنائي والاعتراف لها بحجية قاطعة وكذلك النص على وسائل التأكد من سلامة الدليل الالكتروني التي تعتبر شرطا لقبوله .

المراجع:

1- أمير فرج يوسف ، الجرائم المعلوماتية على شبكة الإنترنت ، دار المطبوعات الجامعية الإسكندرية ، 2009.

2-عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر والانترنت ، دار الكتب القانونية مصر 2006 .

3- هشام محمد رستم , الجوانب الإجرائية للجرائم المعلوماتية, مكتبة الآلات الحديثة. أسيوط مصر 1999.

4- عبد الفتاح مراد , شرح جرائم الكمبيوتر و الانترنت , دار الكتب والوثائق المصرية , 2005.

5- محمد عادل ريان ، جرائم الحاسب الآلي وأمن البيانات، بيروت،2002.

6- منى الأشقر ، القانون والانترنت " تحدي التكيف والضبط " ، بيروت ، الناشر ش م م, مصر, 2011.

7- سامي جلال فقي حسين , الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي, د.ط ,دار الكتب القانونية مصر, 2012 .

8 - عائشة بن قارة مصطفى , حجية الدليل الالكتروني في مجال الإثبات الجنائي , دار الجامعة الإسكندرية , 2013.