التنظيم القانوني للجريمة المعلوماتية

أدلة إثبات الجريمة المعلوماتية

سحتوت نادية.

أستاذة جامعية .

الرتبة : ماجستير .

المؤسسة : المركز الجامعي سوق أهراس

المقدمـــة

رغم إيجابيات الحاسب الآلي و الشبكة المعلوماتية الدولية إلا أنه تولدت عنهما العديد من الأنماط السلبية أذكر منها الجريمة المعلوماتية ، حيث تنوعت أساليب ارتكابها و تزايدت مخاطرها و حجم الخسائر الناتجة عنها فباتت تشكل مصدرا من مصادر تهديد الاقتصاد و الأمن القومي ومساسا بحرمة الحياة الخاصة وكذا النظام والآداب العامة ، ومع ذلك فالتشريعات العربية لم تتطرق لها إلا فيما ندر، و عليه ولتصدي لهذا النوع المستحدث من الجرائم لابد من الخوض فيها من كافة جوانبها. و قد اقتصرنا نحن على الجانب الأكثر قيمة وأهمية فيها و هو دليل إثباتها إذ به تثبت الإدانة أو البراءة، كما ان هذا الدليل يختلف تماما عن الدليل الجنائي في الجرائم التقليدية و ذلك من حيث طبيعته الخاصة ، المتمثلة في الكم الهائل من البيانات المدونة في جهاز الحاسب الآلي لذلك حددنا كيفية البحث و الكشف عن الدليل وكذا حمايته للوصول إلى الهدف الأسمى وهو القبض على مرتكبها .

ومن هنا يمكن طرح الإشكالية التالية : إلى أي مدى يمكن تطبيق القواعد المنظمة لأدلة الإثبات الجريمة التقليدية وإجراءات التحري عنه على الجريمة المعلوماتية ؟

و للإجابة على هذه الإشكالية اعتمدنا خطة ثنائية المباحث .

المبحث الأول : مفهوم أدلة إثبات الجريمة المعلوماتية.

المطلب الأول : تعريف ادلة الإثبات .

المطلب الثاني :مصادر أدلة الإثبات .

المبحث الثاني : صعوبات اثبات الجريمة المعلوماتية .

المطلب الأول : صعوبات متعلقة بالدليل ذاته .

المطلب الثاني : صعوبات التحري عنه .

المبحث الأول : مفهوم أدلة إثبات الجريمة المعلوماتية : سنتعرض لهذا المفهوم في مطلبين المطلب الأول ونحدد تعريف أدلة الإثبات أما المبحث الثاني فنتطرق إلى مصادر أدلة الإثبات.

المطلب الأول : تعريف أدلة الإثبات : هو معنى يدرك من مضمون واقعة تؤدي إلى ثبوت الإدانة أو ثبوت البراءة ويتم ذلك باستخدام الأسلوب العقلي واعمال المنطق في وزن وتقدير تلك الواقعة ليصبح المعنى المستمد منها أكثر دقة في الدلالة على الإدانة أو البراءة([1]1).

المطلب الثاني : مصادر أدلة الإثبات : و تتمثل في مصادر مادية تدرك بالحواس حيث يجب أن يتسم هذا الأخير بالوضوح والتحديد والا صار تقديريا و مصادر معنوية :

1-المصادر المادية: وهي كمايلي:

1-1- الأوراق : أجهزة الحاسب الآلي والطابعات تخلق في وقت قصير الكثير من الأوراق وهي من الأدلة التي يجب الاهتمام والاعتناء بها عند معاينة لمسرح الجريمة ومن هذه الأوراق :

أ – أوراق تحضيرية يتم إعدادها بخط اليد كمسودة تصوير العملية التي يتم برمجتها .

ب– أوراق تالفة تم طباعتها للتأكد من تمام الجريمة تلقى في سلة المهملات .

ج– أوراق أصلية تطبع ويتم الاحتفاظ بها كمرجع أو لأغراض الجريمة .

د – أوراق أساسية وقانونية محفوظة في الملفات العادية ولها علاقة بالجريمة المعلومات خاصة عند تقليد وتزوير هذه الأوراق بواسطة الحاسب الآلي.

1-2 – جهاز الحاسب الآلي وملحقاته :

لكي تعتبر الجريمة معلوماتية لابد من وجود جهاز حاسب آلي فكلما كانت هذه الأجهزة أكثر قدرة وسرعة في معالجة البيانات ، وكذلك الدقة العالية في الحصول على النتائج و القدرة على حل المسائل والعمليات المعقدة ، فان دورها في مساعدة المجرم المعلوماتي يتعاظم.

وجهاز الحاسب الآلي يتكون من المكونات المادية التي تعتبر من ماديات و قرائن لإثبات الجريمة المعلوماتية التي ينبغي البحث عنها و فحصها و الاستفادة منها في التحقيق من أجل إثبات الإدانة أو البراءة (1) ، و هذه المكونات هي :

أ –**وحدات الذاكرة الرئيسية :** Main Memory وهي الوحدة التي تقوم بحفظ البيانات والنتائج بشكل مؤقت وتقاس بالوحدات التالية : بت BIT وهي أصغر وحدة قياس ، بايت

[1][1] -Robert, W. Fergusson and Allan , H. Stokke. Legal espects of evidence, Harcourt Barce jovanorich : / NC New York 1941 P1

Byte وهي تساوي 18 Bit ، كيلوبايت وهو يساوي 1024 Byte . وحدة حساب المنطق

Arithmatic logic Unit ALU. وحدات التحكم Control Unite Cu.

ب: وحدات التخزين : تعتبر من الأجزاء المهمة جدا الارتكاب الجريمة المعلوماتية إذ باقتحام الملفات المخزنة يمكن الحصول على ما يريد من بيانات أو تخريب و تدمير هذه المعلومات أو تزييفها وتزويرها

ومن الأجزاء التي تستخدم لتخزين المعلومات :

* الأقراص الصلبة : Hard desks تكون عادة مركبة داخل حافظة الجهاز لكبر حجمها وهي تتسم بكفاءة عالية و حجم التخزين الكبير .

* الأقراص المرنة : FLappy disks حجمها التخزيني قليل وتحفظ في مكان بعيد وآمن كخزائن البنوك التجارية .

* أقراص الليزر : CD Rom تمتاز بسعة تخزين عالية ولكن لم تصل بعد لسعة التخزين للقرص الصلب أو سرعته فهي تعتبر الدليل اللازم لاثبات الجريمة الالكترونية طالما كانت محتوياتها

عنصرا من عناصر الجريمة (1)

1- د/ محمد الأمين البشري ،بحث بعنوان " التحقيق في جرائم الحاسب الآلي " مقدم إلى مؤتمر القانون والكومبيوتر والانترنت "المنعقد في الفترة من 1إلى 3 ماي 2000 بكلية الشريعة والقانون بدولة الإمارات، ص 6 .

* الذاكرة المضيئة : FM Flacher Memory قطعة صماء تشبه تماما القرص الصلب و سعته في التخزين تقترب إلى ما هو مدون بالفعل في القرص .

* المودم : وهو الوسيلة التي تمكن أجهزة الحاسب من الاتصال ببعضها البعض عبر خطوط الهاتف وقد تطورت المودم لتكون أجهزة استقبال و إرسال فاكس والرد على المكالمات الهاتفية وتبادل البيانات وتعديلها .

* الكروت أو البطاقات PCMCIA cards: وهذه البطاقات تستعمل في أجهزة الحاسب الآلي

الصغيرة ومن أنواعها (النوت بوك) و (اللاب توب) وهي تشبه البطاقات الانتمائية

*البطاقات الممغنطة : و بطاقات الإئتمان القديمة و المواد البلاستيكية المستعملة في إعداد البطاقات

-المصادر المعنوية : (2) لا بد من أسلوب علمي للكشف عن البرامج المعدة لإتلاف برامج الحاسب الآلي التي تعتبر من أدلة إثبات الإدانة ، و تتمثل برامج التدمير في :

1- د- محمد أمين البشري ، المقال السابق ص 35

2- المصادر المعنوية : وهي معلومات الدخول و الإشتراك و النفاذ و البرمجيات و قد أثارت أمام القضاء إشكالا ت من حيث مدى قبولها و

حجيتها .أنظر لتفصيل أكثر :

-عياد سامي على حامد ، الجريمة المعلوماتية و إجرام الإنترنت ، دار الفكر الجامعي ، الإسكندرية ، سنة2007 ، ص 102.

1-1-- الفيروسات : (1) من أبرز هذه الفيروسات "حصان طروادة "و هو يتمتع بقدرة فائقة على الاختفاء داخل البرنامج الأصلي بحيث يؤدي إلى تعديل ، تغيير ومحو المعلومات ، كذلك فيروس "مايكل أنجلو "الذي تم ابتكاره في 1992/3/6فهذا الفيروس ينشط في هذا اليوم من كل سنة. أيضا" فيروس الكر يساس"الذي ينشر عبر البريد الإلكتروني فبعد أن يتمثل للقارئ بطاقة تهنئة بمناسبة العيد في خلال هذا الوقت يقرا الملفات التي تحتوي على عناوين المشتركين في الشبكة، و يرسل نسخا من نفسه إلى هؤلاء مما يترتب عليه توقف النظام حتى يتم القضاء عليه .

1-2-برامج الدودة : وهي عبارة عن برامج تستغل أية فجوة في نظم التشغيل كي تنتقل من حاسب إلى آخر و من شبكة إلى أخرى عبر الوصلات التي تربط بينها و تتكاثر أثناء عملية إنتقالها .

1-3-القنابل المنطقية أو الزمنية : القنابل المنطقية: هي برنامج أو جزء من البرنامج ينفذ في لحظة محددة أو في فترة زمنية منتظمة يوضع على شبكة المعلومات بهدف تحديد الظروف أو حالة فجوى النظام بغرض تسهيل عمل غير مشروع .

القنبلة الزمنية (2) : هي التي تثير حدثا في لحظة زمنية محددة بالساعة و اليوم و السنة، كانفجار القنبلة الإلكترونية التي استهدفت نظام البريد الإلكتروني للجامعة التي ترتبط به أعمال على درجة من الأهمية كالتسجيل و تبادل الأبحاث ، حيث تمكن فريق تحقيق من تحديد اليوم و الساعة وعنوان الكمبيوتر المستخدم في الجريمة .

1-فادي سالم ، هجمات الفيروسات اسلحة المستقبل المصوبة نحو الإنترنت ، مقال منشور في مجلة الإنترنت العالم العربي ، السنة الثالثة ، العدد التاسع ، سنة 2000 ، ص 56.

2-عبابنة محمود أحمد ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة لنشر و التوزيع ، سنة 2005، ص 104.

المبحث الثاني : صعوبات إثبات الجريمة المعلوماتية تعترض سلطة جمع الاستدلالات و التحقيق صعوبات بالنسبة للدليل ذاته و كذا إجراءات التحري لذا سنتعرض لكل منهما من خلال المطلبين التاليين :

المطلب الأول : صعوبات تتعلق بالدليل ذاته : وهي على النحو التالي :

1- عدم ظهور الدليل المادي :

يمكن للجاني عن طريق نبضات الكترونية لاترى العبث في بيانات الحاسب أو برامجه (1) في وقت قياسي وهذه البيانات التي يتم العبث بها يمكن محوها كذلك في وقت قياسي قبل أن تصل إلى يد العدالة . فالجريمة المعلوماتية عكس الجرائم العادية الأخرى تتم دون رؤية لدليل الإدانة وحتى في حالة وجود

الدليل يمكن للجاني محو الدليل وفي حضور أجهزة العدالة غير المختصة بعد تنفيذه للجريمة ، ولذلك

فغالبية الجرائم المعلوماتية تكشف مصادفة وليس بطريقة الإبلاغ عنها (2) .

فقد دلت دراسة ميدانية قامت بها إدارة الصحة وخدمات الإنسان بالولايات المتحدة عام 1983 أن

الحوادث المصادفة مثل (الشكوى – الفضول – الانتقام من المبلغ ضده أو النشاط غير العادي للجناة

شكلت نسبة 49% كعوامل ساعدت في كشف الاحتيال(3) أما الرقابة الداخلية والخارجية فكان لها ذات الأثر بنسبة 26%. و من بين بعض أنواع الجرائم التي يختفي فيها الدليل أذكر على سبيل المثال :

– اختلاس المال مثلا عن طريق الجريمة المعلوماتية: قد يكون أساس النشاط الإجرامي هو

1- حاول بعض الفقهاء التمييز بين المعلومات و بين البيانات المعالجة إلكترونيا. حيث ينفون الطابع المادي للصنف الأول و يؤكدون عليه للثانية، تأسيسا على أن هذه الأخيرة عبارة عن :"نبضات أو دبدبات إلكترونية و إشارات و موجات كهرومغناطيسية قابلة لأن تخزن على وسائط معينة و يمكن قياسها وبالتالي يجوز إخضاعها للقواعد التقليدية للقانون الإجراءات الجزائية .أنظر بتفصيل أكثر :

- درقاوي عبد القادر ، جريمة السرقة في عصر المعلوماتية ، مذكرة لنيل شهادة الماجستير في القانون الخاص ،جامعة أبي بكر بلقايد تلمسان ،
سنة 2004 ، ص 174.

2- في دراسة مسحية تمت من فبل لجنة تدعى " لجنة التدقيق في أنجلترا شملت 6000 من المؤسسات تبين أن ما يقارب نصف حالات الاحتيال اكتشفت مصادفة- لتفصيل أكثر أنظر :

- د/ هشام محمد فريد رستم : الجرائم المعلوماتية أصول التحقيق الجنائي الفني و إقتراح بإنشاء آلية عربية موحدة للتدريس التخصص ، بحث مقدم إلى مؤتمر القانون والكومبيوتر والإنترنت)المنعقد في الفترة من 1-3 ماي 2000 بكلية الشريعة والقانون بدولة الامارات، ص 23 . أيضا :

-Harold Goseph Highland " The hidden dangers of Fraud " Abstracts of revent articles and literature ; computer; securty ; vol 10 no 4 juin

3- د/ البشري محمد الأمين ، مقال سابق ، ص 38.

أيضا -د/ هشام محمد فريد رستم ، المرجع السابق ، ص 24.

التلاعب في نظام الحاسب الآلي ويتم ستر وإخفاء الدليل عن طريق العبث ببيانات النهائية التي تخرج من الجهاز و ذلك بمعالجته في نظام الحاسب ذاته(1) .

- وقد ترتكب السرقة عن طريق التجسس على ملفات البيانات و اختراقها كما هو الحال في ايطاليا

حيث حاول الجناة سرقة معلومات وبيانات وذلك باختراق نبضات الكترونية عبر ألياف بصرية تنتقل ما بين البنك وأجهزة السحب الآلي للنقود(2) .

يقسم المجرمون بحسب خفاء الدليل إلى :

- **المخادعون :** لديهم مقدرة عالية على إخفاء دليل الجريمة المعلوماتية وتنصب جرائمهم على

شبكات تحويل الأموال والتلاعب في حسابات المصارف (3).

- **الجواسيس** : وهؤلاء يسعون إلى جمع المعلومات لمصلحة دولهم أو لمصلحة بعض الأشخاص أو

الشركات التي تتنافس فيما بينهم فهم لديهم مقدرة فائقة على طمس الأدلة (4) .

1- فيما يخص الاختلاس أذكر بعض الأمثلة و هي :

- الموظف المسؤول عن ادخال بيانات العمل الاضافي .

– المحاسب الذي يتولى التدقيق والمراجعة لشركة شحن فاكهة وخضروات حيث أختلق 17شركة وهمية لتفصيل أكثر أنظر :

– د/ البشري محمد الأمين، المقال السابق، ص 39 . أيضا :

–Adrian ; R.D. Norman . Computer insecuritry, charman and hall U.S P74-75

2– د/ عبد الفتاح حجازي ، الاثبات الجنائي في جرائم الكومبيوتر والأنترنت . دار الكتب القانونية مصر 2007 ص 113.

ص30-3– د/ هشام محمد فريد رستم ، المرجع السابق

–أيضا : عيادسامي علي حامد : المرجع السابق : ص 101

4– القاضي / عالكوم وليد ' بحث بعنوان مفهوم ظاهرة الاجرام المعلوماتي ، مؤتمر القانون والكومبيوتر والأنترنت ، المقال السابق ،
ص 4 وما بعدها

<u>فقدان الآثار التقليدية للجريمة</u> : الجرائم المعلوماتية ليست كالجرائم التقليدية فهي لا تخلف آثارا مادية 2-و يرجع السبب في إفتقاد الآثار التقليدية حسب ما لاحظه جانب من الفقه ، من أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسب الآلي دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها كما لو كان البرنامج معدا و مخزنا على جهاز الكمبيوتر، و يمكن هنا إقتراف بعض أ نواع الجرائم كالإختلاس و التزوير، و ذلك بإدخال بيانات غير مطلوبة و غير معتمدة في نظام الحاسب الآلي أو تعديل البرنامج المخزن في جهاز الكومبيوتر و تكون النتيجة مخرجات على هوى مستعمل الجهاز دون إستخدام وثائق أو مستندات ورقية، و بالتالي تفقد الجريمة آثارها التقليدية (1)، كذلك من الأسباب التي تساهم في تعذر الحصول على آثار تقليدية تتمثل في كون الجاني بنفسه يملك محو الأدلة التي تدينه أو تدميرها في زمن قصير جدا ، و حتى لو تم ضبطه فقد يرجع هذه الجريمة إلى خطء في نظام الحاسب أو الشبكة (2) .

و يتعين عند البحث عن آثار الجريمة المعلوماتية و أدلتها لا بد ان توجه التحريات إلى دائرة المتعاملين في نطاق المؤسسة التي وقعت بها الجريمة سواء أكانوا موظفين أو متعاملين معها، و ذلك

برصد حركة المعاملات التجارية و مراقبة المشبوهين داخل المؤسسات المالية و حولها ، و يتعين على

رجال الأمن جمع المعلومات السرية عن حركة السوق و تداول الأموال و الممتلكات و التغيرات

2- للتوضيح أكثر أنظر بعض الحالات التي حدثت في النمسا و ألمانيا الإتحادية و الإمارات العربية المتحدة حول قدرة مجرمي المعلوماتية
على تدمير البيانات و محوها و المذكورة في المرجع التالي :
د/ هشام محمد فريد رستم ، مرجع السابق ،ص 35 وما بعدها .

الاجتماعية و السلوكية للموظفين و صغار رجال الأعمال الذين هم على مقربة من أسرار برامج
الحاسب الآلى(1)

3 – تعذر الحصول على الأدلة بسبب طريقة الحماية الفنية و القانونية و آثار ذلك إجرائيا : على الرغم من قيام الجهات ذات الأنظمة المعلوماتية بحماية نظمها عن طريق الترميز و التشفير (2)فإن قراصنة الحاسب الآلي و العاملين في ذات المؤسسات يستطيعون اختراق هذه الأنظمة، و من ثم يجعلون حمايتها عديمة الجدوى ، و ليست الأمور تقف عند هذا الحد بل إن هؤلاء يقومون بفرض تدابير أمنية لمنع التفتيش المتوقع بحثا عن أدلة إدانتهم و ذلك باستخدام كلمات سر حول مواقعهم، تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة الإطلاع على أي دليل يخلفه نشاطهم الإجرامي. كذلك إستخلاص الدليل العلمي في الجريمة المعلوماتية هو من المسائل الفنية التي يقوم بها الخبير (3) وهو يخضع لوزن و تقدير القاضي في ضوء الأدلة التي قدمت في الدعوى ، و هناك من إعتبر الوسائل العلمية في أغلب حالاتها ليست دليلا مستقلا في ذاته و إنما هي قرائن يتم دراستها و إستخلاص دلالتها و هذا القول يؤدي إلى إفلات المجرم المعلوماتي من العقاب. لذاعلى المشرع التحرر من القواعد التقليدية شرط عدم المساس بالحقوق الدستورية و مبدأ المشروعية .

-Tappolet ,la Fraude informatique ,rec .int .crim .poltech .19FF,p 351. 1

2-في التجارة الإلكترونية يتم إستخدام أسلوب التشفير و التحقيق من شخصية المتعاقد
-ففيما يتعلق بالشفرة : فهي متفق عليها بين الطرفين و يعرف كلاهما مفتاح الشفرة لضمان عدم قراءة الرسالة إلا لمن هو مصرح له بذلك .

-أما التحقيق من شخصيه المتعاقدين فيتم عن طريق إستخدام شفرة المفتاح العام حيث يمكن للطرفين المتعاقدين أن يوقعا على المستندات بطريقة

رقمية و يتأكد كل طرف من توقيع الطرف الآخر بإستخدام المفتاح العام للشفرة

أنظر بتفصيلا أكثر :

د/ حجازي سهير ،التهديدات الإجرامية للتجارة الإلكترونية ،بحث مختصر لدى مركز البحوث و الدراسات بإدارة الشرطة

بدبي ،الإمارات العربية المتحدة ، عدد9 جويلية 1999،ص 3عمود 2

د/محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، دار النهضة العربية ، 1988، ص 475-3

<u>المطلب الثاني</u> : <u>صعوبات التحري عنه</u> : جمع الأدلة عن طريق المعاينة و التفتيش يطرح العديد من الصعوبات و لذا سنتعرض لهما بشيء من التفصيل

1-<u>المعاينة في الجريمة المعلوماتية كوسيلة للحصول على الدليل</u> :معاينة الجرائم التقليدية(1) و الإطلاع على مسرح الجريمة له أهمية المتمثلة في تصور كيفية و قوع الجريمة و ظروف و ملابسات إرتكابها و توفير الأدلة المادية التي يمكن تجميعها عن طريق المعاينة ، لكن هذه المعاينة لا تؤدي ذات الدور في كشف غموض الجريمة المعلوماتية و ضبط الأشياء التي تفيد في إثبات وقوعها و نسبتها إلى مرتكبها(2) و يرجع السبب في ذلك أن مسرح الجريمة يعطي المجال واسعا أمام سلطة الاستدلالات و التحقيق في الكشف عن الجريمة و الأدلة و التحفظ على الأثار المادية التي خلفتها لكن فكرة مسرح الجريمة المعلوماتية يتضاءل دوره و ذلك لسببين:

الأول : أن الجريمة المعلوماتية قلما تخلف آثارا مادية.

الثاني : كثيرا من الأشخاص يردون إلى مسرح الجريمة خلال الفترة من زمان وقوع الجريمة و حتى

إكتشافها و هي فترة طويلة نسبيا الأمر الذي يعطي الفرصة للجاني أن يغير الآثار المادية إن وجدت مما

يورث الشك في دلالة الأدلة المستقاة من المعاينة (3) و الجريمة المعلوماتية قد تكون جريمة مستمرة كما في حالة الجرائم الإقتصادية السرقة و الإحتيال و قد يكون مسرحها كالجرائم الأخرى كما في التزوير و إتلاف البرامج أو تفجير المباني ففي النوع الأول من الجرائم تكون المعاينة هدفها المداهمة و ضبط الأدلة على الطبيعة و في الحالة الثانية و بعد وقوع الجريمة فالأمر متوقف على إعترافات المتهمين متى تم القبض عليهم و القرائن

المعاينة لمسرح الجريمة هي : إثبات لحالة الأماكن و الأشخاص و و كل مايفيد في كشف الحقيقة .

للتفصيل أكثر أنظر : 1-

– درقاوي عبد القادر ، المذكرة السابقة الذكر ، ص 166.

2––د/هشام محمد فريد رستم، المرجع السابق ، ص 101 و ما بعدها

3–نفس المرجع السابق ، ص 102

وفي كل الأحوال يتعين مراعاة الآتي قبل التحرك إلى مسرح الجريمة :

*وجود معلومات مسبقة عن مكان الجريمة من حيث عدد الأجهزة المطلوبة معاينتها و شبكاتها و

الخزائن و الملفات أو خرائط توضح الموقع الذي ستتم معاينته و تفاصيل المبنى أو الطابق موضوع

البلاغ .

* تحديد الأجهزة المحتمل تورطها في الجريمة المعلوماتية حتى يتم تحديد كيفية التعامل معها فنيا قبل

المعاينة سواء من حيث الضبط أو التأمين أو حفظ الأوراق و المستندات المتداولة .

*تأمين الأجهزة و المعدات التي سيتم الإستعانة بها في عملية المعاينة سواء كانت أجهزة أو برامج

صعبة أو لينة .

*إعداد فريق متخصص يتولى المعاينة و تحديد اختصاصات المطلوبة من كل عضو على حدى .

*إعداد خطة معاينة موضحة بالرسومات مع تمام المراجعة التي تكفل تنفيذها على الوجه الأكمل

*تأمين عدم إنقطاع التيار الكهربائي .

لأدلة و ذلك لتعطيل الإتصالات لمنع تخريب ا *إذا وجدت شبكة إتصالات يجب البحث عن خادم الملف الموجودة أو محوها و يراعى تصوير الأجهزة الموجودة خاصة الأجهزة الخلفية منها– خادم الملف يسمى

. FILE SERVER–

*إبطال مفعول أجهزة الهاتف التي قد تساعد عن طريق تقنية معينة في تدمير أدلة الجريمة المعلوماتية

متى تم توصيلها بالأجهزة محل المعاينة (1)

* عدم نقل المواد المعلوماتية خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسب

من مجالات القوى المغناطسية –الممرات المغناطسية– التي قد تتسبب في محو البيانات

1–د/ ممدوح عبد الحميد عبد المطلب ، جرائم إستخدام شبكة المعلومات الدولية ، بحث مقدم للمؤتمر القانون و الكمبيوتر

و الإنترنت ، بكلية الشريعة و القانون ، جامعة الإمارات ، عام 2000 ، ص 22

أيضا –د/ هشام محمد فريد رستم ، المرجع السابق ، ص 103

أيضا – البشري محمد الأمين ، المرجع السابق ، ص 29

*التحفظ على محتويات سلة المهملات و ما فيها من أوراق ممزقة و شرائط و أقراص ممغنطة و رفع البصمات

و كذلك التحفظ على المستندات الإدخال و المخرجات الورقية لجهاز الحاسب الآلي و التي قد تكون ذات صلة بالجريمة (1)

إجراءات التفتيش : يختلف التفتيش بحسب نوعية الجرائم ، فالجرائم العادية يتعلق التفتيش بها على أشياء مادية، أما الجرائم المعلوماتية فهي تطرح العديد من الصعوبات لأنها تخص برامج في الحاسوب أي مكونات معنوية كماأن الدليل الناتج عن هذا الإجراء قد يتصف بعدم المشروعية بسبب الغموض الذي يطرح حول مدى إتباع الأصول العامة في التفتيش ؟

الأصل أن قواعد التفتيش شرعة لأجل حماية الخصوصية و حقوق الإفراد ، كما أنه لابد من تحقيق أفضل ضمانات للمتهم تتفق ومقتضيات البراءة، لذا لا بد من إتباع القواعد العامة فيما يخص إستصدار مذكرات التفتيش كما أنه لضبط حدود التفتيش لابد من مراعاة مايلي :

– **أولا:** إذا كانت الجريمة الإلكترونية مرتبطة بأحد أنظمة الكمبيوتر فإن مذكرة التفتيش يجب أن تكون واضحة في تحديد النظام محل التفتيش حتى لا يؤدي إلى كشف بيانات شخصية ،و كذا الخاصة بسرية المهنية(2) .

– **ثانيا :**إذا كان النظام أو مكان وجود الدليل غير معروف فيتعين أن تجئ عبارة مذكرات التفتيش عامة كأن يكون النظام المعلوماتي داخل أحد المساكن مع وجود النهاية الطرفية له في مكان آخر بحيث يملك الجاني الفرصة لتدمير البيانات**(3)** .

– **ثالثا :**إستصدار أمر كف يد المشتبه بمجرد البدأ بإجراءات التفتيش .

1- أعتند من السلطة التابعة للإدارة الأمنية لمركزالمعلومات الكندية صيغة إذن تفتيش أستخلص من واقع الخبرة العلمية . انظر

بتفصيل أكثر : درقاوي عبد القادر ، المذكرة السابقة ، ص 176.

2- د/ هشام محمد فريد رستم ، المرجع السايق ، ص 104

3- أجاز قانون جريمة الحاسوب الهولندي في المادة 1/25إمكانية تمديد تفتيش مسكن آخر غير مسكن المتهم في النهاية الطرفية التي يتصل بها

النظام المعلوماتي دون الحصول على إذنه مسبق و لكن بقيود هي :

– أن تحتوي على بيانات ضرورية لإظهار الحقيقة .

– ألا تكون النهاية الطرفية المتصل بها الحاسوب موجودة في إقليم دولة أخرى .

–أن يحل قاضي التحقيق محل الشخص صاحب المكان الذي ينبغي تفتيشه بصورة مؤقتة.أنظر بتفصيل أكثر :

درقاوي عبد القادر ، المرجع السابق ،ص 176

– **رابعا :**ملاحظة الطريقة المعد بها النظام المعلوماتي و الآثار التي يخلفها و معرفة السجلات الإلكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الإتصال و نوع الجهاز المتصل عن طريق الدخول إلى النظام أو الموقع أو الدخول معه في حوار و بروتكولات الإتصالات عبر الإنترنت وإن تعلقت الجريمة بهذه الشبكة و التي تعرف إختصارا ب(ip) (1)

خامسا :قياسا على منع ضباط الشرطة القضائية من الإطلاع على الأوراق المختومة أو المغلقة أثناء

التفتيش فإنه يمنع عليهم الإطلاع على نظام الحماية الآلية للبيانات المخزنة و المحمية بطريق التشفير

أو الترميز أو بأي وسيلة فنية أخرى ضد الإختراق ، و ذلك لإتفاقهما في نفس العلة و هي رفض مسبقا

عمليات الإطلاع الغير مصرح به ، لكن يجب أن يقابل ذلك رسم حدود للقاعدة العامة الموجودة في التشريعات العقابية وهي " إعفاء المتهم من تقديم ما من شأنه إثبات إدانته بطريقة مباشرة " بحيث يجبر المتهم على تقديم أكواد الدخول و الكلمات السرية للمرور للملفات(2) .

سادسا : لا بد من مراعاة خاصية هذه الجرائم من كونها عابرة للحدود أثناء التفتيش فالجرائم العادية

يسهل تحديد مكان إرتكابها في حين أنه من الصعوبة بمكان تحديد مكان وقوع الحادثة عند التعامل مع جرائم الإنترنت، لأنه لا يقف أمام تنقل الملفات و الرسائل الحاسوبية أي حدود جغرافية ، كما أنه لا توجد معاهدات

تسمح بالتعاون الدولي أو عدم كفايتها لمواجهة المتطلبات الخاصة بجرائم الكمبيوتر و ديناميكية التحريات

و كفالة السرعة للحصول على أدلة الإثبات .

سابعا – القضاء على الدور السلبي للمجني عليهم : خشية أن تهتز سمعة المجني عليهم أمام العملاء، خاصة في قطاع الأعمال و المصارف فيحجمون عن الإبلاغ على الجرائم المعلوماتية و يكتفون بإجراءات تأديبية للموظف و محو آثار الجريمة و إصلاح الضرر بدل المحافظة على مسرح الجريمة ، مما يؤدي إلى ضياع الدليل والبراهين بحيث يصبح التفتيش الذي تقوم به الجهات المختصة دون فائدة مرجوة منه .

1- د/ممدوح عبد الحميد المطلب ، المرجع السابق ، ص 21و ما بعدها

2- هذا ما نص عليه مشروع قانون جريمة الحاسوب الهولندي في المادة 25 منه . للتفصيل أكثر أنظر :

– درقاوي عبد القادر ، المذكرة السابقة ، ص 175.

<u>الخـــــــاتـــــمة</u> :

بعد التعرض لأدلة إثبات الجريمة المعلوماتية و الصعوبات المتعلقة بالدليل ذاته وكذا إجراءات التحري عنه توصلنا إلى نتيجة وهي أن هذه الصعوبات ناتجة عن كون القواعد التقليدية قاصرة في الكشف عن الادلة لذلك لا بد من وجود قواعد خاصة تراعي طبيعة الدليل و تقرر إجراءات خاصة يجب اتباعها وقد تم معالجة ذلك خلال مشوارنا البحثي وتم التوصل إلى التوصيات التالية :

1–العمل على إيجاد أجهزة للرقابة والتدقيق ذات تخصص وخبرة داخل الإدارات و الشركات للكشف عن الجريمة من ثم إظهار الدليل الخفي الذي تم به بأحدث الطرق في التعامل مع الكمبيوتر .

2–إستعمال نظام التشفير خاصة في نظام الدفع الآلي للبطاقات الإئتمانية بالتعاون مع شركة كمبيوتر عملاقة متخصصة– كمايكروسوفت– و ذلك حتى لا يتمكن محترفوا إختراق اجهزة الكمبيوتر من إسترجاع أرقام البطاقة الإئتمان و إستعمالها في مشتريات إلكترونية بواسطة البطاقة المزيفة .

3- إنشاء فرقا متخصصة من خبراء الكمبيوتر لمكافحة هذه الجريمة مزودة بالعدة الكافية .

4- لابد من القيام بدورات تكوينية حول كيفية إكتشاف الجرائم المعلوماتية .

5-الاتصال بالشبكات الدولية المتخصصة في مكافحة جرائم الكمبيوتر و تبادل المعلومات حول وسائل الإحتيال وكيفية الكشف عنها .

6-تطوير ثقافة الحاسب الآلى وسط رجال الأمن و ذلك من حيث القدرة على الملاحظة و مراعاة تصرفات الأشخاص العاملين في مجال الحاسب الآلي بدقة أو المهتمين بالبرمجة أو هواة صناعة الأنظمة المعلوماتية و تقليدها فدراسة تصرفات هؤلاء و رقابتها تعد مدخلا جيدا للسيطرة الأمنية عليهم و ضبطهم .

7-وضع تشريع عقابي موضوعي و إجرائي متكامل لمواجهة الجريمة المعلوماتية يراعي مبادئ المشروعية و المبادئ الدستورية و في الوقت ذاته يتحرر من القواعد التقليدية في قانون العقوبات و إجراءات الجنائية التقليدية و التي تكون غالبا قاصرة عن مواجهة الجريمة المعلوماتية .

8-لا بد على المشرع من حصر نماذج الإجرام المعلوماتي و تقرير صور العقاب عليه و كذلك الإجراءات الجنائية المتبعة عند القيام بالإستدلالات والتحقيق الجنائي .

9- إنشاء الإجراءات الأمنية الفعالة و الملائمة القائمة لحماية الكمبيوتر من البرامج المدمرة و إختراع أساليب الكشف عنها .

هذه النتائج و التوصيات التي تم التوصل إليها تعتبر ميدان خصب لبحوثات معمقة جديدة ،خاصة الدليل الرقمي الذي سيؤخذ بالبحث و التفصيل في دراساتنا القادمة لما يطرحه من العديد من الإشكاليات ، فيما يخص مفهومه و كيفية التعامل معه ، و إستخلاصه و كذا المحافظة عليه ؟و مدى حجيته كدليل إثبات ؟

المراجع المعتمدة :

المراجع باللغة العربية

1- د/ حجازي عبد الفتاح ، الاثبات الجنائي في جرائم الكومبيوتر والأنترنت . دار الكتب القانونية مصر 2007.

2-عبابنة محمود أحمد ، جرائم الحاسوب و أبعادها الدولية ، دار الثقافة لنشر و التوزيع ، سنة 2005.

3- عياد سامي على حامد ، الجريمة المعلوماتية و إجرام الإنترنت ، دار الفكر الجامعي ، الإسكندرية ، سنة2007 .

4- د/ مصطفى محمد موسى ، الجهاز الإلكتروني لمكافحة الجريمة ، دار الكتب القانونية ، مصر ، سنة 2006.

5- د/محمود نجيب حسني ، شرح قانون الإجراءات الجنائية ، دار النهضة العربية ، 1988،

- المراجع باللغة الفرنسية

1-Adrian ; R.D. Norman . Computer insecuritry, charman and hall U.

2-Harold Goseph Highland " The hidden dangers of Fraud " Abstracts of revent articles and literature

3-Robert, W. Fergusson and Allan , H. Stokke. Legal espects of evidence, Harcourt Barce jovanorich : / NC New York 1941

البحوث و المقالات

1- د/ حجازي سهير :التهديدات الإجرامية للتجارة الإلكترونية ،بحث مختصر لدى مركز البحوث و الدراسات

بإدارة الشرطة بدبي ،الإمارات العربية المتحدة ، عدد9 جويلية 1999.

2- رستم هشام محمد فريد: الجرائم المعلوماتية أصول التحقيق الجنائي الفني و إقتراح بإنشاء إلية عربية موحدة للتدريس التخصص ، بحث مقدم إلى مؤتمر القانون والكومبيوتر والإنترنت)المنعقد في الفترة من 1-3 ماي 2000 بكلية الشريعة والقانون بدولة الامارات

3-فادي سالم :هجمات الفيروسات اسلحة المستقبل المصوبة نحو الإنترنت ، مقال منشور في مجلة الإنترنت العالم العربي ، السنة الثالثة ، العدد التاسع ، سنة 2000

- د/ محمد الأمين البشري :بحث بعنوان " التحقيق في جرائم الحاسب الآلي " مقدم إلى مؤتمر القانون والكومبيوتر والانترنت "المنعقد في الفترة من 1إلى 3 ماي 2000 بكلية الشريعة والقانون بدولة الإمارات.

الرسائل و المذكرات

درقاوي عبد القادر ، جريمة السرقة في عصر المعلوماتية ، مذكرة لنيل شهادة الماجستير في القانون الخاص ، جامعة أبي بكر بلقا يد تلمس**ان ، سنة 2004**