العنوان:	متطلبات هيئة الادعاء في الجرائم الإلكترونية
المصدر:	مجلة العدل
الناشر:	وزارة العدل - المكتب الفني
المؤلف الرئيسي:	درف، عبدالله محمد
المجلد/العدد:	س8, ع18
محكمة:	نعم
التاريخ الميلادي:	2006
الشهر:	أغسطس
الصفحات:	306 - 322
رقم MD:	678362
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	IslamicInfo
مواضيع:	الإثبات الرقمي
رابط:	http://search.mandumah.com/Record/678362

٢ـ متطلبات هيئة الادعاء في الجرائم الإلكترونية

بقلم المستشار/ عبدالله درف

رئيس لجنة التشريع والأمن والحكم المحلي – ولاية كسلا

تمهيد :-

منذ عقد مضى لم نكن نتصور أن الحياة سوف تعتمد بصفة أساسية ومطلقة على جهاز الحاسب الآلي وملحقاته، إلا أن ذلك صار واقعاً وحقيقة وأصبح الأفراد والمؤسسات والهيئات العامة والخاصة والحكومات تعتمد اعتماداً أساسياً في كثير من معاملاتها على جهاز الحاسب الآلي ثم تطور الأمر بدخول آليات وتقنيات التزاوج الذي تم بين تكنولوجيا الاتصالات وتكنولوجيا الحاسب الآلي بما يعرف بشبكة المعلومات الدولية مما جعل العالم قرية صغيرة من حيث الأحداث والوقائع التي يمكن متابعتها في أي زمان ومكان.

ومن الطبيعي أن يصاحب هذا التقدم التقني تطور في الظاهرة الإجرامية المرتبطة به وظهرت العمليات الإجرامية الإلكترونية الرقمية وهي العمل الإنساني الإلكتروني الرقمي المخالف للقانون والذي يقوم به المجرم بالتقنية الإلكترونية الرقمية وشبكة الإنترنت لارتكاب جريمة إلكترونية رقمية لتحقيق غرض إجرامي معين، وظهرت نواة الجريمة الإلكترونية بظهور الاتصالات الهاتفية وكان أغلب العاملين بالشركات من الشباب المتحمسين لمعرفة المزيد من هذه التقنية الحديثة ولذلك بدءوا يتصنتون على المحادثات الهاتفية التي تتم في هذه الشركات وكانوا يغيرون الخطوط الهاتفية فمثلاً المكالمة المرسلة لمحمد تصل لعلي وكل هذا من أجل التسلية، وهؤلاء كانوا (الهاكرز) قراصنة الحاسوب، ثم ظهر الحاسب الآلي الرقمي، وتطورت تبعاً لذلك الجريمة المرتبطة بالحاسب الآلي وظهرت في هذا

المجال ما يعرف (بجريمة الحاسب الآلي والإنترنت) أو ما يعرف بالجريمة الإلكترونية.

في هذه الورقة سنتطرق في المطلب الأول إلى تعريف الجريمة الإلكترونية والمقصود بالجرائم عبر الحاسب الآلي وتكييف جرائم تقنية المعلومات وتصنيفها ثم في المطلب الثاني سنتطرق لمتطلبات هيئة الادعاء لمكافحة الجريمة الإلكترونية ثم في المطلب الثالث سنتناول الإثبات الرقمي والتكييف القانوني وعلوم الأدلة ومساهمتها في كشف الجريمة الإلكترونية ثم نتناول جمع الدليل الرقمي والصعوبات التي تواجه جمع الأدلة الرقمية ثم نتناول الدليل الرقمي ومعامل الأدلة الرقمية ومتطلبات إنشاء المعامل الرقمية وشروط استخدام الدليل الرقمي في المسائل الجنائية ونختتم الورقة بالتوصيات التي نعتقد أنها ستسد الثغرات المتعلقة بمكافحة الجريمة الإلكترونية.

المطلب الأول

الجرائم الإلكترونية

جرائم الحاسب الآلي والإنترنت

لفهم المقصود بالجرائم عبر الحاسب الآلي ينبغي أن نفرق بين الحاسب الآلي كجهاز تقني والشبكة العالمية للمعلومات أو ما يعرف باسم (الويب) وهي مجموعة كاملة من الوثائق والنصوص والمعلومات والصور والصوت والفيديو، وهي ذات شكل تشعبي مرتبط على مستوى العالم، والإنترنت هي آلية نقل المعلومات عن طريق البروتوكولات الخاصة بالاتصال السلكي واللاسلكي، وعلى ذلك فان الجرائم عبر الحاسب الآلي على أربعة أنواع :

١/ جرائم الحاسب الآلي Computer Crime :

وهي النوع الأول من جرائم الحاسب الآلي وتعرف، أنها سلوك إنساني يشكل فعلاً غير مشروع قانوناً ويقع على أجهزة الحاسب الآلي سواء هذا السلوك غير المشروع على Hardware أو المكونات المعنوية Software أو قواعد البيانات الرئيسية Database ومن أمثلتها التخريب لمكونات الحاسب الآلي المادية كالشاشة أو الطابعة أو وسائط التخزين المرنة أو الصلبة وكذلك الفيروسات وتعديل أو محو البيانات الرئيسية أو غيرها.

٢/ جرائم الشبكة العالمية Web Computer Crime :

وهي النوع الثاني وتعرف بأنها أي سلوك ثاني يشكل فعلاً غير مشروع قانوناً ويقع على أي وثيقة أو نص موجود بالشبكة ومن أمثلتها قرصنة المعلومات وسرقة أرقام بطاقات الائتمان وانتهاك الملكية الفكرية للبرامج والأغاني والأفلام والموسيقى وغيرها، ويلاحظ أن جرائم الشبكة العالمية تتطلب اتصالاً بالإنترنت على عكس جرائم الحاسب الآلي التي قد يتصور حدوثها سواء كان هناك اتصال بالإنترنت أو عدمه.

٣/ جرائم الإنترنت Internet Crime :

وهي النوع الثالث وتعرف بأنها أي سلوك إنساني يشكل فعلاً غير مشروع قانوناً تقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات ومن أمثلتها الدخول غير المسموح لمواقع غير مصرح للدخول إليها واستخدام عناوين IP غير حقيقية أو زائفة للولوج إلى الشبكة العالمية للمعلومات.

٤/ جرائم باستخدام الحاسب الآلي :

ونشير إلى وجود نوع من الجرائم لا يعتبر استخدام الحاسب الآلي أو الشبكة العالمية للمعلومات أو الإنترنت من طبيعة الفعل المجرم أو ركناً من أركان الجريمة

بمعناها القانوني مثل الجرائم التي يتم فيها استخدام الحاسب الآلي والشبكة والإنترنت في عمليات غسل الأموال أو نقل المخدرات من مكان إلى آخر وغيرها، فهنا الحاسب الآلي أو الإنترنت أو الشبكة هي وسيلة ارتكاب الجاني للجريمة والتي يمكن ارتكابها بأي وسيلة أخرى و تسمى هذه الجرائم جرائم باستخدام الحاسب الآلي.

تكييف جرائم تقنية المعلومات :

هي الجرائم التي تستهدف المكونات غير الملموسة (المعلومات ــ البيانات ــ البرامج) أي معطيات الحاسب الآلي، وتستهدف تلك الجرائم الحقوق المعنوية للمعلومات والأسرار والبيانات الشخصية في كافة صورها ومراحلها.

أسس تصنيف جرائم المعلومات :

يصنف الفقهاء جرائم تقنية المعلومات وفقاً لعدة معايير حيث يستهدف بعضها جهاز الحاسب الآلي بينما يقوم البعض الآخر وفقاً للمنهجيات والأساليب المستخدمة ويصنف تبعاً للبواعث.

تصنف الجرائم تبعاً لمحل الجريمة :

(١) الجرائم الماسة بمكونات الحاسب الآلي :

وهي أما جرائم إتلاف وتخريب للبيانات والمعلومات وبرمجيات جهاز الحاسب الآلي كاستخدام الفيروسات أو الجرائم التي تمس الأموال مثل جرائم غش الحاسوب وتخريب المكونات المتعلقة بالبيانات والمعلومات.

(٢) الجرائم الماسة بالبيانات الشخصية :

وهي الجرائم التي تمس المعلومات الشخصية والبيانات المتعلقة بها.

(٣) جرائم الملكية الفكرية للبرمجيات :

وهي عمليات النسخ غير المصرح به للبرامج والاعتداء على براءات الاختراع.

تصنيف الجرائم تبعاً لدور جهاز الحاسب الآلي :

لقد قسمت الاتفاقية الأوروبية جرائم تقنية المعلومات وفقاً لما يلي :

١. الجرائم التي تستهدف السلامة والسرية :

- الدخول غير المسموح.
- الاعتراض غير القانوني.
- تدمير المعطيات.
- اعتراض النظم.
- تعطيل وعطب الأجهزة.

٢. الجرائم المرتبطة بجهاز الحاسب الآلي :

- التزوير.
- الاحتيال.

٣. جرائم المحتوى المضار :

وهي الطائفة المتعلقة بالأفعال الإباحية واللاأخلاقية.

٤. جرائم الملكية الفكرية :

مثل الاعتداء على حقوق المؤلف وقرصنة النظم والبرمجيات.

تصنيف الجرائم تبعاً لمساسها بالأموال والأشخاص :

وهي مثل الجرائم الواقعة على الأشخاص والأموال وجرائم السرقة والاحتيال والتزوير والمغامرة وجرائم الآداب.

أولاً : الجرائم ضد الأشخاص :

وتشمل التحريض على الأفكار والتحريض على القتل عبر الإنترنت والمضايقة عبر الرسائل الإلكترونية والاطلاع على البيانات الشخصية وبث المعلومات المضللة.

ثانياً : جرائم العرض والآداب العامة :

وتشمل إغواء القاصرين للقيام بأنشطة جنسية أو نشر معلومات تحثهم للقيام بتلك الجرائم ونشر المواد الفاضحة عبر الإنترنت وجرائم الدعارة وهتك العرض.

ثالثاً : جرائم الأموال (عدا السرقة) :

وتتضمن الاعتداء على الملكية وكذلك أنشطة الاختراق والإتلاف.

رابعاً : جرائم الاحتيال والسرقة :

وتشمل الجرائم المتعلقة بالحصول على أرقام بطاقات الائتمان دون ترخيص، والاختلاس عبر جهاز الحاسب الآلي.

خامساً : جرائم التزوير :

وتشمل تزوير البريد الإلكتروني وتزوير الوثائق والسجلات وتزوير الهوية.

سادساً : جرائم المغامرة :

وتشمل إدارة مشروعات المغامرة على الإنترنت وتشجيع استخدام المواقع لترويج الكحول ومواد الإدمان.

سابعاً : الجرائم ضد الحكومة Crime Against Government **:**

وهي الجرائم التي تهدف إلى أضرار الحكومات وتعطيل أعمالها وتنفيذها للقانون وتستهدف الحصول على معلومات سرية، وجرائم البلاغات الكيدية وتهديد السلامة العامة وبث البيانات التي تعتبر إرهاباً إلكترونياً.

المطلب الثاني

متطلبات هيئة الادعاء لمكافحة الجريمة الإلكترونية

يعتبر تضافر الجهود الدولية والتنسيق الشامل للمعلومات هي البنية الأساسية لقضايا مكافحة الجريمة الإلكترونية وذلك من خلال رصد وتجميع المعلومات عن أنشطة المجرمين الإلكترونية وجرائمهم هو أحد مصادر الأداء الناجح للمكافحة، وذلك من خلال إنشاء جهاز إلكتروني للمكافحة، حيث أصبحت المعلومات اليوم محور أساسي لا يمكن غض البصر عنه لأنها عنصر جوهري في مجال مكافحة الجريمة سواء على مستوى وزارة العدل أو وزارة الداخلية أو القضاء والمشرع وكلها مرتبطة بالحد من الجريمة أو ضبطها وبدون المعلومات لا يمكن بأي حال من الأحوال مكافحة قضية إجرامية إلكترونية بأسلوب علمي، إضافة إلى أن البحث والتحقيق الجنائي في الجرائم الإلكترونية تتطلب أساليب جديدة في التحري تستلزم توافر خبرات تقنية وعلمية عالية، إذ أن مسألة البحث والتحقيق في الجرائم الإلكترونية مسألة في غاية الأهمية والصعوبة لاعتبارات التكوين العلمي والتدريب والخبرات المكتسبة لرجال إنفاذ القانون والعدالة الجنائية، وحداثة هذه الجرائم وتقنياتها العالية التي تتطلب من القائمين بالبحث والتحقيق الإلمام الكافي بها، فلا يكفي أن يتمتع رجال القانون بالخلفية القانونية فقط وإنما يجب أن يتمتعوا بخبرة فنية في هذا المجال، حيث أن دور الإثبات العلمي للدليل المادي تطور مع ظهور الأدلة الرقمية المطلوبة في إثبات الجرائم الإلكترونية، وأصبح الدليل الرقمي ضرورة لكشف أنماط الجرائم الإلكترونية كما أصبح إنشاء المعامل الجنائية الرقمية مطلباً ملحاً لفحص الأدلة الرقمية ولتقييم عملية الإثبات الرقمي وتحليل الجرائم في نطاق ما يعرف باسم نظم الخبرة الأمنية.

وعلى ذلك فان مكافحة الجرائم الإلكترونية تتطلب كما أسلفنا إنشاء جهاز لمكافحة الجريمة الإلكترونية ويكون من مهامه إنشاء قواعد البيانات والنظم والتطبيقات وتوفير المعلومات عن الجريمة والمجرم الإلكتروني لمساعدة المختصين ومتخذي القرار أو لرصد وحل المشكلات أو التوصية بسن القوانين وعمل التقارير السنوية عن الجرائم الإلكترونية إضافة إلى الاهتمام والتطوير اللازم للتحري والبحث عن المعلومات عبر شبكة الإنترنت.

فالجرائم الإلكترونية وقضايا الحد منها وضبطها تعد من قضايا المشاركة التي لا يمكن أن يتحملها فرد بعينه أو دولة بمفردها، بل لابد من وجود رؤية سياسية محددة وواضحة معتمدة على المعلومات، وسنتناول في المطلب الثالث الإثبات الرقمي والتكييف القانوني وعلوم الأدلة الرقمية وجمع الأدلة الرقمية ومعامل الأدلة الرقمية وقبول الدليل الرقمي كأحد متطلبات هيئة الادعاء لمكافحة الجريمة الإلكترونية.

المطلب الثالث

الإثبات الرقمي والتكييف القانوني

تطورت وسائل الإثبات في الجرائم التقليدية على كافة الأصعدة إلا أن الأمر ليس كذلك بالنسبة للجرائم الإلكترونية الأمر الذي يحتم ضرورة التفاعل بين ما اصبح يعرف بالمشهد الرقمي للجريمة وبين الوسائل التقليدية المتعارف عليها في الإثبات.

والمشهد الرقمي أو الدليل الرقمي هي الآثار التي يتركها مستخدم جهاز الحاسب الآلي أو الشبكة المعلوماتية أو الإنترنت وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الأفعال التي تمت من خلال جهاز الحاسب الآلي أو الشبكة العالمية

أو الإنترنت وهذه الآثار تكون في شكل رئيسي هو الشكل الرقمي لأن البيانات داخل جهاز الحاسب الآلي سواء أكانت نصوص أم أحرف أو أرقام أم أصوات أو صور أم فيديو تتحول إلى صيغة رقمية لذلك تسمى الأدلة المستخرجة من أجهزة الحاسب الآلي والتي لها علاقة بال Hardware أو Software أو Internet بأنها أدلة رقمية.

ويمتاز الدليل الرقمي عن الدليل المادي المأخوذ من مسرح الجريمة المعتاد بما يلي :

١ــ طريقة نسخ الدليل الرقمي من أجهزة الحاسب الآلي تقل أو تعدم تقريباً مخاطر إتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الإنشاء.

٢ــ باستخدام التطبيقات والبرامج الصحيحة، يكون من السهولة تحديد ما إذا كان الدليل الرقمي قد تم العبث فيه أو تعديله وذلك لإمكانية مقارنته بالأصل.

٣ــ الصعوبة النسبية لتحطيم أو محو الدليل، ففي حالة إصدار أمر من الجاني لإزالته من أجهزة الحاسب الآلي فيمكن للدليل الرقمي أن يعاد تظهيره من خلال الحـــاسب الآلي Desk.

٤ــ نشاط الجاني لمحو الدليل يسجل كدليل أيضاً، حيث أن نسخة من هذا الفعل (فعل الجاني لمحو الدليل) يتم تسجيلها في جهاز الحاسب الآلي ويمكن استخلاصها لاحقاً لاستخدامها كدليل إدانة ضده.

٥ــ امتيازه بالسعة التخزينية العالية، فآلة الفيديو الرقمية يمكنها تخزين مئات الصور، Desk صغير يمكنه تخزين مكتبة صغيرة وهكذا.

٦ــ يمكن من خلال الدليل الرقمي رصد المعلومات عن الجاني وتحليلها في ذات الوقت، فالدليل الرقمي يمكنه أن يسجل تحركات الفرد كما أنه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فإن البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي.

علوم الأدلة الرقمية :

وهي العلوم التي تمكننا من استخلاص الدليل الرقمي وجمعه من مسرح الجريمة لتحديد البصمة الرقمية، وتشمل هذه العلوم علوم الحاسب الآلي وعلوم الأدلة الجنائية وعلوم التحليل السلوكي للأدلة الرقمية.

وعلوم المعامل الرقمية مجتمعة تساهم فيما يلي :

١ــ الكشف عن الدليل الرقمي.

٢ــ إجراء الاختبارات التكنولوجية والعلمية عليه لاختباره والتحقق من أصالته ومصدره كدليل يمكن تقديمه لأجهزة إنفاذه وتطبيق القانون.

٣ــ تحديد الخصائص الفريدة للدليل الرقمي.

٤ــ إصلاح الدليل وإعادة تجميعه من المكونات المادية لجهاز الحاسب الآلي Hard Drive.

٥ــ عمل نسخة أصلية من الدليل الرقمي للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاص الدليل.

٦ــ جمع الآثار المعلوماتية الرقمية التي قد تكون تبدلت خلال الشبكة المعلوماتية.

جمع الدليل الرقمي :

جمع الأدلة الرقمية من بروتوكولات النقل والشبكات والاتصالات يمكن أن يشكل صعوبة نسبية من وجهة نظر أجهزة إنفاذ القانون، والصعوبة تأتي من أن جمع المعلومات يحتوى على كمية هائلة من المعلومات الجنائية وفي الغالب تكون مختلطة بغيرها من معلومات مستخدمي الحاسب الآلي الأبرياء مما قد يشكل تهديداً لخصوصية هؤلاء ويعتبر في ذات الوقت ضبطاً بدون تفويض أو تصريح أو أمر قانوني أو قضائي، لذلك من المستحسن أن يتم استخدام أسلوب القص والرصد إلى ملف جديد خاص بجمع الأدلة وقبل غلق الأجهزة، ورغم أن أسلوب القطع واللصق أسلوب ناجح لجمع الأدلة إلا أن المشاكل القانونية المترتبة على قانونية هذا

الأسلوب قد يثير بعض الشك في مدى سلامة جمع المعلومات وحجيتها أمام أجهزة العدالة، لذلك يقترح ما يلي لسلامة الجمع والتوثيق :

١/ أخذ نسخة كاملة من بينات الجداول التشغيلية من ضبط الجهاز المستخدم وقبل فصل الجهاز من التيار الكهربائي وذلك بطباعة هذه النسخة.

٢/ القيام بعمليات النسخ واللصق والتجميع في File محدد بعد التأكد من خلوه من أية معلومات أخرى.

٣/ مراعاة ترقيم البيانات المجزئة طبقاً للتسلسل الحادث بحيث يتم الاستدلال بشكل متسلسل ومنطقي وطبقاً للأصل.

وهذه الإجراءات رغم إنها طويلة وتتطلب وقتاً إلا إنها مهمة للتدوين والحفظ لإمكان اعتمادها كدليل أمام أجهزة العدالة الجنائية.

صعوبات جمع الأدلة الرقمية :

تواجه الخبير الجنائي في مجال الأدلة الرقمية صعوبات متعددة في جمع تلك الأدلة من أجهزة الحاسب الآلي أو الشبكات الرقمية وتشمل هذه الصعوبات ما يلي:

١/ نظم تشغيل أجهزة الحاسب الآلي النشطة والنظم السائرة :

أنه من المتعارف عليه أن عملية إغلاق جهاز الحاسب الآلي تعني أن قدراً ضئيلاً من الأدلة لا يمكن استرجاعها كذلك في حالة عدم تخزينها بالذاكرة، وبذلك ينصح قبل قفل الجهاز تخزين الأدلة الموجودة في الذاكرة وذلك لمنع مسح الأدلة، إلا أن قطع التيار الكهربائي المفاجئ عن الجهاز يسبب العديد من المخاطر وتتمثل في محو المعلومات من الذاكرة من جراء غلق الجهاز، بمعنى فقدان كافة العمليات التي كان يتم تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة.

٢/ الأدلة وتجزئة الملفات :

ينبغي من وجهة الفحص الفني التمييز بين الوسائط المادية التي تحوي بيانات بصورتها الثنائية وبين التمثيل المنطقي لهذه المعلومات، لأهمية ذلك في إجراءات اعتماد الدليل الرقمي أمام جهات إنفاذ القانون حيث يحتاج الخبراء في بعض المواقف إلى إجراء عملية التحليل على البيانات الخام وفي حالات أخرى فأنهم يرغبون في فحص البيانات حسب ترتيبها من خلال نظام التشغيل.

٣/ طبيعة الشبكات :

بالرغم من أن انتشار الأجهزة المحمولة والمتصلة بشبكات اللاسلكي عد بمثابة نقلة نوعية كبيرة في عصر الحاسب الآلي، إلا أنه اعتبر أحد أهم تحديات البحث والتحقيق في الأنشطة الإجرامية في مجال أنشطة الحاسب الآلي المنتشرة على مستوى العالم، وتمثلت هذه الصعوبات في كيفية الحصول على كافة الأدلة من هذه الأجهزة ذات العلاقة بالواقعة محل البحث الجنائي.

وتساهم على وجه العموم عوامل عديدة في هذا التحدي أولها ينتج عن طبيعة الشبكات الموزعة توزيعاً لمسارح الجريمة مما يؤدي إلى مشاكل عملية وتشريعية، مثال لذلك قد لا يكون ممكناً الحصول على الأدلة من أجهزة الحاسب الآلي الموجودة في دولة أخرى.

وثاني هذه الصعوبات تتمثل في طبيعة البيانات الرقمية نفسها التي يمكن مسحها أو تغييرها بسهولة لذلك من الضروري جمعها والاحتفاظ بها بسرعة كلما أمكن ذلك. ويكمن العامل المساهم الثالث في هذا التحدي الكبير في الحجم المطلوب من الخبرة الفنية عند استخدام الشبكات في جريمة ما.

أما العامل المساهم الرابع فهو حجم البيانات الضخمة التي غالباً ما تستخدم في التحقيق من خلال أنظمة جهاز الحاسب الآلي، والبحث عن الأدلة في كم كبير من البيانات الرقمية أمر بالغ الصعوبة ويتطلب جهداً ومهارة عالية.

٤/ الشبكات لاخفاء الهوية :

مشكلة أخرى تواجه جمع الأدلة الجنائية الرقمية من مسرح الحادث وتتمثل هذه المشكلة عند تعمد المستخدم إلى إخفاء هويته وينشأ عن ذلك مزيد من التحديات الأمنية حتى عندما لا يبذل المجرمون جهداً في إخفاء هويتهم فإنهم لا يستطيعون الإدعاء بأنهم لم يكونوا مسئولين عن ذلك.

٥/ الشبكات وإخفاء المعلومات :

تضع عملية إخفاء المعلومات تحديات مماثلة لخبراء الأدلة الرقمية مما يجعل الأمر صعباً أو مستحيلاً للعثور على البيانات الرقمية.

قبول الدليل الرقمي :

إن مدى قبول الأدلة المستمدة من جهاز الحاسب الآلي ليس ضرورياً فقط لاستخدام سجلات جهاز الحاسب الآلي في عملية المحاكمة الجنائية ولكن أيضاً شيء جوهري في تعريف مدى الصلاحيات الضبطية المعطاة لرجال إنفاذ القانون، وكذلك في المسائل ذات الصفة الدولية وفي معظم الدول تعتبر الصلاحيات الضبطية منطبقة فقط على المادة التي تكون مقبولة كدليل في المحاكمة.

إن مدى قبول الأدلة المستمدة من جهاز الحاسب الآلي في المحاكم تعتمد إلى حد كبير على المبادئ الأساسية المقبولة للإثبات لكل دولة.

معامل الأدلة الرقمية :

معامل الأدلة الرقمية تستخدم لفحص الأدلة الرقمية لبيان مشروعية استخلاصها ومصداقيتها للقبول أمام المحاكم والنيابات المختصة وعليه سنتناول متطلبات انتشار هذه المعامل.

١. المتطلبات البشرية والتدريبية :

يعد تدريب العاملين على مكافحة الجريمة عبر الإنترنت العنصر الرئيسي في إنشاء المعامل الجنائية الرقمية ويشمل هذا التدريب كل العاملين في مجال إنفاذ القانون بمفهومه الواسع الشرطة ــ النيابة ــ القضاء.

وينبغي أن يتم التدريب من خلال الدورات التدريبية والمؤتمرات وابتعاث العاملين في أجهزة إنفاذ القانون للحصول على درجات علمية متخصصة في البحث الجنائي الرقمي ويجب إنشاء فرع جديد في علوم المعمل الجنائي يهتم بدراسة الأدلة الرقمية، ويجب أن يتضمن التدريب الأساليب التقنية الحديثة النظرية والعلمية في هذا المجال.

٢. المتطلبات القانونية :

يتطلب إنشاء المعامل الرقمية صدور تشريعات لمكافحة صور الجريمة عبر جهاز الحاسب الآلي حتى يمكن تحديد الأفعال غير المشروعة وغيرها من الأفعال المباحة، فالتجريم القانوني لهذه الأفعال في معظم الدول العربية مازال يعتمد على التشريعات الخاصة بحماية حقوق المؤلف والحقوق الأخرى المرتبطة بها.

ويجب تعديل القوانين الجنائية وقوانين الإجراءات الجنائية في العالم العربي لتشمل نصوص صريحة للجرائم عبر الإنترنت والإجراءات التي تتبع في الدعوى والمتعلقة بهذه الجرائم، ويجب أن يكون هنالك تشريع منفصل يتناول الجانب الإجرائي والجانب العقابي لاستخدام جهاز الحاسب الآلي.

٣. المتطلبات التنظيمية الإدارية :

تتطلب مواجهة الجرائم عبر الإنترنت إنشاء إدارة خاصة في أجهزة إنفاذ القانون تختص بضبط الجرائم التي تتم عبر الحاسب الآلي على أن نمد هذه الإدارة بنوعية من الأفراد يتمتعوا بخلفية أكاديمية شاملة لنظم الحاسب الآلي، وتقوم هذه الإدارة بالتنسيق مع قسم الأدلة الرقمية الذي اقترحنا إنشاءه في المعامل الجنائية.

ويمكن أن يشمل قسم الأدلة الرقمية المعامل الجنائية التقسيمات الثلاثة التالية :

<أ> شعبة الأدلة الرقمية لشبكات الحاسب الآلي : وتختص هذه الشعبة بالأدلة الرقمية التي قد توجد في شبكات الحاسب الآلي المحلية أو في أجهزة الحاسب الآلي الخاصة.

<ب> شعبة الأدلة الرقمية للشبكة العالمية للمعلومات : وتختص هذه الشعبة بالأدلة الرقمية التي تدل على انتهاك حقوق الملكية الفكرية للمواد المعلوماتية المدرجة بالشبكة.

<ج> شعبة الأدلة الرقمية لبروتوكولات الإنترنت : وتختص هذه الشعبة بالأدلة الرقمية التي قد توجد في نظم الاتصال السلكي واللاسلكي والتي تكون لها علاقة بالجريمة عبر الإنترنت.

٤. المتطلبات التقنية :

من الناحية الفنية لا يمكن حصر المتطلبات التقنية نظراً لأن جهاز الحاسب الآلي وما يتصل به من أجهزة أو معدات أو تقنيات أو برامج ذات تطور سريع نسبياً بمعدل يكاد يكون سنوياً وبالرغم من ذلك فإن السنوات القليلة الماضية قد شهدت تزايداً في مقدار الاهتمام الموجه لبرامج الحاسب الآلي والدور الذي يمكن أن تلعبه في التقنية القادمة، وعلى ذلك فإن تحديد المتطلبات التقنية اللازمة لإنشاء المعامل الرقمية التي تتعامل في مجال الأدلة الرقمية أمر صعب التحديد في الوقت الحالي وينبغي أن يترك للوقائع والحركة التقنية للأجهزة المرتبطة بالإنشاء مستقبلاً.

شروط استخدام الدليل الرقمي في المسائل الجنائية :

يمكن تحديد شروط استخدام الدليل الرقمي في مجال الجرائم الإلكترونية فيما يلي :

١/ أن يتم استخلاص شروط استخدام الدليل ضمن ضمانات قانونية إجرائية تضمن سلامة وصحة ودقة هذا الاستخلاص.

٢/ أن يتم التأكد من حجية هذا الدليل بإجراء اختبارات الثقة التي تشمل ثلاثة عناصر، الأول ــ القائم على استخراج الدليل والثاني ــ الجهاز المستخدم والثالث ــ التطبيقات المقارنة.

٣/ إذا اجتاز الدليل اختبارات الثقة أصبح ذا حجية قضائية.

٤/ أن يتم استخلاص الدليل طبقاً لمبادئ المشروعية الإجرائية والقانونية.

وعلى ذلك إذا استوفى الدليل الرقمي الشروط الموضوعية لاعتماده كدليل قضائي انحصر دور أجهزة إنفاذ القانون وتطبيقه في بحث مدى الملائمة الموضوعية لظروف استخراجه واستخلاصه فقط.

التوصيات :

١ــ مراجعة التشريعات الحالية وبحث مدى كفايتها إجرائياً وموضوعياً لمواجهة جرائم المعلوماتية مع وضع الحلول المناسبة.

٢ــ تدريب أجهزة إنفاذ القانون (الشرطة ــ النيابة ــ القضاء) على البحث الجنائي الرقمي وأن يكونوا ملمين بتقنية المعلومات والتعامل مع أجهزة الحاسب الآلي في كل مجالاته وإنشاء فرع للمعامل الجنائية يهتم بدراسة الأدلة الرقمية.

٣ــ سن التشريعات الخاصة بالأحكام الجنائية وبالإجراءات الجنائية في مجال الجريمة المعلوماتية.

٤ــ مراجعة الأحكام الصادرة في جرائم المعلوماتية لسد الثغرات وإصلاحها تشريعياً وذلك بتعديل التشريعات لمواكبة ما يستحدث من أساليب إجرامية في هذا المجال.

٥ــ التوسع في ثقافة الحاسب الآلي لدى مستخدميه والأشخاص المحتمل تعرضهم للجريمة المعلوماتية وتطوير البرامج التي تحد من اختراق شبكات الحاسب الآلي.

٦ــ تأهيل الخبراء على بحث تكنولوجيا المعلومات ومعالجة البيانات للوصول إلى صياغة معايير أمنية مشتركة وإجراءات فنية تحد من جريمة المعلومات في كل قطاعات الدولة والقطاع الخاص.

٧ــ تأمين شركات القطاع العام والخاص ضد الجريمة المعلوماتية على أن يكون التأمين إجبارياً لبعض القطاعات الحساسة.

٨ــ إنشاء إدارة خاصة في أجهزة إنفاذ القانون تختص بضبط الجرائم التي تتم عبر جهاز الحاسب الآلي على أن تزود بأفراد يتمتعون بخلفية أكاديمية شاملة لنظم الحاسب الآلي، على أن تنسق هذه الإدارة مع قسم الأدلة الرقمية.

٩ــ تطوير ونشر أخلاقيات استعمال جهاز الحاسب الآلي.

١٠ــ تشجيع المجني عليهم على ضرورة الإبلاغ عن الجريمة المعلوماتية.

١١ــ تعليم وتدريب الأفراد على كل ما يتعلق بالدعوى الجنائية بالجريمة المعلوماتية من إبلاغ وضبط وتحقيق ونظام قضائي خاص به.

١٢ــ بحث التعاون مع الدول الأخرى في مجال الخبرة والمعلومات في شأن الحاسب الآلي والإنترنت وكل ما يتعلق بالجريمة الإلكترونية.

١٣ــ تعزيز التعاون الدولي في مكافحة الجريمة المعلوماتية عن طريق تبادل الخبرات القانونية.

١٤ــ إيجاد معاهدة جماعية بين كافة الدول العربية في مجال الجريمة المعلوماتية على أن تشمل المعاهدة نص موحد للسلوك الإجرامي في الجريمة المعلوماتية تحد من الصعوبات المتعلقة بارتكاب المجرمين لأفعالهم في مناطق جغرافية مختلفة تشريعياً وتجعل مشكلة الاختصاص المكاني في هذه الجرائم محلولة على الأقل في العالم العربي.