مجلة جامعة الملك سعود، م ٢٥، الحقوق والعلوم السياسية(١)، ص ص ٥٥-٨٢، الرياض (٢٠١٣م/ ١٤٣٤هـ)

الإثبات بالدليل الإلكتروني في الجرائم المعلوماتية

أسامة بن غانم العبيدي
أستاذ القانون المشارك
معهد الإدارة العامة، الرياض

(قدم للنشر في ٢٣/ ١٠/ ١٤٣٢هـ، وقبل للنشر في ٢١/ ٢/ ١٤٣٣هـ)

ملخص البحث. أدى الإنتشار الكبير في استخدام الحاسب الآلي وشبكة الإنترنت إلى زيادة كبيرة في الجرائم المرتكبة باستخدام هذه التقنية. حيث يستطيع مرتكب مثل هذا النوع من الجرائم استخدام وسائل حديثة تساعد في ارتكاب جرائمه دون أن يترك آثاراً تساعد في الوصول إليه ومحاكمته. ويتناول هذا البحث الإثبات الإلكتروني في الجرائم المعلوماتية والمشاكل التي تعترض الإثبات في الجرائم المعلوماتية، وكيفية التعامل معها. وقد بيّنا في المبحث الأول مفهوم الدليل المعلوماتي وخصائصه وشروطه. كما أوضحنا في المبحث الثاني تفتيش وضبط الدليل المعلوماتي وإجراءات استخلاصه والتعامل معه. كما بينا في المبحث الثالث الصعوبات التي تواجه إثبات الجرائم المعلوماتية. وأوضحنا في المبحث الرابع حجية الدليل المعلوماتي في بعض القوانين المقارنة.

مقدمة

صاحب التطور الكبير في وسائل الاتصال الحديثة، ظهور أنماط جديدة من الجرائم لم تتضمنها التشريعات العقابية التقليدية، وتبدو النصوص الجزائية التقليدية عاجزة عن مكافحتها. فهناك ضرورة لوجود نصوص قانونية تقرر الإجراء القانوني الواجب إتباعه في مثل هذه الجرائم مع مراعاة الطبيعة الخاصة لها. فإثبات الجريمة المعلوماتية يختلف تماماً عن إثبات الجريمة التقليدية. فالجريمة المعلوماتية لا تترك أي آثار مادية في مسرح الجريمة، إضافة إلى أن مرتكبيها لديهم القدرة على إتلاف الدليل خلال فترة زمنية قد لا تتجاوز الثواني المعدودة. إضافة إلى كم البيانات والمعلومات المخزنة في جهاز الحاسب الآلي وكيفية إثباتها، سواء من حيث وسيلة الإثبات أو الشخص القائم بالإثبات. وما إذا كانت تتوافر لديه القدرة والخبرة في استخلاص الدليل المعلوماتي. فاستخلاص الدليل المعلوماتي ينصب على المعطيات والبيانات والبرامج المخزنة في النظام المعلوماتي محل الإثبات. وهو ما يثير العديد من المشاكل، منها المعايير المقبولة للضبط والإثبات في الجرائم المعلوماتية ومعايير التحريز، إضافة إلى مدى

مساس إجراءات ضبط محتويات نظام معلوماتي ما بخصوصية صاحبه. إذ قد يتضمن النظام المعلوماتي معلومات وبيانات يحرص صاحبها على سريتها أو تكون محل حماية.

ويناقش هذا البحث موضوع الإثبات الإلكتروني في الجرائم المعلوماتية من حيث مفهوم الدليل المعلوماتي وخصائصه وشروطه إضافة إلى تفتيش وضبط الدليل المعلوماتي وإجراءات استخلاصه والتعامل معه كما سيناقش الصعوبات التي تواجه إثبات الجرائم المعلوماتية إضافة إلى حجية الدليل المعلوماتي في بعض التشريعات المقارنة.

مشكلة البحث

مع الزيادة المتسارعة في الجرائم المرتكبة باستخدام تقنية الحاسب الآلي والإنترنت نشأت مشكلة ترتبط بالصعوبات التي تعترض إثبات مثل هذا النوع من الجرائم المستحدثة بما توجده من مشاكل تتعلق بعدم تركها لأثار مادية في مسرح الجريمة وصعوبات إستخلاص الدليل، إضافة إلى مشاكل التفتيش وضبط الدليل المعلوماتي وكيفية إستخلاصه والتعامل معه، سواء من جهات التحقيق أو النيابة العامة أو المحاكم، ومن هنا تتحدد مشكلة هذا البحث في كيفية استخدام والتعامل مع الدليل في إثبات مثل هذا النوع من الجرائم.

الدراسات السابقة

معظم الدراسات السابقة التي تناولت جرائم المعلوماتية لم ترتكز بشكل كبير على إثبات مثل هذا النوع من الجرائم، بل تناولت هذا الجانب بشكل موجز ومختصر. وقد تم ذكر العديد من المراجع ذات العلاقة بجرائم المعلوماتية في قائمة المراجع لهذا البحث ويمكن الرجوع إليها عند الحاجة.

هدف البحث وأهميته

صاحب التطور الكبير الذي شهده العالم تطوراً كبيراً في وسائل الاتصال تمثل في الاستخدام الكبير للحاسب الآلي وشبكة الإنترنت. إلا أن هذا التطور صاحبه انتشار كبير في جرائم الحاسب الآلي والإنترنت، مما جعل نصوص قانون العقوبات والإجراءات الجنائية التقليدية عاجزة عن مواجهتها والتصدي لها.

وهذه الجرائم تثير عدداً من الصعوبات من ناحية إكتشافها وصعوبة إثباتها. كما أنها لا تترك آثاراً خارجية، ويشكل انعدام الدليل عقبة كبيرة أمام كشف هذا النوع من الجرائم، كما أن سهولة مسح الدليل في وقت قصير تعد من أهم الصعوبات التي تواجه إثبات مثل هذا النوع من الجرائم، كما يمكن إرتكاب مثل هذا النوع من الجرائم من مسافات بعيدة، فقد يكون مرتكب الجريمة في دولة، ويرتكب جريمته في دولة أخرى. هذا فضلاً عن مسألة صعوبة ملاحقة مرتكبي مثل هذا النوع من الجرائم إذا ما كانوا يقيمون في دولة أخرى لا تربطها إتفاقيات بالدولة التي تحققت فيها الجريمة أو جزء منها، كما تثور مسائل تتعلق بصعوبات تعود للإختصاص القضائي مما يحد من إمكانية إثبات مثل هذا النوع من الجرائم، ولا شك أن معالجة هذه العقبات والصعوبات وحلها سيساهم إلى حد بعيد في إثبات جرائم المعلوماتية ومعاقبة مرتكبيها وبالتالي الحد من ارتكاب مثل هذا النوع من الجرائم. وهو ما نهدف إلى تحقيقه في هذا البحث ونأمل أن نوفق فيه.

خطة البحث

سوف يقسم هذا البحث إلى:

المبحث الأول: مفهوم الدليل الإلكتروني وخصائصه وشروطه.

المبحث الثاني: تفتيش وضبط الدليل الإلكتروني وإجراءات استخلاصه والتعامل معه.

المبحث الثالث: الصعوبات التي تواجه إثبات الجرائم المعلوماتية.

المبحث الرابع: حجة الدليل الإلكتروني في بعض التشريعات الوطنية.

وسوف ننهي البحث بخاتمة نستعرض فيها النتائج والتوصيات.

منهج البحث

يعتمد هذا البحث على أسلوب الدراسة التحليلية بالاعتماد على المراجع العلمية القانونية والنصوص القانونية والنظامية ذات العلاقة في المملكة وبعض القوانين المقارنة.

المبحث الأول: مفهوم الدليل المعلوماتي وخصائصه وأنواعه وشروطه

سيتضمن هذا البحث تحديداً لمفهوم الإثبات الجنائي وتعريف الدليل الإلكتروني إضافة إلى خصائص الدليل الإلكتروني وأنواع المخرجات الحاسوبية وشروط قبول الدليل الإلكتروني وذلك في خمسة مطالب على النحو التالي:

المطلب الأول: مفهوم الإثبات الجنائي

يقصد بالإثبات الجنائي إقامة الدليل لدى السلطات المختصة بالإجراءات الجنائية على حقيقة واقعة ذات أهمية قانونية. وذلك بالطرق التي حددها القانون ووفق القواعد التي أخضعها لها. (حسني، ١٩٨٨).

أما الدليل فيعرف على أنه «تحقق أو برهان من أجل معرفة القضاء لحقيقة حجج معينة تثبت على سبيل القطع والجزم حدوث واقعة يترتب عليها نتائج قانونية[(١)]».

ويتضح لنا من التعريفين السابقين ضرورة فهم الإثبات بمعناه الواسع الذي يجمع مجمل الأفكار والقواعد العامة المتعلقة بالبحث عن الأدلة وإقامتها أمام القضاء، وتقديرها من جانبه، وأن مهمة قواعد الإثبات هي تحديد ما هو واجب وما هو جائز وما هو غير مشروع في هذه الأدلة.

المطلب الثاني: تعريف الدليل الإلكتروني

يمكن تعريف الدليل الإلكتروني بأنه «الدليل الذي يجد له أساساً في العالم الافتراضي ويقود إلى الجريمة». (يونس، ٢٠٠٤؛ إبراهيم، ٢٠٠٩) فهو ذلك الجزء المبني على الاستعانة بتقنية المعالجة التقنية للمعلومات، والذي يؤدي إلى إقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة باستخدام الحاسب الآلي وشبكة الإنترنت.

كما عرف البعض الآخر الدليل الإلكتروني بأنه «الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتقنية خاصة وهي

---

(١) كما يمكن النظر إلى الإثبات من خلال النتيجة التي يسفر عنها الدليل وهي إما الإدانة أو البراءة، كما يمكن النظر إليه من زاوية طرق الإثبات أو الوسائل التي يتوصل بها أطراف الدعوى لإثبات حقيقة واقعة معينة، كما يمكن النظر إلى الإثبات من ناحية إقامة الأدلة، أي البحث عنها وتقديمها إلى جهات التحقيق والمحاكم. أي وضع العناصر التي تبنى عليها الواقعة من حيث حدوثها ونسبتها إلى الجاني تحت نظر المحكمة، وهو ما يتضمن إجراءات البحث عن الأدلة وهو ما يقتضي ويتطلب مشروعية تلك الأدلة.
انظر: (إبراهيم، ٢٠٠٩: ص ٢٧٤ وما بعدها)، و(فضل، ٢٠٠٧: ص ٣٥١ وما بعدها.

مكون رقمي لتقديم بيانات ومعلومات في أشكال متنوعة كالنصوص المكتوبة أو الصور أو الأشكال والأصوات والرسوم وذلك من أجل الاستناد إليه واعتماده أمام القاضي المختص». (إبراهيم، ٢٠٠٩؛ Rossein, 2010)

ومن ثَم فإن الدليل الإلكتروني هو أي بيانات أو معلومات يتم استخلاصها من جهاز الحاسب الآلي وبشكل يمكن قراءته وتحليله بالاستعانة بأشخاص لديهم القدرة والمهارة على ذلك وبالاستعانة ببرامج الحاسب الآلي.

المطلب الثالث: خصائص الدليل الإلكتروني

هناك عدد من الخصائص التي تميز الدليل الإلكتروني عن غيره نوردها على النحو الآتي:

أولاً: الدليل الإلكتروني دليل علمي تقني

فهو يحتاج إلى بيئة تقنية يتكون فيها لكونه من طبيعة تقنية المعلومات. والدليل الإلكتروني ليس بدليل مرئي يمكن فهمه واستيعابه بمجرد قراءته، ويتمثل في بيانات ومعلومات غير مرئية. وتبدو هذه المشكلة بشكل خاص بالنسبة لجرائم الحاسب الآلي والإنترنت مثل الجرائم التي يستخدم البريد الإلكتروني في ارتكابها، إذ يكون من الصعوبة على جهات التحقيق تحديد مصدر إرسال البريد الإلكتروني، ومن ثَم فإنه لا وجود لدليل إلكتروني خارج بيئته الرقمية أو الإلكترونية، وهي في إطار جرائم الحاسب الآلي والإنترنت تتمثل في العالم الافتراضي أو الرقمي (Virtual World) وهو العالم المكون من أجهزة الحاسب الآلي والخوادم والمضيفات والشبكات. (فضل، ٢٠٠٧؛ إبراهيم، ٢٠٠٩).

ونتيجة للطبيعة العلمية والتقنية للدليل الإلكتروني فإنه يمتاز عن الدليل المادي التقليدي المأخوذ من مسرح الجريمة التقليدي بما يلي:

١- يستطيع المحققون باستخدام التطبيقات والبرامج المخصصة لهذا الغرض تحديد ما إذا كان الدليل الرقمي، قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل. (إبراهيم، ٢٠٠٩؛ حجازي، ٢٠٠٧).

٢- صعوبة محو أو إزالة الدليل الإلكتروني، حتى في حالة قيام الجاني بإصدار أمر إزالته من جهاز الحاسب الآلي، فيمكن استرجاعه مرة أخرى بوسائل تقنية معينة في أحيان كثيرة، بل أن حتى محاولة الجاني محو أو إزالة الدليل يسجل كدليل أيضاً، حيث أن محاولة الجاني تلك يتم تسجيلها في ذاكرة الحاسب الآلي ويمكن استخدامها كدليل إثبات في مواجهته.

٣- إمكانية إحتواء الدليل الإلكتروني على سعة تخزينية عالية، فديسك أو فلاش صغير يمكنه تخزين آلاف الصفحات والصور الرقمية.

٤- يمكن عن طريق الدليل الرقمي تسجيل معلومات عن الجاني وبالتالي تحليلها واستخدامها كدليل إدانة ضده. (حجازي، ٢٠٠٧؛ إبراهيم، ٢٠٠٩).

ثانياً: الدليل الإلكتروني متنوع

فالدليل الإلكتروني يشمل كافة أنواع وأشكال البيانات والمعلومات الممكن تداولها إلكترونياً ويشمل هذا التنوع في البيانات الإلكترونية الرقمية مظاهر عدة، كأن يكون هذا المحتوى معلومات متنوعة قد تتضمن نصوصاً أو صوراً أو بيانات أو أصوات سمعية، فالعالم الرقمي عالم متجدد ومتطور ولا حدود له، وبالتالي فإن الدليل الإلكتروني هو الآخر دليل متنوع ومتطور. (فضل، ٢٠٠٧؛ إبراهيم، ٢٠٠٩).

المطلب الرابع: أنواع الأدلة الإلكترونية في الجرائم المعلوماتية

يمكن تقسيم الأدلة التي يتم ضبطها والتحفظ عليها في الجرائم المعلوماتية والتي لها قيمة في إثبات تلك الجرائم إلى ثلاثة أنواع على النحو الآتي:

١- الأدلة الورقية

قد ينتج عن الجريمة المعلوماتية أوراقاً أو مستندات ناتجة عن استخدام الحاسب الآلي وشبكة الإنترنت في ارتكاب الجريمة، فقد يقوم الجاني بطباعتها وذلك لأغراض المراجعة للتأكد من تنسيق الوثيقة أو المستند المستخدم في ارتكاب الجريمة. ويستخدم الجاني في ذلك الطابعات (Printers)، للقيام بنسخ البيانات والمعلومات، مثل التقارير المالية وغيرها. وتلك البيانات أو البرامج قد تكون مخزنة بالحاسب الآلي أو متاحة على شبكة الإنترنت. والأوراق تعد من الأدلة التي يجب منحها الاهتمام عند القيام بالمعاينة لمسرح الجريمة والتفتيش عن الأدلة المتعلقة بالجريمة[٢].

٢- جهاز الحاسب الآلي المستخدم في الجريمة وملحقاته

يعد وجود جهاز الحاسب الآلي وفحصه فحصاً دقيقاً في غاية الأهمية للقول بأن الجريمة الواقعة هي جريمة معلوماتية أو حاسوبية، وأن الجريمة مرتبطة بالمكان أو الشخص الحائز لجهاز الحاسب الآلي. ويمكن للمتخصصين في مجال الحاسب الآلي تمييز نوع الحاسب الآلي المستخدم في ارتكاب الجريمة وسرعته وأسلوب التعامل معه في حالة ضبطه وتحريزه. حيث أن أجهزة الحاسب الآلي تتفاوت من حيث سرعتها في معالجة البيانات، وقدرتها على تخزين البيانات والمعلومات واسترجاعها عند الحاجة، وكذلك قدرتها على القيام بالمسائل والعمليات المختلفة. وكلما كانت هذه الأجهزة أكثر تطوراً من الناحية التقنية، فإن ذلك سيساعد مرتكب الجريمة المعلوماتية على ارتكاب جريمته. ويمكن فحص أجهزة الحاسب الآلي العائدة للمتهم والمجنى عليه وخاصة وحدة التخزين الدائمة والوحدات الفرعية الملحقة وتشمل القرص المرن وأقراص الليزر وأية وحدة تخزين أخرى يمكن استخدامها من قبل الجاني مثل الفلاش (Flash Memory) وغيرها. وكل هذه الأجهزة يمكن فحصها وتحديد الوسيلة والطريقة التي اتبعها الجاني في ارتكاب جريمته المعلوماتية. (منصور، ٢٠٠٩؛ إبراهيم، ٢٠٠٩)

ولا شك أن فحص جهاز الحاسب العائد للمجنى عليه يمكن المحقق من تتبع كيفية الدخول والوصول إلى المصدر الذي استخدمه الجاني في ارتكاب جريمته. والمجنى عليه قد يكون شخصاً طبيعياً أو معنوياً كمؤسسة أو شركة أو هيئة حكومية أو غيرها.

---

(٢) ومن هذه الأوراق:

أ) أوراق تحضيرية للجريمة يتم إعدادها بخط اليد كمسودة للتخطيط للجريمة المعلوماتية وكيفية ارتكابها أو تتضمن خطوات إرشادية لكيفية ارتكاب الجريمة المعلوماتية.

ب) أية أوراق تمت طباعتها للتأكد من تمام الجريمة.

ج) أية أوراق أصلية يطبعها الجاني ويحتفظ بها كمرجع أو لارتكاب الجريمة.

د) أية أوراق ذات علاقة بالجريمة أو أوراق يستخدمها الجاني عند تقليد أو تزوير هذه الأوراق باستخدام الحاسب الآلي. انظر: (عبدالله، ٢٠٠٧: ص ٤٦ وما بعدها؛ حجازي، ٢٠٠٩: ص ١٥ وما بعدها).

انظر أيضاً: (Burke, 2010: 15).

ومن الأجزاء التي تستخدم في تخزين البيانات والمعلومات في الحاسب الآلي:

١ - الأقراص المغناطيسية (Magnetic Disks)

وتعد الأقراص المغناطيسية من أفضل أنواع الوسائط (Mediums) والتي يمكن استخدامها في تخزين البيانات والمعلومات، وتتميز بإمكانياتها وقدراتها التخزينية العالية وسرعة تداول المعلومات التي تخزن عليها، ومن أهم الخصائص التي تميز الأقراص المغناطيسية إمكانية تعديل أي ملف مخزن عليها دون الحاجة إلى إنشاء ملف جديد.

٢ - الأقراص المرنة (Floppy Disks)

وتستخدم الأقراص المرنة لتخزين الملفات التي لا تحتاج حجم تخزين عالي، لأن قدرتها التخزينية منخفضة، وهي قابلة للتلف بشكل أسرع وأسهل من وسائل تخزين المعلومات الأخرى. ويمكن مسح البيانات من القرص وإعادة تخزينها مرات عدة دون أن يفقد القرص المرن كفاءته. (إبراهيم، ٢٠٠٩؛ فضل، ٢٠٠٧؛ حجازي، ٢٠٠٧)

٣- الأقراص الصلبة (Hard Disks)

وهي عبارة عن أقراص معدنية رقيقة ومغطاة بمادة ممغنطة، علماً بأن طبقة التغطية المغناطيسية لهذه الأقراص تتم على سطح صلب مصنوع من سبائك الألمنيوم ومن هنا جاءت تسميتها بالأقراص الصلبة، والأقراص الصلبة هي من أكثر وحدات التخزين استخداماً لسرعتها وكفاءتها العالية، إضافة إلى قدراتها التخزينية العالية التي توفرها، وتكون عادة مركبة داخل حافظة جهاز الحاسب الآلي (Case) نظراً لحجمها الكبير.

٤ - أقراص الليزر (CD rom)

وتمتاز هذه الأقراص بالسعة التخزينية العالية، ولكنها أقل في قدراتها التخزينية وسرعتها من الأقراص الصلبة، وتبدو أهمية هذه الأقراص في الجرائم المعلوماتية في وجود عدد كبير من هذه الأقراص عامة مع جهاز الحاسب الآلي للمتهم، وعادة ما يدون الأشخاص على غلاف هذه الأقراص بيانات توضح محتوياتها، ويفترض بالمحقق الاستعانة بخبير مختص في الحاسب الآلي ليقوم بإفراغ هذه الأقراص والحصول على الأدلة المتمثلة في البيانات والمعلومات المتحصلة من هذه الأقراص لتقديمها أمام جهات التحقيق أو القاضي[٣].

٥ - أقراص الكارتريج (Cartridge Disks)

وهي أقراص تجمع بين خصائص القرص الصلب من حيث القدرة التخزينية الكبيرة وبين القرص المرن من حيث إمكانية تغييره من مكانه بقرص آخر. (حجازي، ٢٠٠٧).

وتناولنا السابق لمكونات الحاسب الآلي التخزينية إنما هو توضيح للآثار التي تنتج عن الجرائم المعلوماتية عادة، أو هي جزء من ماديات ومكونات الجرائم المعلوماتية التي ينبغي على المحقق البحث عنها وفحصها، واستخدامها في التحقيق لغرض إثبات أدلة الإدانة أو

---

(٣) ولا يشترط في جرائم الحاسب الآلي والإنترنت أن يتم ضبط وتحرير أقراص الليزر مع جهاز الحاسب الآلي الشخصي للمتهم، فقد يتم ضبطها وتحريزها في مكان آخر، ولكن ذلك لا يمنع ولا يحد من اعتبارها جزءاً لا يتجزأ من ماديات ومكونات الجريمة أو الأدلة اللازمة لإثباتها ما دامت محتوياتها تشكل عنصراً من عناصر الجريمة. انظر: (حجازي، ٢٠٠٧: ص ٢١ وما بعدها).

النفي. وهو ما يحتاج إلى خبرة فنية كبيرة لا تتوافر إلا لمختص وخبير في مجال الحاسب الآلي والإنترنت.

المطلب الخامس: شروط قبول الدليل الإلكتروني

١- أن تكون هذه الأدلة يقينية

أي أن لا تكون ظنية وأن تقترب من الحقيقة قدر الإمكان. ويترتب على ذلك أن كافة مخرجات الوسائل الإلكترونية من مخرجات ورقية أو إلكترونية أو أقراص مغناطيسية (CD) أو غيرها تخضع لتقدير المحكمة ويجب أن تقوم المحكمة باستنتاج الحقيقة منها بما يتفق مع اليقين ويبتعد عن الشك والظن.

٢- أن تكون هذه الأدلة قد تم التحصل عليها بطرق مشروعة

أي أن تلك الأدلة الإلكترونية قد تحصل عليها ضمن أطر المشروعية[٤] أي وفقاً لأحكام ونصوص القانون. فمبدأ المشروعية يقتضي عدم قبول أي دليل تم الحصول عليه بشكل غير مشروع. وبالتالي فإن أي دليل تم الحصول عليه بشكل مخالف للقانون يجب أن يستبعد ولا يؤخذ به. فالإدانة في أي جريمة يجب أن تُبنى على أدلة مشروعة.

٣- أن تكون هذه الأدلة ذات علاقة بموضوع الجريمة

أي أن تكون هناك علاقة بين الدليل المتحصل وبين الواقعة محل الدعوى. كما يشترط مطابقة الدليل الإلكتروني المستخلص من الحاسب الآلي للأصل الموجود بداخله. بحيث لا يكون هناك دفع بأن المعلومات أو البيانات غير صحيحة أو غير دقيقة بسبب عدم صحة أو عدم دقة عمل الحاسب الآلي. كما يتعين مناقشة هذه الأدلة في المحكمة إعمالاً لمبدأ شفوية المحاكمة. فمخرجات الوسائل الإلكترونية تعد أدلة إثبات قائمة في أوراق الدعوى التي ينظرها القاضي، ولكن لا بد أن يسمح القاضي بمناقشتها في حضور الخصوم في الدعوى حتى يمكن الاعتماد عليها كأدلة أمام المحكمة. (منصور، ٢٠٠٩؛ إبراهيم، ٢٠٠٩).

٤- أن تكون هذه الأدلة قد تمت مناقشتها في المحاكمة الجنائية

وهذا من المبادئ الأساسية في الإجراءات الجنائية، فلا يصح أن يأخذ القاضي بدليل قدمه أحد الخصوم إلا إذا عرضه بشكل شفوي وعلني في جلسة المحاكمة بحيث يعلم به الخصوم الآخرين فتتاح لهم مناقشته والرد عليه إن شاؤوا أو أن يبدو رأيهم في قيمته الإثباتية. ويستطيع القاضي بناء على هذه المناقشات بين الخصوم أن يصل إلى تكوين عقيدته بخصوص قيمة هذا الدليل الإثباتية. وقد نص قانون الإجراءات الجنائية الفرنسي في الفقرة (٢) من المادة (٤٢٧) منه على أنه «لا يجوز للقاضي أن يؤسس حكم إلا على أدلة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الأطراف». كما نص نظام الإجراءات الجزائية السعودي في المادة (١٤٢) منه على أنه «إذا رفعت الدعوى على عدة أشخاص في واقعة واحدة وحضر بعضهم وتخلف بعضهم رغم تكليفهم بالحضور فيسمع القاضي دعوى المدعي وبيناته على الجميع. ولا يحكم على الغائبين إلا

(٤) ويستلزم مبدأ المشروعية عدم قبول أي دليل يكون تم الحصول عليه بطريقة غير مشروعة، فحرية القاضي في تكوين عقيدته في الإثبات لا يعني قبول الدليل بأية طريقة تم الحصول عليه، بل أن ذلك مقيد بالالتزام بالنصوص القانونية وبالتالي فإن الدليل الذي يتم الحصول عليه بشكل غير مشروع يكون باطلاً. انظر: (فضل، ٢٠٠٧: ص ٣٧١؛ إبراهيم، ٢٠٠٩: ص ١٨٩ وما بعدها).

بعد حضورهم». وهذا يدل على أن المنظم السعودي أكد على حق الخصوم في معرفة جميع الأدلة المقدمة ضدهم حتى يستطيعوا تفنيدها والرد عليها إن شاؤوا أو القبول بها إن أرادوا ذلك(٥).

المبحث الثاني: تفتيش وضبط الدليل الإلكتروني وإجراءات استخلاصه والتعامل معه

سنبين في المطلب الأول من هذا المبحث كيفية التحضير للقيام بالتفتيش والضبط للدليل الإلكتروني، ثم نتناول في المطلب الثاني كيفية التعرف على أماكن وجود الدليل الإلكتروني، ثم سنتطرق في المطلب الثالث لكيفية القيام بالتفتيش والضبط في الأدلة الإلكترونية، ثم سنتناول في المطلب الرابع إجراءات استخلاص الدليل الإلكتروني. أما في المطلب الخامس فسنتطرق إلى قواعد التعامل مع الأدلة الإلكترونية. ثم سنتطرق في المطلبين السادس والسابع إلى البرامج المستخدمة في جمع الأدلة الإلكترونية والأنظمة التي يجب على المحقق فحصها للحصول على الدليل الإلكتروني.

المطلب الأول: شروط تفتيش وضبط الدليل الإلكتروني

حتى يمكن استخدام الدليل الإلكتروني الذي تم التحصل عليه من الحاسب الآلي المضبوط يجب أن يتوافر إذن قانوني صحيح ونافذ أو أن يكون هناك استثناء من هذا الإذن كما في حالات التلبس مثلاً. كما يجب على المحقق استخدام طرق تحصيل الأدلة المناسبة حتى لا يتلف أو يغير الدليل. ويستعين المحقق في ذلك بخبراء مختصين في مجال الحاسب الآلي وجرائم الحاسب الآلي. (Tegland,2010, Overly, 2010).

المطلب الثاني: التعرف على أماكن وجود الدليل الإلكتروني

يمكن أن يكون جهاز الحاسب الآلي هو محل جريمة السرقة، أو أنه تم استخدامه في ارتكاب جرائم معلوماتية، أو أنه مستودع تخزين الأدلة التي تدين الجاني في الجرائم المعلوماتية بارتكاب جرائمه. وقد تكون هذه الأدلة مخزنة في جهاز «بلاكبيري» (Blackberry) مثلاً أو قرص مرن (Floppy Disk) أو قرص صلب أو سي دي (CD) أو شريحة إلكترونية صغيرة (Electronic Chip) ومن السهولة على الجاني أن يعدل أو يغير أو يتلف أي صور أو كتابة أو صوت أو أية بيانات أو معلومات مخزنة على تلك الوسائط. ويجب بالتالي على المحقق أو الخبير وكذلك رجال الشرطة أن يقوموا بحماية وتحريز وتفتيش وقبل ذلك التعرف على هذه الأجهزة وفقاً للاشتراطات القانونية ووفقاً لأفضل الممارسات المهنية. ويجب أولاً التعرف على محل جريمة السرقة. وهل كان الحاسب الآلي هو محل جريمة السرقة أم أن المسروق هو برامج هذا الحاسب الآلي؟ أم هل استخدم الحاسب الآلي من قبل الجاني في ارتكاب جرائم؟ وهل تم استخدام بطاقات هوية مزورة أو مسروقة في ارتكاب الجريمة؟ أو أن الحاسب الآلي المسروق قد استخدم في تزوير بطاقات هوية أو مستندات مزورة؟ وينطبق هذا الأمر أيضاً على الماسحات (Scanners) والطابعات الملونة (Colored Printers) وهل تم استخدامهم في ارتكاب الجرائم بواسطة الجاني؟ أم أن الحاسب الآلي استخدمه الجاني فقط في تخزين البيانات والمعلومات فقط؟ كما هو الحال لو خزن تاجر مخدرات أسماء زبائنه وأرقام هواتفهم في حاسبه الآلي مثلاً. أم أن الجاني

---

(٥) نظام الإجراءات الجزائية السعودي، الصادر بقرار مجلس الوزراء رقم (م/ ٣٩) وتاريخ ٢٨/ ٧/ ١٤٢٢هـ والمرسوم الملكي رقم م/ ٣٩ وتاريخ ٢٨/ ٧/ ١٤٢٢هـ. انظر أيضاً: (فضل، ٢٠٠٧: ص ٣٧٣ وما بعدها).

استخدم هذا الحاسب في اختراق موقع بنك مثلاً وقام بسرقة معلومات ائتمانية عائدة لعملاء هذا البنك وقام بتخزينها في حاسبه الآلي أيضاً، وبالتالي يعد هنا الحاسب الآلي أساسياً في ارتكاب الجريمة وفي تخزين المعلومات المسروقة وهي الدليل الإلكتروني هنا.

وهنا تبرز مسألة هامة وهي هل سيقوم المحقق بتفتيش جهاز الحاسب الآلي في مكان وجوده أم أنه سيقوم بنقله إلى المعمل الجنائي للقيام بهذا الفحص والتفتيش؟ وتبرز مسألة هامة أخرى وهي هل يعيد المحقق جهاز الحاسب الآلي وبرامجه والملفات المتعلقة به لمالكه أم لا؟ وهل يفعل ذلك قبل المحاكمة أم بعدها؟ هذه كلها أسئلة هامة تعتمد في إجابتها إلى ما تقرره القواعد الإجرائية المنظمة للتحقيق وظروف القضية وهي تتفاوت من قضية لأخرى والإجابة عليها تعتمد على ما يراه المحقق محققاً لمصلحة القضية في الدرجة الأولى ثم مصلحة الأطراف في الخصومة. (Overly, 2010 ; Mauet, 2009).

المطلب الثالث: القيام بالتفتيش والضبط في الأدلة الإلكترونية

عند القيام بتفتيش الحاسب الآلي أو ضبطه يجب على المحقق الالتزام بالأمور التالية:

١- حماية مسرح الجريمة (Crime Scene)

يجب على المحقق، عند وصوله إلى مسرح الجريمة (المكان الذي يوجد فيه الحاسب الآلي) منع الأشخاص غير المصرح لهم بدخول مسرح الجريمة والذين قد يفسدوا الدليل، كما يجب على المحقق القيام بتوثيق مسرح الجريمة ومواقع جمع الأدلة والحالة التي وجدت عليها، كما يجب عليه أخذ البصمات من مسرح الجريمة وجهاز الحاسب الآلي.

٢- حماية جهاز الحاسب الآلي والأجهزة المرتبطة به والأدلة الناتجة عنه

وينبغي على المحقق عند وصوله إلى مسرح الجريمة المعلوماتية أن يقوم بتوزيع المسئوليات للقيام بالتفتيش، ومن الضروري أن يكون لدى المحقق ومعاونيه فهم للأشياء التي قد يعثروا عليها وكيفية التعامل معها. وعند القيام بالتفتيش يجب على المحقق أن يضع في اعتباره أنه قد لا يجوز له التفتيش أو الضبط في أماكن معينة لم ينص عليها في إذن التفتيش. وإذا استدعت الظروف تفتيش أشياء أو أماكن غير مذكورة في إذن التفتيش فيجب هنا استصدار إذن جديد أو تعديل الإذن الصادر. (حجازي، ٢٠٠٧؛ موسى، بدون تاريخ)

ويجب على المحقق تصوير مسرح الجريمة وجهاز الحاسب الآلي وجميع الأجهزة المرتبطة به ويجب أن يحدد ما إذا كان من الممكن إقفال جهاز الحاسب الآلي ويجب على المحقق أن يستعين بالخبير في تحديد ذلك. وإذا أقفل الجهاز فيجب أن يدرك المحقق أن إطفاءه للجهاز يمكن أن يؤدي إلى ضياع المعلومات المخزنة فيه، وهنا يجب على المحقق عمل نسخة احتياطية (Backup) للملفات المخزنة في الحاسب الآلي. كما يجب عليه وضع شريط لاصق خاص بالأدلة على فتحات جهاز الحاسب ضماناً لعدم إدخال أو إخراج أي شيء فيه أو العبث بالأدلة المخزنة فيه. ويجب على المحقق أيضاً وضع ملصقات لتمييز أجهزة الحاسب في حال تعددها. كما يجب عليه نقل المضبوطات بحرص تام لإتمام عملية التحريز على النحو الصحيح. كما يجب على المحقق إبقاء جميع المضبوطات بعيدة عن التأثيرات المغناطيسية وغيرها من الظروف البيئية والتخزينية المؤذية للديسكات

والفلاشات المضبوطة وغيرها من الأجهزة المرتبطة بعمل الحاسب الآلي المضبوط.

وعند وصول الحاسب الآلي وملحقاته إلى المعمل الجنائي يجب تفريغ هذا الجهاز بحرص شديد. ويجب على المحقق التأكد من وجود جميع المحتويات حسب ما دون في سجل النقل. كما يجب توثيق تاريخ ووقت وصول المواد واسم الشخص المسؤول عن استلامها وتفريغها. كما يجب على المحقق التأكد من عدم حصول أي عبث أثناء نقل تلك الأجهزة. (حجازي، ٢٠٠٧؛ موسى، ٢٠٠٩؛ Overly, 2010).

المطلب الرابع: إجراءات استخلاص الدليل الإلكتروني

تتمثل إجراءات استخلاص الدليل الإلكتروني وتقديمه للنيابة العامة والقضاء في عدة مراحل نوردها كالآتي:

١- مرحلة إعداد المعدات المستخدمة في استخلاص الدليل الإلكتروني

وتتمثل هذه المرحلة في عدد من الإجراءات التحضيرية قبل ضبط الدليل الإلكتروني وتشمل الحصول على الإذن بالتفتيش للحاسب الآلي والمعدات المرتبطة به، وضبط وفحص الحاسب الآلي محل التفتيش. والالتزام بهذه الإجراءات يجنب المحقق طعن المتهم ببطلان الدليل أو عدم مشروعيته لعدم إتباع الإجراءات القانونية. كما تتضمن هذه المرحلة توثيق الأدلة الإلكترونية للتحقق من صحة ومشروعية الإجراءات المستخدمة لاستخلاص الدليل الإلكتروني.

وتشكل عملية التوثيق والتدقيق للدليل الإلكتروني جزءاً من الاختبار والفحص (Examination) بخصوص تتبع أو تعقب جميع النشاطات المؤثرة على البيانات والمعلومات. وتشمل عملية التوثيق والتدقيق الزمان والمكان الذي تم فيه التعامل مع الملف المحتوي للدليل الإلكتروني وتنزيل البيانات محل الاتهام. كما تشمل على ضمان تشغيل جهاز الحاسب الآلي بالطريقة الفنية الصحيحة، والتحقق من عدم وجود وسائل حماية على برامج الحاسب الآلي محل التفتيش من شأنها إعاقة الوصول إلى الدليل الإلكتروني. (موسى، بدون تاريخ؛ عبدالمطلب، ١٤٢٨).

٢- مرحلة استخلاص وضبط الدليل الإلكتروني

يجب تحديد كيفية تسليم وتسلم الدليل الإلكتروني وقت نقل الحيازة الفعلية له حيث تنتقل بموجب هذا التحديد مسئولية التعامل مع هذا الدليل الإلكتروني من المتهم إلى الشرطة والمحقق. ويجب على المحقق عمل نسخ للملفات الموجودة في القرص الصلب وحفظها في الأرشيف. (موسى، بدون تاريخ؛ عبدالمطلب، ١٤٢٨) كما يمكن الاستعانة بمزودي خدمة الإنترنت (Internet Providers) في الحصول على الأدلة الإلكترونية. وهذه الشركات كشركة جوجل (Google) وياهو (Yahoo) ونيت سكيب (Netscape) وإم إس إن (msn) وغيرها من مزودي خدمة الإنترنت تقوم بتحميل بيانات مستخدميها ومن ثم يمكن الاستعانة بمثل هذه الشركات للوصول إلى مرتكبي الجرائم المعلوماتية. كما يمكن الرجوع إلى البريد الإلكتروني (e-mail) للتعرف على بيانات المستخدم وبالتالي تحديد هوية المتهم عن طريق الرجوع إلى الرسائل المرسلة منه، ومن ثم تحديد المكان الذي تم إرسال الرسالة الإلكترونية منه. (إبراهيم، ٢٠٠٩).

٣- مرحلة حماية الدليل الإلكتروني

يجب على المحقق أو الخبير أن يقوم بحماية الدليل الإلكتروني لأن ذلك من شأنه منع الطعن بصحة الدليل أمام القضاء.

٤- مرحلة تقديم الدليل الإلكتروني أمام القضاء

وهذه المرحلة تتمثل في تقديم الدليل الإلكتروني الذي يتم التحصل عليه أمام المحكمة المختصة لتقرر رأيها فيه وفي صحته وتقرر إما أن تعتمد عليه أو أن ترفضه. (موسى، بدون تاريخ؛ عبدالمطلب، ١٤٢٨؛ Rossein, 2010; Kotler, 2009).

المطلب الخامس: قواعد التعامل مع الأدلة الإلكترونية

ينبغي على الخبير أو المحقق المكلف بالتفتيش أو التحقيق في الجرائم الإلكترونية أن يتبع القواعد الآتية عند تعامله مع الأدلة الإلكترونية:

١- أن يتجنب تدمير أو إتلاف الدليل الإلكتروني بشكل غير مقصود، فتشغيل المحقق أو الخبير للحاسب الآلي العائد للمتهم أو للمجنى عليه أو تشغيل أحد البرامج المخزنة عليه من الممكن أن يؤدي إلى تغيير أو إتلاف، أو العبث بمحتوى الدليل الإلكتروني. ويفترض بالمحقق أو الخبير أن يصنع نسخة من القرص الصلب قبل تشغيل الحاسب الآلي.

٢- أن يقوم المحقق أو الخبير بتوثيق نظام الحاسب الآلي بشكل عام. أي تحديد نوع جهاز الحاسب الآلي ونظامه التشغيلي (Operating System)، ونوعية البرامج المستخدمة فيه (Software) والتي تم استخدامها في صنع الدليل. كما ينبغي على المحقق أو الخبير إجراء فحص يدوي على نظام الحاسب الآلي (Physical inspection) وأخذ صور لهذا النظام بما في ذلك أي أجهزة أو معدات مرتبطة بنظام الحاسب الآلي محل التحقيق. (Tegland, 2010; Overly, 2010).

٣- يجب على المحقق أو الخبير أن يحافظ على الدليل الإلكتروني في حرز مغلق مناسب ضماناً لعدم العبث به أو تعديله أو تغييره بأي شكل من الأشكال. وحتى لا يتم الدفع من المتهم بأنه تم العبث بهذا الدليل.

٤- يجب على المحقق أو الخبير أن يتنبه لمسألة وجود فيروسات في الدليل الإلكتروني والذي من الممكن أن يؤدي إلى إفساد أو إتلاف الدليل ويجب استعمال برامج مضادة للفيروسات للتحقق من عدم وجود فيروسات في البرامج الحاسوبية التي يتم فحصها.

٥- يجب على المحقق أو الخبير أن يقوم بنقل وتعزيز الدليل الإلكتروني بشكل جيد وبحرص شديد حيث أن العوامل البيئية وظروف التخزين ممكن أن تؤثر بشكل سلبي على الدليل الإلكتروني، حيث أن الحرارة والمجالات المغناطيسية، والدخان، والرطوبة، كل هذه العوامل ممكن أن تؤدي إلى تلف الدليل الإلكتروني. فمجرد وضع القرص المرن (floppy disk) بالقرب من جهاز هاتف أو ستريو (Stereo) ممكن أن يعرض القرص المرن لموجات كهرومغناطيسية ممكن أن تؤدي إلى تلف هذا القرص المرن وبالتالي يصبح لا قيمة له.

٦- يجب على المحقق أن يستعين بخبير متمرس في مجال الحاسبات الآلية وشبكة الإنترنت. ويشترط في هذا الخبير أن يجمع بين المؤهل العلمي المناسب والخبرة العملية. ويجب على هذا الخبير أن يكون متقناً للغات البرمجة وأنظمة التشغيل الجديدة وتحليل البرامج وأنظمة التشغيل حتى يستطيع أن يصل إلى مصادر الأدلة الإلكترونية وحفظ هذا الدليل من التلف أو التدمير. (Carlson, 2010 ; Overly, 2010).

المطلب السادس: البرامج المستخدمة في جمع الأدلة الإلكترونية

١- برنـامج إذن التفتـيش (Computer Search Warrant Program)

وهـو برنـامج قـاعدة بيانات (Data Base)، يسمح بإدخال المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها. ويستطيع هذا البرنامج إصدار إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان وجود دليل معين أو تحديد الظروف المرتبطة بضبط هذا الدليل.

٢- قرص بدء تشغيل الحاسب الآلي (Bootable Diskette)

وهو قرص يمكن المحقق من تشغيل الحاسب الآلي، إذا كان نظام التشغيل فيه محمياً بكلمة مرور (Password)، ويجب أن يكون القرص مزوداً ببرنامج مضاعفة المساحة، لأن الجاني من الممكن أنه استخدم هذا البرنـامج لمضاعـفة مساحة القـرص الصلب. (Overly , 2010)

٣- برنامج النسخ (Copy Program)

وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الحاسب الآلي الخاص بالمتهم ونقلها إلى قرص آخر. وهذا البرنامج يفيد في الحصول على نسخة من المعلومات قبل أي محاولة لإتلافها من الجاني. ومن هذه البرامج على سبيل المثال برنامج (Lap Link)

٤- برنامج معالجة الملفات

وهو برنامج يمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يمكن المحقق أو خبير الحاسب الآلي من البحث عن أسماء ملفات معينة أو كلمات معينة.

٥- برامج كشف الديسك (مثل برنامج (AMA Disk, View Disk

ويمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن، مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد ونسخة خاصة بالشرطة ورجال الأمن. (Carlson, 2010)

٦- برامج اتصالات (مثل برنامج LAN TASTIC)

وهذا البرنامج يستطيع ربط جهاز الحاسب الآلي العائد للمحقق بجهاز الحاسب الآلي العائد للمتهم لنقل ما به من معلومات وبيانات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.

والطرق السابقة هي من أهم الطرق المتبعة لجمع وتحصيل الأدلة الإلكترونية. والتي يفترض بالمحقق وخبراء الحاسب الآلي القيام بها واستخدامها للوصول إلى تلك الأدلة نظراً لدقة هذه الأدلة والتقنية العالية التي يتم استخدامها في ارتكاب هذه الجرائم. (داود، ٢٠٠٠؛ Carlson, 2010)

المطلب السابع: الأجهزة والأنظمة التي يجب على المحقق فحصها للحصول على الدليل الإلكتروني

للحصول على الدليل الإلكتروني يوجد أنظمة يجب أن يقوم المحقق أو الخبير بفحصها. وهذا يتطلب أولاً أن يقوم المحقق أو الخبير بفحص نظام الاتصال بالإنترنت، وثانياً يجب أن يقوم المحقق أو الخبير بفحص مكونات الحاسب الآلي وذلك على النحو الآتي:

١ - فحص نظام الاتصال بشبكة الإنترنت وتتبع مسارها

ينبغي على المحقق أو الخبير أن يقوم بفحص نظام الاتصال بشبكة الإنترنت لغرض تحديد مكان ارتكاب الجريمة وجهاز الحاسب الآلي الذي استخدم في ارتكاب الجريمة وبالتالي تحديد هوية الجاني. ويقتضي ذلك قيام المحقق أو الخبير بفحص كل ما يتعلق بنظام الاتصال بشبكة الإنترنت، كالشبكات المحلية والعالمية والبيانات والنظام الأمني لشبكة الإنترنت ونظام الاتصالات القائم وبرمجيات الإنترنت. فالبحث في نظام البريد الإلكتروني مثلاً قد يؤدي إلى الوصول إلى دليل يفيد في إثبات الجريمة، كما لو كان مرتكب الجريمة قد قام بوضع نسخة من هذا الملف في خادم البريد الإلكتروني (e-mail server) عبر شبكة الإنترنت والخاص بهذا الشخص بحيث يمكنه الوصول إليه في أي وقت ومن أي مكان. (حجازي، ٢٠٠٩).

كما يجب على المحقق تتبع مسار شبكة الإنترنت أي الحركة التراسلية للنشاط الممارس من خلال الإنترنت. فالحاسب الآلي بمجرد تعرفه على المسار يقوم تلقائياً باختيار البروتوكول التراسلي الذي من خلاله يقوم باستدعاء البيانات. ويستخدم في تتبع مسار الإنترنت نظام الفحص الإلكتروني (Electronic Trail) وهو يستخدم في تتبع الحركة العكسية لمسار الإنترنت[٦].

وهناك رأيان في مسألة إمكانية تحديد مسار شبكة الإنترنت من عدمه، فيذهب رأي إلى أنه لا يمكن تحديد مسار ارتكاب الجريمة، ويستند هذا الرأي إلى أنه حتى وإن أمكن للمحقق أو الخبير تحديد مسار الإنترنت فإن ما يتحصل عليه هو دليل رقمي يحتاج إلى تكملته وتقويته بأدلة إثبات أخرى. إذ أنه لا يكفي وحده في الإثبات. ذلك أن ما يتوصل إليه من خلال الدليل الإلكتروني إنما هو عنوان إلكتروني فقط (IP Address) وهذا غير كافي في نسبة الفعل الإجرامي إلى مالك الحاسب الآلي. إذ من الجائز ألا يكون هو مرتكب الفعل الإجرامي كما لو كان جهاز الحاسب الآلي التابع له قد سُرق أو أنه كان مؤجراً (كما هو الحال في مقاهي الإنترنت مثلاً) أو قد يكون الفاعل الحقيقي قد مارس الاحتيال باستخدامه للعنوان الإلكتروني لشخص آخر، أما الرأي الثاني فيرى إمكانية تتبع مسار الإنترنت وبالتالي يمكن الوصول بواسطة هذا التتبع إلى تحديد مسار الفعل الإجرامي وبالتالي تحديد الفاعل.

٢ - فحص النظام الأمني للشبكات

ينبغي على المحقق أو الخبير فحص النظام الأمني للشبكات. وتعد الشبكات غير المحصنة بالتشفير (Encryption) أكثر عرضة للاختراق، وبالتالي فإن فحصها يتطلب وقتاً أكبر للحصول على دليل إلكتروني. في حين أن الشبكات المحصنة بالتشفير تكون ذات صعوبة أقل في الحصول على الدليل الإلكتروني. حيث أن الاختراق هنا يكون أكثر وضوحاً من خلال فحص حركة الدخول إلى الشبكة[٧].

---

(٦) وقد تم تطبيقه في أكثر من جريمة، مثل تتتبع مبتكر فيروس ميلسا (Melisa Virus). انظر: (إبراهيم، ٢٠٠٩: ص ٢٠٣ وما بعدها).
انظر أيضاً: (Hill, 2010. Qt 24-).

(٧) كما يمكن للمحقق أو الخبير استخدام خاصية التتبع التصفحي (ID Track Number) والتي تسمح لمن يطلع عليها معرفة العنوان الإلكتروني (IP Address)، ومن ثم تتبع مسار الشبكة التي تزود حركة التصفح، ومن ثم يستطيع الخبير الوصول إلى عنوان المشترك في الشبكة. انظر: (إبراهيم، ٢٠٠٩: ص ٢٠٨ وما بعدها).

٣- فحص بروتوكول شبكة الإنترنت

يجب على المحقق أو الخبير أن يبحث في قواعد البيانات لدى مسجلي بروتوكول الإنترنت. وأي شخص يحصل على بروتوكول الإنترنت يستطيع استخدام شبكة الإنترنت. ويستطيع المحقق أو الخبير أن يقوم بتحديد صاحب هذا البروتوكول بواسطة البحث في قاعدة البيانات الخاصة بالمسجلين في شبكة الإنترنت. كما يستطيع المحقق أو الخبير استخدام برامج خاصة متوافرة عبر شبكة الإنترنت تستطيع أن ترصد بروتوكولات شبكة الإنترنت.

٤ - فحص الخادم (Server)

يجب على المحقق أو الخبير أن يقوم بفحص الخادم (Server). والخادم هو حاسب ضخم وظيفته تحقيق حركة الاتصال بالمواقع والصفحات الإلكترونية. (موسى، بدون تاريخ؛ حجازي، ٢٠٠٧).

المبحث الثالث: الصعوبات التي تواجه إثبات الجرائم المعلوماتية

تتميز جرائم الحاسب والإنترنت بصعوبة اكتشافها وإثباتها، وترجع صعوبة إثبات تلك الجرائم إلى خصائص تقنية المعلومات ذاتها، وبشكل خاص السرعة الفائقة التي ترتكب بها، وهو ما يسهل عملية إرتكابها ويسهل طمس وتغيير معالمها ومحو آثارها قبل اكتشافها، إذ يستطيع الجاني أن يرتكب جريمته دون أن يترك أية آثار تدل عليه، وإذا كان هناك دليل أو أثر فيستطيع الجاني تدميره والتخلص منه خلال ثوان معدودة. فمرتكب هذه الجريمة يسعى إلى طمس وتدمير معالمها. إضافة إلى أن رغبة المجنى عليه في كثير من الأحيان في إخفاء مسألة ارتكاب الجريمة في حقه رغبة في حماية سمعته وإخفاء أسلوب ارتكاب الجريمة حتى لا تتفشى طريقة ارتكابها لآخرين، وهذا يدفع المجنى عليه إلى عدم الإبلاغ عن ارتكاب الجريمة والامتناع عن مساعدة السلطات المختصة في الكشف عن الجريمة وإثباتها وتعقب مرتكبيها. (هروال، ٢٠٠٧؛ فضل، ٢٠٠٧)

وسنتناول في هذا المبحث الصعوبات التي تعترض إثبات الجرائم المعلوماتية وذلك على النحو الآتي:

أولاً: امتناع المجنى عليه عن الإبلاغ عن الجريمة

يحرص المجنى عليه وخاصة إذا كان مؤسسة أو بنكاً أو شركة على إخفاء حقيقة تعرضه لإحدى الجرائم المعلوماتية كالإختراق أو السرقة أو الإحتيال أو الإتلاف أو غيرها من الجرائم المعلوماتية. ومن ثَم عدم بيان عدم قدرتها عن تحقيق أمن معلوماتها وبياناتها أو معلومات عملائها وبياناتهم، وبالتالي ما يؤدي إلى ضعف ثقة عملائها بقدرتها على حماية بياناتهم ومعلوماتهم وبالتالي أموالهم. فتكتفى تلك المؤسسات أو الجهات عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عن الجرائم التي تعرضت لها للجهات الأمنية المختصة. (رستم، ١٩٩٤؛ فضل، ٢٠٠٧) وفي إحدى الدراسات التي أجريت في الولايات المتحدة الأمريكية أظهرت نتائجها أن ٢٪ فقط من كل جرائم الحاسب الآلي والإنترنت هي التي يتم الإبلاغ فيها للسلطات المختصة. وفي دراسة أخرى تمت لهذا الغرض تبين أن المؤسسات والشركات تدخل في حسابها ضرورة الموازنة بين ضرورة الإفصاح عن الجرائم المرتكبة ضدها وبين ضرورة الحفاظ على سمعتها عند عملائها والخسائر التي قد تترتب على العلانية[٨].

---

(٨) انظر http:/ new, bbc.co.uk/90/pr/Arabic/world- news/ newsadi.stm.

انظر أيضاً: (حجازي، ٢٠٠٩: ص٦٨ وما بعدها).

كما أن تلك المؤسسات والشركات تدخل ضمن حساباتها أن الإبلاغ عن الجرائم المعلوماتية التي ترتكب ضدها قد يؤدي إلى إحاطة المجرمين علماً بنقاط الضعف في الأنظمة المعلوماتية لدى تلك المؤسسات والشركات المجنى عليها. ويختلف المشرعون في مسألة إلزام المجنى عليه أو غيره بالإبلاغ عن وقوع الجريمة المعلوماتية من عدمه. فبعض التشريعات تلزم في ذلك وبعضها لا تلزم الإبلاغ عن وقوع الجريمة.

فالتشريع الإماراتي على سبيل المثال يجعل من الإبلاغ عن الجرائم إلزاماً كقاعدة عامة، ومن يخالف ذلك يتعرض لعقوبة، فقد نص قانون الإجراءات الجزائية الاتحادي الإماراتي على أنه «كل من علم بوقوع جريمة ما يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب، أن يبلغ النيابة العامة أو أحد مأموري الضبط القضائي عنها[٩]، كما نص القانون نفسه على أنه « يجب على كل من علم من الموظفين العموميين أو المكلفين بخدمة عامة أثناء تأدية عمله أو بسبب تأديته بوقوع جريمة من الجرائم التي يجوز للنيابة العامة رفع الدعوى عنها بغير شكوى أو طلب أن يبلغ فوراً النيابة العامة أو أقرب مأموري الضبط القضائي»[١٠].

كما نص قانون العقوبات الاتحادي الإماراتي على أنه «يعاقب بالغرامة كل موظف غير مكلف بالبحث عن الجرائم أو ضبطها أهمل أو أرجأ إبلاغ السلطة المختصة بجريمة علم بها في أثناء أو بسبب تأديته وظيفته، ولا عقاب إذا كان رفع الدعوى معلقاً على شكوى[١١] كما نصت المادة (٢٧٤) من قانون العقوبات الاتحادي الإماراتي على أنه «يعاقب بغرامة لا تتجاوز ألف درهم كل من علم بوقوع جريمة وامتنع عن إبلاغ ذلك للسلطات المختصة. أما القانون المصري وكذلك النظام السعودي فلا يعاقبان جنائياً على عدم الإبلاغ عن وقوع الجريمة المعلوماتية[١٢].

ثانياً: الصعوبات المتعلقة بكون الجرائم المعلوماتية لا تترك آثاراً مادية ملموسة

جرائم الحاسب الآلي والإنترنت تتميز بأنها جرائم لا يتخلف عنها آثار كتابية، كما أن الجاني في تلك الجرائم يستطيع تدمير الأدلة والتخلص منها في ثوان معدودة. فالآثار الناتجة عن جرائم الحاسب الآلي والإنترنت ليست كالآثار التي تتخلف عن الجرائم التقليدية، وذلك لأن جرائم الحاسب الآلي هي عبارة عن نبضات إلكترونية ولا يترك فيها الجاني آثاراً مادية ملموسة كالبصمات أو الحامض النووي أو سلاح الجريمة أو حتى المسروقات أو الجثة كما هو الحال في الجرائم التقليدية. فالجاني في الجرائم المعلوماتية يستطيع أن يرتكب جريمته من بيته، أو من أي مكان آخر. وكون الآثار المتخلفة عن جرائم الحاسب الآلي والإنترنت هي آثار ذات طبيعة غير مادية فإن هذا يمثل صعوبة بخصوص إثباتها ولا يمكن التغلب على هذه الصعوبة إلا بالاعتماد على نمط في الإثبات يتفق وطبيعة هذه الجرائم. لكن هذا لا يعني أن جرائم

(٩) المادة (٣٧)، قانون الإجراءات الجزائية الاتحادي الإماراتي رقم (٣٥) لعام ١٩٩٢م.

(١٠) المادة (٣٨)، قانون الإجراءات الجزائية الاتحادي الإماراتي.

(١١) م (٢٧٢)، فقرة (٢)، قانون العقوبات الاتحادي الإماراتي.

(١٢) لكن توجد نصوص في القانون المصري تعاقب على عدم الإبلاغ عن جرائم معينة مثل جرائم أمن الدولة. انظر المادة (٩٨) من قانون العقوبات المصري.

الحاسب الآلي والإنترنت لا تتخلف عنها آثار أو أدلة مادية بشكل مطلق، بل من الممكن أن تترك بعض الآثار والأدلة المادية تتخذ شكل المعلومات المخزنة في البرامج الحاسوبية على سبيل المثال أو البرامج أو المعلومات أو البيانات أو الصور والوثائق التي قام الجاني بالاستيلاء عليها أو التلاعب بها وتغييرها. كل هذه يمكن الاعتماد عليها كأدلة إثبات على إرتكابه الجريمة. (فضل، ٢٠٠٧؛ عبدالله، ٢٠٠٧؛ الهيتي، ٢٠٠٢).

وبسبب صعوبة تحصيل الأدلة في جرائم الحاسب الآلي والإنترنت يرى الخبراء في مجال الحاسب الآلي، أن هذه الجرائم تمثل تحدياً كبيراً لرجال الشرطة والمحققين ذلك أن رجل الشرطة أو المحقق الذي انحصرت معلوماته ومهاراته وخبراته في الجرائم التقليدية سيجد صعوبة بالغة في التعامل مع الجرائم المعلوماتية التي تستخدم فيها تقنية الحاسب الآلي والإنترنت. (فضل، ٢٠٠٧؛ حجازي، ٢٠٠٧) وتبرز هنا أهمية وجود رجال شرطة ومحققين متخصصين في مجال التعامل مع جرائم الحاسب الآلي والإنترنت مع ما تتميز به هذه الجرائم من ضرورة توافر مهارات وتخصص كبيرين لدى المحققين في هذه التقنية حتى يستطيعوا كشف هذه الجرائم والوصول إلى الجناة والكشف عن الأدلة التي تدينهم سيما وأن المجرم في هذه الجرائم لديه الخبرة الفنية والمعرفة الكبيرة التي تمكنه من اقتراف جريمته، والأمثلة العملية على ذلك كثيرة، ومن هذه الأمثلة:

١- أعلنت وزارة الداخلية المصرية أنها قبضت على ٢٣ متهماً، وصادرت معدات استخدموها في سحب أموال من بنوك أمريكية، وذلك بالتعاون مع مكتب التحقيقات الفيدرالية (FBI) وتوقعت أن يصل عدد المقبوض عليهم إلى أكثر من ١٠٠ شخص، وذكرت وزارة الداخلية المصرية أن المشتبه بهم كانوا ضمن تشكيل إجرامي يضم أمريكيين، قاموا بالإستيلاء على أموال عائدة لمواطنين أمريكيين من خلال حصولهم على بيانات بطاقاتهم الائتمانية بطرق احتيالية متنوعة، منها قيامهم بعمل تحويلات من تلك البطاقات لحسابات وهمية داخل الولايات المتحدة الأمريكية خاصة بالمشتبه بهم الأمريكيين. وبعد وصول الأموال لشركائهم الأمريكيين، عن طريق سحب تلك الأموال، وتقسيمها فيما بينهم بنسب محددة، يتم تحويل النسب الخاصة بالمشتبه بهم المصريين عن طريق إحدى شركات تحويل الأموال. وذكرت وزارة الداخلية المصرية أنها ضبطت مع المتهمين المصريين الذين ألقي القبض عليهم داخل مصر، ٢١ جهاز حاسب آلي، و ٨ حاسبات آلية محمولة، و٥ فلاش ميموري (ذاكرة حاسوبية فلاش)، و ٢ USB مودم للدخول على شبكة الإنترنت، إضافة لعدد كبير من الأسطوانات المدمجة، و ٣ كاميرات ويب، و٣٣ جهاز تلفون محمول، و٢٣ كارت ذاكرة، و١٢ خط تلفون لشركات مختلفة. وذكرت الداخلية المصرية أن القبض على هذه المجموعة الإجرامية جرى في إطار التعاون الدولي بين أجهزة وزارة الداخلية المصرية، وقسم جرائم الحاسبات الآلية بالولايات المتحدة الأمريكية في مكتب التحقيقات الفيدرالية (FBI). بعد أن أكدت التحريات وجود أشخاص مشتبه بهم من الأمريكيين المتواجدين في الولايات المتحدة، اتفقوا فيما بينهم مع أشخاص مصريين متواجدين في مصر، على تكوين تشكيل إجرامي تخصص في الاستيلاء على أموال مواطنين أمريكيين من خلال تحصلهم على بيانات بطاقاتهم الائتمانية بطرق احتيالية متنوعة.

وذكرت الـ (FBI) أن ضحايا هذه الشبكة قد خسروا لحد الآن ما يزيد على مليوني دولار أمريكي[١٣].

٢- ألقت شرطة محافظة جدة القبض على هاكر سعودي يبلغ من العمر ١٥ عاماً، بعد اعترافه بارتكاب جريمة اختراق المواقع وسرقة البريد الإلكتروني لدواعي العبث والتسلية، واعترف الحدث الملقب «رينو» أمام المحقق بقيامه بسرقة البريد الإلكتروني واختراقه المواقع[١٤].

٣- اتهم مكتب الإدعاء العام في ولاية ماسا شوسيتس الأمريكية شخصاً يدعى (فان دنه) البالغ من العمر ١٩ عاماً، بالاحتيال في السندات المالية، والاحتيال عن طريق البريد والإنترنت، والتسبب في خسائر عن طريق الاستخدام غير المشروع للحاسب الآلي. واتهم دنه باختراق الحسابات الخاصة للعملاء في شركات السمسرة الأمريكية بهدف بيع وشراء أسهمهم، بالإضافة إلى انتحاله لشخصيات وهمية على شبكة الإنترنت للتغطية على حركاته. واتهم دنه بأنه قام بشراء ٩١٠٠ إحتمالية أسهم في إحدى شركات التقنية وهي شركة سيسكو سيستمز بسعر عشرة دولارات للوحدة الواحدة في أواخر يونيو، والتي بدت في حينها أنها ستصبح بلا قيمة بسبب اقتراب موعد انتهاء مدة صلاحيتها وهو منتصف يونيو من ذات العام وقام دنه بالحصول على البريد الإلكتروني لمشترين آخرين، وأرسل لهم برنامجاً يبدو وكأنه أداة للتخطيط، إلا أنه كحصان طروادة (Trojan Horse) الذي يسمح له بالتجسس على أعمالهم وأسرارهم عن طريق اختراق حاسباتهم الآلية. وقالت لجنة الرقابة المالية الأمريكية أن المتهم قام باستخدام كلمة السر ومعلومات شخصية أخرى تحصل عليها بنفس الطريقة باختراق حساب في شركة ووترهاوس (Water House) واستخدمه كمشتري مزيف لأسهمه عديمة القيمة تقريباً[١٥].

وقالت لجنة الرقابة المالية إن هذه الصفقة الوهمية أنقذته من خسارة قدرها ٣٧ ألف دولار أمريكي، ولكن المالك الشرعي لحساب ووتر هاوس لاحظ الخسائر الكبيرة. وحاول المتهم تغطية عملياته غير المشروعة عبر استخدام شبكات الإنترنت في ألمانيا وإيرلندا وأستراليا. وطالبت لجنة الرقابة المالية برد كل المبالغ التي استولى عليها منه، بالإضافة إلى دفع تعويضات عن الأضرار التي تسبب بها.

ويتضح لنا من الأمثلة السابقة الحاجة إلى محققين ورجال شرطة مؤهلين تأهيلاً جيداً في مجال تقنية الحاسب الآلي حتى يستطيعوا تحصيل هذه الأدلة الإلكترونية اللازمة للوصول إلى الجناة وإثبات ارتكابهم لجرائمهم أمام القضاء ليحكم عليهم بالعقوبة المناسبة إذ بدون ذلك لن يستطيع هؤلاء المحققين أن يصلوا إلى الجناة ولا أن يتحصلوا على أدلة الإثبات ومن ثَم يفلت الجناة بأفعالهم الإجرامية[١٦].

---

(١٣) وتوضح المضبوطات المذكورة مدى الحاجة إلى رجال شرطة ومحققين متخصصين في تقنية الحاسب الآلي حتى يستطيعوا التعامل مع هذه الأجهزة والأدوات وبالتالي الوصول إلى أدلة الإثبات التي تؤدي إلى إدانة المتهمين بارتكاب جرائمهم. إذ بدون الحصول على هذه الأدلة لن تتمكن جهات العدالة من إدانة هؤلاء المتهمين وبالتالي معاقبتهم على جرائمهم. انظر جريدة الشرق الأوسط، ٩٠ أكتوبر ٢٠٠٩م، العدد ١١٢٧٣، ص ٢٢.

(١٤) انظر جريدة الحياة، الأحد، ١٩ أبريل ٢٠٠٩م، العدد ١٦٨١٦. ص ٧.

(١٥) انظر جريدة الشرق الأوسط، ٩ أكتوبر، العدد ١١٢٧٣. ص ٢٢.

(١٦) BBC Arabic News at http: // news vote. bbc. Co. uk / Arabic /business.

ثالثاً: الصعوبات المتعلقة باتخاذ الجناة احتياطات تمنع الحصول على الأدلة

من الإشكالات التي تصعب مسألة إثبات جرائم الحاسب الآلي والإنترنت هي عدم إمكانية الحصول على الدليل بسبب استخدام الجناة لوسائل تتجاوز مسألة تدمير الأدلة التي تدينهم. فالجناة في مثل هذه الجرائم يعتمدون على التخفي عبر شبكة الإنترنت تحت ستار فني وتقني، فجرائم الحاسب الآلي والإنترنت تتم في بيئة لا علاقة لها بالأوراق والمستندات وإنما تتم باستخدام الحاسب الآلي وشبكة الإنترنت. ويستطيع الجاني أن يعبث في بيانات الحاسب الآلي وبرامجه، وذلك خلال مدة قصيرة قد لا تتجاوز الثواني المعدودة، كما يستطيع الجاني أن يقوم بمحو هذه البيانات والمعلومات خلال ثوان معدودة، قبل أن تصل السلطات إليه. (هروال، ٢٠٠٧؛ حجازي، ٢٠٠٩) كما قد يلجأ الجناة إلى استخدام كلمات المرور (Passwords) لمنع أي شخص من الدخول إلى مواقعهم وملفاتهم والوصول إليهم.

رابعاً: الصعوبات المتعلقة بضخامة حجم البيانات والمعلومات للدليل المعلوماتي

من الصعوبات التي تواجه رجال الشرطة وسلطات التحقيق في الجرائم المعلوماتية الكم الضخم من البيانات والمعلومات التي قد تكون مخزنة في النظام المعلوماتي محل التحقيق، إذ تحتاج هذه البيانات والمعلومات إلى دراسة وفحص حتى يستطيع المحقق أن يستخلص منها الدليل المعلوماتي، وبالتالي يتعين على المحقق أن يتحلى بالصبر والقدرة على فحص ودراسة هذا الكم الهائل من البيانات والمعلومات المخزنة في النظام المعلوماتي، وتشكل ضخامة هذه البيانات والمعلومات تحدياً كبيراً للمحقق في الجرائم المعلوماتية. ذلك أن طباعة كل ما هو موجود ومخزن في النظام المعلوماتي قد يتطلب آلاف الصفحات، وقد لا ينتج عن هذه الأوراق أية معلومات تفيد التحقيق[١٧].

خامساً: الصعوبات المتعلقة بنقص الخبرة لدى القائمين على مكافحة الجرائم المعلوماتية

من الصعوبات التي تواجه عملية استخلاص الدليل المعلوماتي نقص الخبرة لدى رجال الشرطة والمحققين وكذلك القضاة، إذ قد لا تكون لدى هؤلاء معرفة جيدة بالحاسب الآلي وشبكة الإنترنت والأدلة المعلوماتية وكيفية التعامل معها. وهذا يدعو إلى ضرورة تأهيل رجال الشرطة والمحققين وكذلك القضاة بخصوص الجرائم المعلوماتية وطبيعة الأدلة المعلوماتية ودورها في الإثبات. وقد نص النظام السعودي على تولي هيئة الاتصالات وتقنية المعلومات تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم والتحقيق فيها وأثناء المحاكمة. على اعتبار أن هيئة الاتصالات وتقنية المعلومات في المملكة لديها الإمكانيات المادية والبشرية للقيام بهذه المهمة وتقديم الدعم الفني والتقني للجهات الأمنية [١٨].

---

(١٧) وهذا على عكس ما هو الأمر عليه في الجرائم التقليدية كالسرقة أو القتل أو السطو، ذلك أن وفرة المعلومات والأدلة في مثل هذه الجرائم يساعد سلطات التحقيق ويساعد المحكمة في استخلاص الدليل الجنائي في مثل هذه الجرائم، وهذا الأمر يوضح أهمية ندب خبراء متخصصين في مجال الحاسب الآلي والإنترنت حتى يستطيعوا فرز وتصنيف ودراسة وتحليل هذا الكم الهائل من البيانات والمعلومات الذي قد ينتج عن الجريمة المعلوماتية. انظر: (حجازي، ٢٠٠٩: ص ١٠٩ وما بعدها). انظر أيضاً: (هروال، ٢٠٠٧: ص ٣٥ وما بعدها).

(١٨) م (١٤)، نظام مكافحة الجرائم المعلوماتية السعودي الصادر بقرار مجلس الوزراء رقم (٧٩) وتاريخ ٧/ ٣/ ١٤٢٨هـ. والمرسوم الملكي رقم م/ ١٧ وتاريخ ٨/ ٣/ ١٤٢٨هـ.

سادساً: الصعوبات الناشئة عن قصور التشريعات الخاصة بمكافحة الجرائم المعلوماتية

من الصعوبات التي تواجه القائمين على مكافحة جرائم الحاسب الآلي والإنترنت قصور التشريعات والقوانين التقليدية عن مواجهة هذا النوع من الجرائم المستحدثة. فالتطور التقني المتسارع والتنامي الكبير في استخدام تقنية الحاسب الآلي وشبكة الإنترنت واكبه انتشار الجرائم التي تستخدم فيها هذه التقنية. لأن الجريمة المعلوماتية تتقدم وتنتشر بسرعة كبيرة توازي سرعة تقدم التقنية نفسها، مما يؤثر سلباً في محاربة هذه الجرائم ومعاقبة مرتكبيها. فهذا التطور الكبير في تقنية الحاسب الآلي والإنترنت لا يواجهه بذات المستوى تطور في النصوص والتشريعات القانونية. فالقوانين التقليدية بنصوصها الحالية لا تكفي لمواجهة تلك الصور المستحدثة من الجرائم، وحيث تشترط غالبية النصوص القانونية الصفة المادية في الشيء محل ارتكاب الجريمة مما يتعارض مع الطبيعة المعلوماتية، وبالتالي لا تدخل تلك الصور ضمن طائلة التجريم والعقاب. (حجازي، ٢٠٠٩؛ فضل، ٢٠٠٧).

سابعاً: الصعوبات المتعلقة بكون جرائم المعلوماتية جرائم عابرة للحدود

تعد جرائم الحاسب الإنترنت جرائم مستحدثة وهي من الجرائم العابرة للحدود الوطنية للدول وهو ما يزيد من الصعوبات التي تواجه السلطات المختصة في الدول المختصة في شأن اكتشافها ومن ثم إثباتها. فهي ليست جرائم ترتكب في أماكن قريبة من مكان المجنى عليه، بل قد تكون بعيدة عنه، الشيء الذي يجعل من تحديد المكان الذي إرتكب منه الجاني جريمته أمراً صعباً. إضافة إلى ما يترتب على هذا الأمر من إشكاليات قانونية تتعلق بقواعد الاختصاص، ونطاق سريان القانون، وعدم وجود مفهوم عام حول تعريف القانون للنشاط الإجرامي المتعلق بهذه الجرائم المعلوماتية. كذلك عدم وجود معاهدات لتسليم المجرمين أو للتعاون بين الدول المختلفة لمواجهة الجرائم المعلوماتية والتحقيق فيها ومحاكمة مرتكبيها، فمع الزيادة الهائلة في استخدام شبكة الإنترنت حول العالم، أصبحت هذه الجرائم لا تقف عند الحدود الجغرافية وبالتالي تبرز صعوبات حول مدى إمكانية تطبيق النصوص الجنائية خارج إقليم الدولة. (عبدالله، ٢٠٠٧) ولهذا تبرز أهمية التعاون الدولي بين دول العالم في إطار مواجهة هذه الجرائم المستحدثة بحيث يمكن إرسال المعلومات والأدلة بخصوص الجريمة إلى الدولة التي يوجد فيها المتهم ومطالبتها بالتحقيق فيها ومحاكمته أو تسليمه للدولة التي تضررت من جريمته.

المبحث الرابع: حجية الدليل الإلكتروني لدى بعض التشريعات الوطنية

لم تتفق التشريعات الوطنية في الدول المختلفة على مسألة الإثبات في الجرائم المعلوماتية. فمن التشريعات من أوجد قوانين خاصة للتعامل مع الجرائم المعلوماتية وقبول الأدلة الإلكترونية. واكتفت دول أخرى ومنها غالبية الدول العربية بالقوانين التقليدية للتعامل مع مثل هذه الجرائم بتطويعها لمعاقبة مرتكبي الجرائم المعلوماتية ومنها قانون العقوبات وقانون الإثبات. وسنتطرق في هذا المبحث إلى موقف تشريعات بعض الدول الغربية والعربية من مفهوم الإثبات الإلكتروني واستخدام وسائل الإثبات الإلكترونية وقبول الدليل الإلكتروني وذلك في مطلبين على النحو الآتي:

المطلب الأول: حجية الدليل الإلكتروني في بعض الدول الغربية

أولاً: فرنسا

يأخذ المشرع الفرنسي بمبدأ حرية الأدلة وحرية القاضي في تقدير هذه الأدلة، كما أن الفقه الفرنسي يتناول مسألة قبول الأدلة الإلكترونية في المواد الجنائية ضمن موضوع أشمل وهو مسألة قبول الأدلة الناشئة من الآلات أو الأدلة العلمية مثل رادارات قياس سرعة السيارات وآلات التصوير والتسجيل وغيرها. ومن ثَم فإن القاضي الفرنسي يملك حرية تقدير الأدلة بما فيها الأدلة المعلوماتية. ولكن يشترط القانون الفرنسي أن يكون الدليل المعلوماتي يقينياً حتى يستطيع القاضي الحكم بالإدانة، ويتم الوصول إلى ذلك عن طريق ما يستنتجه القاضي مما يعرض عليه من أدلة سواء كانت أدلة ورقية تنتجها الطابعات، أو كانت أدلة لا ورقية أو إلكترونية كالأشرطة والأقراص المغناطيسية وغيرها من الوسائط الإلكترونية غير الورقية. كما ينص قانون الإجراءات الجنائية الفرنسي في المدة (٤٢٧) منه على أنه « لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت أثناء المحاكمة ونوقشت أمامه في مواجهة الأطراف. ومن ثَم فإن القاضي الجنائي الفرنسي ليس له أن يأخذ بأدلة إثبات أو نفي لم تكن قد عرضت أثناء المحاكمة، ولم يناقشها أطراف الدعوى، وينطبق ذلك على الأدلة الإلكترونية بجميع أشكالها، فإذا قدمت كأدلة فلا بد من مناقشتها وتمكين الخصوم من الإطلاع عليها، ولا بد أن يفحصها القاضي ويقرر رأيه فيها. وهو ما يتطلب أن يكون له معرفة ودراية بمثل هذه الأدلة. (حجازي، ٢٠٠٧)

ثانياً: بريطانيا

اعترف المشرع الإنجليزي بحجية الدليل الإلكتروني. ولكنه اشترط دقة وسلامة المعلومات والبيانات الناتجة عنه، فقد نصت المادة (٦٩) من قانون الإثبات الجنائي لعام ١٩٨٤م على أن الناتج من الوسائل الإلكترونية لا يقبل كدليل إذا تبين وجود سبب معقول يدعو إلى الاعتقاد بأن هذا الناتج غير دقيق أو أن بياناته غير سليمة أو أن الحاسب الآلي محل التفتيش لا يعمل بصورة سليمة. والجدير بالذكر إلى أن الأدلة الإلكترونية الناشئة عن الوسائل الإلكترونية تقبل كوسائل إثبات في المملكة المتحدة وذلك بالنسبة للبرامج والبيانات المخزنة فيها، وبالنسبة للنسخ (Copies) المستخرجة من البيانات والمعلومات المخزنة في الحاسب الآلي، شريطة أن تكون هذه الأدلة قد تم الحصول عليها بطريقة مشروعة[١٩].

---

(١٩) ومن أمثلة الطرق غير المشروعة التي قد تستخدم ضد المتهم في الجرائم المعلوماتية استخدام وسائل الإكراه المختلفة من أجل حمله على فك الشفرة للنظام المعلوماتي المحمي أو إنهاك قواه حتى يدلي بمعلومات معينة حول قاعدة بيانات أو غيرها. ونصت المادة (٧٦) من قانون الإثبات الجنائي الإنجليزي لعام ١٩٨٤م أن اعتراف المتهم يتم رفضه باعتباره دليلاً إذا لم تستطع سلطة الإدعاء أن تثبت أنه لم يتم الحصول عليه بواسطة الإكراه أو أنه كان نتيجة سلوك معين يجعل هذا الاعتراف مشكوكاً في صحته، كما أن المادة (٧٨) من القانون نفسه تخول المحكمة سلطة استبعاد الدليل الإلكتروني إذا ثبت لها أنه يتعارض مع عدالة إجراءات الدعوى. كما أن المادة (٧٦) من القانون ذاته تنص على أنه «إذا كان الاعتراف غير مقبول فإن كل ما يترتب عليه من نتائج تصبح غير مشروعة وغير مقبولة» وتستوي في ذلك الأدلة التقليدية والأدلة المعلوماتية. انظر: (هروال، ٢٠٠٧: ص ٤٥ وما بعدها). انظر أيضاً: (فضل، ٢٠٠٧: ص ٣٧٣ وما بعدها).
انظر أيضاً: (Overly, 2010-2011ed at 3-5).

ثالثاً: الولايات المتحدة الأمريكية

أقر المشرع الأمريكي بالحجية للأدلة الإلكترونية. ونصت التشريعات للعديد من الولايات الأمريكية على ذلك. فقد نص قانون الحاسب الآلي لعام ١٩٨٣م الصادر في ولاية نيويورك على أن مخرجات الحاسب الآلي تعتبر مقبولة بوصفها أدلة إثبات فيما يتعلق ببيانات وبرامج الحاسب الآلي المخزنة بداخله.

كما نص قانون الإثبات (Rules of Evidence) الصادر في ولاية نيويورك على أن النسخ المستخرجة من البيانات والمعلومات التي يحتويها الحاسب الآلي تكون مقبولة في الإثبات. وقد أصدر القضاء الأمريكي العديد من الأحكام التي تدلل على قبول الأدلة الإلكترونية كأدلة إثبات شريطة توافر المشروعية في الحصول على الدليل الإلكتروني ودون وجود تعدٍ على الحياة الخاصة للأفراد [٢٠].

المطلب الثاني: حجية الدليل الإلكتروني في بعض التشريعات العربية

أولا: جمهورية مصر العربية

ترك المشرع المصري لأطراف الخصومة حرية الإثبات في تقديم كل الأدلة التي بحوزتهم شريطة كونها مشروعة إلى القضاء. ويكوِّن القاضي عقيدته من أي دليل يقدم أمامه. وللقاضي كامل الحرية في أن يستعين بكافة طرق الإثبات للوصول إلى الحقيقة ما دامت مشروعة. وينطبق ذلك أيضاً على الأدلة الإلكترونية، فالقاضي يستطيع أن يأخذ بالدليل الإلكتروني ما دام تم التحصل عليه بشكل مشروع، وما دام القاضي قد اقتنع بصحته وسلامته. (حجازي، ٢٠٠٧؛ إبراهيم، ٢٠٠٩).

وقد حظر قانون الإجراءات الجنائية المصري إطلاع مأموري الضبط القضائي على الأوراق المختومة أو المغلقة الموجودة في منزل المتهم أثناء تفتيشه، ونرى أن الأمر ذاته ينطبق على البيانات المخزنة في الحاسب الآلي والمحمية بشكل كلي أو جزئي ضد الإطلاع إما عن طريق التشفير أو الترميز أو بأي وسيلة فنية ضد الاختراق. والسبب في حظر الإطلاع على الأوراق المغلقة والمغلفة والمختومة، هو رغبة صاحبها في عدم الإطلاع عليها، بدليل أنه قام بإغلاق هذه الأوراق أو تغليفها بأي طريقة. (حجازي، ٢٠٠٧) وذات العلة

---

(٢٠) وتظهر أهمية اعتماد الأدلة الإلكترونية كوسيلة إثبات ما أعلنه مكتب التحقيقات الفيدرالية (FBI) من أن مستخدمي الإنترنت في الولايات المتحدة قدموا مليوني شكوى تتعلق بأنشطة إجرامية مزعومة على شبكة الإنترنت إلى المركز المختص التابع له والذي أنشيء عام ٢٠٠٠م. وتراوحت الشكاوى من سرقة الهوية الشخصية إلى الاستخدام غير المشروع لبطاقات الائتمان أو الحسابات البنكية، وذلك بإجمالي خسائر تقدر بـ ١,٧ مليار دولار على الأقل.
وذكر مكتب التحقيقات الفيدرالي بأن مركز شكاوى جرائم الإنترنت التابع له سجل أول مليون شكوى قبل نهاية عام ٢٠٠٧م، أي في السنوات السبع الأولى من العمل. ولم يستغرق الأمر سوى ثلاث سنوات أخرى ليسجل المركز المليون الآخر، وذلك حتى شهر نوفمبر من عام٢٠١٠م. وتعكس هذه الزيادة الكبيرة في عدد الشكاوى التزايد المستمر بجرائم الإنترنت. وتوضح هذه الزيادة الكبيرة أهمية وضرورة قبول الأدلة الإلكترونية في مجال الإثبات وتدريب المحققين والقضاة على كيفية التعامل معها =

= وشروطها. انظر جريدة الرياض، الرياض الاقتصادي الخميس، ١٨ نوفمبر ٢٠١٠م. العدد ١٥٤٨٧. ص ٦.
انظر أيضاً: (إبراهيم، ٢٠٠٩: ص١٩٧ وما بعدها).
انظر أيضاً: (Shreves, 2010 ed at 1-2).
انظر أيضاً: (A. Mauet and D. Wolfson, 2009. at 2-6).

تتوافر في البيانات المعلوماتية، حيث لا يمكن الدخول إلى النظام المعلوماتي بدون الحصول على مفتاح الشفرة أو كلمة السر (Password).

وبذلك يكون صاحب ذلك النظام قد أعلن رفضه مسبقاً الإطلاع غير المصرح به من الغير ما لم يكن الراغب في الإطلاع مصرحاً له بالإطلاع عن طريق توافر كلمة السر إلى هذه البيانات وذلك ما لا يتوافر لمأمور الضبط القضائي القائم بالتفتيش. فالمادة (٥٢) من قانون الإجراءات الجنائية المصري تحظر الإطلاع على البيانات والمعلومات التي قام صاحبها بحمايتها ضد الإطلاع غير المصرح به أياً كان الوسط الذي يحتوي على البيانات والمعلومات، ويستوي في ذلك أن يكون الوسط تقليدياً كالأوراق والمستندات أو غير تقليدي كالوسائط الإلكترونية والشرائط الممغنطة والأقراص المرنة، والذاكرات الداخلية للحاسب الآلي، وشبكة الإنترنت، فمتى تحقق الغلق أو الإقفال بأي طريقة فإنه يحظر على مأمور الضبط القضائي الإطلاع على هذه البيانات والمعلومات المخزنة في النظام المعلوماتي. ونرى صحة هذا التوجه ولكننا نرى أيضاً ضرورة إصدار المشرع المصري لتشريع يتعامل مع الجرائم المعلوماتية نظراً للطبيعة الخاصة لمثل هذا النوع من الجرائم والتي قد لا تتوافق مع نصوص القوانين التقليدية. (فضل، ٢٠٠٧؛ الرومي، ٢٠٠٨) إذ أن القوانين التقليدية لا يمكنها استيعاب هذه الصور الإجرامية المستحدثة لأن ذلك يتعارض مع مبدأ المشروعية الجنائية ومنهج التفسير الضيق للنصوص العقابية، وما يتطلبه ذلك من عدم جواز القياس عليها.

ثانياً: المملكة العربية السعودية

أخذ المنظم السعودي بحجية الدليل الإلكتروني في الإثبات. فلقد نص نظام التعاملات الإلكترونية السعودية في المادة (٢) منه على أن من أهداف هذا النظام هو» إرساء قواعد نظامية موحدة لاستخدام التعاملات والتوقيعات الإلكترونية، وتسهيل تطبيقها في القطاعين العام والخاص، بوساطة سجلات إلكترونية يُعوَّل عليها». فاستخدام المنظم السعودي لكلمة «يعول عليها» يعني أن لها كامل الحجية في الإثبات[٢١].

كما أكد المنظم السعودي على حجية الأدلة الإلكترونية والمستخلصات الإلكترونية بنصه على أن يكون للتعاملات والسجلات والتوقيعات الإلكترونية حجيتها الملزمة، ولا يجوز نفي صحتها أو قابليتها للتنفيذ، ولا منع تنفيذها بسبب أنها تمت – كلياً أو جزئياً – بشكل إلكتروني، بشرط أن تتم تلك التعاملات والسجلات والتوقيعات الإلكترونية بحسب الشروط المنصوص عليها في هذا النظام[٢٢] كما نص المنظم السعودي على أنه إذا اشترط أي نظام في المملكة حفظ وثيقة أو معلومات لأي سبب، فإن هذا الشرط يتحقق عندما تكون تلك الوثيقة أو المعلومة محفوظة أو مرسلة في شكل إلكتروني بشرط مراعاة ما يلي:

أ) حفظ السجل الإلكتروني على نحو يتيح استخدامه والرجوع إليه لاحقاً.

ب) بقاء السجل الإلكتروني محفوظاً على نحو يتيح استخدامه والرجوع إليه لاحقاً.

ج) أن تحفظ مع السجل الإلكتروني المعلومات التي تمكِّن من معرفة المنشئ والمرسل إليه، وتاريخ

---

(٢١) الفقرة (١)، المادة (٢) نظام التعاملات الإلكترونية السعودي الصادر بقرار مجلس الوزراء رقم م/ ١٨ وتاريخ ٨/ ٣/ ١٤٢٨هـ.

(٢٢) الفقرة (١)، المادة (٥)، نظام التعاملات الإلكترونية السعودي.

إرسالها وتسلمها وقتها[٢٣]. كما ساوى المنظم السعودي بين الوثيقة أو السجل أو المعلومة المقدمة في شكل إلكتروني مع تلك المقدمة بشكل مكتوب[٢٤].

ونص المنظم السعودي على أنه يعد السجل الإلكتروني أصلاً بذاته عندما تستخدم وسائل وشروط فنية تؤكد سلامة المعلومات الواردة فيه من الوقت الذي أنشئ فيه بشكله النهائي على أنه سجل إلكتروني[٢٥].

كما نص النظام السعودي على أن التعامل الإلكتروني أو التوقيع الإلكتروني يعد دليلاً في الإثبات إذا استوفى سجله الإلكتروني متطلبات حكم المادة (الثامنة) من هذا النظام[٢٦].

كما نص المنظم السعودي على قبول التعامل الإلكتروني أو التوقيع الإلكتروني قرينة في الإثبات، والقرينة لا ترقى إلى مرتبة الدليل، حتى وإن لم يستوف سجله الإلكتروني متطلبات حكم المادة (الثامنة) من هذا النظام.

وأكد المنظم السعودي على أن كل من التعامل الإلكتروني، والتوقيع الإلكتروني، والسجل الإلكتروني حجة يُعتد بها في التعاملات، وأن كلاً منها على أصله (لم يتغير منذ إنشائه) ما لم يظهر خلاف ذلك.

كما نص المنظم السعودي على أنه «يراعى عند تقدير حجية التعامل الإلكتروني مدى الثقة في الآتي:

أ) الطريقة التي استخدمت في إنشاء السجل الإلكتروني أو تخزينه أو إبلاغه، وإمكان التعديل عليه.

ب) الطريقة التي استخدمت في المحافظة على سلامة المعلومات.

ج) الطريقة التي حددت بها شخصية المنشئ[٢٧].

كما ساوى المنظم السعودي بين التوقيع الإلكتروني والتوقيع الخطي في حجية الإثبات[٢٨].

كما عهد المنظم السعودي إلى هيئة الاتصالات وتقنية المعلومات تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط الجرائم المعلوماتية والتحقيق فيها وأثناء المحاكمة. وهي تساعد الجهات الأمنية في الحصول على الأدلة الإلكترونية[٢٩].

الخاتمة

مع الإنتشار الكبير في استخدام الحاسب الآلي وشبكة الإنترنت أصبحت الجرائم المعلوماتية من المخاطر التي يمكن أن يتعرض لها كل من يستخدم شبكة الإنترنت. فالمجرمون يستخدمون هذه التقنية كوسيلة لإرتكاب جرائمهم المختلفة من سرقة واحتيال واختراق وإتلاف وغيرها من الجرائم المعلوماتية الآخذة بالتزايد والانتشار يوماً بعد يوم. كما أن الحاسب الآلي وملحقاته وكذلك شبكة الإنترنت يتم استخدامها لإخفاء الأدلة التي تدينهم. ويثار في شأن إثبات الجرائم المعلوماتية الحاجة إلى الاعتماد على الأدلة

(٢٣) المادة (٦)، نظام التعاملات الإلكترونية السعودي.
(٢٤) المادة (٧)، نظام التعاملات الإلكترونية السعودي.
(٢٥) المادة (٨)، نظام التعاملات الإلكترونية السعودي.
(٢٦) الفقرة (١)، المادة (٩)، نظام التعاملات الإلكترونية السعودي.
(٢٧) الفقرات (٢)-(٤)، المادة (٩)، نظام التعاملات الإلكترونية السعودي.
(٢٨) الفقرة (١)، المادة (١٤)، نظام التعاملات الإلكترونية السعودي.
(٢٩) المادة (١٤)، نظام مكافحة الجرائم المعلوماتية السعودي، الصادر بقرار مجلس الوزراء رقم (٧٩) وتاريخ ٧/ ٣/ ١٤٢٨هـ. والمرسوم الملكي رقم م/ ١٨ وتاريخ ٨/ ٣/ ١٤٢٨هـ.

الإلكترونية على اعتبار أن هذه الجرائم هي جرائم غير تقليدية ولا يمكن الوصول إلى هذه الأدلة وتحديدها إلا بواسطة خبير متخصص في مجال الحاسب الآلي. فالدليل الإلكتروني اللازم لإثبات الجريمة المعلوماتية مختلف عن الدليل الجنائي في الجريمة التقليدية، وذلك من حيث كمية البيانات والمعلومات في الحاسب الآلي وكيفية إثباتها، سواء من حيث وسيلة الإثبات أو من يقوم بالإثبات، وما إذا كانت تتوافر لدى رجال الشرطة الخبرة اللازمة من عدمها.

وهناك العديد من التحديات والصعوبات التي تواجه المحققين في البحث عن الأدلة الإلكترونية التي تدين مرتكب مثل هذه الجرائم، وقد تطرقنا لتلك التحديات في هذا البحث ومنها امتداد نطاق التفتيش إلى نظم معلوماتية غير النظام المعلوماتي محل التفتيش، وهذا يثير مسألة مدى مشروعية مثل هذا الإجراء ومدى مساسه بحق الخصوصية للمعلومات العائدة لأصحاب تلك النظم المعلوماتية التي يمتد إليها التفتيش. وتثير أيضاً مشاكل حول مدى مساس إجراءات ضبط محتويات النظام المعلوماتي بخصوصية معلومات مالكه (المتهم). فقد يتعدى نطاق التفتيش المدى المقبول ليشمل جميع محتويات النظام المعلوماتي وما قد يتضمنه من معلومات وبيانات وصور خاصة تعود للمتهم قد تكون سرية أو تتمتع بحماية القانون أو لطبيعتها أو تعلقها بجهات أخرى.

وقد هدفنا في هذا البحث إلى دراسة موضوع حجية الأدلة الإلكترونية في الإثبات ومدى هذه الحجية.

وبناء على ما ذكر تم التوصل في نهاية هذا البحث إلى النتائج والتوصيات الآتية:

أولاً: النتائج

١- تثير الجرائم المعلوماتية بعض الصعوبات في مجال الحصول على الأدلة الجنائية، فسلطات التحقيق اعتادت على كون الإثبات مادياً وملموساً، ولكن في البيئة الإلكترونية لا يستطيع المحقق تطبيق إجراءات ووسائل الإثبات التقليدية على البيانات والمعلومات المخزنة في الحاسب الآلي.

٢- يتسم التحقيق في الجرائم المعلوماتية بصعوبة وتعقيد بالغين مما يتطلب تأهيل رجال الشرطة والمحققين تأهيلاً مناسباً في مجال الحاسب الآلي والإنترنت وطرق مكافحة الجرائم المعلوماتية وتدريبهم على آليات الوصول إلى الأدلة المعلوماتية وحفظها من التلف أو الضياع تمهيداً لاستخدامها أمام المحاكم المختصة. وليس بالضرورة أن يكون المحقق خبيراً في الحاسب الآلي وشبكة الإنترنت، لكن لا بد له من أن يكون ملماً بآلية عمل الحاسب الآلي حتى يستطيع التعامل مع خبراء الحاسب الآلي وبالتالي كشف الجرائم وجمع الأدلة.

٣- يجب على المحقق في الجرائم المعلوماتية اتخاذ كافة الإجراءات الاحتياطية التي ينبغي عليه اتخاذها في مسرح الجريمة في الجرائم المعلوماتية، واتخاذ التدابير اللازمة لحماية الأدلة المعلوماتية من التلف أو الضياع أو العبث بها. إذ أن هناك إمكانية للتلاعب في هذه البيانات والمعلومات المخزنة في الحاسب الآلي أو محوها عن طريق تدخل الجاني أو أي شخص آخر عبر شبكة الإنترنت عن طريق وحدة طرفية، كما أن الجاني يستطيع طمس معالمها ومحو آثارها.

٤- يوجد قصور في التشريعات الإجرائية الواجب اتباعها لمواجهة الجرائم المعلوماتية في مرحلة

الإستدلال والتحقيق خاصة تلك المتعلقة بإجراءات التفتيش والمعاينة وضبط الأدلة في البيئة الإلكترونية.

٥- لم يتعرض المنظم السعودي لحجية الأدلة المعلوماتية، وعلى الرغم من خلو النظام السعودي من التطرق لهذه المسألة فإنه يمكن الاعتماد على الأدلة الإلكترونية في إثبات أو نفي الجريمة، وتكون لها قوة القرائن في الإثبات.

٦- يشترط في الأدلة المعلوماتية أن تكون يقينية حتى يمكن الحكم على المتهم بالإدانة، ويحدث ذلك عن طريق ما يستنتجه القاضي من خلال ما يقدم إليه من هذه الأدلة المعلوماتية.

ثانياً: التوصيات

١- ضرورة قيام المشرعين في الدول المختلفة بإصدار تشريعات خاصة بجرائم الحاسب الآلي والإنترنت وتطوير قواعد الإجراءات الجنائية وقواعد الإثبات وذلك نظراً لأن طبيعة هذه الجرائم تصعب من عمل سلطات التحقيق فيما يتعلق بالحصول على الأدلة التي تدين المتهم بارتكاب تلك الجرائم.

٢- ضرورة استحداث وحدة متخصصة في التحقيق والتحري في جرائم المعلوماتية لتتولى التحقيق في هذه الجرائم والوصول إلى مرتكبيها والحصول على الأدلة التي تدينهم تمهيداً لتقديمهم إلى المحاكمة.

٣- ضرورة تأهيل رجال الشرطة والمحققين تأهيلاً جيداً في مجال تقنية الحاسب الآلي والإنترنت حتى يستطيعوا التحقيق في هذا النوع من الجرائم. كما ينبغي عقد دورات تدريب أثناء الخدمة لهم لتحديث معلوماتهم وقدراتهم على مكافحة هذه الجرائم.

٤- ضرورة عقد دورات تدريبية للقضاة الذين يقومون بنظر مثل هذه القضايا حتى يستطيعوا فهمها وبالتالي تقدير الأدلة المعروضة عليهم والحكم فيها بشكل صحيح.

٥- ضرورة الاستعانة بخبير متخصص في مجال الحاسب الآلي والإنترنت حتى يستطيع تحديد الآثار التي ترتبت على اختراق الحاسب الآلي وتجميع الأدلة التي تساعد في إثبات الجريمة على الجاني.

٦- ضرورة عقد إتفاقيات دولية تعالج السلبيات التي تنتج عن تطبيق القوانين الوطنية على جرائم المعلوماتية ومنها تعدد القوانين والقانون الواجب التطبيق وجمع الأدلة والإثبات الجنائي وغيرها، كما يجب على الدول المختلفة الدخول في اتفاقيات ثنائية تنظم المسائل المتعلقة بتلك الجرائم والتعاون فيما بينها لمكافحة مثل هذه الجرائم.

٧- ضرورة إلزام مزودي خدمة الإنترنت (Service Providers) بالتحقق من هوية مستخدمي شبكة الإنترنت من العملاء الذين يقومون بتوصيلهم بالحاسبات الخادمة (Servers) حتى يمكن تحديد هوياتهم في حالة ارتكابهم لجرائم معلوماتية.

المراجع

أولاً: الكتب والبحوث العربية

إبراهيم، خالد ممدوح. *فن التحقيق الجنائي في الجرائم الإلكترونية*. الإسكندرية: دار الفكر الجامعي، ٢٠٠٩م.

إبراهيم، خالد ممدوح. *حجية البريد الإلكتروني في الإثبات: دراسة مقارنة*. الإسكندرية: دار الفكر الجامعي، ٢٠٠٨م.

إبراهيم، خالد ممدوح. *الجرائم المعلوماتية*. الإسكندرية: دار الفكر الجامعي، ٢٠٠٩م.

حجازي، عبدالفتاح بيومي. *الإثبات الجنائي في جرائم الكمبيوتر والإنترنت*. القاهرة: دار الكتب القانونية، ٢٠٠٧م.

حجازي، عبدالفتاح بيومي. *الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت*. د.ب: د.ن، ٢٠٠٩م.

حسني، محمود نجيب. *شرح قانون الإجراءات الجنائية*. ط٢. القاهرة: دار النهضة العربية، ١٩٨٨م.

داود، حسن طاهر. *جرائم نظم المعلومات*. الرياض: جامعة نايف العربية للعلوم الأمنية، ٢٠٠٠م.

رستم، هشام فريد. *الجوانب الإجرائية للجرائم المعلوماتية: دراسة مقارنة*. أسيوط: مكتبة الآلات الحديثة، ١٩٩٤م.

الرومي، محمد أمين. *المستند الإلكتروني*. القاهرة: دار الكتب القانونية، ٢٠٠٨م.

عبدالله، عبدالكريم عبدالله. *جرائم المعلوماتية والإنترنت: الجرائم المعلوماتية*. بيروت: منشورات الحلبي الحقوقية، ٢٠٠٧م.

عبدالمطلب، ممدوح عبدالحميد. «أدلة الصور الرقمية.» *ندوة المجتمع والأمن*. الدورة الخامسة. كلية الملك فهد الأمنية، ١٤٢٨هـ.

فضل، سليمان أحمد. *المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)*. القاهرة: دار النهضة العربية، ٢٠٠٧م.

منصور، محمد حسين. *الإثبات التقليدي والإلكتروني*. الإسكندرية: دار الفكر الجامعي، ٢٠٠٩م.

موسى، مصطفى محمد. *التحقيق الجنائي في الجرائم الإلكترونية*. القاهرة: د.ن، ٢٠٠٩م.

هروال، نبيلة هبة. *الجوانب الإجرائية لجرائم الإنترنت*. الإسكندرية: دار الفكر الجامعي، ٢٠٠٧م.

الهيتي، محمد مرهج. *جرائم الحاسوب*. عمان: دار المناهج للنشر والتوزيع، ٢٠٠٢م.

يونس، عمر أبوبكر. *الجرائم الناشئة عن استخدام الإنترنت*. القاهرة: جامعة عين شمس، ٢٠٠٤م.

ثانياً: المراجع الأجنبية

Burke, Sturat. *Use of Electronic Records in Litigation: Protecting Electronic Evidence*. Guide to Records Retention, (2010).

Carlson, Ronald L. *Electronic Evidence: Trial Handbook for Georgia Lawyers*. 2010-2011 ed.

Hill, Clark. *Legal and Practical Implications of Advancements in Information Technology and Other Electronic Evidence*. Michigan Construction Law Manual, (2010).

Kotler, James. "A Survey of Sanctions Awarded for E-Discovery Violations." *Proof*, Vol. 17, No. (2), American Bar Association, (Winter 2009).

Mauet, Thomas A. and Wolfson, Warren D. *Electronic Evidence*. Aspen Publishers Trial Evidence, (2009).

Overly, Michael R. *Best Practice for Seizing Electronic Evidence in California*.

Rossein, Merrick T. *Nuts and Bolts of Electronic Evidence*. Employment Discrimination Law and Litigation, (November 2010).

Shreve, H. Bruce. *Electronic Evidence*. Louisiana Series, 2010 ed.

Tegland, Karl B. *Electronic Copies as Evidence*. Washington Practice, Handbook Washington Evidence, (2010).

ثالثاً: القوانين والأنظمة

قانون الإجراءات الجنائية المصري.

قانون العقوبات المصري.

قانون الإجراءات الجنائية الفرنسي.

قانون الإجراءات الجزائية الإتحادي الإماراتي رقم (٣٥) لعام ١٩٩٢م.

قانون العقوبات الإتحادي الإماراتي.
قانون الإثبات الجنائي الإنجليزي لعام ١٩٨٤م.
نظام الإجراءات الجزائية السعودي الصادر بالمرسوم الملكي رقم (م/ ٣٩) وتاريخ ٢٨/ ٧/ ١٤٢٢هـ ونشر بجريدة أم القرى في العدد رقم (٣٨٦٧) وتاريخ ١٧/ ٨/ ١٤٢٢هـ.
نظام مكافحة الجرائم المعلوماتية السعودي الصادر بقرار مجلس الوزراء رقم (٧٩) وتاريخ ٧/ ٣/ ١٤٢٨هـ، والمرسوم الملكي رقم م/ ١٧ وتاريخ ٨/ ٣/ ١٤٢٨هـ.
نظام التعاملات الإلكترونية السعودي، الصادر بقرار مجلس الوزراء رقم (م/ ١٨) وتاريخ ٨/ ٣/ ١٤٢٨هـ، والمرسوم الملكي رقم م/ ١٨ وتاريخ ٨/ ٣/ ١٤٢٨هـ.

رابعاً: الصحف

جريدة الشرق الأوسط، ٩ أكتوبر ٢٠٠٩م، العدد ١١٢٧٣. ص٢٢.
جريدة الحياة، الأحد، ١٩ إبريل ٢٠٠٩م، العدد ١٦٨١٦.
جريدة الرياض، الرياض الاقتصادي، الخميس، ١٨ نوفمبر، ٢٠١٠م العدد ١٥٤٨٧. ص ٦.

خامساً: الإنترنت

http:/ new, bbc.co.uk/90/pr/Arabic/world- news/ newsadi.stm.
BBC Arabic News at http: // news vote. bbc. Co. uk/ Arabic /business.

Electronic Evidence in Information Crimes

Osama Ghanem Alobaidy (J.S.D)
Associate Professor of Law
Institute of Public Administration, Riyadh, Saudi Arabia

(Received 23/10/1432 H.; accepted for publication 21/2/1433 H.)

Abstract. With the proliferation of computers and related storage devices as well as the internet, so does the use of these devices in conducting criminal activities. Technology is employed by criminals as a means of communication, a tool for theft and extortion, and a repository to hide incriminating evidence of contraband materials. Computers and digital media are increasingly involved in unlawful activities. The computer may be contraband Fruits of the crime, a tool of the offense, or a storage container, holding evidence of the offense. Investigation of any criminal activity may produce electronic evidence. Computer and related evidence range from the mainframe computer to the Pocket- sized personal data assistant to the floppy diskette, CD, or the Smallest electronic chip device. It is important that investigators and judges recognize, protect, seize and search such devices in accordance with applicable laws, Policies and best practices and guidelines. This paper deals with electronic evidence in electronic crimes and difficulties encountered in Proving such crimes and how to deal with such crimes.